tyco | Software House

C•CURE Software Configuration Guide

Access Control and Event Management

C•CURE v3.00

www.swhouse.com

8200-2102-13

Rev. A

April 2022

Johnson Controls

C•CURE and Software House are registered trademarks of Johnson Controls.

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

Product offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region; contact your regional sales manager. This manual is proprietary information of Johnson Controls. Unauthorized reproduction of any portion of this manual is prohibited. The material in this manual is for information purposes only. It is subject to change without notice. Johnson Controls assumes no responsibility for incorrect information this manual may contain.

Table of Contents

Preface

This *C•CURE 9000 Software Configuration Guide* is for new and experienced security system users. The manual describes the software features of the C•CURE 9000 Administration Client Configuration pane and presents procedures for configuring and using them.

You should have read the installation procedures described in the *C•CURE 9000 Installation and Upgrade Guide*, and 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 installation media.

You can access the manuals if you copy the appropriate PDF files from the C•CURE 9000 installation media Manuals\CCURE folder.

The available C•CURE 9000 and Software House manuals are listed in the *C•CURE 9000 Installation and Upgrade Guide* on the C•CURE 9000 installation media Manuals\CCURE folder.

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

Online Help

You can access C•CURE 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 or warning. A caution contains information essential to avoid damage to the system. A caution can pertain to hardware or software. 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 an electrical hazard that users must avoid to prevent a risk of death or serious injury.

Software House Customer Support Center

Technical Support Portal

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

Qualified Integrators can register to access the Technical Support Portal at http://www.swhouse.com. Click **Support** and select **Support Portal** to access the Support Portal log in page.

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

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

Telephone Technical Support

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

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

Before Calling

Ensure that you:

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

Hours	Normal Support Hours	Monday through Friday, 8:00 a.m. to 8:00 p.m., 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 http://www.swhouse.com/support/contact_technical_support.aspx.	

EMEA

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

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

Local Direct Dial Numbers:

- UK: +44 330 777 1300
- Israel: +972-772 201 350

- Spain: 900 99 31 61
- Denmark: +45-4494 9001
- France: 0800 90 79 72
- Germany: 0800 1806 757
- Italy: +39-0230 510 112
- Belgium: 0800 76 452
- Ireland: 1800943570
- Nordic: 04494 9001
- Greece: 00800-312 294 53
- South Africa: +27-211 003 882
- Russia: 81080020521031
- Turkey: 00800-31923007
- UAE: 800-03107123
- Bahrain: 800-04127

Asia Pacific

Hours: 9:00 a.m. to 5:00 p.m. CST

- Toll Free: +800 CALLTYCO or (+800-2255 8926)
- Direct: +86 21 61916510
- China only Hotline: 4006711528
- India only Hotline: 1-800-1082-008
- Australia: 02-9684-3980

Latin America

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

1

Overview

The *C•CURE 9000 Software Configuration Guide* provides information and instructions for using the Configuration menu of the C•CURE 9000 Administration Client. The guide is organized with a chapter for each Configuration pane selection, so that users can look up information about a given menu selection easily and quickly.

In this chapter

The Configuration Pane

The **Configuration** pane is used to set up non-hardware components of a C•CURE 9000 access control system. The objects that you can create and configure from this menu work together to define the security relationships between Doors, Areas, Elevators, Clearances, Time Specifications, and other security objects within C•CURE 9000.

Each chapter of this guide includes a section that explains how each pane selection is used within C•CURE 9000, and how objects created by that pane choice are used with other objects to establish access control security.

There are three common configuration objects:

- Viewing a List of an Object Type on Page 22
- Using the Object List Context Menu on Page 23
- Using the Object Editor Groups Tab on Page 26

Table 1 on Page 20 outlines each of the Configuration menu selections.

Table 1: Configuration Menu Selections

Menu Selection	Description
Audit Trigger	You can configure a Trigger that can pulse an Event when a specified Audit Log entry occurs. An Audit Trigger is a Query-like object that evaluates Audit Log entries and pulses an Event when the criteria specified in the Trigger is logged in the Audit Log. See Audit Triggers Editor on Page 29 for more information.
Data Export	You export data with this selection. See Exporting Overview on Page 210 for more information.
Data Import	You can import data with this selection. See Data Import Editor on Page 67 and LDAP Data Import Overview on Page 145 and ODBC Data Import Overview on Page 180 for more information.
Document	You can add URLs and different types of files to C•CURE 9000 as Documents that you can assign to Personnel and Events with this selection. See Document Overview on Page 229 for more information.
Event	You can configure Events, including their priority and the actions that occur when the Event is activated with this selection. See Understanding Events on Page 237 for more information.
Group	You can configure Groups of like security objects, for example, a group of doors, so that multiple objects can be easily assigned the same access with this selection. See Group Editor Overview on Page 311 for more information.
Holiday	You can define Holidays, which are dates and times that use a different time schedule than the default Monday through Friday schedule with this selection. See Holiday Overview on Page 319 for more information.
Journal Trigger	You can define Triggers with the Journal Triggers editor that can activate an Event when a specified Journal Message occurs. See Journal Triggers Editor on Page 330 for more information.
Operator	An operator is a person who has the right to use access control objects such as readers, doors, inputs, outputs and schedules. An operator gains entry to the system after successful operator authentication on the domain or workgroup of which they are a part. See Operator Overview on Page 355 for more information.
Partition	A Partition is a sub-division of the C•CURE 9000 database. You can separate C•CURE 9000 security objects into different partitions for both creation and viewing. See Partition Overview on Page 380 for more information.
Predefined Log Message	You can create multiple predefined log messages that can be associated with Events and Guard Tours with this selection. See Predefined Log Message Overview on Page 404 for more information.
Privilege	A Privilege is a collection of rights to use access control objects such as readers, doors, inputs, outputs and privileges. See Privilege Overview on Page 416 for more information.

Table 1: Configuration Menu Selections (continued)

Menu Selection	Description
Recurring Schedule	Recurring Schedules define hourly, weekly, bi-weekly, monthly, quarterly, semi-annual, and annual time schedules that can be used with Guard Tours and other objects. See Recurring Schedule Overview on Page 448 for more information.
Schedule	The Schedule object in C•CURE 9000 is used to define time schedules that can be used throughout the system for access control and to perform certain activities, such as time-based events, at specified times. You can use these schedules to control access to doors, schedule imports, and system tasks and trigger events. See Schedule Overview on Page 466 for more information.
Schedule by Time Zone	You can display a Dynamic View with Schedule by Time Zones that lists the Schedules and Holidays in the C•CURE 9000 database, and whether that Schedule/Holiday is active in each Time Zone in which it is used. See Schedule by Time Zones on Page 488 for more information.
Sound	You can create Sound objects with the Sound editor that reside in the C•CURE 9000 database. You can then use the Event editor to configure Sound actions using these Sound objects. See Sound Editor on Page 491 for more information.
Time Zone	You can define Time Zones that can be assigned to security objects. See Time Zones Overview on Page 495 for more information.
User-defined Fields	You can add User-defined Fields to Personnel, hardware, and video objects. See User-defined Fields Editor on Page 502 for more information.
Workstation	A **Workstation** object appears in a C•CURE 9000 server automatically when an operator logs on to the same C•CURE 9000 server from a different computer. See Workstation on Page 528 for more information.

Creating Configuration Pane Objects and Templates

You can create a new Configuration pane object for each Configuration pane object type.

You can also create a template that you can use to create additional objects by starting with common settings pre-defined in the Template.

Creating a New Configuration Pane Object

To Create a Configuration Pane Object

1. In the Navigation Pane of the Administration Client, click the **Configuration** pane button.
2. Select an object type (such as **Journal Trigger**) from the Configuration pane drop-down list.
3. Click **New** to create a new object of that type. The editor for the object type opens and you can configure the object.

Creating a New Configuration Pane Template

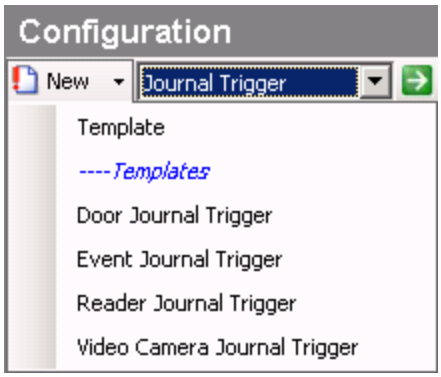
You can create a new template for a Configuration pane object. A template saves you time because you can reuse the same configuration repeatedly.

To Create a Configuration Pane Template

1. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select an object type (such as **Journal Trigger**) from the Configuration pane drop-down list.
3. Click the drop-down arrow next to **New** and select **Template**. The object type's Template editor opens.
4. Configure the object template.
5. To save your new Configuration pane object Template, click **Save and Close**.

The new object type template appears in the Template drop down list of the Configuration pane in alphabetical order.

You can select the object type (such as **Journal Trigger**), then click the drop-down arrow next to **New**, as shown below, to choose a template.



Creating a Configuration Pane Object from a Template

You can use a Configuration pane object template that you have created as the basis of a new Configuration pane object.

To Create a Configuration Pane Object from a Template

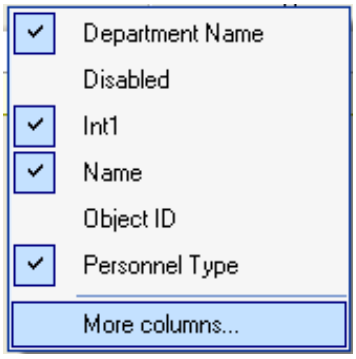
1. In the Navigation Pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select a Configuration pane object type (such as **Journal Trigger**) from the Configuration pane drop-down list.
3. Click the drop-down arrow next to **New**, then click the name of the template you want to use under Templates. The Configuration pane Object's editor opens and you can configure the object you created from the Template.

Viewing a List of an Object Type

You can view a list of all objects of a specific type by opening the default Dynamic View for the object type.

To View a List of an Object Type

1. In the **Navigation** Pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select the object type you wish to view in a list (for example, select **Operator** from the Configuration pane drop-down list).
3. Click  to open a Dynamic View listing all the objects of this type. (You can also click the down-arrow of this button to either view the list in the current tabbed view or open a new tabbed view).
4. You can sort, filter, and group items in the list using the Dynamic View toolbar icons. See the section on Dynamic Views in the *C•CURE 9000 Data Views Guide* for more information on using Dynamic Views.
5. You can right-click an object in the list to open the context menu (see Using the Object List Context Menu on Page 23) and perform any of the functions on that menu.
6. You can right-click on a column heading (such as **Name**) in the view to display a context menu that lets you change the columns displayed by the Dynamic View.



- Click the name of a column to add it to the view.
- Click a column that is currently displayed in the view (marked with), to remove that column from the view.
- Click **More Columns** to choose additional columns to display, if there are additional columns that are not displayed. Select one or more columns from the dialog box that appears, using **CTRL+Left-click**, or a range of columns using **SHIFT+Left-click**, then click **OK** to display the additional columns.

Columns that you add or remove from a Dynamic View in this manner are only in effect until you close the Dynamic View. If you want additional columns to appear each time you open the view, you must edit and save changes to that specific dynamic view.

NOTE If you add new object records to the database while you have a Dynamic View open, the new records are automatically added to the Dynamic view. You can also click to refresh the list to see the new records.

Using the Object List Context Menu

The context menu opens when you right-click on one or more objects in the Dynamic View. It includes some standard selections and often contains additional selections that are specific to the object type.

You can select one or more objects in the Dynamic View (using multiple selection combinations such as **SHIFT+Left-click** and **CTRL+Left-click)** and perform functions such as **Set property**, **Add to group**, **Export selection**, and **Find in Journal** using the context menu. See Table 2 on Page 23 for definitions of the standard context menu selections.

Table 2: Object List Context Menu

Selection	Description
Edit	Click this menu selection to edit the object. The object's editor opens. You can rename the record, change its **Description**, and the objects and fields to include in it.
Delete	Click this menu selection to delete the selected object. A prompt appears asking you to confirm that you want to delete the object. Click **Yes** to delete the object or **No** to cancel the deletion.
Set property	Click this menu selection to change the Property value of a field in all the selected objects. For example, you could select multiple Personnel and change their **Personnel Type** to "Employee". 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 this property by changing the **Value** field.
Add to group	You can add one or more selected objects to a Group of that object type. When you click this menu choice, a dialog box appears for you to select the Group to which to add the object. When you click a Group of the Object type in the list, the selected object is added to the Group.
Export selection	Click this menu selection to Open an Export...to XML or CSV file dialog box to export one or more of the selected objects to either an XML or a CSV file. This allows you to quickly and easily create XML/CSV reports on the selected data. See Exporting an Object on Page 24 for more information.

Table 2: Object List Context Menu (continued)

Selection	Description
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 object. When found, the results display in a separate Dynamic View. See the *C•CURE 9000 Data Views Guide* for more information.
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 object. When found the results display in a separate Dynamic View. See the *C•CURE 9000 Data Views Guide* for more information.
Set GIS Location	This selection is available if the object has a monitoring attribute. Click to open the GIS map window where you can assign a GIS location to the selected object. See the *C•CURE 9000 Data Views Guide* for more information.
Show GIS Location	This selection is available if the object has a monitoring attribute. Click to open a GIS map viewer window showing the location of the object using a push-pin on the GIS map. See the *C•CURE 9000 Data Views Guide* for more information.
Change Partition	This selection is available if your system is partitioned. Click to open a dialog box that allows you to change the Partition to which the object belongs. See Changing the Partition of an Object on Page 395 for more information.

Exporting an Object

From a Dynamic View of an object, you can export an object as an .XML file or a .CSV file.

NOTE Although XML is the initial default file type, once you choose a type in the **Save as type** field, whether XML or CSV, that becomes the default the next time this dialog box opens.

- When you export to an XML file, all available data for the selected object(s), whether displayed in the Dynamic View or not—as well as all the child objects of the selected record(s), is exported.
- When you export to a CSV file, you can view the exported data in an Excel spreadsheet and further manipulate it for your use. 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.

NOTE CSV-formatted exports **cannot** be imported into C•CURE 9000. If you require importing functionality (such as importing a object into a different C•CURE 9000 server, export to XML.

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:

\\ComputerName\Program Files\Tyco\CrossFire\Export

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

To Export an Object to an XML or CSV File

1. Open a Dynamic View of the object type (see Viewing a List of an Object Type on Page 22).
2. Select one or more objects from the list, then right-click.
3. Select **Export Selection** from the context menu. A Windows file selection dialog opens to allow you to export the object (s).
4. Navigate to the folder where you want to save the exported objects.

5. Choose the type of export from the drop-down list in the **Save as type** field (either Export as XML file or Export as CSV file).
6. Type a file name in the **File name** field, or click on a file in the folder (that file will be overwritten by the export) and click **Save** to export the object.

Deleting an Object

You can delete a Configuration pane object from C•CURE 9000 if it is no longer needed.

To Delete an Object

1. Display a Dynamic View list of the object (see Viewing a List of an Object Type on Page 22).
2. Select the object you wish to delete.
3. Right-click the selected object and choose **Delete** from the context menu.
4. Click **Yes** in the dialog box that appears to confirm that you want to delete the object. A dialog box appears to show the progress of the deletion.
5. Click **OK** to complete the deletion.

Setting a Property for an Object

You can use **Set Property** to set properties for a Configuration pane object. **Set Property** enables you to quickly set a property for an Object without opening the editor for the Object.

To Set a Property for an Object

1. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select the Object type for which you want to set a property from the Configuration pane drop-down list.
3. Click  to open a Dynamic View showing all Objects of that type.
4. Right click on the Object in the list for which you want to set the property and select **Set Property** from the context menu.
5. Click  to see a list of properties and select the desired property for the Object.
6. Change the Value as appropriate and click **OK**.

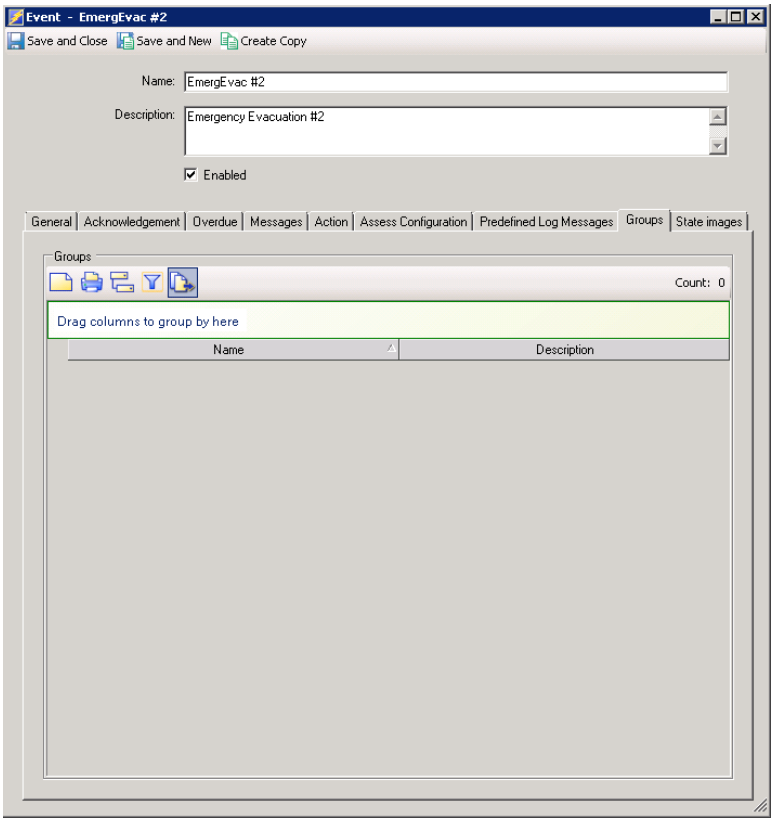
Object Editor Groups Tab

All editors include a Groups tab. The Groups tab displays a list of groups belonging to the object being edited. The Groups tab is not visible when you create a new object configuration using the editor.

Figure 1 on Page 26 shows an example of the Groups tab in the Event editor.

The Groups table on this tab is a Dynamic View that you can Filter, Group, Print, and view in Card View using the buttons listed in Table 3 on Page 26.

Figure 1: Object Groups Tab



You can select any of the Groups in the list and double-click  to edit it, or right-click to display the Groups Context menu (described in Using the Object List Context Menu on Page 23). You can also right-click in the **Name** or **Description** field of a Group row to display a standard edit menu.

For an object to belong to a group, you need to find or create a group of that object type, and add the object to the Group. Then, the Group you added the object to will appear on the Groups tab.

For more information, see:

- Creating a Group on Page 313
- Modifying a Group on Page 315

Table 3: Groups Tab Definitions

Field/Button	Description
Card View	Displays the list of Groups in Card View.

Groups Tab Definitions (continued)

Field/Button	Description
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.

2

Audit Triggers

This chapter explains how to configure Audit Triggers in C•CURE 9000.

In this chapter

Audit Triggers Editor

The Audit Triggers editor lets you define Triggers that can pulse an Event when a specified Audit Log entry occurs. An Audit Trigger is a Query-like object that evaluates Audit Log entries and pulses an Event when the criteria specified in the trigger is logged in the Audit Log.

Example:

Audit Triggers that you could configure to pulse an Event:

- A selected Object Type appears in the Audit Log.
- An object deletion operation is performed.
- An Operator action appears in the Audit Log.
- A visitor is appended to a specified Group when they check in and removed from the group when they check out.

See the following sections for information about Audit Triggers and how to use them.

- Audit Triggers General Tab on Page 31
- Audit Trigger Definitions on Page 32
- Audit Triggers in an Enterprise on Page 36
- Audit Triggers Tasks on Page 37

Maximum Number of Audit Triggers Per Server

Because Audit Triggers are evaluated for each generated Audit Log message, the number of Audit Triggers that can be configured for a C•CURE 9000 server is limited to 500, in order to manage memory usage.

Audit Triggers for Host and Panel Events

Audit Triggers can be configured to pulse either host Events or panel Events (Events downloaded to a controller), including panel Events and objects on different controllers. If the home controller of a panel Event is offline, pulsing that Event has no effect. If the home controller of a panel object is offline, the pulsing of an Event affecting that object is postponed until communications with the controller is restored.

Import and Export of Audit Triggers

You can export Audit Triggers from the context menu, or by creating a Data Export object with an Export Schema selector of **Audit Trigger**.

You can import a Audit Trigger by creating a Data Import object. Name, Evaluation Order, and Schedule Name are available as Match Fields.

Reporting on Audit Triggers

You can create a Report on Audit Triggers by choosing Audit Trigger as the **Report type** in the Report editor. Available Sub types are:

- Basic Configuration - create a report about Audit Trigger objects.
- Audit Trigger Audit Log - create a report about Audit Trigger entries in the Audit Log.
- Audit Trigger Journal- create a report about Audit Trigger entries in the Journal.
- Audit Trigger Group - create a report about Groups containing Audit Trigger objects.

Journal Messages about Audit Triggers

When a Audit Trigger pulses an Event, a Journal Message is logged that identifies:

- The Event that was pulsed.
- The Audit Trigger name.
- The Audit Log entry type that caused the Audit Trigger to activate.
- The primary object of the Audit Log entry.

Example:

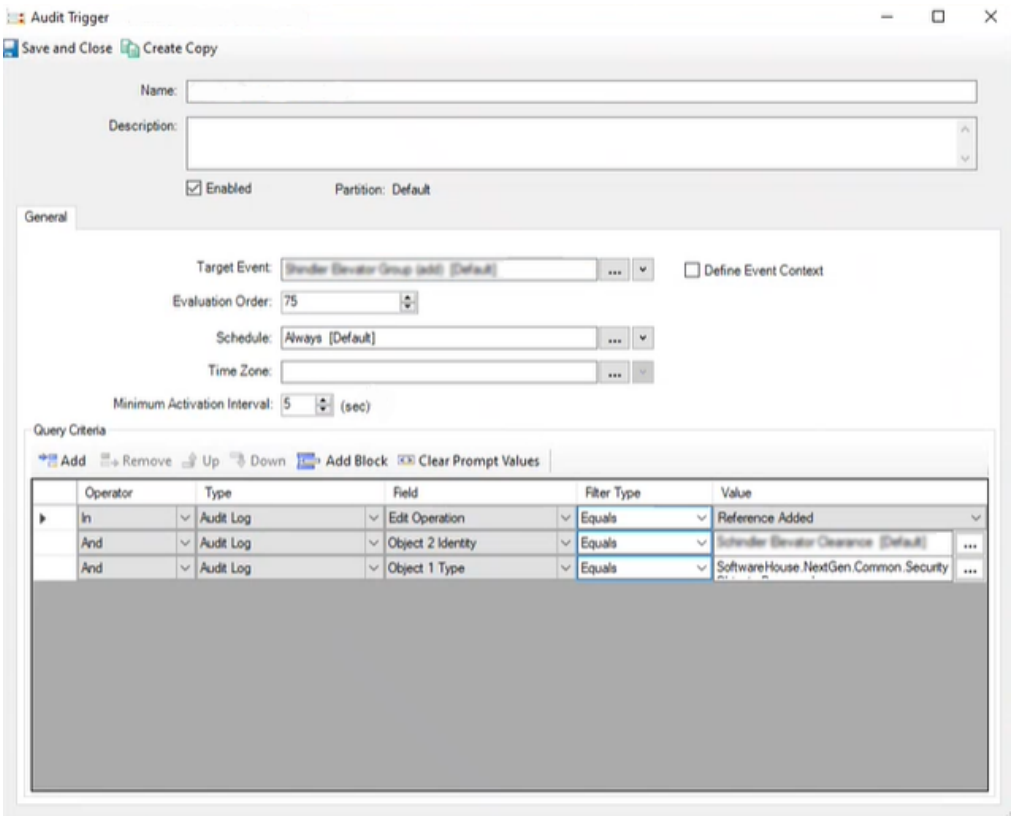
System Activity: Event EVENT NAME is pulsed by Audit trigger TRIGGER NAME on message OPERATION (OBJECT NAME).

NOTE It is important to make sure that the Audit Triggers you configure are not activated again by the Audit Log entries generated by the Triggers, causing a looping condition, such as an Event that changes the value for which the Audit Trigger is querying. The **Minimum Activation Interval** is provided to help guard against this, by telling Audit Triggers to ignore additional triggering within a specified time period. See Audit Trigger Definitions on Page 32.

Audit Triggers General Tab

The Audit Triggers General tab lets you configure query-like triggers that monitor Audit Log Messages coming into the C•CURE 9000 database for specified state changes and conditions. Figure 2 on Page 31 shows the Audit Triggers editor General tab.

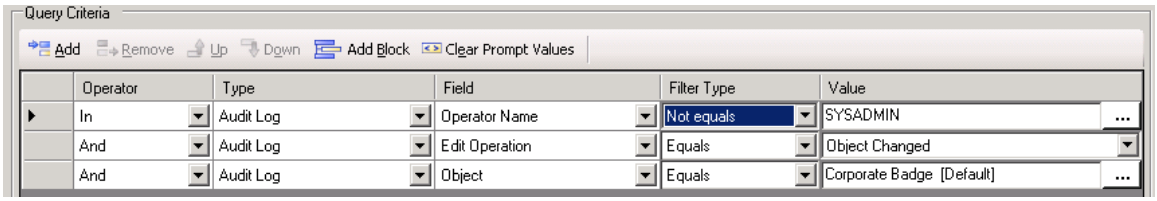
Figure 2: Audit Triggers General Tab



You can create Triggers with multiple Query Criteria rows, to construct a complex watch for specific Audit Log entries.

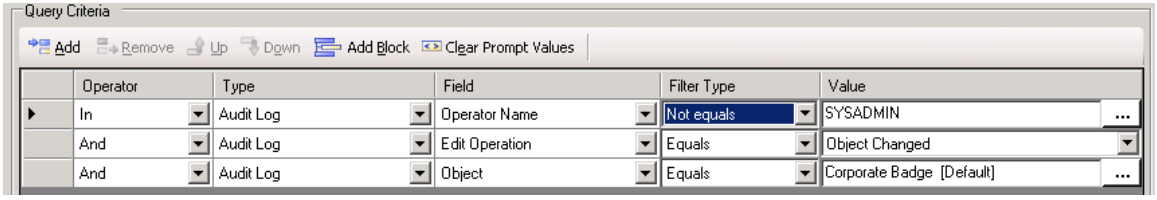
Example:

You could create an Audit Trigger to watch for an Operator other than the SYSADMIN making a change to the Corporate Badge Layout.



Example:

You could create an Audit Trigger to trigger an event when a particular clearance is added or removed from a person.



For information about the definitions of the fields and buttons on the Audit Triggers General tab:

- Audit Trigger Definitions on Page 32

Audit Trigger Definitions

Definitions for the fields and buttons in the Audit Triggers editor are described in Table 4 on Page 32.

Definitions for the Field column (the objects you can have your trigger watch for) are described in Table 5 on Page 33.

Table 4: Audit Triggers Editor Query Definitions

Field/Button	Description
Name	Enter the name you want to assign this Audit Trigger in C•CURE 9000.
Description	Enter a textual description for this Audit Trigger.
Enabled	If selected, the Audit Trigger is enabled, and its query is evaluated upon receiving an Audit Log entry.If cleared, the Audit Trigger is disabled (its query is not evaluated upon receiving an Audit Log entry).
Partition	A read-only field displaying the name of the Partition to which this Audit Trigger belongs. (This field is visible only if the C•CURE 9000 system is Partitioned.)
Target Event	Select an event from a list of the existing events. This event is pulsed if the Query expression you define below evaluates as **True** for an incoming Audit Log entry. This field must be populated for a trigger to be valid. (If you create an Audit Trigger template, you can leave the target Event blank if you do not set the template as **Enabled**.
Evaluation Order	This field allows you to configure the priority of a trigger. You can choose a number between 1 and 200 (the higher the value, the higher the priority). For a given Target Event, the Triggers with the highest priority are evaluated first. If at least one trigger of that priority level is evaluated as **True**, other Audit Triggers for that Target Event with lower priorities are not evaluated.
Schedule	Allows you to assign a Schedule for this Audit Trigger. When the Schedule is active, the Audit Trigger is evaluated (can be activated); when the Schedule is inactive, the Audit Trigger is not evaluated (cannot be activated). The Schedule field cannot be blank.
Time Zone	Allows you to assign a Time Zone for this Audit Trigger. If you assign a Time Zone, the Schedule that you assign is activated and deactivated according to that Time Zone. If a Time Zone is not assigned, the Audit Trigger uses the C•CURE 9000 server Time Zone for Schedule activation/deactivation.
Minimum Activation Interval	Allows you to specify the number of seconds which must elapse before the next activation of this Audit Trigger, after the trigger has been activated. This interval is used to prevent a Audit Message from this Audit Trigger from starting a potential looping condition by re-triggering. The range of values is 0 to 99 seconds, with a default value of 5 seconds. Typically the default value of 5 seconds is long enough to suppress unintended re-activations. A value of 0 means that rapid activations are not prevented.
Define Event Context	Instructs Audit Log trigger to define event context for the event being pulsed.
Query Criteria Buttons	
Add	Click to add a row to the Query Criteria table.
Remove	Click to remove the selected row(s) from the Query Criteria table.
Up	Click to move the selected row(s) up one row in the table.
Down	Click to move the selected row(s) down one row in the table.

Audit Triggers Editor Query Definitions (continued)

Field/Button	Description
Add Block	Click to add a block that groups rows logically. For example, if you needed to group two query terms so that the filter would evaluate correctly, you can use a block to have those terms calculated separately.
Clear Prompt Values	Click this button to clear all rows in the **Value** column.
Query Criteria Table Columns	
Operator	Select the logical operator you want the row to use: And - Creates an **And** logical relationship Or - Creates an **Or** logical relationship between this row and the preceding row.
Type	Specifies the type of messages being queried. Only Audit Log is available.
Field	Identifies the field in the Audit Log that is being queried.
Filter Type	Specifies the relationship between the field and value columns. The type of field you select determines the type of filters you can use. **Example:** If you pick **Partition**, the only choices available for Filter are Equals, Not equals, and In list. If you pick **Server Date/Time**, you have additional Filters such as Equals, Not equals, In range, In custom range, <, >, <=, and >=
Value	Specifies the value(s) for the field you chose in the **Field** column.

Table 5: Field Column Definitions

Field Object	Available Filter Types	Values
Edit Operation	Equals Not equals In list Not in list In Query	Select a value from the drop-down list of edit operations: • Object Changed • Object Created • Object Deleted • Reference Added • Reference Removed • Unknown
Object Type		Select an Object Type value from the Name Selection control that appears when you click ... .
Partition		Select a Partition object from the Name Selection control that appears when you click ... .
Object	Equals Not equals In list Not in list In Group In Query	Select an Object Type and an Object name value from the Name Selection control that appears when you click ... .

Table 5: Field Column Definitions (continued)

Field Object	Available Filter Types	Values
Server Date/Time	Equals Not Equals > >= < <= In range In custom range	Click  to open a calendar to pick a date. Click in the field to select a time.
Transaction Sequence	Equals Not Equals > >= < <= In List	Type in an integer value to look for Audit Log entries related to that Transaction Sequence.

Table 5: Field Column Definitions (continued)

Field Object	Available Filter Types	Values
Operator Name	Equals Not Equals Contains Starts with Ends with > >= < <= In List	Type a full or partial value for the Operator Name. Or Select an Operator Name from the Name Selection control that appears when you click ... .
Primary Object Name		Type in a full or partial value for Primary Object Name. Or Select an Object Type and an Object name from the Name Selection control that appears when you click ... .
Primary Object Type		Type in a full or partial value for Primary Object Type. Or Select an Object Type from the Name Selection control that appears when you click ... .
Primary Partition Name		Type in a full or partial value for Primary Partition Name. Or Select a Partition Name from the Name Selection control that appears when you click ... .
Secondary Object Name		Type in a full or partial value for Secondary Object Name. Or Select a Object Type and Object name value from the Name Selection control that appears when you click ... .
Secondary Object Type		Type in a full or partial value for Secondary Object Type. Or Select an Object Type value from the Name Selection control that appears when you click ... .
Secondary Partition Name		Type in a full or partial value for Secondary Partition Name. Or Select an Object name value from the Name Selection control that appears when you click ... .
Server Name		Type in a full or partial value for Server Name.

Audit Triggers in an Enterprise

While Audit Triggers are local-only objects, Audit Triggers can operate in an Enterprise environment. The Events they can trigger are local to the home server of the objects and Events named in the trigger.

The partition where a Audit Trigger is created is based on the Operator's "New object partition" selection. Audit Triggers cannot be created on the Global partition (because they are local-only objects).

However, from a SAS you can create Audit Triggers that reference Global Objects. When you create and edit a Audit Trigger on a SAS, you can select any objects (local or Global) to be used in the query expression, as allowed by Operator Privileges.

The MAS can display Audit triggers from all SAS's, but each SAS is not aware of the Audit Triggers on the MAS or other SAS's. In turn, the MAS does not evaluate any triggers created on the other SAS's, only the MAS local triggers.

Editing a SAS Audit Trigger from the MAS

Editing a SAS Audit Trigger via the Administration station connected to the MAS does not allow selection of objects from other SAS servers. Because the Trigger itself is local to a Particular SAS, it can only be configured with objects and Events that are local to that SAS, or Global.

Audit Triggers on the MAS

Editing a Audit Trigger located in a local partition of the MAS limits the trigger to selecting only events that are local to the MAS. The selection of objects used in the query expression of the trigger is not limited to local objects.

NOTE The Audit Log entries that are generated on SAS servers and replicated to MAS are not included in the Audit Trigger mechanism because these messages do not generate creation notification messages on the MAS itself - they are replicated to the MAS, not created on the MAS.

Maximum Number of Audit Triggers for the MAS

The MAS displays all configured Audit Triggers from all SASs, but only 500 Audit Triggers can be created local to the MAS, because the MAS evaluates only its local triggers.

Pre-defined Audit Triggers

C•CURE 9000 includes one pre-defined Audit Trigger. You can modify or disable the pre-defined Audit Trigger. When a visitor from the Watchlist is appended to a Visit registered in the system, the Watchlist Visitor Schedule Audit Trigger pulses the Watchlist Visitor Scheduled Trigger Event by default. You can use the trigger as defined or as the basis of your own Audit Triggers, using **Create Copy** to make adifferent version of the trigger. The Watchlist Visitor Schedule Audit Trigger is enabled by default. You can disable the Trigger if it is not needed.

For more information on the Watchlist, see the Personnel chapter in the *C•CURE 9000 Personnel Guide*.

NOTE Pre-defined Audit Triggers can be modified or disabled but cannot be deleted.

If you modify an Audit Trigger, installation of a new version of C•CURE 9000 may revert the trigger back to it's original state. Software House recommends that you make new custom triggers if you need behavior that is different than the standard trigger.

Audit Triggers Tasks

You can perform the following tasks using the Audit Triggers editor:

- Accessing the Audit Triggers Editor on Page 37
- Creating Configuration Pane Objects and Templates on Page 21
- Viewing a List of an Object Type on Page 22
- Using the Object List Context Menu on Page 23
- Deleting an Object on Page 25
- Setting a Property for an Object on Page 25
- Configuring an Audit Trigger on Page 38
- Pulsing an Event on an Object Type Audit Log Entry on Page 39

Accessing the Audit Triggers Editor

You access the Audit Triggers editor from the C•CURE 9000 Configuration pane.

To Access the Audit Triggers Editor

1. Click the **Configure** pane button.
2. Click the Configure drop-down list and select **Audit Triggers**.
3. Click  to open a Dynamic View showing all Audit Triggers objects.
4. Double-click on the Audit Trigger in the list that you want to edit, and the Audit Triggers editor opens.

Creating a New Audit Trigger or Template

You can create a new Audit Trigger that can activate an Event when a specified Audit Log entry occurs.

You can also create a Audit Trigger Template that you can use to create additional Audit Triggers starting with common settings pre-defined in the Template.

Creating a New Audit Trigger

To Create a Audit Trigger

1. In the Navigation Pane of the Administration Client, click the **Configuration** pane button.
2. Select **Audit Trigger** from the Configuration pane drop-down list.
3. Click **New** to create a new Audit Trigger. The Audit Triggers Editor on Page 29 opens and you can configure the Audit Trigger.

Creating a New Audit Trigger Template

You can create a new template for a Audit Trigger. A Audit Trigger template saves you time because you can reuse the same configuration repeatedly.

To Create a Audit Trigger Template

1. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.

2. Select **Audit Trigger** from the Configuration pane drop-down list.
3. Click the drop-down arrow next to **New** and select **Template**. The Audit Trigger Template opens.
4. Configure the Audit Trigger template.
5. To save your new Audit Trigger Template, click **Save and Close**.

The new Audit Trigger template appears in the Template drop down list of the Configuration pane (select **Audit Trigger**, then click the drop-down arrow next to **New**).

Creating a Audit Trigger from a Template

You can use a Audit Trigger template that you have created as the basis of a new Audit Trigger object.

To Create a Audit Trigger from a Template

1. In the Navigation Pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Audit Trigger** from the Configuration pane drop-down list.
3. Click the drop-down arrow next to **New** and select **Template**.
4. Click the name of the template you want to use under Templates. The Audit Triggers Editor on Page 29 opens and you can configure the Audit Trigger you created from the Template.

Configuring an Audit Trigger

You can configure the Query Criteria for a Audit Trigger.

To Configure a Audit Trigger

1. Create a new Audit Trigger (see Creating a New Audit Trigger or Template on Page 37).
2. Enter a name and textual description for the Audit Trigger in the **Name** and **Description** fields.
3. Select a **Target Event** for the Audit Trigger. This is the Event that is pulsed if an Audit Log entry matching the trigger criteria is found.
4. You can adjust the **Evaluation Order** (Priority of the trigger). The default value is 75; the minimum is 1; the maximum is 200.
5. You need to select the **Schedule** for when this Audit Trigger should be evaluated. When the **Schedule** you chose is Active, the Audit Trigger evaluates incoming Audit Log entries.
6. You should identify the **Time Zone** to which you want the Schedule to apply. This is important if you have controllers in a different time zone than the C•CURE 9000 server, and you want the triggers to use local time.
7. Click **Add** to add a row to the Query Criteria table.
8. In the **Field** column, select the Audit Log field you want the trigger to query for from the drop down box. For example, pick **Object Type** if you want to trigger on Audit Log entries that are related to a specific object type.
9. In the **Filter Type** column, select the type of filter you wish to define. For example, for an Object field, you can choose either **Equals**, **Not equals**, **In list**, which allows you to specify a list of objects, **Not in list**, or **In Query**.
10. In the **Value** column, click  to select the values to filter on, or for some field values (such as Server Name), type in the text that you wish to find.
11. If you want to define additional Query Criteria, click **Add** again and repeat the above steps. In addition, you can change the Operator column to choose the **And** operator or the **Or** operator.

12. If you want to group Query Criteria rows so that they are evaluated together, click **Add Block**. Three rows are added:
    - Begin block expression
    - A Query Criteria row
    - End Block.
13. Click **Save and Close** to save your Audit Trigger.

Pulsing an Event on an Object Type Audit Log Entry

You can configure an Audit Trigger to pulse an Event each time an Audit Log entry occurs for an Object Type (for example when one or more Personnel records are edited).

When configuring an Audit Trigger, the user can combine objects and their states, so the Trigger will pulse an Event when one of the conditions occurs.

In the task below, an Audit Trigger is configured that will pulse an Event whenever a Personnel record is edited and changed while the Schedule is active.

To Pulse an Event When an Object is Edited and Changed

1. Create a New Audit Trigger (see Creating Configuration Pane Objects and Templates on Page 21).
2. Click ... in the **Target Event** field to select the Event you want triggered.
3. You can set the **Evaluation Order** (the priority for the Trigger) by adjusting the **Evaluation Order** spinner up or down, or typing a value into the **Evaluation Order** field.
4. Click ... in the **Schedule** field to select a Schedule for the Audit Trigger (when the Schedule is Active and the Query Criteria are met, the Event is pulsed).
5. Click ... in the **Time Zone** field to select the Time Zone for the Event.
6. **Optional:**To pulse the Event every time the trigger criteria has been met in the audit message, set the **Minimum Activation Interval**parameter to 0. Otherwise, leave the parameter at the default value unless you experience complications with an Audit Log entry re-triggering the Audit Trigger.
7. **Optional:**To send information about the audit message to the activated Event, select the **Define Event Context** check box. When **Define Event Context** is selected, the Event is pulsed every time the trigger criteria is met, similar to setting the **Minimum Activation Time** parameter to 0.
8. Click **Add** in the Query Criteria table.
9. In the **Field** column, click the drop-down list and choose **Object Type**.
10. In the Value column choose the Object Type to for the trigger.

    Example:

    Choose **Personnel** if you want to query for an for a Personnel object being edited.
11. Click **Add** in the Query Criteria table to add another row.
12. In the **Field** column, click the drop-down list and choose an Audit Log field for the trigger.

    Example:

    Choose **Edit Operation** if you want to query for an for an object being edited.
13. Choose a **Filter Type** from the drop-down list.

Example:

Choose **Equals** if you want to query for a Equals result.

14. Choose a Value from the drop-down list.

Example:

Choose **Object Changed** if you want to query for an edit operation that changed an object.

15. Click **Save and Close** to save the Audit Trigger.

3

Data Import

This chapter provides an overview of the import process, and describes how to define imports, run imports, and examine the results of importing data into C•CURE 9000. (Information specific only to imports from a Lightweight Directory Access Protocol (LDAP) compliant data source is covered in Chapter 4. Information specific only to imports from an Open Database Connectivity (OBDBC) compliant data source is covered in Chapter 5.)

In this chapter

Importing Overview

C•CURE 9000 lets you update the C•CURE 9000 database by importing records in another C•CURE 9000 database or a human resources (HR) or other external database. Depending on your C•CURE 9000 access privileges, you can import records at any time, schedule imports to run at predetermined intervals, or import records in response to events monitored by the system.

NOTE Software House also provides a data migration tool through the Integrator to let you migrate information from iSecure or C•CURE 800/8000 to C•CURE 9000. The tool converts information in your iSecure or C•CURE 800/8000 database to a format suitable for import into C•CURE 9000. You then use the import function in C•CURE 9000 to add the information to C•CURE 9000. For details, see the *C•CURE 9000 Database Migration Guide*.

C•CURE 9000 manages imported information as objects. In C•CURE 9000, the term 'Object' is used to refer to the collection of definable properties that are saved in a database to describe elements of the system (such as Readers and Controllers), and the activities and individuals that are monitored by the system. You import Objects into C•CURE 9000 according to uniquely named Import Definitions, that are themselves Objects managed by C•CURE 9000.

When you create an Import Definition, you specify data source input (usually files containing the data you want to import) and establish rules used to add that information to the C•CURE 9000 database. C•CURE 9000 maintains a record of imports to the system and provides a means to let you review the import history at any time.

C•CURE 9000 Imports let you do the following:

- Import data received from another C•CURE 9000 database or an HR or other external database.
- Import data from XML files, CSV files, ODBC-compliant data sources, and LDAP-compliant data sources.
- Import files in both manual and automated modes.
- View historical logs for all imports.
- Convert external data schema to the internal C•CURE 9000 data schema.

The XML and CSV import sources support all three of the import modes below. The LDAP import source supports only Listening on data; the ODBC import source supports only Activated by event or Listening on data.

- Manual only - You can run manual imports at any time. When you run a manual import, it is recorded in the Journal as a system activity. The information includes the name of the Import definition and the name of the Operator who performed the action.
- Activated by Event (automated) - the Import Definition listens for C•CURE 9000 Events, such as a scheduled Event, that trigger the Import Definition to poll its import source for existing data.
- Listening on Data (automated) - the import source object is initialized by the Import Watcher server component and starts listening for external events, such as the creation of new files in a specified folder. When an external event is received, the import source initiates import of the received data.

For more information about importing data, see:

- Data Import Editor on Page 67
- LDAP Data Import Overview on Page 145
- ODBC Data Import Overview on Page 180

NOTE For information about importing Objects exported from another C•CURE 9000 system, see Exportable Objects on Page 210.

Data Conversion

Using Data Conversion in C•CURE 9000, you can import files in comma separated value (CSV) format, XML files that do not conform to the C•CURE 9000 schema, ODBC records, and LDAP records. You use the Data Conversion function to specify exactly how these are to be imported into the C•CURE 9000 database.

For more information, see:

- Data Import Data Conversion Tab on Page 89
- Personnel Mapping Tool Editor on Page 92
- Operator Mapping Tool Editor on Page 98
- Field Mapping Tool Editor on Page 104.

Mapping Fields

Import Definitions allow you to import data received from external data sources with schema (data structure) similar to the C•CURE 9000 schema directly into the C•CURE 9000 database. If the external database used as the source for the import does not have the same structure and format as the C•CURE 9000 database, you can create a plan to convert (map) the fields in the source database to fields in the C•CURE 9000 database. The Personnel and Field Mapping Tools help find corresponding records in C•CURE 9000 based on your mapping plan.

Example:

As part of your mapping plan, you map from the fields *Last*, *Middle*, and *ID* in an external database to the corresponding fields *Last Name*, *Middle Name*, and *Text1*.

For additional details about how to map fields, see:

- Using the Personnel Mapping Tool to Convert Personnel Data on Page 95
- Using the Operator Mapping Tool to Convert Operator Data on Page 102
- Field Mapping Tool Editor on Page 104

XSLT Custom Conversion

If you are an advanced user, you can use the Custom Stylesheet (XSLT Import converter) to perform the complex transformation of an incoming XML document that is supported by the standard XSLT transformation engine implemented by Microsoft for .NET platform. This converter can help you solve very difficult cases that can occur on your customer site during the automation of data transfer between C•CURE 9000 and external applications. The Custom Stylesheet can also be used together with other mapping tools to complete complex conversions.

Example:

Storing SSNs or phone numbers as integer fields, the former requiring removing dashes from the SSN string and the latter requiring removing parentheses as well as dashes.

Only users with an excellent understanding of the XSLT language can use this tool without consulting with their dealer or the Software House Customer Support Center.

See Custom Stylesheet Editor on Page 114 for more information.

Matching Fields

When configuring an Import Definition, you have the option to simply add information from the external data source to the C•CURE 9000 database, or to selectively import only information from the external data source that does not already exist in

C•CURE 9000. To selectively import data, you must specify how to correlate records in the external data source with those in the C•CURE 9000 database. You do this in the import definition by specifying how the system matches records by matching fields.

You match fields only when **updating** records in C•CURE 9000 using information from an external data source. You do not use match fields when simply adding records from an external data source to the C•CURE 9000 database, although the system will not add duplicate records. To successfully update records using matching fields, the XML files you import must conform to the C•CURE 9000 schema. If the files you want to import are not in XML format, or do not conform to the C•CURE 9000 schema, you must perform data conversion.

For details, see:

- Data Import Data Conversion Tab on Page 89
- Personnel Mapping Tool Editor on Page 92
- Operator Mapping Tool Editor on Page 98
- Field Mapping Tool Editor on Page 104
- Custom Stylesheet Editor on Page 114

During an import for updating existing records, the Data Import function searches each field designated in the external data source as a matching field for records that correspond to those already in the C•CURE 9000 database. When a matching record is found, the Data Import function imports any data not already contained in the C•CURE 9000 record. As part of the plan for selecting matching fields, you can specify various characteristics in the records to assure a unique match.

Example:

Last Name, *Middle Initial*, and *Text1*.

If you select either of the update options, you must specify matching fields on the **Match Fields** tab. When matching records, C•CURE 9000 evaluates each record individually:

- The system considers a record a match only if all fields designated as matching fields match the corresponding fields in **only one** record in the C•CURE 9000 database.
- If more than one record with the matching fields is found, the system logs an error and rejects the record.

For details about matching fields, see Data Import Match Fields Tab on Page 120 and Specifying Match Fields on Page 123.

Using Sample Inputs

Configuration of an Import Definition is a complex process that cannot be completed unless you know the structure of the file to be used during the import—whether any data conversion is required and which fields in the input file can be used for matching on the **Match Field** tab. Because
C•CURE 9000 has a significant number of top-level importable Objects that can be partially exported and also allows you to import XML documents generated by external applications, it is impossible to automatically predict the structure of the incoming data.

Consequently, the **Data Import Editor** provides the following group of buttons that can help define the structure of the incoming data and be used later for configuring data conversions and field matching:

- Select Sample Input
- View Sample Input
- View Converted Sample
- Verify Sample

See the detailed descriptions of the buttons and their functionality in Data Import Editor on Page 67.

The Import Process

In C•CURE 9000, successfully importing records requires a specific sequence of preparation, execution, and review. The process depends on a set of parameters referred to as an Import Definition that you configure in advance. In addition, you must complete other system configuration tasks even before you can begin to create an Import Definition and import data. The configuration tasks depend on whether you are importing data manually or automatically.

Requirements for Manual Imports

Before you can create an Import Definition for the type of records you want to import into C•CURE 9000, you must:

- Establish appropriate access privileges . For more information about how to determine and update your access permissions, see Privilege Overview on Page 416. (Edit, View, Delete and New) for the account of any Operator(s) who will perform manual imports. Also, you will need to provide the Operator(s) with permissions to objects in specific partitions, if the system has more than the default partition.

Requirements for Automatic Imports

Before you can create Import Definitions to run imports automatically—either according to a schedule in response to an Event or by using the Import Watcher server component to listen for external events (such as a new file being put into folder), you must complete the preceding requirement for running an import manually. Then, you must do the following:

- To import by schedule, configure an Event and associate a Schedule with the Event. For details about scheduling an import, see Scheduling Imports on Page 52.
- To import using the Import Watcher server component to listen for external events, confirm that the Import Watcher is running on the **Server Components** tab of the Server Management Application. For details, see Running an Import by Listening on Data from the Import Watcher on Page 53.
- (Optional) Configure an Event to report connectivity problems.

The Import Definition

The Import Definition specifies the parameters that the system will follow when adding, updating, or deleting C•CURE 9000 database information during the import operation.

Depending on the information you are importing, the data's conformance to the C•CURE 9000 schema, and the configuration of your import definition, some records may not import successfully. C•CURE 9000 provides tools that allow you to review and correct the import results.

In general, to import records into C•CURE 9000, do the following:

1. Configure an Import Definition that describes how to retrieve the records you want to add, or that you want to use to update existing records. For details, see Creating an Import Definition on Page 47 and Configuring an Import Definition on Page 49.
2. Run the pre-configured Import manually or have the system run it automatically. If you are importing different types of Objects, due to dependencies between Objects in C•CURE 9000, you must perform the imports in a specific sequence. For details, see Running an Import on Page 50.

   Import objects in the following sequence:

   a. Schedule objects

   b. Hardware objects

   c. Clearance objects

   d. Personnel objects

   e. Events

f. Group objects

g. Action items

NOTE Due to multiple parent-child dependencies between object types, attempting to import objects in any order other than the sequence described may cause the import to fail.

3. Examine the results of the Import to confirm what was added or updated, and to identify records that did not import as expected. For details, see Viewing Import Results History on Page 71.

Important Data Import Notes

NOTE If the import of a single XML document generates a significant number of rejected records, the error log file stored on the Server becomes too large to be processed by the client. If this happens, you should do the following:

1. Use the Operator's name to find the name of the error log file in the Data Import History record.
2. Find the Import Logs folder located in the folder where the Server is installed.
3. Open the file in an external editor for review.

NOTE If an LDAP Import in progress is interrupted by a Windows shutdown or power button shutdown, when the system restarts and completes the LDAP Import, the Import History will have two records. These count the personnel records imported before and after the system restart. However, the total record count in both records can be less than the actual number of records imported into the system.

NOTE Using the "memberOf" Data Source Field in the LDAP Import does not cause the timestamp for this record to change. Therefore, mapping it to a C•CURE 9000 field, such as "Clearance [Replace All]" or "Clearance [Modify]" does not cause the Personnel Record to update when used with the Microsoft Timestamp Method. Instead, configure the LDAP Import to use Full Scan Method.

Basic Importing Tasks

The primary tasks related to the importing of data that the C•CURE 9000 Data Import Editor allow you to accomplish are:

- Accessing the Data Import Editor on Page 47
- Creating an Import Definition on Page 47
- Creating an Import Definition Template on Page 48
- Configuring an Import Definition on Page 49
- Running an Import on Page 50

Accessing the Data Import Editor

You can access the **Data Import Editor** from the C•CURE 9000 **Configuration** pane of the **Navigation** Pane of the Administration Client.

To Access the Data Import Editor

1. Click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Data Import**.
3. Click **New**to create a new Import Definition.

   - or -

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

   The **Data Import Editor** opens with the **General** tab displayed. See Data Import General Tab on Page 74.

Creating an Import Definition

You can create a new Import Definition using the **Data Import Editor**. For information on import prerequisites, see The Import Process on Page 45.

To Create an Import Definition

1. In the **Navigation** Pane of the Administration Client, click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Data Import**.
3. Click **New** to create a new Import Definition. The **Data Import Editor** opens.
4. You can now configure the Import Definition—selecting the source type, automation mode, import mode, and the default import partition; selecting a sample input and mapping the fields between the import source and the C•CURE 9000 database, if necessary; selecting match fields if you are using the import to update the C•CURE 9000 database; configuring template rules to be applied in modifying object(s) by the import; and configuring triggers to activate a selected event whenever the import's status matches that defined for the trigger.
5. Make sure that the **Enabled** check box is selected (the default) so that this Import Definition is operational.
6. To save your new Import Definition, click **Save and Close**.

   - or -

   Alternatively, if you want to save the Import Definition and then create a new one, click **Save and New**. The current Import Definition is saved and closed, but the **Data Import Editor** remains open ready for a new Import Definition (either blank or including template information if you were using a template to create the saved Import definition).

Creating an Import Definition Template

You can create an import definition from a data import template. Import templates can save time and effort if you are creating multiple import definitions with similar characteristics.

Example:

If you want multiple import definitions to use the same import source type (such as CSV) but different import modes, you can create a template that specifies CSV as the source type. Then use that template to create multiple import definitions with the CSV import source, but differing import modes.

You can create a new import template or, if you have the appropriate access permissions, you can use any existing import definitions as the basis for a template. Using an existing import definition as the basis for an import template allows you to create the template quickly.

Creating a New Import Definition Template

To Create an Import Template

1. In the **Navigation** pane of the Administration Client, click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Data Import**.
3. Click the down-arrow on the **New** button, and click **Template**.

   The **Data Import Editor** where you can configure the import template opens.
4. Configure the template to meet your requirements. Any fields for which you configure values become part of the template; then when you subsequently create a new Import Definition from that template, these field values are already filled in.
5. In the **Name** field, enter the name you wish to use for the template (**Import Def 1**, for example).
6. To save the template, click **Save and Close**.

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

Creating a Template From an Existing Import Definition

If you have appropriate access privileges, you can use any Import Definition as the basis for an import template. You must have **Set Property** permission to be able to convert an Import Definition into an import template.

For more information about how to determine and update access permissions, see Privilege Overview on Page 416.

To Make an Import Definition into an Import Template

1. In the **Navigation** Pane of the Administration Client, click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Data Import**.
3. On the Search pane, in the **Name** field, enter the name of the existing import you want to open (making sure that the **Template** check box is not selected), or search for existing Import Definitions by clicking  .

   The system displays your search results in the right pane as a dynamic view.
4. Select the Import Definition you want to use to create a template and right-click to open the Data Import Context menu (for information see Using the Object List Context Menu on Page 23).
5. From the Import Context menu, select **Set Property**.

   The system displays a dialog box that allows you to modify a property and value for the import definition.
6. In the dialog box, at the **Property** field, click  to display the **Import** view to see the properties you can modify.

7. Select **Template**. The **Value** field becomes a check box.
8. In the dialog box, select **Value** and click **OK**. The dialog box closes.
9. Double-click to open the Import Definition. Confirm that the title bar of the Import Definition indicates the Import Definition is now a template.

Configuring an Import Definition

Configuring an Import Definition is the process of specifying the source type, automation mode, import mode; selecting a sample input and mapping the fields between the import source and the C•CURE 9000 database, if necessary; selecting match fields if you are using the import to update the C•CURE 9000 database; selecting template(s); and configuring triggers.

You configure an import by opening it in the **Data Import Editor**.

To Configure an Import

1. Open an existing Import Definition using the **Data Import Editor**, or create a new one.
2. Use the Data Import General Tab on Page 74 to specify the import source type and automation mode, configure the data source as required by the type and mode you chose, select an Import mode rule, select a Partition for the newly imported objects if you wish and the C•CURE 9000 is partitioned, and click the **Select Sample Input** button to select and open a sample input file.
3. Use the Data Import Data Conversion Tab on Page 89 to set up the data conversion process, if needed, by choosing one or more converters to specify how data elements in the external database correlate with the data objects in the C•CURE 9000 database. You can open one of the following converters:
   - Personnel Mapping Tool Editor on Page 92 – recommended for importing Personnel if conversion is necessary.
   - Operator Mapping Tool Editor on Page 98 - recommended for importing Operator privileges if conversion is necessary.
   - Field Mapping Tool Editor on Page 104 – recommended for importing other security objects if conversion is necessary.
   - Custom Stylesheet Editor on Page 114 – not recommended for general use. This tool should be used only by customers with an excellent understanding of the XSLT language or in consultation with their dealer or the Software House Customer Support Center.
4. When configuring an Import Definition to update the C•CURE 9000 database, use the Data Import Match Fields Tab on Page 120 to select fields on which to match records.
5. Use the Data Import Templates Tab on Page 127 to select template(s) for top-level importable object types to be applied as rules in modifying those object(s) by the import.
6. Use the Data Import Triggers Tab on Page 140 to set up triggers to activate specific events when an Import's status has a specified value.
7. Make sure that the **Enabled** check box on top of the **Data Import Editor** is still selected (the default) so the Import Definition is operational.
8. To save your Import Definition, click **Save and Close**.

   - or -

   Alternatively, if you want to save the Import Definition and then create a new one, click **Save and New**. The current Import Definition is saved and closed, but the **Data Import Editor** remains open ready for a new Import Definition (either blank or including template information if you were using a template to create the saved Import Definition).

Running an Import

You can run imports manually or automatically. When using either method, you must specify a pre-configured Import Definition. When running an import automatically, you must also consider how you want to initiate the import. You can launch an import according to a schedule, in response to a predetermined event that can be monitored by C•CURE 9000, or in response to an external event, such as a new file being put into folder. Because they run independently, executing automatic imports requires that you ensure in advance that the import that you specify in the import definition is properly configured when the import attempts to start.

The **order in which you import objects** into C•CURE 9000 is especially important. This is especially true if you are importing Objects exported from another C•CURE 9000 system.

NOTE For more detailed information about importing Objects exported from another C•CURE 9000, see Exportable Objects on Page 210.

Import objects in the following sequence:

1. Schedule objects
2. Hardware objects
3. Clearance objects
4. Personnel objects
5. Events
6. Group objects
7. Action items

NOTE Due to multiple parent-child dependencies between object types, attempting to import objects in any order other than the sequence described in the preceding list may cause the import to fail.

You can run imports in several ways:

- Manually at any time. See Running Imports Manually on Page 50.
- Scheduled at a specified time. See Scheduling Imports on Page 52.
- Listening on Data from the C•CURE 9000 Import Watcher. See Running an Import by Listening on Data from the Import Watcher on Page 53.
- From the Data Import Dynamic View in response to the **Run on Server** context menu selection. See Running an Import on the Server from Data Import Dynamic View on Page 53.

Running Imports Manually

You can run a predefined Import Definition at any time. You must define an Import before you can use it to import data into C•CURE 9000.

When you run an Import manually, it is recorded in the Journal as a system activity. The information includes the name of the Import Definition and the name of the Operator who performed the action. For information, see the “Historical Tracking of System Activity” chapter in the *C•CURE 9000 System Maintenance Guide*.

To Run an Import Manually

1. In the Administration Client, on the Navigation pane, select **Configuration**.
2. On the navigation toolbar, in the drop-down menu, select **Data Import**.

3. On the Search pane, in the **Name** field, enter the name of the Import you want to run, or search for existing Import Definitions by clicking .

   From the search results displayed in the right pane as a dynamic view, select the Import you want to run.

4. To run the selected Import,

   - Right-click the selection to open the Data Import context menu and click **Manual Import**.

     -or -

   - Double-click the selection to open the **Data Import Editor** for the selected import and click the **Manual Import** button.

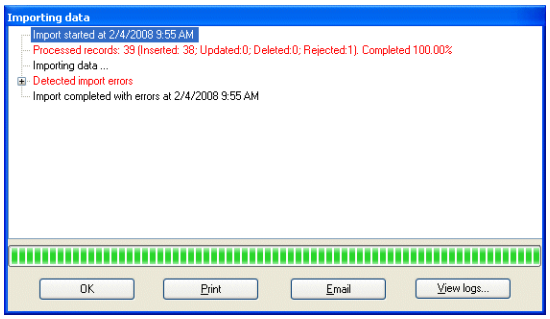
NOTE

- Neither the **Manual Import** option on the Context menu, nor the **Manual Import** button on the Editor are available if the Import Definition is configured for Automated Import.
- The **Manual Import** option is not supported for some data source types, such as LDAP and ODBC.
- When you click **Manual Import**, you are running the selected Import on the client computer. Consequently, the system does not use the Default Import 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 Import server directory, if you wish. For more information, see "Import and Export Settings" in the *C•CURE 9000 System Maintenance Guide*.

5. On the **Open file to Import** dialog box, select the desired file and click **Open**.

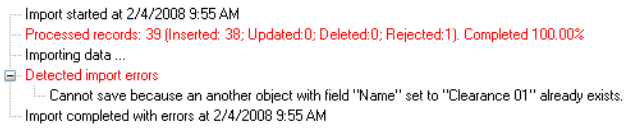
   The progress of the import displays in the **Importing Data** dialog box.



   - If you want to stop the import process while the import is running, click the **Cancel** button that is available.
   - Once the import has completed, a message displays in the **Importing Data** dialog box.

   The information given includes: the duration of the process and the number of records inserted, rejected, deleted, and updated—as well as a list of errors detected during the import process.

   - Click ⊞ or ⊟ to expand and contract the information as necessary.



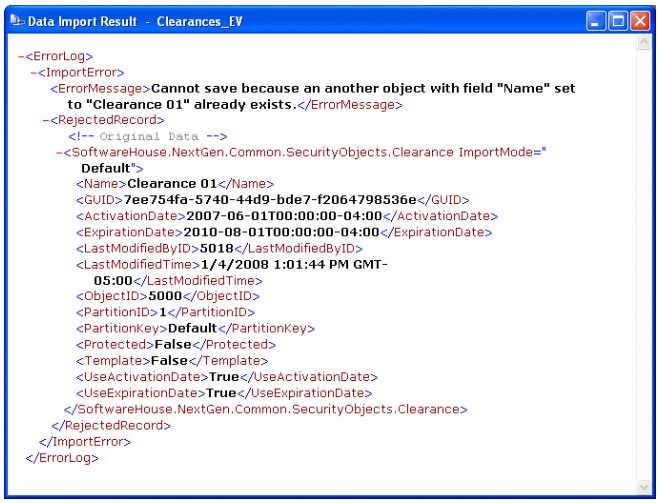
6. You can use the buttons on the dialog box to do any of the following:

   - Click **Print** to print a copy of the information on this dialog box.
     - On the standard Windows **Print** dialog box, click **OK**.
     - On the **Print Preview** dialog box that displays, click .
   - Click **Email** to send a copy of the information on this dialog box.

- Click **View Logs** to review rejected records and errors encountered during the import. (This button is available only if there were errors.)

Example:

You can examine rejected records to determine how to modify them so you can successfully re-import them.



- Click **OK** to close the Importing Data dialog box.

Running Imports Automatically

In C•CURE 9000, you can run Imports automatically, as follows:

- According to a Schedule or another event
- From the Import Watcher listening to external events

The Data Import Dynamic View context menu also allows you to affect automated imports as follows:

- Cause an Import that ordinarily runs automatically on schedule (by activating by event) to run on the server whenever you wish.
- Stop and start the Import Watcher from listening for external events for selected Import Definition(s) with a 'Listening on data' automation mode.

Automated Imports run in the context of a specified Operator. The Operator must have the appropriate permissions to run the Import. For details, see Privilege Overview on Page 416.

In all cases, you must have previously configured an Import Definition to manage the automated Import. For details, see Creating an Import Definition on Page 47.

Scheduling Imports

To schedule an Import, you must first configure the appropriate Import Definition, and then configure an Event, associated with a predefined Schedule, that runs the Import as an Action. For details about configuring Events, see Understanding Events on Page 237.

To Run an Import on Schedule

1. Open an existing Import Definition on the **Data Import Editor**, or create a new one.
2. Configure your Import Definition appropriately according to the directions in this chapter, making sure that on the Data Import General Tab on Page 74 you specify the following:

- Automation mode as **Activated by event**
- Path to a folder on the server where the files you are importing will be placed
- File pattern to be used to filter when retrieving files from the preceding

3. Save the Import Definition by clicking **Save and Close**.
4. Configure the Event to run the import by schedule as follows:
   a. Assign the Event a unique name.
   b. On the **General** tab of the **Event Editor**, select a Schedule that you want to use to determine when the Import runs.

      You can select from Schedules already defined in C•CURE 9000. To run the Import at a time different from those configured in the available Schedules, you must create and save a new Schedule. For information, see Schedule Overview on Page 466.
   c. On the **Action** tab of the **Event Editor**, specify **Run Import** as an Action for the Event and select the Import you want to run from the Imports currently saved in the system.

NOTE The system automatically enters the name of the Operator who is configuring/modifying the Event Action (and in a partitioned system, their Partition) indicating that the 'Run Import' Action is occurring with their Privilege. (This Operator's name [and Partition, if existing] will be entered in the Import History that records the running of this Import at its scheduled times.)

   d. You can configure other aspects of the Event. Among the parameters that you can configure are the following:
      — Priority of the Event
      — Messages sent when the Event runs the import
      — Acknowledgement requirements
      — Messages or secondary Event triggered if this Event is deactivated.
   e. Make sure that the Event is both **enabled** and **armed**.

Running an Import on the Server from Data Import Dynamic View

In addition to running an Import on a Schedule (Automation mode: Activated by event), as described in the preceding section Scheduling Imports on Page 52, you can initiate the immediate one-time running of such an Import on the server.

You can use this method to test an existing Automated Import.

To Run a Data Import on the Server

1. In the **Navigation** Pane of the Administration Client, click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Data Import**.
3. Click  to open a **Dynamic View** showing a list of all Data Import objects.
4. Select an Import Definition with an automation mode of 'Activated by event' and right-click to open the Data Import Context menu (for information see Using the Object List Context Menu on Page 23).
5. From the Import Context menu, select **Run on server**. The import starts running importing records.

Running an Import by Listening on Data from the Import Watcher

Import Watcher is a special server component that can run on a separate computer, but usually starts on the same computer as the main server. This component lets you import records into C•CURE 9000 on demand without Operator intervention,

predetermined Schedule, or Event notification. Import Watcher constantly monitors external events, usually for creation of new files in a specified folder.

The Import Watcher component does the following:

1. Loads all the Import Definitions at start time and initializes the import sources configured for listening to external events.
2. Listens for any changes to the listening import sources and re-initializes them if the server or one of the clients modifies their configuration.

Import Watcher also cleans up the status of the Import Definitions so they all have a 'Disconnected' value before initialization (After initialization, the status is 'Listening'). This provides needed recovery from any abnormal termination of the server's process, which could leave the statuses in the wrong state indicating that the Imports were active.

To Run an Import by Listening on Data from Import Watcher

1. Open an existing Import Definition on the **Data Import Editor**, or create a new one.
2. Configure your Import Definition appropriately according to the directions in this chapter, making sure that on the Data Import General Tab on Page 74 you specify the following:
   - Automation mode as **Listening on data**
   - Path to a folder on the server where the files you are importing will be placed
   - File pattern to be used as a filter when retrieving files from the preceding

NOTE Make sure that different Import Definitions use different folders and/or file patterns so the imports are not trying to import the same file. See the information in Data Import Editor General Tab Fields on Page 75.

3. Save the Import Definition by clicking **Save and Close**.
4. To confirm that the Import Watcher is running on the C•CURE 9000 Server computer, click **Start**>**All Programs**>**Software House**>**C•CURE 9000**>**Server Configuration Application**.
5. On the Services tab, make sure that the Software House CrossFire Import Watcher has a Status of **Running**.
6. If the Import Watcher needs to be started, click **Start Service**.

You can also stop/start the Import Watcher from listening for selected Import Definitions from the Data Import Dynamic View context menu. For information, see Stopping/Starting Listening from the Import Watcher on Page 54, and Table 7.

Stopping/Starting Listening from the Import Watcher

Two menu selections on the Data Import Dynamic View context menu let you select one or multiple Import Definitions with an automation mode of 'Listening on data" to stop or start the Import Watcher listening for these Imports, as follows:

- Stop Listening – available for an Import Definition with 'Listening' status
- Start Listening – available for an Import Definition with 'Disconnected' status

When you select multiple Import Definitions on the Dynamic View, as long as one of them has the required automation mode and required status, the 'Stop Listening' and/or 'Start Listening' selections become available on the context menu. However, the relevant action will not be applied to Imports that do **not** actually meet the criteria.

Once you have stopped the Import Watcher listening for specific Import(s), you must use the 'Start Listening' selection to reactivate listening for the import(s).

NOTE

- The Stop/Start Listening menu selections work only when the Import Watcher server component is running.
- Restarting the C•CURE 9000 driver automatically restarts the Import Watcher listening for any Import Definition(s) stopped by the 'Stop Listening' selection.

To Stop Listening for an Import from Import Watcher

1. In the **Navigation** Pane of the Administration Client, click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Data Import**.
3. Click  to open a **Dynamic View** showing a list of all Data Import objects.
4. Select one or more Import Definitions with the 'listening on data' automation mode and 'Listening' status and right-click to open the Data Import Context menu (for information see Using the Object List Context Menu on Page 23.
5. From the Import Context menu, select **Stop Listening**.

   The Import Watcher stops listening for data for the selected Import Definition(s).

To Start Listening for an Import from Import Watcher

1. In the **Navigation** Pane of the Administration Client, click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Data Import**.
3. Click  to open a **Dynamic View** showing a list of all Data Import objects.
4. Select one or more Import Definitions with the 'listening on data' automation mode and 'Disconnected' status and right-click to open the Data Import Context menu (for information see Using the Object List Context Menu on Page 23
5. From the Import Context menu, select **Start Listening**.

   The Import Watcher starts listening again for data for the selected Import Definition(s).

Example Importing Tasks

You may find the how-to steps for the following import tasks helpful:

- Creating a New Personnel Record with a Credential, Primary Portrait and Clearances by Importing a CSV File on Page 56.
- Updating Personnel Records through an Import that Matches on Card Number on Page 58.
- Deleting Personnel Records Via an Import on Page 62.
- Assigning or Removing Personnel From Personnel Groups Through an Import on Page 65.

Creating a New Personnel Record with a Credential, Primary Portrait and Clearances by Importing a CSV File

As a C•CURE 9000 Administrator, you want to configure an Import Definition that can import personnel records from a CSV, ODBC, LDAP, or XML external data source. The external Personnel record can have information about Personnel itself and about its Credential, Clearances, Portrait images, etc. Therefore it is necessary to map the external fields to the proper fields in the Personnel record being imported, as well as to the child records such as Credential.

To Create Personnel Records from a CSV Import Using the Personnel Mapper

1. Create a new Import Definition on the **Data Import Editor**, giving it a name and description and selecting **CSV file import source** from the drop-down list in the **Select Type** field on the **General** tab.
2. Click the **Select Sample Input** button, and when the **Select File with Sample** dialog box opens, select a sample file, such as the following:

Example:

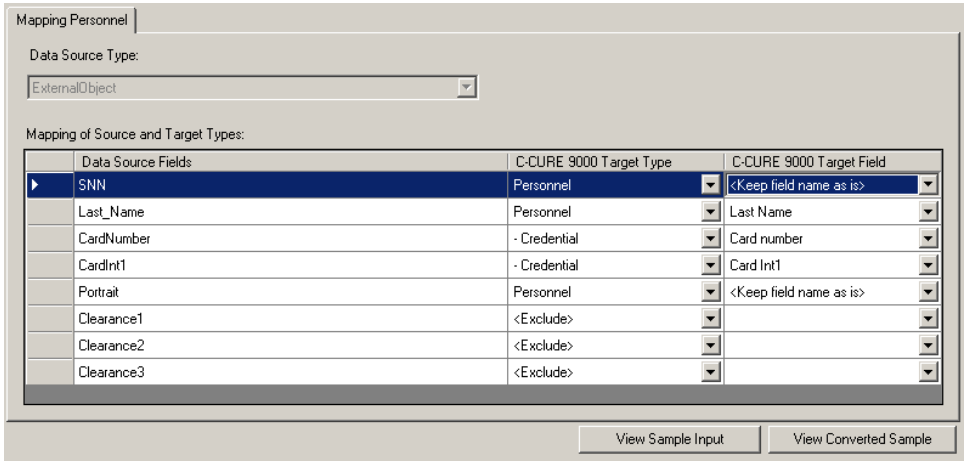
A Personnel file in CSV flat-structure format a portion of which might look as follows:

```
SSN, Last_Name,CardNumber,CardInt1,Portrait,Clearance1,Clearance2,Clearance3
01-23-4567,Smith,100,10,C:\images\Smith.jpg,LobbyDoor
11-23-4567,Rabbit,101,15,C:\Images\Rabbit.jpg,LobbyDoor,FrontDoor,RearDoor
```

3. Click **Open**.

   A message displays saying "Sample input does not contain any tags the system can recognize. You must configure a proper data conversion before you can proceed further."
4. Click **OK** to proceed. The **Data Conversion** tab opens.
5. Click the arrow next to the **Add** button and then click **Personnel mapping tool** from the drop-down list.

   The **Personnel Mapping Tool** opens with the CSV data fields mapped as well as the system is able to map them.



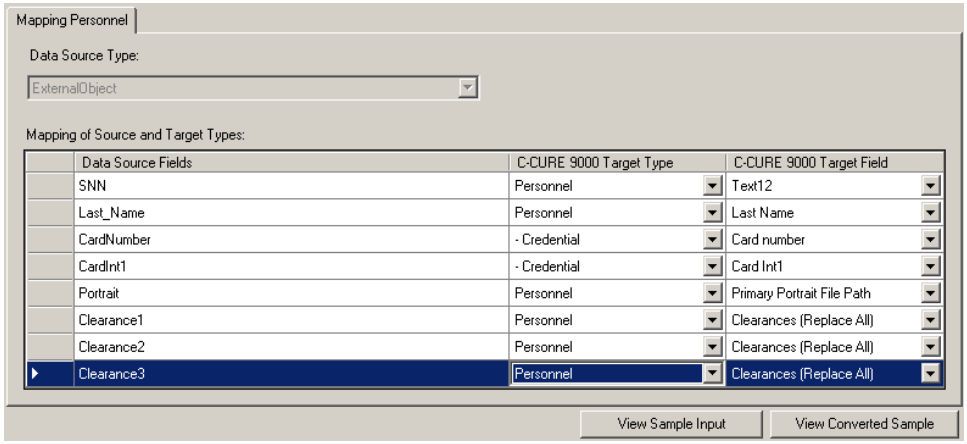
6. If you click the **View Sample Input** button, the data in the XML format would look as follows:

```
<CrossFire culture-info=" en-US".>
    <ExternalObject ImportMode=" Default">
        <SSN>01-23-4567</SSN>
        <Last_Name>Smith</Last_Name>
        <CardNumber>100</CardNumber>
        <CardInt1>10</CardInt1>
        <Portrait>C:\Images|Smith.jpg</Portrait>
        <Clearance1>LobbyDoor</Clearance1>
        <Clearance2>FrontDoor</Clearance2>
        <Clearance3>RearDoor</Clearance3>
    </ExternalObject>
</CrossFire>
```

Such an external flat record format is not recognized by the C•CURE 9000 Data Import function until it is converted into a structure that maps to the Personnel record's internal structure. Two kind of changes are needed:

- The field names must be changed from the external names to the names used by C•CURE 9000 objects.
- The fields related to the child records, such as 'Credential', must be wrapped with the nested tags.

7. Use the down-arrows next to the entries in the **C•CURE 9000 Target Type** and **C•CURE 9000 Target Field** columns to map the external Data Source Fields. You might map the fields as shown in the following example:



8. To see how your mapping will act on the sample input, click the **View Converted Sample** button. The converted output document would look as follows:

```
<CrossFire culture-info=" en-US".>
    <SoftwareHouse.NextGen.Common.SecurityObjects.Personnel ImportMode=" Default">
        <Text12>01-23-4567</Text12>
        <LastName>Smith</LastName>
        <PrimaryPortraitImageFile>C:\images|Smith.jpg</PrimaryPortraitImageFile>
        <ClearancesAll>LobbyDoor|FrontDoor|RearDoor</ClearancesAll>
        <SoftwareHouse.NextGen.Common.SecurityObjects.CredentialImportMode=" Default">
            <CardNumber>100</CardNumber>
            <CardInt1>10</CardInt1>
        </SoftwareHouse.NextGen.Common.SecurityObjects.Credential>
    </SoftwareHouse.NextGen.SecurityObjects.Common.Personnel>
</CrossFire>
```

9. If the mapping is satisfactory, click **Save and Close**.

   The **Data Conversion** tab reappears with the Personnel Mapping tool conversion you just completed listed at the top.

10. To check the conversion, click the **Verify Sample** button.
11. If the message confirms that the system recognizes every field in the sample, return to the **General** tab and finish configuring the Import Definition.
    a. Make sure the **Enabled** option is selected.
    b. If your system is partitioned, enter a destination partition for the imported records into the **Default Import Partition** field, if you wish.
12. Click the **Manual Import** button to perform the import immediately or click **Save and Close** if this is an automated type import.

The new personnel records are added to the C•CURE 9000 system.

Updating Personnel Records through an Import that Matches on Card Number

As a C•CURE 9000 Administrator, you want to configure an Import definition that can update Personnel records from a supported external data source such as CSV, ODBC, LDAP, or XML. The external Personnel record has a field storing the number of a credential assigned to a C•CURE 9000 personnel record. The Data Import function uses the Card Number to

match a Personnel record in the C•CURE 9000 database. The Import then uses the matched record to update the Personnel fields and the fields in its child records according to the fields defined in the external data. The example in the following procedure updates the Personnel **Text 12** and **Clearance** fields and the **Activation Date/Time** and **Expiration Date/Time** fields in its Credential .

To Update Personnel Records from a CSV Import that Matches on Card Number

1. Create a new Import Definition on the **Data Import Editor**, giving it a name and description and selecting the following on the **General** tab:
   - **CSV file import source** from the drop-down list in the **Select Type** field.
   - **Update when matched; otherwise add** in the **Default Import Mode** box.

   Once you select an 'Update' option, the system displays the following message: "To complete import configuration it is necessary to select the matching fields. Do you want to do it now?"
   - If you click **Yes**, the **Select File with Sample** dialog box opens for you to select a sample file. Go to Step 2.
   - If you click **No**, click the **Select Sample Input** button to open the **Select File with Sample** dialog box and proceed to Step 2
2. Select a sample file, such as the following:

   Example:

   A Personnel file in CSV flat-structure format a portion of which might look as follows:

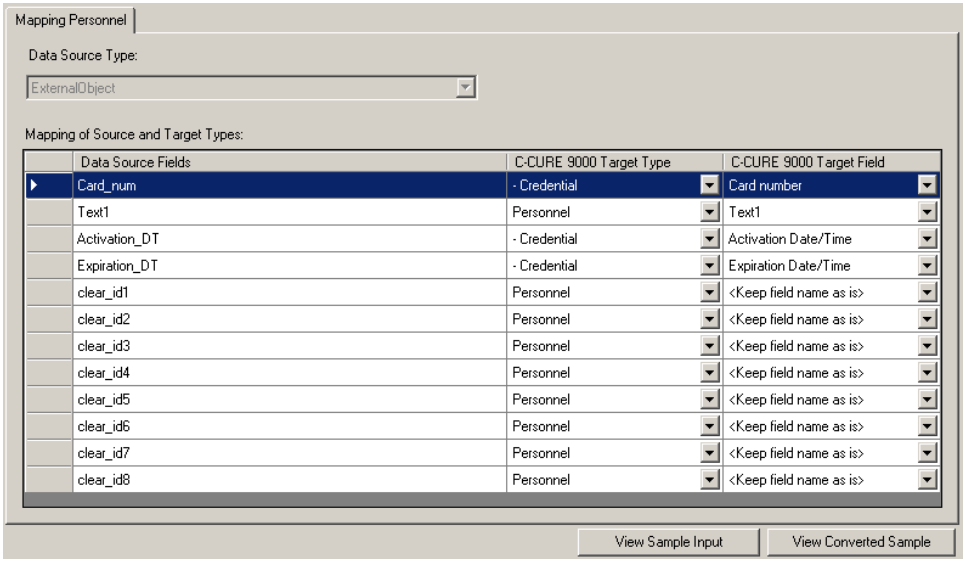
   ```
   Card_num,Text1,Activation_DT,Expiration_DT,clear_id1,clear_id2,clear_id3,clear_
   id4,clear_id5,clear_id6,clear_id7,clear_id8

   976056500,,5/13/11 0:00,6/13/11 0:00,FIRST FLOOR LOBBY,SECOND FLOOR LOBBY,SECOND FLOOR
   CONFERENCE ROOM,,,,,

   976056501,Administration Offices,5/13/11 0:00,6/13/11 0:00,,FIRST FLOOR LOBBY,SECOND
   FLOOR LOBBY,SECOND FLOOR CONFERENCE ROOM,,,,,
   ```
3. Click **Open**.

   A message displays saying "Sample input does not contain any tags the system can recognize. You must configure a proper data conversion before you can proceed further.
4. Click **OK** to proceed. The **Data Conversion** tab opens.
5. Click the arrow next to the **Add** button and then click **Personnel mapping tool** from the drop-down list.

   The **Personnel Mapping Tool** opens with the CSV data fields mapped as well as the system is able to map them.



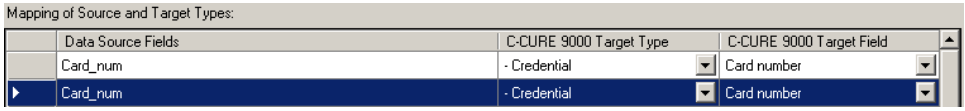
6. If you click the **View Sample Input** button, the data in the XML format would look as follows:

```
<CrossFire culture-info=" en-US".>
    <ExternalObject ImportMode=" Default">
        <Card_Num>976056500</Card_Num>
        <Text1>Administration Offices</Text1>
        <Activation_DT>5/13/11 0:00</Activation_DT>
        <Expiration_DT>6/13/11 0:00</Expiration_DT>
        <Clear_id1>FIRST FLOOR LOBBY</Clear_id1>
        <Clear_id2>SECOND FLOOR LOBBY</Clear_id2>
        <Clear_id3>SECOND FLOOR CONFERENCE ROOM</Clear_id3>
        <Clear_id4>THIRD FLOOR REC ROOM</Clear_id4>
        <Clear_id5>OUTSIDE PATIO</Clear_id5>
        </Clear_id6>
        </Clear_id7>
        </Clear_id8>
    </ExternalObject>
</CrossFire>
```

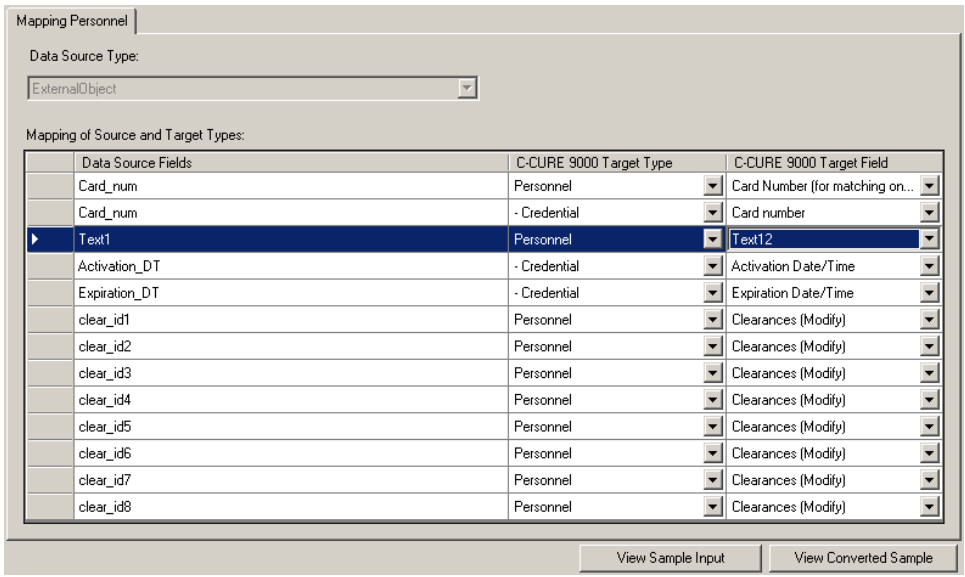
   Such an external flat record format is not recognized by the C•CURE 9000 Data Import function until it is converted into a structure that maps to the Personnel record's internal structure. Two kind of changes are needed:

   - The field names must be changed from the external names to the names used by C•CURE 9000 objects.
   - The fields related to the child records, such as 'Credential', must be wrapped with the nested tags.

7. Use the down-arrows next to the entries in the **C•CURE 9000 Target Type** and **C•CURE 9000 Target Field** columns to map the external Data Source Fields.
   a. In order to map data from the **Card_Num** external data source field to two different fields in the C•CURE 9000 personnel Object (the **Personnel** type **Card Number (for matching only)** field and the **Credential** type **Card Number** field), right-click in the **Card_Num** field.
   b. Click **Duplicate Current Row** on the context menu that appears. The mapper copies the row.



8. You might then map all the fields as shown in the following example:



Notice that the eight Clear_id **Data Source Fields** have all been mapped to the same **C•CURE 9000 Target Field**. When two or more rows are mapped to the same target field, the values of the source fields are combined into a pipe-delimited value before being assigned to the target field. This pipe-delimited value is used by the fields "Clearances (Modified)" or "Clearances (Replace All)" in the Personnel target type as described in Special Fields on Page 552.

9. To see how your mapping will act on the sample input, click the **View Converted Sample** button. The converted output document would look as follows:

```
<CrossFire culture-info=" en-US".>
    <SoftwareHouse.NextGen.Common.SecurityObjects.Personnel ImportMode=" Default">
        <CardNumberForMatching>976056500</CardNumberForMatching>
        <Text12>Administration Offices</Text12>
        ClearancesChanged>First Floor Lobby|Second Floor Lobby|Second Floor Conference Room|Third
        Floor Rec Room|OutsidePatio</ClearancesChanged>
        <SoftwareHouse.NextGen.Common.SecurityObjects.CredentialImportMode=" Default">
            <CardNumber>976056500</CardNumber>
            <ActivationDateTime>5/13/11 0:00</ActivationDateTime>
            <ExpirationDateTime>6/13/11 0:00</ExpirationDateTime>
        </SoftwareHouse.NextGen.Common.SecurityObjects.Credential>
    </SoftwareHouse.NextGen.SecurityObjects.Common.Personnel>
</CrossFire>
```

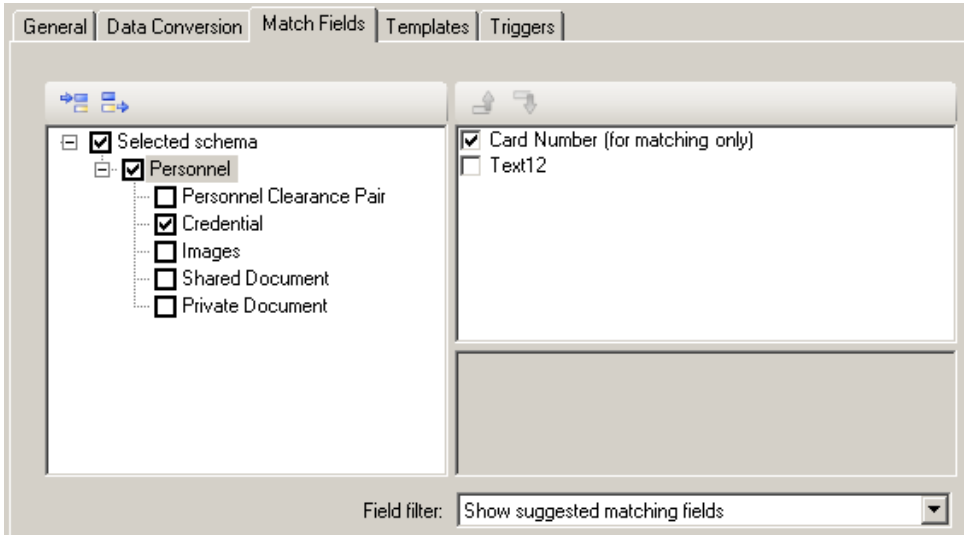
10. If the mapping is satisfactory, click **Save and Close**.

    The **Data Conversion** tab reappears with the Personnel Mapping tool conversion you just completed listed at the top.

11. To check the conversion, click the **Verify Sample** button.

12. If the message confirms that the system recognizes every field in the sample, click to open the **Match Fields** tab .

13. Select the fields to match on for updating the records.
    a. On the tree in the left-hand pane, click **Personnel** and then click **Card Number (for matching only)** in the right-hand pane.
    b. On the tree in the left-hand pane, click **Credential** and then click **Card Number** in the right-hand pane.



14. Return to the **General** tab and finish configuring the Import Definition.
    a. Make sure the **Enabled** option is selected.
    b. If your system is partitioned, enter a default destination partition for the newly imported records into the **Default Import Partition** field, if you wish.
15. Click the **Manual Import** button to perform the import immediately or click **Save and Close** if this is an automated type import.

Once the import process is finished, the Personnel Records with the matching card numbers will have their Clearances and Text12 fields changed, as well as the Activation and Expiration date/times of the specified credentials updated.

Deleting Personnel Records Via an Import

As a C•CURE 9000 Administrator, you want to configure an Import definition that can use an import from a CSV, ODBC, LDAP, or XML external data source to delete Personnel records and/or delete one or more credentials from a Personnel record.

The external personnel record has a field that stores a valid ImportMode value, such as 'Default', 'Add', 'Set', 'Update', 'Delete' or 'DeleteAll'. The Data Import function uses the Personnel mapping tool item "Attribute: Import mode" to map this external value into the value of the ImportMode attribute for the type selected in the **C•CURE 9000 Target Type** column. For more information, see Attribute 'ImportMode' on Page 548.

The behavior of the import depends on the actual mapping of the Import Mode column.

- If it is mapped to the Import Mode attribute of the **Personnel** target type, the import deletes the entire Personnel record matching the external record together with its child records—when the Import Mode value is 'Delete' or 'DeleteAll'.
- If it is mapped to the Import mode attribute of a child target type, such as a **Private Document** or **Credential**, the import deletes a **single** child record—when the value is 'Delete', or **all** the child records of the targeted type—when the value is 'DeleteAll'.

NOTE This example uses a CSV import.

To Delete Personnel Records Using a CSV Import

1. Create a new Import Definition on the **Data Import Editor**, giving it a name and description and selecting the following on the **General** tab:
   - **CSV file import source** from the drop-down list in the **Select Type** field.
   - **Update only matched; do not add records** in the **Default Import Mode** box.

   When you select an Update option, the system displays the following message: "To complete import configuration it is necessary to select the matching fields. Do you want to do it now?"
   - If you click **Yes**, the **Select File with Sample** dialog box opens for you to select a sample file. Go to Step 2.
   - If you click **No**, click the **Select Sample Input** button to open the **Select File with Sample** dialog box and proceed to Step 2.
2. Select a sample file, such as the following:

Example:

A Personnel file in CSV flat-structure format a portion of which might look as follows:

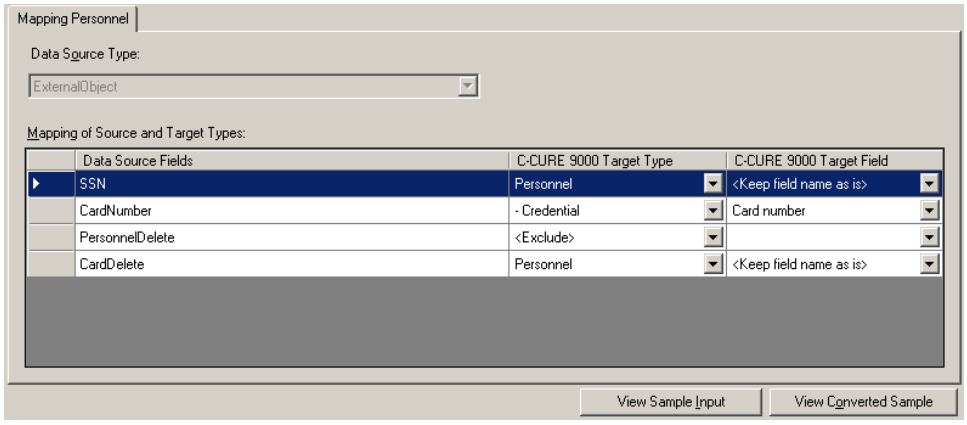
```
SSN,CardNumber,PersonnelDelete,CardDelete
000-00-0001,217,Delete,Default
000-00-0002,218,Default,Delete
```

3. Click **Open**.

   A message displays saying "Sample input does not contain any tags the system can recognize. You must configure a proper data conversion before you can proceed further.
4. Click **OK**.

   The **Data Conversion** tab opens.
5. Click the arrow next to the **Add** button and then click **Personnel mapping tool** from the drop-down list.

   The **Personnel Mapping Tool** opens with the CSV data fields mapped as well as the system is able to map them.



6. If you click the **View Sample Input** button, the data in the XML format would look as follows:

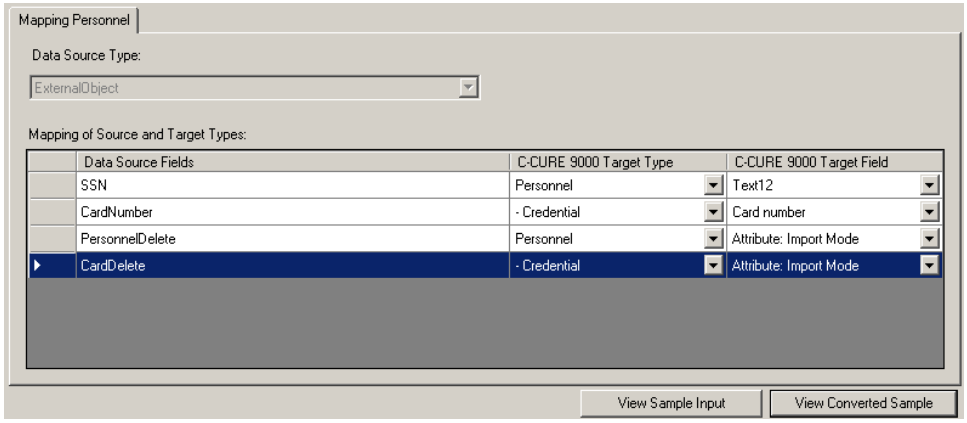
```
<CrossFire culture-info=" en-US".>
   <ExternalObject ImportMode=" Default">
      <SSN>000-00-0001</SSN>
      <CardNumber>217</CardNumber>
      <PersonnelDelete>Delete</PersonnelDelete>
```

```
        <CardDelete>Default</CardDelete>
    </ExternalObject>
</CrossFire>
```

Such an external flat record format is not recognized by the C•CURE 9000 Data Import function until it is converted into a structure that maps to the Personnel record's internal structure. Several kinds of changes are needed:

- The field names must be changed from the external names to the names used by C•CURE 9000 objects.
- The fields related to the child records, such as 'Credential', must be wrapped with the nested tags.
- The PersonnelDelete and CardDelete fields should be mapped to the ImportMode XML attributes of the proper XML tags

7. Use the down-arrows next to the entries in the **C•CURE 9000 Target Type** and **C•CURE 9000 Target Field** columns to map the external Data Source Fields.
8. You might map the fields as shown in the following example:

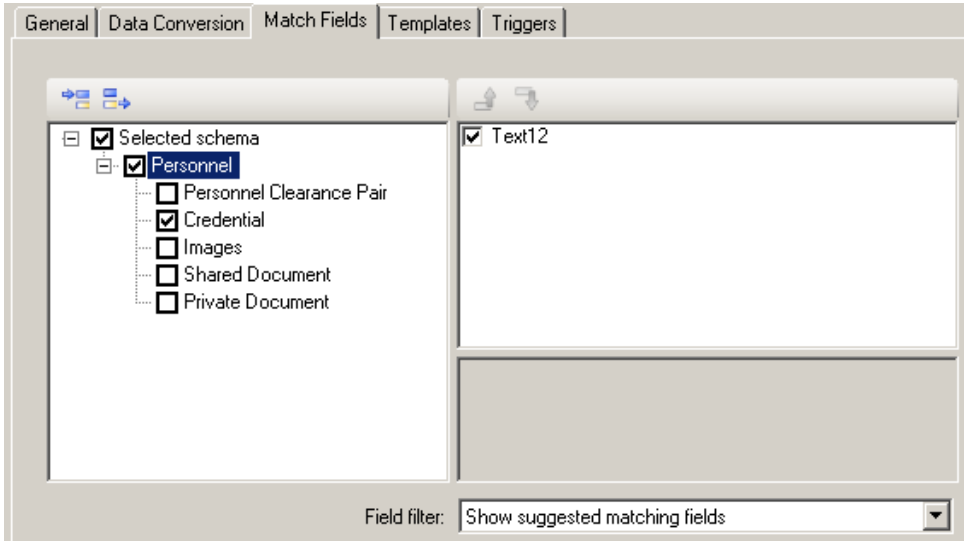


9. To see how your mapping will act on the sample input, click the **View Converted Sample** button. The converted output document would look as follows:

```
<CrossFire culture-info=" en-US".>
    <SoftwareHouse.NextGen.Common.SecurityObjects.Personnel ImportMode=" Delete">
        <Text12>000-00-0001</Text12>
        <SoftwareHouse.NextGen.Common.SecurityObjects.Credential ImportMode=" Default">
            <CardNumber>217</CardNumber>
        </SoftwareHouse.NextGen.Common.SecurityObjects.Credential>
    </SoftwareHouse.NextGen.SecurityObjects.Common.Personnel>
</CrossFire>
```

10. If the mapping is satisfactory, click **Save and Close**.

    The **Data Conversion** tab reappears with the Personnel Mapping tool conversion you just completed listed at the top.
11. To check the conversion, click the **Verify Sample** button.
12. If the message confirms that the system recognizes every field in the sample, click to open the **Match Fields** tab .
13. Select the fields to match on for updating the records.
    a. On the tree in the left-hand pane, click **Personnel** and then click **Text12** in the right-hand pane.
    b. On the tree in the left-hand pane, click **Credential** and then click **Card Number** in the right-hand pane.



14. Return to the **General** tab and finish configuring the Import Definition.
    a. Make sure the **Enabled** option is selected.
    b. If your system is partitioned, enter a default destination partition for the newly imported records into the **Default Import Partition** field, if you wish.
15. Click the **Manual Import** button to perform the import immediately or click **Save and Close** if this is an automated type import.

Once the import process is finished, some Personnel Records will be entirely deleted—child records and all; while other records will only have their Credentials deleted.

Assigning or Removing Personnel From Personnel Groups Through an Import

As a C•CURE 9000 Administrator, you want to configure an Import definition that can use an import from an XML external data source to add or remove a Personnel record from some or all groups.

NOTE This example uses an XML import.

To Assign or Remove Personnel from Groups

1. Follow the steps in Creating an Import Definition on Page 47, configuring the import definition as follows:
    a. From **Automation mode**, select **Manual only**.
    b. From **Default Import Mode**, select **Update when matched; otherwise add**.
2. On the **Data Import** tab, navigate to the imported Personnel record.
3. Right-click the Personnel record and click **Manual Import...**
4. Import the configured Personnel XMLdata source from your PC. In the XML code, include one of the following fields:
    - GroupsChanged
    - GroupsAll

Example

To assign the Personnel to the groups pg1 and pg2, include the field `<GroupsChanged>+pg1|+pg2</GroupsChanged>`.

To remove the Personnel from all groups and to assign the Personnel to the groups pg1 and pg2, include the field `<GroupsAll>+pg1|pg2</GroupsAll>`

For more examples, see GroupsAll and GroupsChanged on Page 554.

5. Open the **Configuration** pane and from the drop-down menu, select **Group**.
6. Right-click a group that you assigned or removed the Personnel from and click **Edit**.
7. From **Objects in Group**, check that any Personnel records that you assigned are present and any removed Personnel records are not present.

Data Import Editor

C•CURE 9000 lets you update the C•CURE 9000 database by importing records contained in another C•CURE 9000 database or a human resources (HR) or other external database. Depending on your C•CURE 9000 access privileges, you can import records at any time, schedule imports to run at predetermined intervals, or import records in response to events monitored by the system.

C•CURE 9000 imports information as objects, according to parameters contained in a named Import Definition.

The Data Import Editor in C•CURE 9000 lets you create multiple Import Definitions, each containing a unique set of import parameters, depending on your needs. You save each Import Definition using a unique name. You can also save Import Definitions as templates, to simplify creation of other Import Definitions.

The following topics give more information about importing data.

- LDAP Data Import Overview on Page 145
- ODBC Data Import Overview on Page 180

Data Import Editor Tabs

- Data Import General Tab on Page 74
- Data Import Data Conversion Tab on Page 89
- Data Import Match Fields Tab on Page 120
- Data Import Templates Tab on Page 127
- Data Import Triggers Tab on Page 140
- Basic Importing Tasks on Page 47
- Creating an Import Definition on Page 47

Importing Tasks

- Accessing the Data Import Editor on Page 47
- Creating an Import Definition on Page 47
- Creating an Import Definition Template on Page 48
- Configuring an Import Definition on Page 49
- Configuring an Import Definition for an LDAP Source on Page 166
- Configuring an Import Definition for an ODBC Source on Page 203
- Modifying a Data Import on Page 71

The **Data Import Editor** has the buttons described in Table 6 on Page 67.

Table 6: Data Import Editor Buttons

Button	Description
Save and Close	Click this button when you have completed any changes to the Import Definition and wish to save those changes. The Import Definition closes.

Data Import Editor Buttons (continued)

Button	Description
Save and New	Click this button when you have completed any changes to the Import Definition and wish to save those changes and also create a new Import Definition. The Import Definition you were editing is saved, and a new Import Definition opens (either blank or including template information if you were using a template to create new Import Definition).
	Click this button when you want to close the **Import Definition 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.
Select Sample Input	Click this button to open a dialog box that lets you select a file from the hard drive (for XML and CSV import sources). The selected file should have the same structure to be used later during import operations (through the import object being configured), though not necessarily the same data. Once you select the file and click **Open**, the system parses the file—using the current configuration defined for the selected import source object—and memorizes its structure. The parsing strips off duplicate information, keeping the structure of the document, **Example:** If the file has 100 Personnel records and 10 records with iSTAR controllers, the structure will contain a single personnel record and a single iSTAR record, including all the fields defined by the parsed 110 records. If the import source object does **not** support reading from the file (an LDAP import source, for example), clicking this button retrieves data from the import source object directly. In this case, either of the following occurs: The system retrieves the first n records from the database from which the import source is configured to get data. The import source object generates a fake set of records based on its current configuration. A special dialog box can be used to select the proper sample records.
View Sample Input	Click this button to open a dialog box with an XML document that represents the structure generated by the system while parsing the sample input document. If the source reads a document in another format, such as CSV, this button shows the result of the conversion of the external document into XML. NOTE: This button is unavailable if sample input has not been selected.
View Converted Sample	Click this button to open a form with the XML document that represents the result of the data conversion applied to the selected sample input (configured on the **Data Conversion** tab). NOTE: This button is unavailable if sample input has not been selected or if the list of converters is empty.
Verify Sample Input	Click this button to take the selected sample input converted by the chain of import converters (if any) and verify that each field and each object type in the resulting XML document can be recognized by C•CURE 9000. If the verification fails, the system informs you and suggests creating a proper data conversion. If only some of the fields cannot be recognized by the system, the system can show the rest of the fields in a form of XML document. This button also verifies that the **Match Fields** tab contains all the recognized types from the sample input, and appends missing types to the list. NOTE: This button is unavailable if sample input has not been selected.

Data Import Editor Tasks

- Creating an Import Definition on Page 47
- Creating an Import Definition Template on Page 48
- Configuring an Import Definition on Page 49
- Configuring an Import Definition for an LDAP Source on Page 166
- Configuring an Import Definition for an ODBC Source on Page 203
- Viewing a List of an Object Type on Page 22
- Deleting an Object on Page 25

NOTE Deleting an Import Definition does not delete its Imports Results history.

- Modifying a Data Import on Page 71

Data Import List Context Menu

The context menu that opens when you right-click a Data Import in the Data Import Dynamic View includes the selections described in Using the Object List Context Menu on Page 23. Context menu options specific to Data Import are described in Table 7 on Page 69.

Table 7: Data Import List Context Menu Options

Menu Selection	Description
Set property	Click this menu selection to change the value of the selected properties in the selected Data Import(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 this property. The following properties can be changed. • **Default Import Partition** – You can indicate/change the Partition where the newly imported objects should be placed. • **Description** – You can change the textual description of the Data Import(s) by selecting this property and typing in a new value. • **Enabled** – You can determine whether or not this Data Import is operational for importing or not by selecting this property and selecting/clearing the value check box. • **Template** – You can determine whether or not this Data Import can be used as a template by selecting this property and selecting/clearing the value check box.
Start Listening	Click this menu selection to restart the Import Watcher listening for external events for the selected Import definition(s). This selection is available only if the selected imports have an automation mode of "Listening on data' and a status of 'Disconnected'. (For more information, see Stopping/Starting Listening from the Import Watcher on Page 54.)
Stop Listening	Click this menu selection to stop the Import Watcher from listening for external events for the selected Import definition(s). This selection is available only if the selected imports have an automation mode of '**Listening on data**' and a status of '**Listening**'. (For more information, see Stopping/Starting Listening from the Import Watcher on Page 54.)
Run on Server	Click this menu selection to cause the selected Import definition to start importing files. This selection is available only if the selected import's automation mode is "**Activated by event' and the Import is not currently running**. (For more information, see Running an Import on the Server from Data Import Dynamic View on Page 53.)
Manual Import	Click this menu selection to select an external file for import. This selection is available only if **Manual only** is selected as the Automation mode and the selected Source type supports manual import.

Table 7: Data Import List Context Menu Options (continued)

Menu Selection	Description
Find Import History	Click this menu selection to open a dialog box that lists all Import Results for this Import definition. (For more information, see Viewing Import Results History on Page 71.)

Data Import Status

The Status field for each Data Import can have any of the values described in Table 8 on Page 70.

NOTE Restarting the C•CURE 9000 server changes the status of all Import Definitions to the correct initial value:

- For Listening on Data to 'Disconnected.'
- For Activated by event to 'Available.'

See Data Import Triggers Tab on Page 140 for information about how these Import Status values can activate events.

Table 8: Data Import Status Descriptions

Status	Description
Available	Indicates the following: • For Manual Imports – always available • For Activated by event – import is not running at this time so you can execute the **Run on Server** option from the right-click context menu to start the import. • For Listening on data – N/A
Completed	Indicates that the Import has finished. NOTE: This Status only pulses and then immediately changes to a Status of "Available" or "Listening". For this Status to be useful, you must configure it to trigger an Event that: • Requires acknowledgement. - or - • Triggers an Action that generates a Report, triggers another Event, or informs appropriate Personnel of this Status—via an email, for example.
Completed with Rejects	Indicates that the Import finished, but included records that were rejected. NOTE: This Status only pulses and then immediately changes to a Status of "Available" or "Listening". For this Status to be useful, you must configure it to trigger an Event that: • Requires acknowledgement. - or - • Triggers an Action that generates a Report, triggers another Event, or informs appropriate Personnel of this Status—via an email, for example.
Connectivity Error	Indicates the following: • For Manual Imports – N/A • For Activated by event/Listening on data – Import Source cannot connect to an external data storage, such as a file folder or LDAP database
Disabled	Indicates the following: • For Manual Imports – N/A • For Activated by event/Listening on data – Import has been manually disabled by a user and is not running any automatic import • For an Import definition template (which can appear in the Dynamic View list) – the status is always disabled

Table 8: Data Import Status Descriptions (continued)

Status	Description
Disconnected	Indicates the following: • For Manual Imports – N/A • For Activated by event – N/A • For Listening on data – Import Watcher is not running or the Import Definition is waiting to be started
Importing	Indicates the following: • For Manual Imports – N/A • For Activated by event/Listening on data – Import is currently busy importing external data on the server. You cannot run this Import Definition on the server again until this import process has finished.
Listening	Indicates the following: • For Manual Imports – N/A • For Activated by event – N/A • For Listening on data – Import Watcher is running and the Import Definition is ready to import new data.
Not licensed	Indicates that you do not have a license to run an import for this Import Definition.

Modifying a Data Import

You can modify an existing Data Import by editing it using the **Data Import Editor**.

To Modify a Data Import

1. In the **Navigation** pane of the Administration Client, click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Data Import**.
3. Click  to open a **Dynamic View** showing a list of all Data Import objects.
4. Right-click the Data Import you want to change and click **Edit** from the context menu that appears.

   - or -

   Double-click the Data Import you want to change.
5. The **Data Import Editor** opens for you to edit the Import making changes as you wish.
6. To save your modified Data Import, click **Save and Close**.

   - or -

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

Changing the source type of an Import Definition during an edit will wipe out the data source configuration. To keep the original source type, cancel the edit operation.

Viewing Import Results History

You can view the history of one or more completed Data Imports from the Data Import Context menu. The Import History log displays records of all completed import operations for the selected Data Import Definition(s). The information displayed for each historical record are detailed in a list on Table 9 on Page 72 and include the number of records added, updated, deleted, and/or rejected. In addition, you can choose which of this information to display.

This Import History Log also lets you open the actual error log file generated during the import, an XML file that lists records that did not import properly. You can use the information in the log to troubleshoot these failures: where possible, the log indicates why the object did not import. C•CURE 9000 allows you to review and repair rejected files until they import successfully.

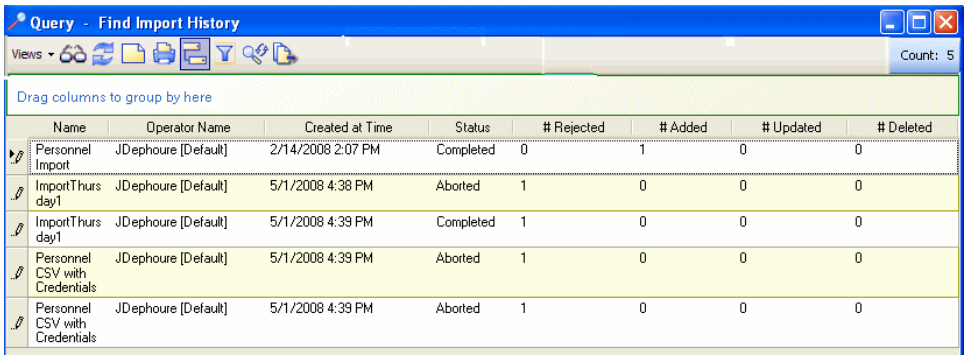
To review the import history for the entire C•CURE 9000, you would use the **Data Import/Export History** option on the **Options and Tools** pane. For information, see the *C•CURE 9000 System Maintenance Guide*.

To View Data Import History

1. In the **Navigation** pane of the Administration Client, click the **Configuration** pane button .
2. Click the **Configuration** drop-down list and select **Data Import**.
3. Click to open a **Dynamic View** listing all existing Data Import objects, as shown in Data Import List Context Menu on Page 69.
4. Right-click the Data Import(s) whose history you want to view and click **Find Import History** from the context menu that appears.

   The Import results history opens on a Query Result list similar to that shown in Figure 3 on Page 72.

Figure 3: Import History List



Details about Import result(s) for each Import Definition you selected are displayed in a Dynamic View. By default, not all the columns display at first. Right-click in the column headings of the view to choose to display more or fewer columns. The Import history includes the following:

Table 9: Import History List Information

Column	Description
Name	Unique name that identifies the import in the system. Not the name of the file containing data being imported.
Operator Name	Name of the operator performing the import. (For an automated import or any import initiated by an Event, this is the name of the operator who configured the Event Action, or last modified it.)
Created at time	Time when the import was started.
End at time	Time when the import finished.
Status	The final status of the import, Completed, for example.
# Rejected	Number of records that were rejected during the import.
# Added	Number of records that were added into the system.

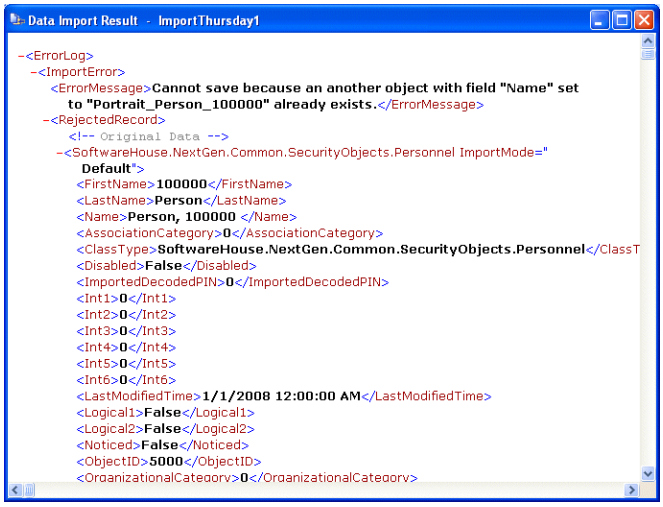
Import History List Information (continued)

Column	Description
# Updated	Number of records that were updated during the import.
# Deleted	Number of records that were deleted during the import.
Import Filename	Information about the import source—usually the name of the file imported.
Description	Description given to the import when configured. No more than 500 characters.
Error Log File	Name of the file on the server containing the error log messages that were generated during the import.
Partition	Name of the Partition of the import. (If your system is non-partitioned, 'Default' is entered.)

5. To view the error log for a particular import result, right-click the import and click **popup view** from the context menu that appears. A window such as the following displays.

NOTE If the size of the error log is greater than 10MB, a warning such as the following displays instead: "The size of the error log file is *n* MB. It could take a long time for the file to open. Do you want continue?"

- If you click **Yes**, the system tries to open the file—which could fail.
- If you click **No**, the popup window displays the message, "Error Log File is too large to be displayed."



6. To delete one or more import results, right-click the import result(s) and click **Delete** from the context menu that appears.

   A confirmation message appears. Click **Yes** to delete the import result(s) or **No** to cancel the deletion.

NOTE Deleting an import result also deletes its error log file stored internally on the server. It does not, however, delete any additional log files (if there are any) stored in the folder from which the import data was taken.

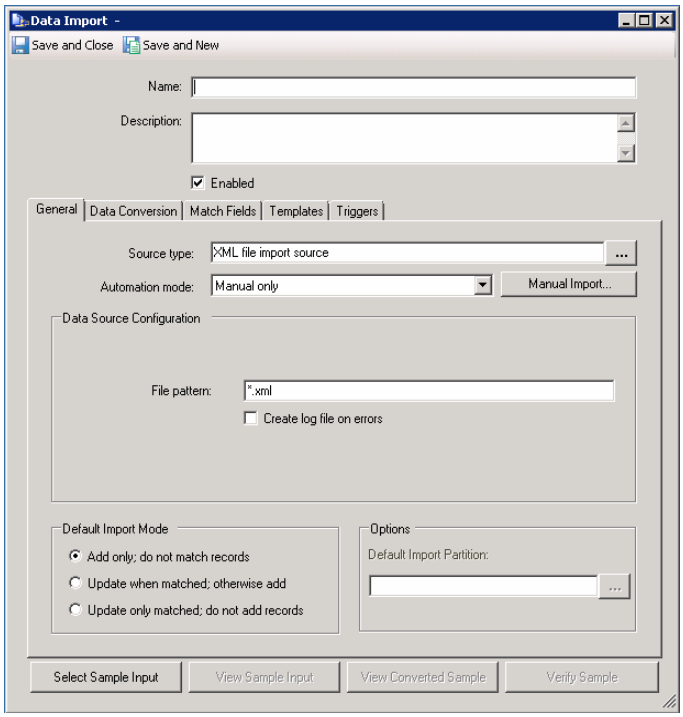
Data Import General Tab

The **General** tab is used to define the following for the Import Definition:

- Source type—the supported import source to use: **CSV file**, **LDAP**, **ODBC** or **XML file** (the default).
- Automation mode— possible choices displayed depend on the Source type selected: **Manual only** or two Automated modes—**Activated by event** or **Listening on data**. (XML and CSV import sources support all three modes; the LDAP import source supports only **Listening on data** mode; and the ODBC import source supports only **Activated by event** or **Listening on data**.)
- Data Source Configuration—choices vary depending on selections in the **Source type** and **Automation mode** fields.
- Default Import Mode—one of three options:
  - Add only; do not match records
  - Update when matched; otherwise add
  - Update only matched; do not add records
- Options—Default Import Partition—select the Partition in which to place **newly imported** records when the records do not include a reference to any partition. (This field is available only if the C•CURE 9000 system is partitioned, and the value in this field is **not** used when the import updates an existing record.)

The Data Import editor General tab is shown in Figure 4 on Page 74.

Figure 4: Data Import Editor General Tab



For more information, see:

- Data Import Editor Tasks on Page 69
- General Tab Definitions on Page 75
- General Tab Tasks on Page 79

General Tab Definitions

The **General** tab has the fields described in Table 10 on Page 75.

Table 10: Data Import Editor General Tab Fields

Fields/Buttons	Description
Name	The name of the Import Definition. This field is required.
Description	A textual description of the Import definition. This field is not required, but if used can make it easier to identify the specific Import definition when you are using it later on.
Enabled	Select this check box to make the Import Definition operational. (The default is selected.)
General Tab	
Source Type	Click ... to select the type of import source to use from the drop-down list: CSV file, LDAP, ODBC, or XML file (the default) are the supported types. NOTE: For information specific to configuring imports from an LDAP data source, see LDAP Data Import Overview on Page 145 and for configuring imports from an ODBC data source, see ODBC Data Import Overview on Page 180.
Automation Mode	Select one of three modes in which the import will operate: • Manual only – allows you to select a file on the client computer and import it into the C•CURE 9000 database. (Selecting this option makes the **Manual Import** button available.) • Activated by event (automated) – the Import Definition listens for C•CURE 9000 events, such as a scheduled event, that trigger the Import Definition to poll its import source for existing data. • Listening on data (automated) – the import source object is initialized by the Import Watcher server component and starts listening for external events, such as the creation of new files in a specified folder. When an external event is received, the import source initiates import of the received data. (For LDAP, this is the **only mode** supported.)
Manual Import	Click this button to select an external file on the client computer for import. NOTE: Since you are running the import on the client, the system does not use the Default Import 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 Import server directory, if you wish). This button is available only if **Manual only** is selected as Automation mode and the selected **Source type** supports manual import.
Data Source Configuration Box (These entries change depending on the import source and/or Automation Mode selected. Entries for LDAP are completely different as are entries for ODBC. See Import Editor General Tab for LDAP on Page 147 and LDAP Data Import General Tab Definitions on Page 147 for LDAP definitions. See Import Editor General Tab for ODBC on Page 186 and ODBC Data Import General Tab Definitions on Page 187 for ODBC definitions.)	

Data Import Editor General Tab Fields (continued)

Fields/Buttons	Description
Folder on server	NOTE: This field is available only for XML/CSV imports in one of the two automated modes. Specify a folder on the server using either an absolute path, UNC path, or one relative to the default path in the 'DefaultImportDirectory' system variable. See the *C•CURE 9000 System Maintenance Guide* "System Variables" chapter. **Example:** Absolute path: C:\SampleInputs\Import UNC path: \\Server_Name\Import Relative path: Import The system validates the folder's existence when you save the Import Definition, and displays error messages if you left the field empty or entered a non-existent directory. NOTE: For the automated Import to be functional, the server must have proper read/write access to the specified folder.
Select Folder	NOTE: This button is available only if you select **Activated by event** or **Listening on data** from the Automation drop-down. Click to select a folder for data source configuration from your directory.
File pattern	Specify a pattern to act as a filter to retrieve files: **Example:** *.xml retrieves any xml file personnel*.xml retrieves personnellist.xml and personnelnew.xml, etc. • For Manual mode XML/CSV imports – specify a pattern to be used as the default in the **Open File** dialog boxes for selecting the import file or sample input files. NOTE: You can override the pattern in the **Open File** dialog boxes, selecting a file that does not match it. • For automated mode XML/CSV imports – specify a pattern to be used by this Import Definition when retrieving files from the Import folder named in the **Folder on server** field. NOTE: If the system contains several Import Definitions configured for an automated import, each Import should have a unique combination of folder and file pattern. The Imports can retrieve files from the same or different folders, but must use patterns that do not match each other. If the preceding is not done, the automated import may try to import the same file twice and the system may not be able to determine which Import Definition to use in this 'overlapped' case. Software House also recommends that you not use the pattern '*.*' because it is too general and the system will try to import files created automatically by C•CURE 9000, such as log files.
Create log file on errors	Select this option to indicate that once the import process has completed, the system will create a special error log file in the same folder where the original import source file is located. This error log file will contain all records rejected during the import operation, stored in the internal XML format. NOTE: For an XML Import, this stored format **could** be different from the format of the incoming records if the import process had applied data conversion to the received data. For a CSV import, the stored format will **definitely differ** from the format of the incoming records since the import process converted the data from CSV to internal XML format. Whether you select this option or not, the same rejected records will be stored on the server, attached to the proper Import Results entry in the Import History Log (described on Viewing Import Results History on Page 71).
Create log file on completion	NOTE: This field is available only for XML/CSV imports in one of the two automated modes. Select this option to indicate that once the import process has completed, the system will create a special log file in the same folder where the original import source file is located. This file will have the same name as the original file with the suffix '.results' appended. It will contain import results summary information similar to the information stored in the Import History Log and including the number of records added, updated, deleted, and/or rejected.

Data Import Editor General Tab Fields (continued)

Fields/Buttons	Description
Delete source file after import	NOTE: This field is available only for XML/CSV imports in one of the two automated modes. Select this option to delete the file specified as the import source when the import process has finished. NOTE: If this option is not selected, the file is renamed by appending the suffix ".completed' to the name of the imported file. Whether you select this option or not—if the input file is not a well-formatted XML document or CSV file, the file is not deleted but renamed by appending the suffix '.rejected' to the current file name.
Advanced	NOTE: This button is available only for CSV imports. Click this button to open the **Advanced Properties** Sheet Figure 9 on Page 84. • For the **Default Culture** property, change the entry or leave the default to control how the CSV date and numeric values are parsed. **Examples:** 12/31/2011 for en-US or 31/12/2011 for en-UK 100,000.00 for en-US or 100 000,00 for fr-FR • For the **Default Tag** property, replace 'ExternalObject' with the name of the top-level object being imported—if you know it; or click ... to select a type from the drop-down list. **Example:** Personnel • For the **Keep Duplicate Columns** property, set to **True** to place values from columns with duplicate names into separate XML entries; set to **False** to concatenate the values from these columns into one single pipe-delimited XML entry. Click **Save** to return to the Data Import Editor.
Default Data Import Mode Box (The import mode can be overridden from the XML file received document. See Attribute 'ImportMode' on Page 548 in Appendix A.)	
Add only; do not match records	Select this import rule option to only add all the records in the import source to the database without performing any matching. (A record is rejected for import, however, if a duplicate already exists in the C•CURE 9000 database.)
Update when matched, otherwise add	Select this import rule option to perform matching as follows: • If the import source contains records with match field values that exactly match those field's values in existing records in C•CURE 9000, the records in C•CURE 9000 are updated using imported records. • If C•CURE 9000 does not contain records that exactly match those being imported from the source, the import adds the non-matching records to C•CURE 9000. Selecting this option requires completing the **Match Fields** Tab to specify matching fields. See • Data Import Match Fields Tab on Page 120. • Match Fields Tab Tasks on Page 123. NOTE: For LDAP and ODBC, this is the only mode supported. For information specific to LDAP imports, see LDAP Data Import Overview on Page 145. For information specific to ODBC imports, see ODBC Data Import Overview on Page 180.
Update only matched: do not add records	Select this import rule option to perform matching as follows: • Only records that exactly match records in the import source are updated. • Any records in the import source that do not exactly match those already in C•CURE 9000 are not imported. Selecting this option requires completing the **Match Fields** Tab to specify matching fields. See: • Data Import Match Fields Tab on Page 120. • Match Fields Tab Tasks on Page 123.
Options Box	

Data Import Editor General Tab Fields (continued)

Fields/Buttons	Description
Default Import Partition	Click ... to select the Partition in which to place newly imported records when the external records do not include a reference to any C•CURE 9000 partition. (This field is available only if the C•CURE 9000 system is partitioned.) NOTE: The Partition can **only** be updated for a record when it is referenced in the external file, not by its entry in this field. Software House recommends that you select a Partition for automated imports to avoid confusion. NOTE: • If the user who invokes a Manual Import does not have a privilege for the Partition referenced in this field, the Import will not start. (In this case, this field will display 'Not available'.) • If this field is left blank in a partitioned system and the files being imported do not refer to any Partition, the Import process will place the files as follows: - For a Manual Import – in the currently selected 'New Object Partition'. - For an Automated Import – in the 'Default' Partition'. • If the Partition referenced by an Import Definition is deleted from the system, you cannot run the import. The Import Definition cannot be used until you edit it and select another Partition.

General Tab Tasks

You use the **General** tab to accomplish the tasks listed below, which are required for configuring a Data Import object. The procedural steps for each task are detailed in the following subsections.

Selecting the Source Type and Automation Mode

An Import must have both a source type and mode of operation defined.

Example:

You configure an Import Definition to import a CSV file with newly added employees in an automated mode, Activated by event weekly.

You select the both the **Source type** and **Automation mode** for an Import on the **Data Import Editor General** tab.

To Choose the Source Type and Automation Mode

1. Create or modify a Import Definition. See Creating an Import Definition on Page 47 or Modifying a Data Import on Page 71.
2. In the **Source type** field, click ... to display a list of supported Import Source types: CSV file, LDAP, ODBC, or XML file (the default).
3. Click an item in the list to select a **Source type** for your Import. (The type you select modifies the fields/options/buttons displayed in the **Data Source Configuration** box.)

NOTE For information specific to configuring imports from an LDAP data source, see Import Editor General Tab for LDAP on Page 147 and for configuring imports from an ODBC data source, see Import Editor General Tab for ODBC on Page 186.

4. In the **Automation mode** field, click the down-arrow to display the list of modes in which the Import can operate (the mode you select can also modify the **Data Source Configuration** box):
   - Manual only mode
   - Activated by event (automated mode)
   - Listening on data (automated mode)

NOTE XML and CSV import sources support all three modes, while the LDAP import source supports only the Listening on data mode, and the ODBC import source supports both the Activated by event and Listening on data modes.

5. Click one of the entries to select an **Automation mode** for your Import.

Configuring the Data Source

The parameters requiring entry in the **Data Source Configuration** box change depending on whether you are configuring an Import for an XML, CSV, ODBC, or LDAP file source type and additionally whether you have selected manual mode or one of the two automated modes.

For detailed information on configuring the data source for an XML file or a CSV file, see:

- To Configure the Data Source for an XML File Import Source on Page 80.
- To Configure the Data Source for a CSV File Import Source on Page 83

For detailed information on configuring the data source for an LDAP record, see:

- Import Editor General Tab for LDAP on Page 147.
- LDAP Data Import General Tab Definitions on Page 147.

For detailed information on configuring the data source for an ODBC record, see:

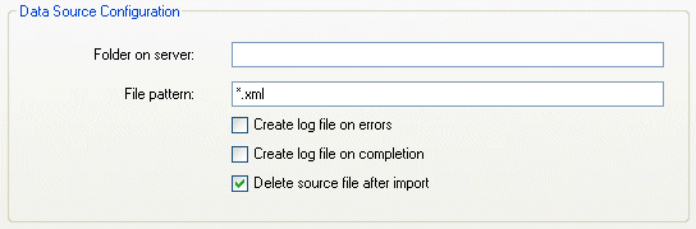
- Import Editor General Tab for ODBC on Page 186.
- General Tab Definitions for ODBC on Page 186.

Configuring an XML Import Source

To Configure the Data Source for an XML File Import Source

1. Create/modify an Import Definition. See Creating an Import Definition on Page 47/Modifying a Data Import on Page 71.
2. In the **Source type** field, leave the default entry, XML file import source, or if necessary, click ... and select it from the list.
3. In the **Automation mode** field,
   - Select one of the Automated modes: **Activated by event** or **Listening on data**. The **Data Source Configuration** box displays as shown in Figure 5 on Page 80.

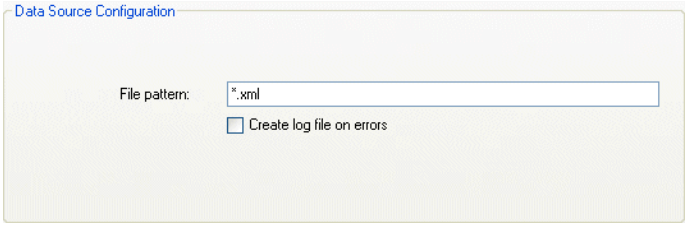
Figure 5: Data Source Configuration Box – XML Import in Automated mode



- or -

   - Select **Manual only**. The **Data Source Configuration** box displays as shown in Figure 6 on Page 80.

Figure 6: Data Source Configuration Box – XML Import in Manual Mode



4. In the **Folder on server** field (available for both Automated mode XML imports), specify a folder on the server using either an absolute path, a UNC path, or one relative to the default path in the 'DefaultImportDirectory' system variable. (See the C•CURE 9000 System Maintenance Guide System Variables chapter.) This is a **required** field.

   Example:

Absolute path: C:\SampleInputs\Import
UNC path: \\Server_Name\Import
Relative path: Import

The system validates the folder's existence when you save the Import Definition and displays error messages if you left the field empty or entered a non-existent directory.

If the folder is deleted after the Import Definition is saved, the Import Status displays 'Connectivity Error.'

NOTE The server must have proper read/write access to the specified folder or the automated Import will not be functional.

5. In the **File pattern** field:
   - (For both Automated mode XML imports) specify a pattern to be used by this Import Definition when retrieving files from the Import folder selected in the **Folder on server** field.

If the system contains several Import Definitions configured for an automated import, each Import should have a unique combination of folder and file pattern. The Imports can retrieve files from the same or different folders, but if the folders are the same, you **must** use patterns that do not match each other.

If the preceding is **not** done, the automated import may try to import the same file twice and the system may not be able to determine which Import Definition to use in this 'overlapped' case.

Software House also recommends that you **not** use the pattern, '*.*'.

   - (For a Manual mode XML import), specify a pattern to be used as the default pattern in the Open File dialog boxes for selecting the import file or sample input files.

NOTE You can override the pattern in the **Open File** dialog boxes and select a file that does **not** match the pattern.

6. Select the **Create log files on errors** option to indicate that once the import process has completed, the system will create a special error log file in the same folder where the original import source file is located.

   This error log file will contain all records rejected during the import operation, stored in the internal XML format. (This stored format could be different from the format of the incoming records if the import process had applied data conversion to the received data).

   Whether you select this option or not, the same rejected records will be stored on the server, attached to the proper Import Result.

7. Select the **Create log file on completion** option (available only for one of the Automated mode XML imports) to indicate that once the import process has completed, the system will create a special log file in the same folder where the original import source file is located. This file will have the same name as the original file with the suffix '.results' appended and contain import result summary information (similar to the information stored in the Import Result, described in Viewing Import Results History on Page 71).

8. Select the **Delete source file after import** option (available for both Automated mode XML imports) to indicate that the incoming file should be deleted once the import process has completed, or clear the option to have the file renamed by appending the suffix '.completed' to the name of the imported file.

   Whether you select this option or not—if the input file is not a well formatted XML document, the file is not deleted but renamed by appending the suffix '.rejected' to the current file name.

   It is necessary to either rename or delete the file to avoid an infinite loop where the same file is imported over and over again.

Configuring a CSV Import Source

The CSV file source behaves similarly to the XML file source with one exception: it assumes the input file has data in the CSV format. The system reads the CSV file record by record, converting it into a well- formatted XML document.

- The first line in the CSV file is interpreted as a list of column names.
- All other lines are interpreted as rows in the table with the specified column names.
- The CSV file source reads every data row and puts the value from every column in the row into a tag with a proper column name within the XML document being created.

Example – conversion from CSV format into XML format:

The value 'ExternalObject' used as the Tag name comes from the value entered for the Default Tag on the **Advanced Properties** sheet, as shown in Figure 9 on Page 84.

Source file:

```
"First Name", "Last Name", "Birthday"
Joe, Shturm, 01/02/2007
Sam, Gulliver, 12/05/1865
```

Converted file:

```
<CrossFire culture-info="en-US">
     <ExternalObject ImportMode="Default">
          <First_Name>Joe</First_Name>
          <Last_Name>Shturm</Last_Name>
          <Birthday>01/02/2007</Birthday>
     </ExternalObject> <ExternalObject ImportMode="Default">
          <First_Name>Sam</First_Name>
          <Last_Name>Gulliver</Last_Name>
          <Birthday>12/05/1865</Birthday>
     </ExternalObject>
</CrossFire>
```

If CSV has a column called 'ClassType', its content is used for each record converted, instead of **Default Tag**.

Example – conversion from CSV format into XML format with 'ClassType':

- In this example, the CSV input contains a header and two lines with information about door objects of different types. The first line represents an iSTAR door and the second line represents an apC door. ('**line 0>**', '**line 1>**', and '**line 2>**' are not part of the actual CSV file, but were inserted to make the example more readable.)
- After conversion into an XML document, the tags are automatically assigned differently for each line. Without having to use any additional field mapping, the first line is correctly interpreted as an iSTAR door while the second is correctly interpreted as an apC door.

Source file:

```
line 0> ClassType,PartitionKey,Name,ControllerClassType,ControllerObjectKey
line 1>SoftwareHouse.NextGen.Common.SecurityObjects.iStarDoor,Default,Kitchen,
SoftwareHouse.NextGen.Common.SecurityObjects.iStarController,Main Controller [Default]
line 2> SoftwareHouse.NextGen.Common.SecurityObjects.ApcDoor,Default,Front
Door,SoftwareHouse.NextGen.Common.SecurityObjects.ApcController,apC 0 [[Default]]
```

Converted file:

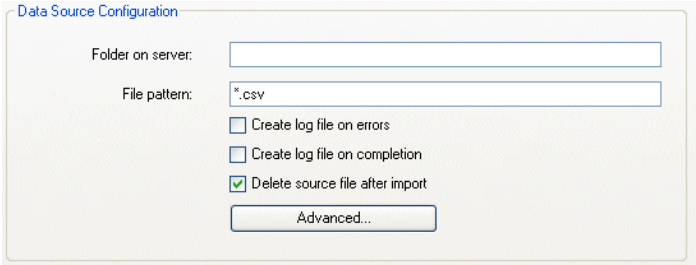
```
<CrossFire culture-info=" en-US">
<SoftwareHouse.NextGen.Common.SecurityObjects.iStarDoor
ImportMode="Default"><ClassType>SoftwareHouse.NextGen.Common.SecurityObjects.iStarDoor</ClassType>
<PartitionKey>Default</PartitionKey><Name>Kitchen</Name>
<ControllerClassType>SoftwareHouse.NextGen.Common.SecurityObjects.iStarController
</ControllerClassType>
```

```
<ControllerObjectKey>Main Controller [[Default]]</ControllerObjectKey>
</SoftwareHouse.NextGen.Common.SecurityObjects.iStarDoor>
<SoftwareHouse.NextGen.Common.SecurityObjects.ApcDoor ImportMode="Default">
<ClassType>SoftwareHouse.NextGen.Common.SecurityObjects.ApcDoor</ClassType>
<PartitionKey>Default</PartitionKey>
<Name>Front Door</Name>
<ControllerClassType>SoftwareHouse.NextGen.Common.SecurityObjects.ApcController
</ControllerClassType>
<ControllerObjectKey>apC 0 [[Default]]</ControllerObjectKey>
</SoftwareHouse.NextGen.Common.SecurityObjects.ApcDoor>
</CrossFire>
```

To Configure the Data Source for a CSV File Import Source

1. Create or modify a Import Definition. See Creating an Import Definition on Page 47 or Modifying a Data Import on Page 71.
2. In the **Source type** field, click ... and select CSV file import source from the list.
3. In the **Automation mode** field,
   - Select one of the Automated modes: Activated by event or Listening on data. The Data Source Configuration box displays as shown in Figure 7 on Page 83.

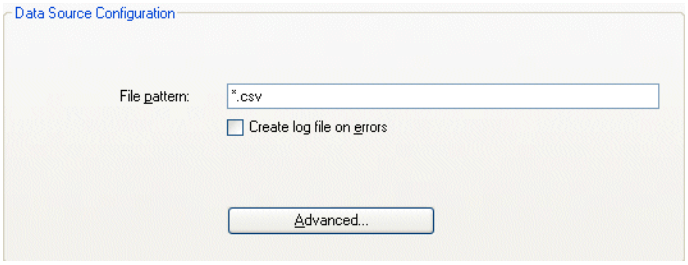
Figure 7: Data Source Configuration Box – CSV Import in Automated Mode



- or -

   - Select **Manual only**. The Data Source Configuration box displays as shown in Figure 8 on Page 83.

Figure 8: Data Source Configuration Box – CSV Import in Manual Mode

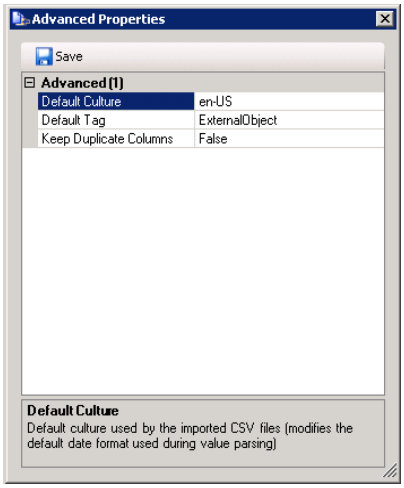


4. Depending on whether the CSV Import is Automated or Manual, enter information in the fields and select options following directions in Step 5 on Page 81.

NOTE If you select the **Create log files on errors** option, the format in which the rejected records are stored will definitely differ from the format of the incoming records since the import process converted the data from CSV to internal XML format.

5. Click the **Advanced** button. The **Advanced Properties** sheet opens, as shown in Figure 9 on Page 84.

Figure 9: Import Advanced Properties Sheet



- For the **Default Culture** property, change the entry or leave the default to control how the CSV date and numeric values are parsed.

  Examples:

  12/31/2011 for en-US or 31/12/2011 for en-UK

  100,000.00 for en-US or 100 000,00 for fr-FR

- For the **Default Tag** property, replace 'ExternalObject' with the name of the top-level object being imported—if you know it; or click ... to select a type from the drop-down list.

  Example:

  Personnel

- For the **Keep Duplicate Columns** property, set as **False**—the default—(recommended) to have the import concatenate (combine) the values from the duplicate columns into one pipe-delimited value; or change the property to **True** to have the import put the values into separate entries.

- Click **Save** to return to the **Data Import Editor** or to cancel the changes.

Selecting the Default Import Mode

An Import must have a defined Import mode rule to follow: whether the process only add records to the C•CURE 9000 database without doing any matching, or updates the database after doing matching in either of two different ways.

Example:

You configure the Import Definition that imports a CSV file with newly added employees by activating by event weekly on schedule with a default import mode of "Add only; do not match records".

You select the **Default Import mode** on the **Data Import Editor General** tab.

NOTE The default Import Mode you choose can be overruled by the imported document on a record-by-record basis. See Attribute 'ImportMode' on Page 548.

To Choose the Default Import Mode

1. Create or modify a Import Definition. See Creating an Import Definition on Page 47 or Modifying a Data Import on Page 71.
2. In the **Source type** field, click ... and select a **Source type**.

3. In the **Automation mode** field, select a mode.
4. In the **Data Source Configuration** box that displays, select options and enter data as necessary.
5. In the **Default Import Mode** box, select one of the following options:
   - Add only; do not match records
   - Update when matched; Otherwise add
   - Update only matched; do not add records

   When you select an Update mode, the **Match Fields** tab is selected on the **Data Import Editor**. A message displays saying that you must select matching fields to complete the import configuration and asking if you want to do it now.
6. If you do want to select match fields right now, click **Yes** or if you do **not**, click **No**.

   You can now click the **Match Fields** tab to open it and select match fields for this Import Definition. For information, see Data Import Match Fields Tab on Page 120.

   - or -

   Click **Yes** to select match fields immediately.

   The **Select File with Sample** dialog box (see Selecting and Viewing a Sample Input on Page 85) opens for selecting (if you have not yet selected a sample input file).

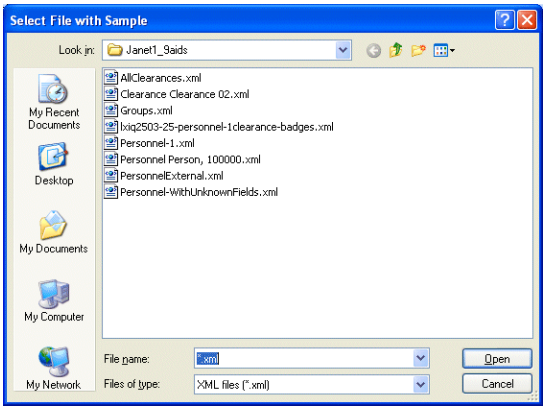
Selecting and Viewing a Sample Input

You can use the **Select Sample Input** and **View Sample Input** buttons on the **Data Import Editor** to help you define the structure of the incoming XML or CSV file. The file can be used in data conversions and field matching.

To Select and View a Sample Input

1. Create or modify an Import Definition, as documented in the preceding sections of the chapter.
2. Click the **Select Sample Input** button. The **Select File with Sample** dialog box opens, as shown in Figure 10 on Page 85.

Figure 10: Select File with Sample Dialog Box



3. Select one of the files in the list, or browse to find the file you want to use, and click **Open**.

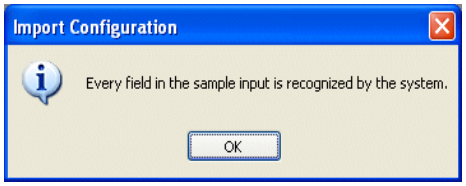
   The system reads the sample file you chose, analyzes the data, and displays one of the following four possible messages:

NOTE These messages also display from the **Match Fields** tab if you selected a file and clicked **Open** on the **Select File with Sample** dialog box after choosing one of the 'Update' options in the Data Input Mode box in Step 5 on Page 85.

All Fields were Recognized

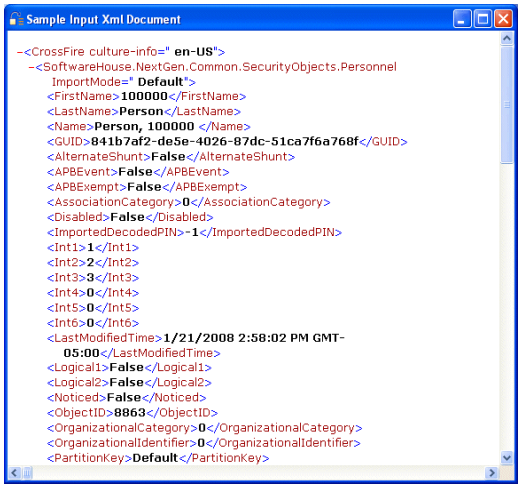
This message indicates that all the fields were recognized—true if you are moving data from another C•CURE 9000. No data conversion is needed.

Figure 11: All Fields Were Recognized Message



- Click **OK** to close the message. The **General** Tab (or the **Match Fields** tab) still displays for you to complete the configuration of the Import Definition. You can also click the **View Sample Input** to see the sample, as shown in the example in Figure 12 on Page 86.

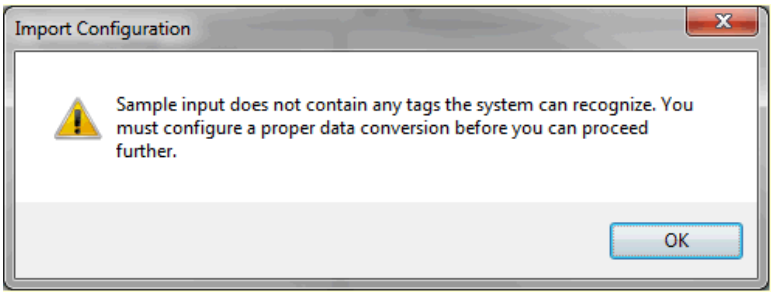
Figure 12: Sample Input File – All Recognized Tags



No Fields Were Recognized

This message indicates that none of the fields were recognized and data conversion is necessary.

Figure 13: No Fields Were Recognized Message



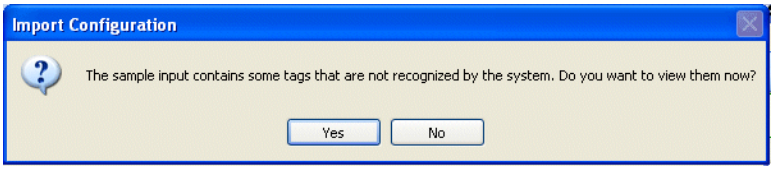
- Click **OK** to close the message.

  The **Data Conversion** Tab opens for you to set up the conversion. (See on Page 89 and Data Conversion Tab Tasks on Page 91.) You can also click the **View Sample Input** to see the sample.

Some Fields Recognized

This message indicates that some of the fields were recognized. In this case, you can decide whether or not to open the **Data Conversion** tab to set up conversion.

Figure 14: Some Fields Recognized Message

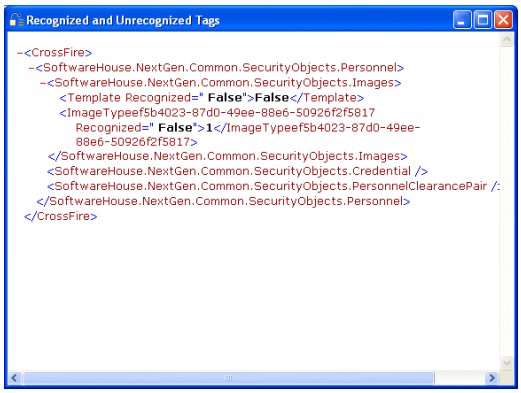


- Click **No** to close the message and display the **General** Tab (or the **Match Fields** tab).

  - or -

- Click **Yes** to view the tags as shown in the example in Figure 15 on Page 87.

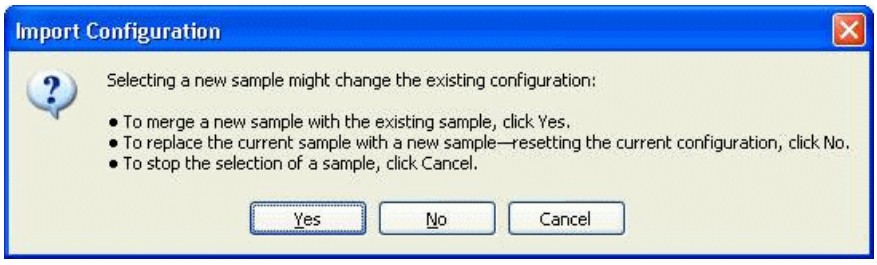
Figure 15: Sample Input File – Recognized and Unrecognized Tags



Selecting a New Sample

This message displays if you have already selected a sample input for the Import Definition and click the **Select Sample Input** button again.

Figure 16: Selecting a New Sample Message



As indicated by the message, there are **three** possible actions you can take:

- If you want this new sample input to be added to and merged with the existing sample, click **Yes**.

  Example:

  Your first sample input included only Personnel files and this new sample has clearance files which you want to import at the same time.

- If you no longer want to use the original sample input, but a totally new sample instead, click **No**.

This also clears all the existing data converters and the match field selections.

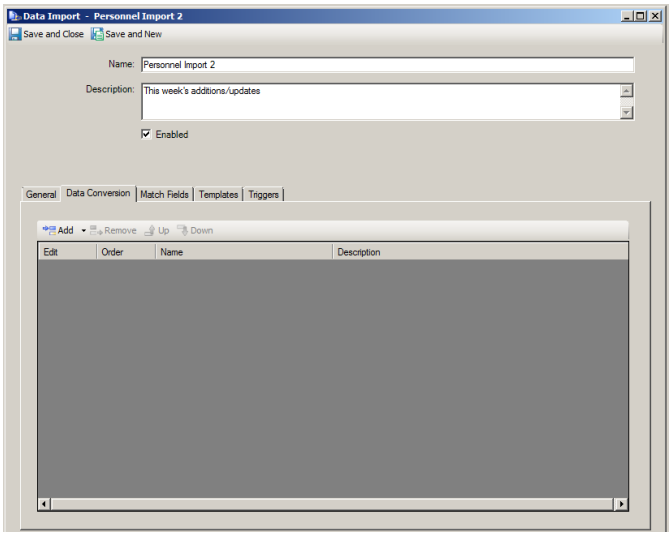
- If you are happy with your original sample and do not want to add another file to it or to replace it, click **Cancel**.

Data Import Data Conversion Tab

The **Data Conversion** tab, as shown in on Page 89, allows you to set up the data conversion process needed when the external data to be imported—such as the CSV file, LDAP record, ODBC record, or the external XML file—does not conform to the C•CURE 9000 schema. Once configured, the tab contains a list of import converters and tools for converting the data. There can be more than one import converter of the same type in the list.

1. The Import process takes the XML document delivered by the current import source and applies data conversion using the first import converter on the list.
2. The output of the first conversion is taken as the input XML document for the second converter from the list, etc.
3. The output of the last converter from the list is taken as the input to the main import algorithm, so the last converter should provide the XML document that matches the internal C•CURE 9000 format.

Figure 17: Data Import Data Conversion Tab



Data Conversion Tab Buttons

Table 11 on Page 89 describes the buttons on the Data Conversion tab.

Table 11: Data Import Data Conversion Tab Buttons

Button	Description
Add	Use this button to create a new Import converter and open its dialog box for configuration; it is then added to a row of the Data Conversion table. Each row in the table acts as a data converter tool. Each new row is added after the last. • If you click the down arrow, a drop-down list displays the current supported converters for you to choose from: - Personnel Mapping Tool Editor on Page 92 - Operator Mapping Tool Editor on Page 98 - Field Mapping Tool Editor on Page 104 - Custom Stylesheet Editor on Page 114 • If you just click the button, the system opens the default converter, the Field Mapping tool.
Remove	Click this button to remove a selected row from the Data Conversion table.

Table 11: Data Import Data Conversion Tab Buttons (continued)

Button	Description
Up	Click this button to move a converter row up in the table. The position of converter rows can affect conversion results. This button is unavailable if the top row is selected.
Down	Click this button to move a converter row down in the table. The position of converter rows can affect conversion results. This button is unavailable if the bottom row is selected.
Select Sample Input	Click this button to open the **Select File with Sample** dialog box. After you select the sample file, the system analyzes the data and displays one of the four possible messages: • All Fields Were Recognized • No fields Were Recognized • Some Fields Recognized • Selecting a New Sample

Data Conversion Tab Definitions

The Data Conversion tab has the fields described in Table 12 on Page 90.

Table 12: Data Import Data Conversion Tab Table Definitions

Field	Description
Edit	Click ... in this field in the row of the Data Converter you want to edit. The Personnel Mapping Tool, Field Mapping Tool, or Custom Stylesheet tool opens for the object you selected.
Order	Indicates the order of the converter in this row in the list of converters.
Name	Name of the type of data converter: Personnel Mapping Tool, Field Mapping Tool, or Custom Stylesheet.
Description	Description of the data converter type.

Data Conversion Tab Tasks

You use the **Data Conversion** tab to set up the data conversion of external files incompatible with the C•CURE 9000 schema:

- Creating and Opening a New Converter on Page 91
- Using the Personnel Mapping Tool to Convert Personnel Data on Page 95
- Operator Mapping Tool Editor on Page 98
- Field Mapping Tool Editor on Page 104
- Custom Stylesheet Editor on Page 114

Creating and Opening a New Converter

The Data Conversion tab is empty the first time it opens for an Import definition. Once you have selected and configured one or more converters, the tab displays them in the list.

NOTE Software House recommends that you use the Personnel Mapping Tool to convert the data when you are importing Personnel, and not the Field Mapping Tool.

To Create and Open a New Converter

1. Create or modify a Import Definition. See Creating an Import Definition on Page 47 or Modifying a Data Import on Page 71.
2. On the **Data Import Editor**, click the **Data Conversion** tab to open.
3. Click the **Add** button down-arrow to display a drop-down list with the supported converters, and click Personnel Mapping tool, Field Mapping tool, or Custom stylesheet.

   - or -

   Click the **Add** button to automatically select the Field Mapping tool.

   Depending on your choice, the system opens the **Personnel Mapping Tool Editor** (see Figure 18 on Page 92), **Operator Mapping Tool** (see **Field Mapping Tool Editor**, (see Figure 24 on Page 105) or the **Custom Stylesheet Editor** (see Figure 30 on Page 114).

NOTE If you have not selected sample input, clicking **Add** or selecting a converter opens the Selection dialog box. If you click **Cancel** here, a new converter is not appended.

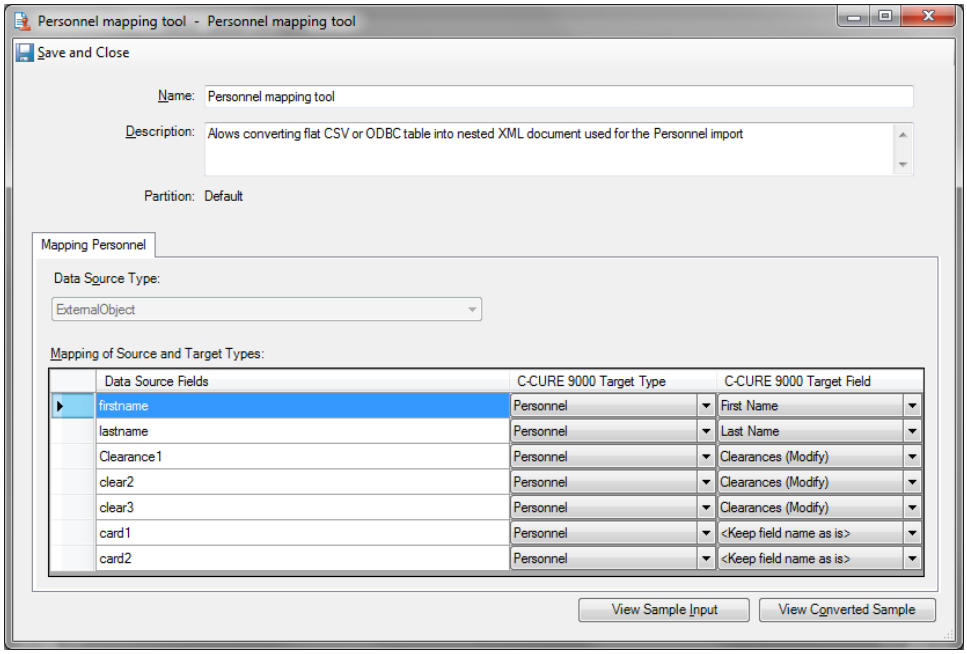
Personnel Mapping Tool Editor

The C•CURE 9000 Personnel Mapping Tool Editor allows you to map Personnel records from CSV flat files, LDAP records, ODBC tables, or XML files that do not conform to the Personnel records of the C•CURE 9000 schema.

Fields mapped from the source file to C•CURE 9000 represent actual Personnel fields to be imported into C•CURE 9000. The converter filters out unmapped fields.

The Personnel Mapping tool tries to automatically map the tags in the sample import personnel records to known fields in the C•CURE 9000 Personnel record and its child records, such as Credential, and then opens populated with the mapping, as shown in Figure 18 on Page 92.

Figure 18: Personnel Field Mapping Tool Editor



The **Personnel Mapping Tool Editor** has the buttons described in Table 13 on Page 92.

Table 13: Personnel Mapping Tool Editor Buttons

Button	Description
Save and Close	Click this button when you have completed any changes to the Personnel Mapping and wish to save those changes. The system validates the mapping and warns you if some of the sample values cannot be converted into the destination field values. The Personnel Mapping Tool Editor closes and returns you to the Data Conversion tab of the Data Import Editor. (If this was the first time the Personnel Mapping Tool was opened for this Import definition, the mapping tool is shown in the list on the Data Conversion tab on a new row.) NOTE: Saved data is not committed to the database until the Import Definition is saved.
	Click this button when you want to close the Personnel Mapping Tool 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. In either case, the Data Conversion tab of the Data Import Editor reappears.

Table 13: Personnel Mapping Tool Editor Buttons (continued)

Button	Description
View Sample Input	Click this button to open a dialog box with the contents of the original CSV, XML, LDAP, or ODBC item in XML document form. This is the item that was: • Selected as the sample input. • Converted by any other converters that precede this one in the list of converters on the **Data Conversion** tab (shown in on Page 114).
View Converted Sample	Click this button to open a dialog box with the contents of the XML document as converted from the sample input document by applying mapping with this Personnel converter.

The **Personnel Mapping Tool Editor** has the fields described in Table 14 on Page 93.

Table 14: Personnel Mapping Tool Editor Fields

Fields/Buttons	Description
Name	"Personnel mapping tool" is automatically entered in this field by the system. You can change the name if it is necessary for identification purposes.
Description	A textual description of the personnel mapping. This field is not required.
Partition	A read-only field displaying the Partition to which this Import Definition belongs. (This field is visible only if the C•CURE 9000 system is partitioned.)
Mapping Personnel Tab	
Data Source type	This field represents a top-level tag in the import document selected from the **Data Import Editor General** tab. • If there is only one such tag, this field is read-only with **ExternalObject** entered for a CSV file, the name of the class entered for LDAP, and the table name entered for ODBC. • If your sample import file has two top-level tags, such as Personnel and Operators, you can click the down-arrow to select a tag from the drop-down list. NOTE: XML files can have two top-level tags, while CSV, LDAP, and ODBC usually have only one top-level tag.
Mapping of Source and Target Types Box	
Data Source Fields	Once a tag is selected (or read-only) in the **Data Source type** field, this left-hand column displays the field names from the source document for the selected tag, including child objects with their fields. **Example:** Nested child object: Personnel/PersonnelClearancePair/ClearanceID
C•CURE 9000 Target Type	This field in the middle column represents an importable Personnel object type within the C•CURE 9000 application (Personnel, Credential, Clearance, Image, Personnel Clearance Pair, Shared Document, or Private Document). Click the down-arrow to select the object type from the drop-down list. NOTE: If the automated mapping has found a match but the field cannot be imported, this field will read **<Exclude>**. You can also select **<Exclude>** as the target type to manually exclude the object field from being imported. **Example: Fields that cannot be imported** Field LastModifiedTime in Personnel type Field PersonnelID in PersonnlClearancePair type Field PartitionKey in the Credential type

Personnel Mapping Tool Editor Fields (continued)

Fields/Buttons	Description
C•CURE 9000 Target Field	Once a **Personnel object type is** selected in the **C•CURE 9000 Data Target Type** field, this right-hand column displays both of the following: • C•CURE 9000 Data Fields (from the C•CURE 9000 target type) that automatically map to the **Data Source Fields**. **Example:** First_Name to FirstName and Last_Name to LastName • <**Keep field name as is**> for each Data Field name you want to keep as is without any changes. The data then goes into the converted document with its original name, which allows it to be passed through the Personnel Mapping tool to another converter, if necessary. Each field in this column—whether it contains a mapped field, such as Last Name, or **<Keep field name as is>**—includes a down-arrow that opens a drop-down list of all the fields from the selected **C•CURE 9000 Data** type. NOTE: It also includes an item, **Attribute: Import Mode**, that allows you to specify the import mode for the personnel record or its child record (whichever type is selected in the **C•CURE 9000 Target Type** field). Using this mapping assumes that the Import Definition was configured for Update mode and that the matching fields were selected. For information, see Attribute 'ImportMode' on Page 548.

Personnel Mapping Tool Editor Tab Context Menus

The context menu that opens when you right-click the **Personnel Mapping** tab in the Personnel Mapping Tool Editor includes the selections described in Table 15 on Page 94.

Table 15: Personnel Mapping Tab Right-Click Context Menu Options

Menu Selection	Description
Perform Mapping	Click this menu selection to have the system re-apply the original automatic mapping if you have altered it.
Clear Mapping	Click this menu selection to totally delete the current mapping without closing the tab. Once the mapping is cleared, 'Personnel' is entered in the **C•CURE 9000 Target Type** column for every Data Source Field item and **<Keep field name as is>** in the **C•CURE 9000 Target Field** column.

The context menu that opens when you right-click one or more rows in the Mapping of Source and Target Types table includes the selections described in Table 16 on Page 94.

Table 16: Mapping of Source and Target Types Right-Click Context Menu Options

Menu Selection	Description
Duplicate Current Row	Click this menu selection to create a copy of the current row, which allows you to map data from one source file field to two different fields in the C•CURE 9000 personnel Object. (This menu option is unavailable if you select more than one row.) **Example:** You can put the same value into the **Personnel** type **Int1** field and into the child **Credential** type **Card Number** field.
Remove Current Row	Click this menu selection to delete a single row created as a duplicate of another row if you no longer want it. (This menu option is available only for deleting a row created by being duplicated.)
Exclude Current Rows	Click this menu selection to put **<Exclude>** into the **C•CURE 9000 Target Type** field for one or more selected rows. This stops the Data Source Field on the row(s) from being imported.

Mapping of Source and Target Types Right-Click Context Menu Options (continued)

Menu Selection	Description
Keep Current Rows	Click this menu selection to put **Personnel** in the **C•CURE 9000 Target Type** field and **<Keep field name as is>**in the **C•CURE 9000 Target Field** for one or more selected rows. This retains the original Data Source Field's name and allows the data to be passed through to another converter if necessary.
Map Selected Rows	Click this menu selection to have the system re-apply the original automatic mapping to one or more selected rows.

Using the Personnel Mapping Tool to Convert Personnel Data

The Personnel mapping tool always tries to automatically map the tags in the sample input file to known fields in C•CURE 9000 and opens with the mapped fields displayed.

NOTE Automatic mapping makes a 'best guess' about the possible links between incoming data and existing C•CURE 9000 types and properties. However, this guess could be incorrect. Consequently, you should verify that the automatic mapping is correct before saving it.

NOTE If you are importing Personnel records with multiple Clearances, in the Personnel mapping tool, set each Clearance import field to:

C•CURE 9000 Target Type: **Personnel**

C•CURE 9000 Target Field: **Clearances(Modify)**

or

C•CURE 9000 Target Type: **Personnel**

C•CURE 9000 Target Field: **Clearances (Replace all)**

rather than:

C•CURE 9000 Target Type: **Personnel Clearance Pair**

C•CURE 9000 Target Field **Clearance Name**.

See Figure 18 on Page 92 for an example showing this mapping.

To Use the Personnel Mapping Tool to Convert Personnel Data

1. In the **Personnel Mapping Tool Editor**, as shown in the example in Figure 18 on Page 92 do the following:
   - In the **Name** field, leave the name as is, or change it if necessary for identification purposes.
   - In the **Description** field, change the description if you wish to better describe this mapping. You can enter up to 500 characters.
2. To ascertain the contents of the Data Source file, click the **View Sample Input** button. The sample opens for your review, as shown in the following example.

3. On the **Mapping Personnel** tab, the **C•CURE 9000 Target type** fields are all set to **Personnel**. Click the down-arrow in each field to open the drop-down list of importable Personnel object types within C•CURE 9000 and select the appropriate target type—

Example:

- **Credential** for the Card_num, Activation_DT, and Expiration_DT **Data Source Fields** from the Sample Input file.
- **<Exclude>** to keep the object field from being imported.

4. Once you have set all the **C•CURE 9000 Target type** fields, you can map the **C•CURE 9000 Target fields** as necessary by clicking the down-arrow and scrolling down to select the relevant C•CURE 9000 field.

Example:

Card_num to **Card number** (with **Credential** as the **C•CURE 9000 Target type)**.

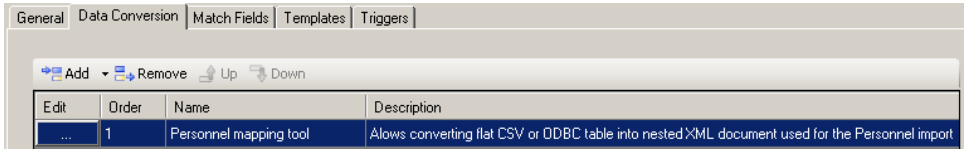
Some of these fields may already be correctly mapped, such as **First_Name** and **Last_Name** to **First Name** and **Last Name** (with **Personnel** as the **C•CURE 9000 Target type)**.

To keep the **Data Source Field** name the same, select **<Keep field name as is>**. The original field name with its value will appear in the converted sample.

5. To see how the Data Source file has been converted by the mapping tool, click the **View Converted Sample** button. The converted file opens for your review, as shown in the following example.

6. To save this mapping, click **Save and Close**. The Data Conversion tab reappears with the Personnel mapping tool added as the first row in the Data Conversion table, as shown in Figure 19 on Page 97.

Figure 19: Data Import Editor - Data Conversion Tab with Personnel Mapping Tool Row



7. To check that the Data Source file has been properly converted, click the **Verify Sample** button. A message displays saying either that the system recognizes every field in the sample input or only recognizes some of the fields.

Operator Mapping Tool Editor

The C•CURE 9000 Operator Mapping Tool Editor allows you to map Operator privilege groups to a field in the records from CSV flat files, LDAP records, ODBC tables, or XML files that do not conform the C•CURE 9000 operator records schema using either of two virtual fields in the Operator record: **Replace All** or **Modify**.

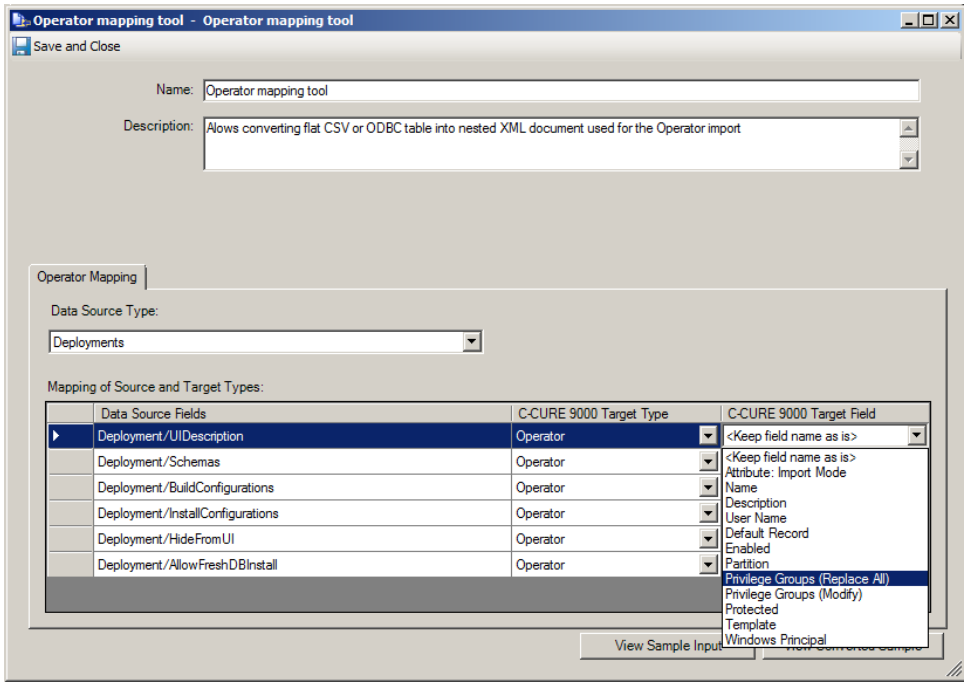
For example, if the XML file has a field called "NewField", you can map this field to "Privilege Groups (Replace All)" or "Privilege Groups (Modify)" in the Mapping tool.

- **Replace All** removes all Privilege groups assigned to the Operator and adds the Privilege groups specified in "NewField".
- **Modify** adds or removes specified Privilege Groups, using Plus ('+) or Minus (-) respectively for add and remove operations.

You can also 'Enable' or 'Disable' Operators through LDAP. See Special Fields on Page 552 for information on importing Operator properties.

The Operator Mapping tool automatically maps the tags in the sample import records to known fields in the C•CURE 9000 Operator record and its child records, such as Deployments, and then opens populated with the mapping, as shown in Figure 21 on Page 99

Figure 20: Operator Field Mapping Tool Editor with Deployments



Other Data Source Types include **Schemas and Snippets** as shown in Figure 21 on Page 99 and Figure 22 on Page 99 respectively.

Figure 21: Operator Field Mapping Tool Editor with Schemas

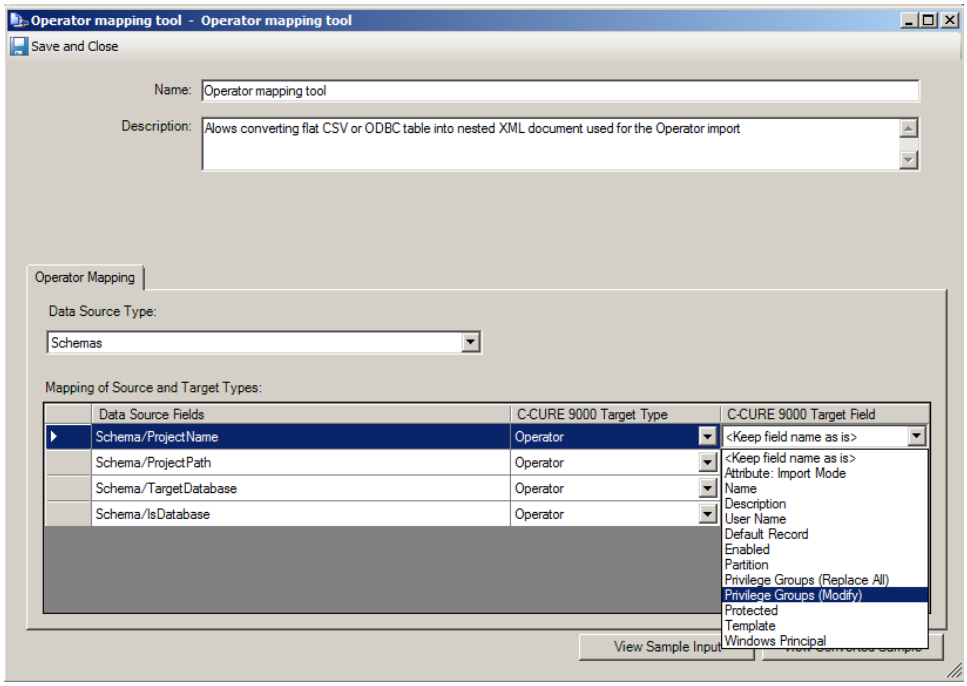
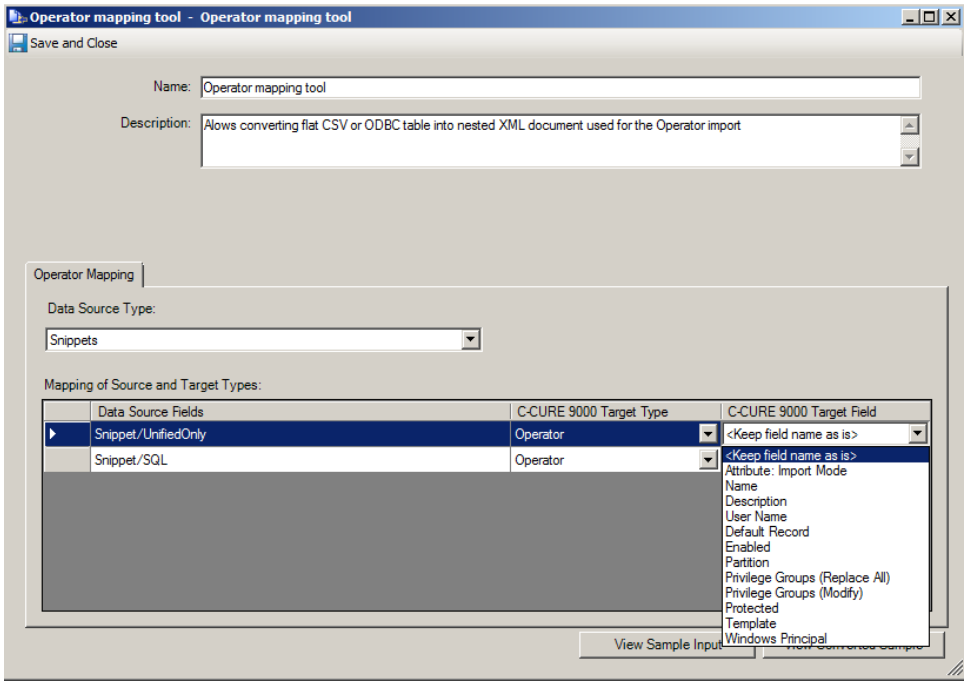


Figure 22: Operator Field Mapping Tool Editor with Snippets



The **Operator Mapping Tool Editor** has the buttons described in Figure 22 on Page 99.

Table 17: Operator Mapping Tool Editor Buttons

Button	Description
Save and Close	Click this button when you have completed any changes to the Operator Mapping and wish to save those changes. The system validates the mapping and warns you if some of the sample values cannot be converted into the destination field values. The Operator Mapping Tool Editor closes and returns you to the Data Conversion tab of the Data Import Editor. (If this was the first time the Operator Mapping Tool was opened for this Import definition, the mapping tool is shown in the list on the Data Conversion tab on a new row.) NOTE: Saved data is not committed to the database until the Import Definition is saved.
	Click this button when you want to close the Operator Mapping Tool 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. In either case, the Data Conversion tab of the Data Import Editor reappears.
View Sample Input	Click this button to open a dialog box with the contents of the original CSV, XML, LDAP, or ODBC item in XML document form. This is the item that was: • Selected as the sample input. • Converted by any other converters that precede this one in the list of converters on the **Data Conversion** tab (shown in on Page 89).
View Converted Sample	Click this button to open a dialog box with the contents of the XML document as converted from the sample input document by applying mapping with this Operator converter.

The **Operator Mapping Tool Editor** has the fields described in Table 18 on Page 100.

Table 18: Operator Mapping Tool Editor Fields

Fields/Buttons	Description
Name	"Operator mapping tool" is automatically entered in this field by the system. You can change the name if it is necessary for identification purposes.
Description	A textual description of the operator mapping. This field is not required.
Partition	A read-only field displaying the Partition to which this Import Definition belongs. (This field is visible only if the C•CURE 9000 system is partitioned.)
Operator Mapping Tab	
Data Source type	This field represents a top-level tag in the import document selected from the **Data Import Editor General** tab. • Deployments • Schemas • Snippets
Mapping of Source and Target Types Box	

Operator Mapping Tool Editor Fields (continued)

Fields/Buttons	Description
Data Source Fields	Once a tag is selected (or read-only) in the **Data Source type** field, this left-hand column displays the field names from the source document for the selected tag, including child objects with their fields. • Deployment/UIDescription • Deployment/Schemas • Deployment/BuildConfigurations • Deployment/InstallConfigurations • Deployment/HideFromUI • Deployment/AllowFreshDBInstall
C•CURE 9000 Target Type	This field in the middle column represents an importable operator object type within the C•CURE 9000 application. Click the down-arrow to select the object type from the drop-down list.: • Operator - Operator Application Layout Pair • Operator - Operator Privilege Pair NOTE: If the automated mapping has found a match but the field cannot be imported, this field will read **<Exclude>**. You can also select **<Exclude>** as the target type to manually exclude the object field from being imported.
C•CURE 9000 Target Field	Once an **Operator object type is** selected in the **C•CURE 9000 Data Target Type** field, this right-hand column displays both of the following: • C•CURE 9000 Data Fields (from the C•CURE 9000 target type) that automatically map to the **Data Source Fields**. • < **Keep field name as is**> for each Data Field name you want to keep as is without any changes. The data then goes into the converted document with its original name, which allows it to be passed through the Operator Mapping tool to another converter, if necessary. Each field in this column—whether it contains a mapped field, such as Last Name, or **<Keep field name as is>**—includes a down-arrow that opens a drop-down list of all the fields from the selected **C•CURE 9000 Data** type. NOTE: It also includes an item, **Attribute: Import Mode**, that allows you to specify the import mode for the personnel record or its child record (whichever type is selected in the **C•CURE 9000 Target Type** field). Using this mapping assumes that the Import Definition was configured for Update mode and that the matching fields were selected. For information, see Attribute 'ImportMode' on Page 548.

Operator Mapping Tool Editor Tab Context Menus

The context menu that opens when you right-click the **Operator Mapping** tab in the Operator Mapping Tool Editor includes the selections described in Table 19 on Page 101.

Table 19: Operator Mapping Tab Right-Click Context Menu Options

Menu Selection	Description
Perform Mapping	Click this menu selection to have the system re-apply the original automatic mapping if you have altered it.
Clear Mapping	Click this menu selection to totally delete the current mapping without closing the tab. Once the mapping is cleared, 'Operator' is entered in the **C•CURE 9000 Target Type** column for every Data Source Field item and **<Keep field name as is>** in the **C•CURE 9000 Target Field** column.

The context menu that opens when you right-click one or more rows in the Mapping of Source and Target Types table includes the selections described in Table 20 on Page 102.

Table 20: Mapping of Source and Target Types Right-Click Context Menu Options

Menu Selection	Description
Duplicate Current Row	Click this menu selection to create a copy of the current row, which allows you to map data from one source file field to two different fields in the C•CURE 9000 personnel Object. (This menu option is unavailable if you select more than one row.) **Example:** You can put the same value into the **Personnel** type **Int1** field and into the child **Credential** type **Card Number** field.
Remove Current Row	Click this menu selection to delete a single row created as a duplicate of another row if you no longer want it. (This menu option is available only for deleting a row created by being duplicated.)
Exclude Current Rows	Click this menu selection to put **<Exclude>** into the **C•CURE 9000 Target Type** field for one or more selected rows. This stops the Data Source Field on the row(s) from being imported.
Keep Current Rows	Click this menu selection to put **Operator** in the **C•CURE 9000 Target Type** field and **<Keep field name as is>**in the **C•CURE 9000 Target Field** for one or more selected rows. This retains the original Data Source Field's name and allows the data to be passed through to another converter if necessary.
Map Selected Rows	Click this menu selection to have the system re-apply the original automatic mapping to one or more selected rows.

Using the Operator Mapping Tool to Convert Operator Data

The Operator mapping tool always tries to automatically map the tags in the sample input file to known fields in C•CURE 9000 and opens with the mapped fields displayed.

NOTE Automatic mapping makes a 'best guess' about the possible links between incoming data and existing C•CURE 9000 types and properties. However, this guess could be incorrect. You should verify that the automatic mapping is correct before saving it.

To Use the Operator Mapping Tool to Convert Operator Data

1. In the **Operator Mapping Tool Editor**, as shown in the example in Figure 20 on Page 98 do the following:
   - In the **Name** field, leave the name as is, or change it if necessary for identification purposes.
   - In the **Description** field, change the description if you wish to better describe this mapping. You can enter up to 500 characters.
2. To see the contents of the Data Source file, click the **View Sample Input** button. The sample opens for your review, as shown in the following example.

3. On the **Operator Mapping** tab, the **C•CURE 9000 Target type** fields are all set to **Operator**. Click the down-arrow in each field to open the drop-down list of importable Operator object types within C•CURE 9000 and select the appropriate target type.
4. Once you have set all the **C•CURE 9000 Target type** fields, you can map the **C•CURE 9000 Target fields** as necessary by clicking the down-arrow and scrolling down to select the relevant C•CURE 9000 field.

Example:

App_Layout to **Application Layout Name** (with **Operator Application Layout** as the **C•CURE 9000 Target type)**.

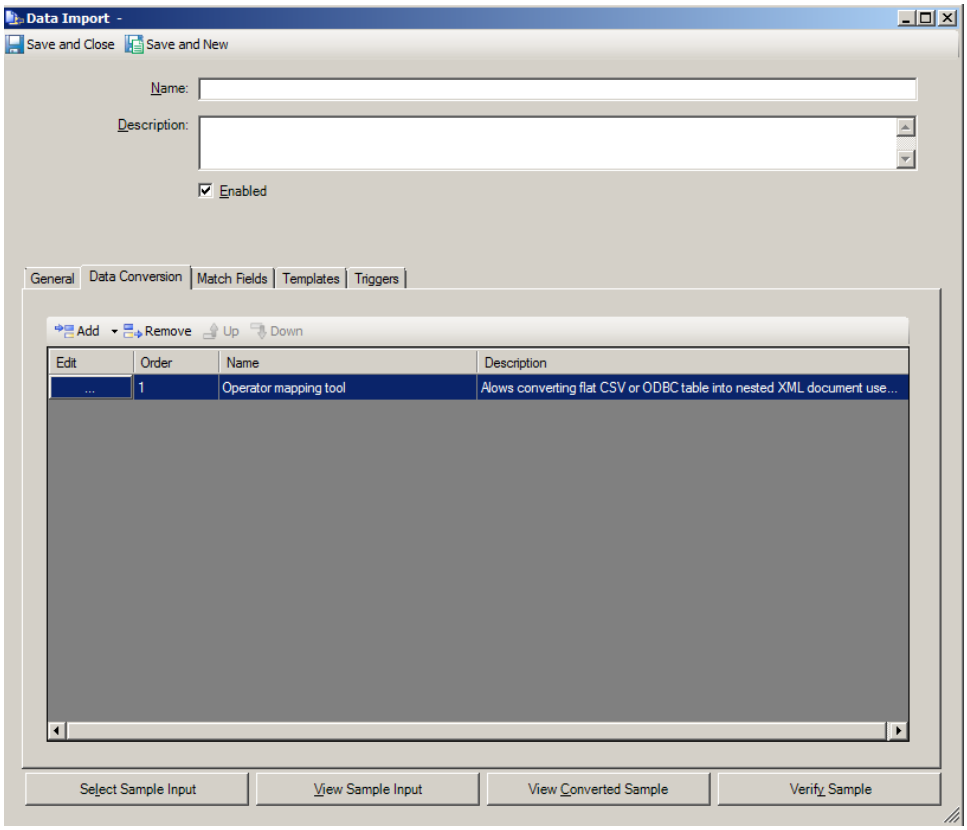
Some of these fields may already be correctly mapped, such as User**_Name** to **User Name** (with **Operator** as the **C•CURE 9000 Target type)**.

To keep the **Data Source Field** name the same, select **<Keep field name as is>**. The original field name with its value will appear in the converted sample.

5. To see how the Data Source file has been converted by the mapping tool, click the **View Converted Sample** button. The converted file opens for your review, as shown in the following example.

6. To save this mapping, click **Save and Close**. The Data Conversion tab reappears with the Operator mapping tool added as the first row in the Data Conversion table, as shown in Figure 23 on Page 104 .

Figure 23: Data Import Editor - Data Conversion Tab with Operator Mapping Tool Row



7. To check that the Data Source file has been properly converted, click the **Verify Sample** button. A message displays saying either that the system recognizes every field in the sample input or only recognizes some of the fields.

Field Mapping Tool Editor

The C•CURE 9000Field Mapping Tool Editor allows you to map CSV files, LDAP records, ODBC, or XML files that do not conform to the C•CURE 9000 schema.

NOTE

Software House strongly recommends that you use the Personnel Mapping Tool Editor on Page 92 to convert the data when you are importing Personnel instead of this Field Mapping Tool.

While the Field Mapping tool can rename the tags in the incoming XML document, it cannot change the document's structure. The Personnel Mapping tool, on the other hand, can convert a flat record into a record with a nested structure—putting Credential fields into a nested tag within a Personnel record, for example.

The Field Mapping process takes XML as an input and using an internal XSLT script, transforms it into XML format suitable for import into C•CURE 9000.

Fields mapped from the source file to C•CURE 9000 represent actual fields to be imported into C•CURE 9000. The converter filters out unmapped fields.

The Field mapping tool tries to automatically map the tags in the sample import file with known fields in the system and will open populated with one tab for each object type recognized and the last tab with a New icon  , as shown in Figure 24 on Page 105.

Example:

Personnel/Credentials/Clearances/ 

If you click the  tab, the system opens an empty tab named Mapping, shown in Figure 25 on Page 105. You can use this blank “Mapping” tab at any time to do manual mapping

Figure 24: Field Mapping Tool – with Entries

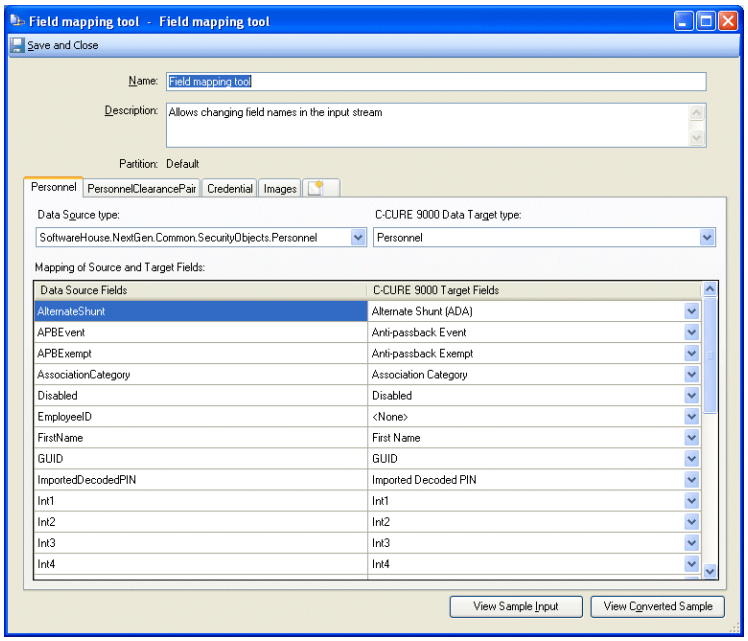
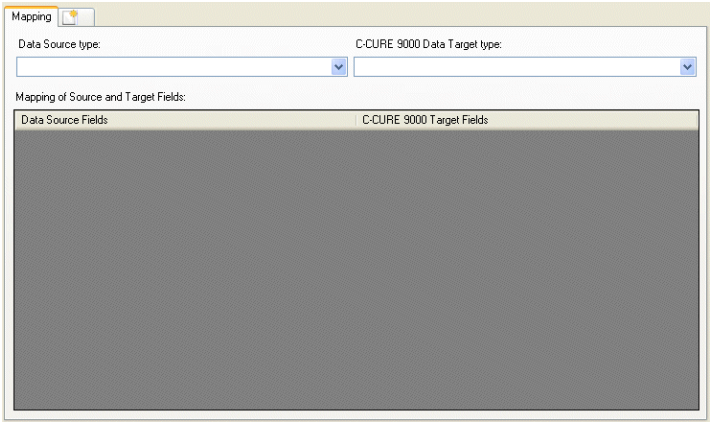


Figure 25: Field Mapping Tool with New Empty Tab



For more information, see:

- Field Mapping Tool Definitions on Page 106
- Using the Field Mapping Tool to Convert Other Security Object Data on Page 108

Field Mapping Tool Definitions

The **Field Mapping Tool Editor** has the buttons described in Table 21 on Page 106.

Table 21: Field Mapping Tool Editor Buttons

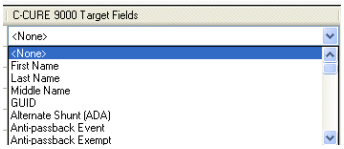
Button	Description
Save and Close	Click this button when you have completed any changes to the Field Mapping and wish to save those changes. The Field Mapping Tool Editor closes and returns you to the Data Conversion tab of the Data Import Editor. (If this was the first time the Field Mapping Tool was opened for this Import definition, it is shown in the list on the Data Conversion tab on a new row.) NOTE: Saved data is not committed to the database until the Import Definition is saved.
	Click this button when you want to close the Field Mapping Tool 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. In either case, the Data Conversion tab of the Data Import Editor reappears.
View Sample Input	Click this button to open a dialog box with the contents of the XML document that was: • Selected as the sample input. • Converted by any other converters that precede this one in the list of converters on the **Data Conversion** tab (shown in on Page 114).
View Converted Sample	Click this button to open a dialog box with the content of the XML document converted from the sample input document by applying field mapping as configured by this converter.

The **Field Mapping Tool Editor** has the fields described in Table 22 on Page 106.

Table 22: Field Mapping Tool Editor Fields

Fields/Buttons	Description
Name	"Field mapping tool" is automatically entered in this field by the system. You can change the name, but it is not necessary for identification purposes: an Import Definition does not require more than one field mapping tool.
Description	A textual description of the field mapping. This field is not required.
Partition	A read-only field displaying the Partition to which this Import Definition belongs. (This field is visible only if the C•CURE 9000 system is partitioned.)
Each Tab	
Data Source type	This field in the left-hand column represents a tag in the input XML document selected from the **Data Import Editor General** tab. Click the down-arrow to select a tag from the drop-down list. **Example:** Credential/Images/Personnel/PersonnelClearancepair
C•CURE 9000 Data Target Type	This field in the right-hand column represents an importable object type within the C•CURE 9000 application. Click the down-arrow to select the object from the drop-down list. Selecting an object type renames the tab with the full name of the selected type. **Example:** if you select **Credential** from the drop-down list, this tab is renamed **Credential**.
Mapping of Source and Target Fields Box	
Data Source Fields	Once a tag is selected in the **Data Source type** field for each tab, this left-hand column displays the field tags from the XML document for that selected tag.

Table 22: Field Mapping Tool Editor Fields (continued)

Fields/Buttons	Description
C•CURE 9000 Target Fields	Once an **object type is** selected in the **C•CURE 9000 Data Target Type** field, this right-hand column displays both of the following: • C•CURE 9000 Data Fields that the system has succeeded in automatically mapping to XML tags. **Example:** First_Name to FirstName and Last_Name to LastName • <None> for each XML tag that the system could not automatically map to a C•CURE 9000 Data Field. **Example:** EmployeeID to <None> Each field in this column—whether it contains a mapped field, such as LastName, or <None>—includes a down-arrow that opens a drop-down list of all the fields from the selected **C•CURE 9000 Data** type, such as that shown in the following example: 

Field Mapping Tool Editor Tab Context Menu

The context menu that opens when you right-click a tab in the Field Mapping Tool Editor includes the selections described in Table 23 on Page 107.

Table 23: Data Field Mapping Tool Editor Tab Right-Click Context Menu Options

Menu Selection	Description
Close Current Tab	Click this menu selection to close the current tab of the Field mapping tool and remove its mapping.
Close All	Click this menu selection to close all the current tabs of the Field mapping tool and create a new blank tab, named **Mapping** (shown in on Page 107) that has no automatic mapping and lets you map manually yourself.
Perform Mapping	Click this menu selection to have the system map as follows: • If the action is performed immediately after closing all the tabs—only one blank tab displays with no mapping—performs complete automatic mapping, creating as many tabs as mapped object types have been found. • If the Field mapping tool already has tabs with proper mapping and you have just created a new tab manually and selected mapping between a Data Source type and a **C•CURE 9000 Data Target Type**—but without mapping the fields—performs automatic mapping for any field of the selected target type and creates proper mappings.
Clear Mapping	Click this menu selection to delete the mapping on the selected tab without closing the tab.

Using the Field Mapping Tool to Convert Other Security Object Data

The Field mapping tool always tries to automatically map the tags in the sample input file to known fields in C•CURE 9000.

- When **none** of the tags can be mapped automatically, the **Field mapping tool Editor** opens, as shown in Figure 26 on Page 108, with a tab named **Mapping**—with the sample input file tag entered in the **Data Source type** field and the unmapped source fields from the sample input file listed in the **Data Source Fields** column.
- When at least some of the tags can be mapped automatically, the **Field mapping tool Editor** opens populated, with one tab for each object type that was mapped, as shown in the example in Figure 27 on Page 108.

NOTE Automatic mapping makes a 'best guess' about the possible links between incoming data and existing C•CURE 9000 types and properties. However, this guess could be incorrect. Consequently, you should verify that the automatic mapping is correct before saving it.

Figure 26: Field Mapping Tool for Sample Input with No Mapped Tags

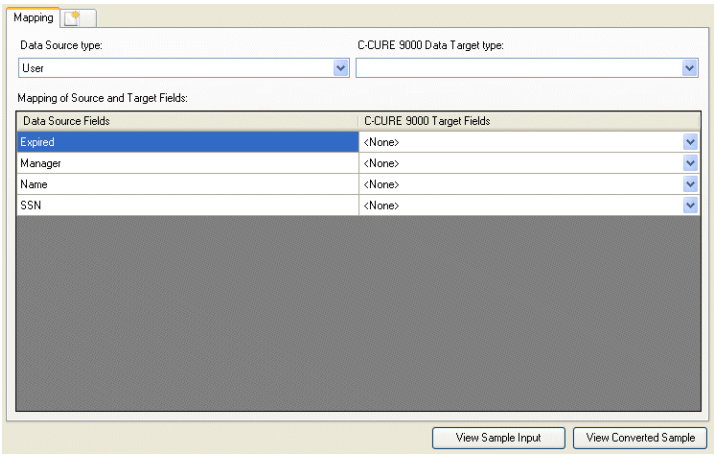
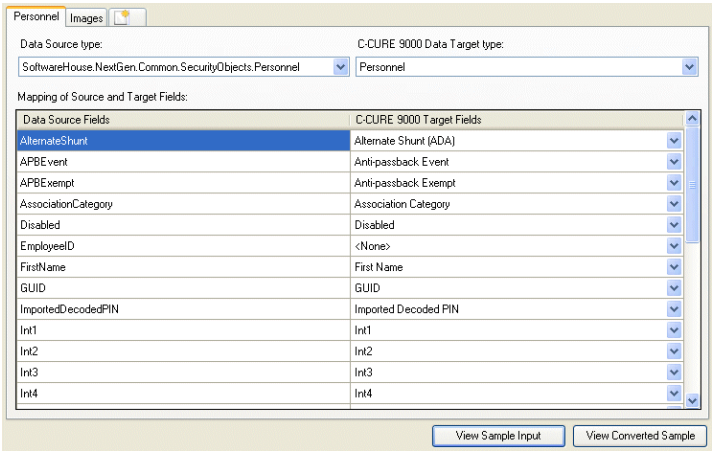


Figure 27: Field Mapping Tool for Sample Input with Some Mapped Tags



Consequently, the process of mapping the fields yourself manually differs somewhat depending on whether the system was able to automatically map any of the tags.

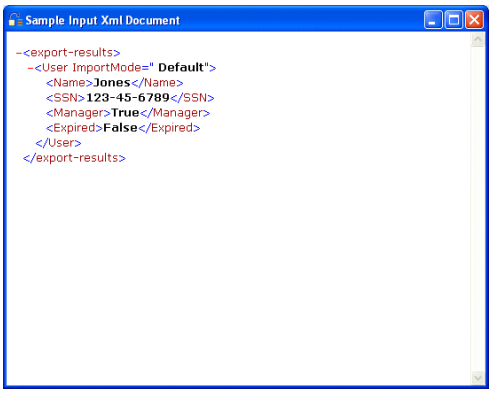
- To Do Field Mapping When No Tags Were Automatically Mapped on Page 108
- To Do Field Mapping When Only Some Tags Were Automatically Mapped on Page 110

To Do Field Mapping When No Tags Were Automatically Mapped

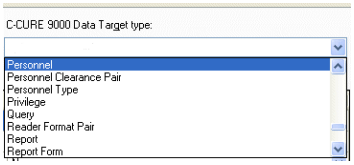
1. In the **Field Mapping tool Editor**, as shown in the example in Figure 26 on Page 108, do the following:

- In the **Name** field leave the name as is.
- In the **Description** field, describe the Field Mapping as you wish. You can enter up to 500 characters.

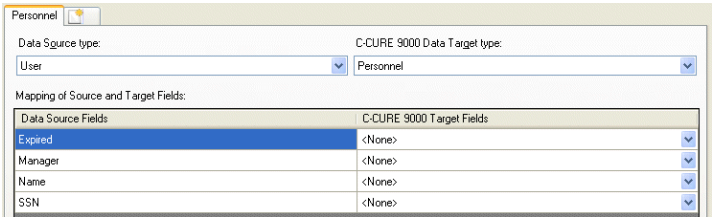
2. To ascertain the contents of the Data Source file, click the **View Sample Input** button. The sample opens for your review, as shown in the following example.



3. On the **Mapping** tab, click the down-arrow in the **C•CURE 9000 Data Target type** field to open the drop-down list, scroll down, and select the appropriate target object—such as **Personnel**, in the example in the following figure.

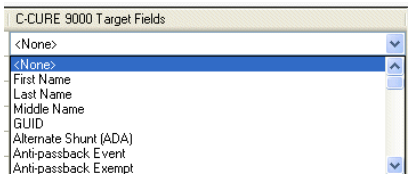


The system renames the **Mapping** tab with the name of the object you selected—Personnel in the example and enters that name in the **C•CURE 9000 Data Target type** field, as shown in the following figure.



Since the system could not map any of the Data Source Fields to the C•CURE 9000 Data Target fields, the Data Target fields are all set to <None>. However, knowing the fields that are included in the Data Source Input file allows you to map each of them to the appropriate C•CURE 9000 Target field.

4. Click the down-arrow next to the first of the <None> fields. The drop-down list displays the fields, as shown in the following example.

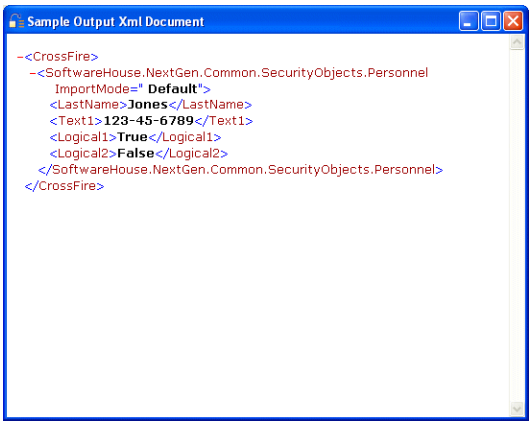


5. Map the fields as shown in the following example:

Example:

Data Source Fields	Target Fields
Expired	Logical2
Manager	Logical1
Name	LastName
SSN	Text1

6. To see how the Data Source file has been converted by the mapping tool, click the **View Converted Sample** button. The converted file opens for your review, as shown in the following example.



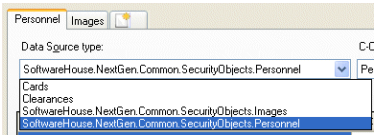
7. To save this field mapping, click **Save and Close**. The Data Conversion tab reappears with the Field mapping tool added as the first row in the Data Conversion table as shown in Figure 28 on Page 110.

Figure 28: Data Import Editor - Data Conversion Tab with Field Mapping Tool Row

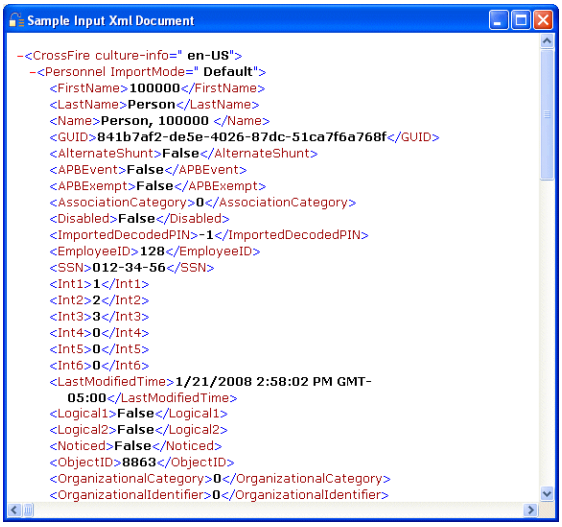
8. To check that the Data Source file has been properly converted, click the **Verify Sample** button. A message displays saying that the system recognizes every field in the sample input.

To Do Field Mapping When Only Some Tags Were Automatically Mapped

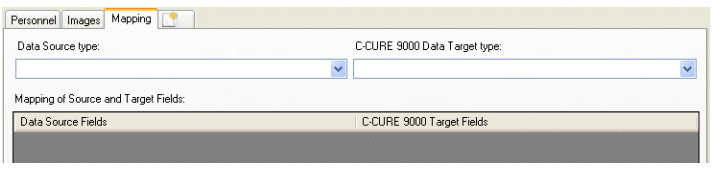
1. In the **Field Mapping tool Editor**, as shown in the example in Figure 27 on Page 108 where the Personnel and Image tags in the sample input file were able to be mapped to known C•CURE 9000 types and there are already two populated tabs named **Personnel** and **Images**, do the following:
   - In the **Name** field leave the name as is.
   - In the **Description** field, describe the Field Mapping as you wish. You can enter up to 500 characters.
2. To see what tags are in the Data Source Input file, click the down-arrow next to the **Data Source Type** field. The drop-down list displays the tags, as shown in the following example.



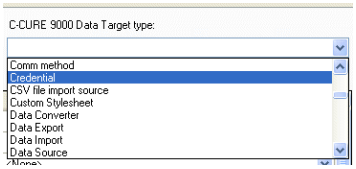
3. To review the Data Source file contents and these tags, click the **View Sample Input** button and scroll through the file, as shown in the following examples.



4. To start mapping the unmapped tags in the Data Source type, click the New  tab. The system opens an empty tab named **Mapping**, as shown in the following figure.

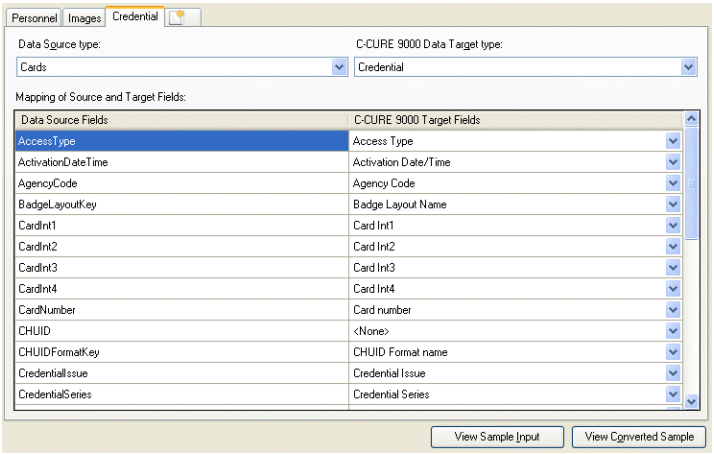


5. Open the drop-down list from the blank **Data Source Type** field and click to select **Cards**.
6. In the **C•CURE 9000 Data Target type** field, click the down-arrow to open the drop-down list; scroll down and select the target object equivalent to **Cards**— in this case **Credential**, as shown in the following example.

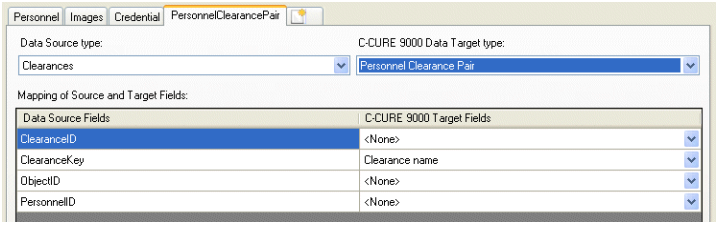


The system renames the **Mapping** tab with the name of the selected object—**Credential** in the example, enters it in the **C•CURE 9000 Data Target type** field, and automatically maps as many fields as possible to related **Data Source Fields,** entering them in the right-hand column. (See the example in Figure 29 on Page 112.)

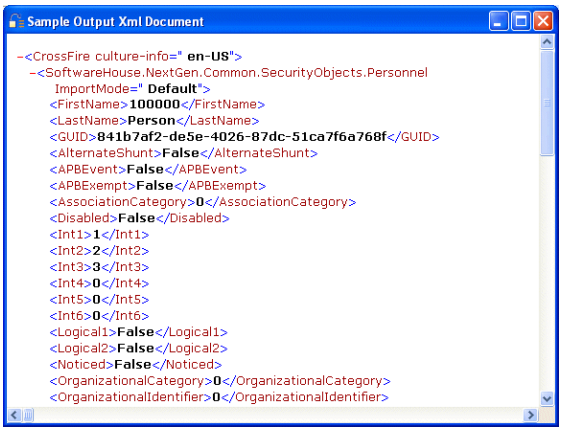
Figure 29: Field Mapping Tool with Credential Tag Mapped

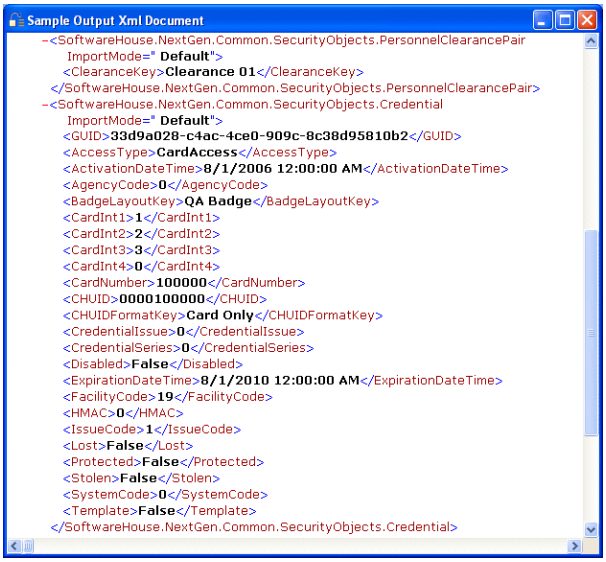


7. Verify that the system mapped each field correctly and, if necessary, fix the mapping manually.
8. Continue mapping any remaining unmapped tags—in this example, **Clearance**—as described in Step 4 through Step 6. When you are finished, the Field Mapping Tool Editor appears.



9. To see how the Data Source file has been converted by the mapping tool, click the **View Converted Sample** button. The converted file opens for your review, as shown in the following examples.





10. To save this field mapping, click **Save and Close**.

    The **Data Conversion** tab reappears with the Field mapping tool added as the first row in the Data Conversion table as shown in Figure 28 on Page 110.

11. To check that the Data Source file has been properly converted, click the **Verify Sample** button. A message displays saying that the system recognizes every field in the sample input.

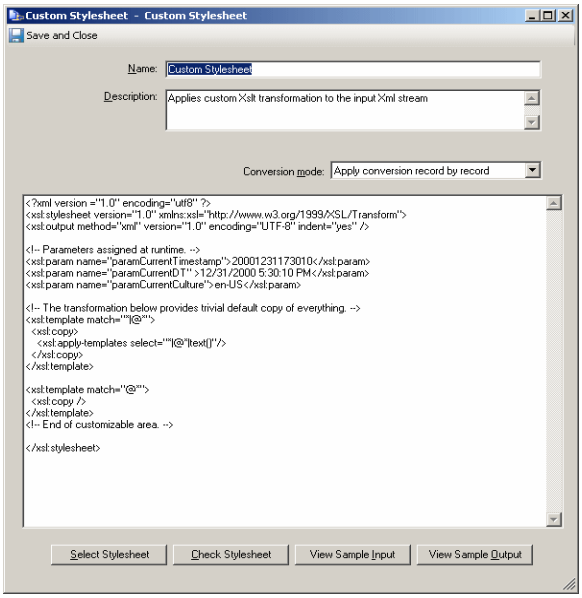
Custom Stylesheet Editor

The **Custom Stylesheet Editor**, which is essentially an XSLT Import converter, allows advanced users with an excellent understanding of the XSLT language to perform complex transformations of incoming XML documents. The Custom Stylesheet can help such users handle difficult conversion cases.

The **Custom Stylesheet Editor** is shown in Figure 30 on Page 114.

Only advanced knowledgeable users should employ this tool without consulting with their dealer or the Software House Customer Support Center.

Figure 30: Custom Stylesheet Editor



- Custom Stylesheet Editor Context Menu on Page 115
- Using the Custom Stylesheet to Convert Data on Page 115

The **Custom StyleSheet Editor** has the buttons described in Table 24 on Page 114.

Table 24: Custom Stylesheet Editor Buttons

Button	Description
Save and Close	Click this button when you have completed any changes to the Custom Stylesheet and wish to save those changes. The **Custom Stylesheet Editor** closes and returns you to the **Data Conversion** tab of the **Data Import Editor**, where the Custom Stylesheet is shown as a new separate row. NOTE: Saved data is not committed to the database until the Import Definition is saved.
	Click this button when you want to close the **Custom Stylesheet 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. In either case, the **Data Conversion** tab of the **Data Import Editor** reappears.
Select Stylesheet	Click this button to open a dialog box where you can select an external file as a style sheet and replace the current contents in the Text Editing box with the contents of the file. (This allows you to avoid lengthy copy and paste operations.)
Check Stylesheet	Click this button to force a syntax check on the current contents in the Text Editing box—check whether it is valid XLST. If the check fails, an error message displays and if possible, the cursor is positioned on the line where the first error was detected.

Table 24: Custom Stylesheet Editor Buttons (continued)

Button	Description
View Sample Input	Click this button to open a dialog box with the contents of the XML document that was: • Selected as the sample input. • Converted by any other converters that precede this one in the list of converters on the **Data Conversion** tab (shown in on Page 89).
View Sample Output	Click this button to open a dialog box with the contents of the XML document generated from the sample input document by applying the current XSLT script from this **Custom Stylesheet Editor**—if the script is valid. If the current script is not valid, the system displays an error message instead of the dialog box.

The **Custom StyleSheet Editor** has the fields described in Table 25 on Page 115.

Table 25: Custom Stylesheet Editor Fields

Fields/Buttons	Description
Name	"Custom Stylesheet" is automatically entered in this field by the system. You can change the name for identification purposes if you want to have multiple custom stylesheets per Import Definition.
Description	"Applies custom Xslt transformation to the input Xml stream" is automatically entered in this field by the system as a textual description. You can change the description for informational purposes. This field is not required.
Text Editing Box	
Text Editing box	This area is basically a text editor into which you enter an XLST stylesheet for converting your input document. The default template that is automatically displayed in this box when you open the **Custom Stylesheet Editor** does **not** perform any conversion. You must replace it with a valid style sheet using one of the following methods: • Clicking the **Select Stylesheet** button to pick a stylesheet from a Windows **Select Stylesheet** dialog box. • Copying text from any external stylesheet and using the **Custom Stylesheet Editor** right-click context menu to paste it in this area. • Editing the existing text.
Conversion Mode	Click the down arrow to select the mode in which the conversion proceeds: • Apply conversion record by record – select this mode (the default) to save memory usage during the import process. Software House recommends using this mode, especially if the import file is more than 100 MB. • Apply conversion to all records together – Select this mode, which is somewhat faster, if your import file is small. This mode is also needed if the script accesses records from different parts of the input document to form one output record—a very rare case.

Custom Stylesheet Editor Context Menu

When you right-click in the Custom Stylesheet Editor, the system displays a standard text editing menu with options to Undo, Cut, Copy, Paste, Delete, and Select All.

If you click **Select All** while the cursor is in either the **Name** or **Description** field, only the entry in that specific field is selected and highlighted. If, on the other hand, you click **Select All** while the cursor is in the **Text Editing** box, the entire text entered in that box is selected.

Using the Custom Stylesheet to Convert Data

The example in the following procedure for using the Custom Stylesheet starts with a sample CSV file containing personnel records exported from a C•CURE 800 system. Importing these records into a C•CURE 9000 system requires certain field names and field values to be altered.

NOTE The example CSV Source file exported from C•CURE 800 includes field **values** that must be changed to match the related C•CURE 9000 values. While field **names** can be changed by the Personnel Mapping tool, field **values** can be changed only with a custom stylesheet.

To Use the Custom Stylesheet and Multiple Converters to Convert Data

1. Configure the Import Definition's Import Source and select the sample Input file.
2. In the Custom Stylesheet Editor, as shown in on Page 115, do the following:
   - In the **Name** field leave the default name "Custom Stylesheet" as is, or change it to a unique name for identification purposes if you plan to have multiple custom stylesheets for this Import Definition.
   - In the **Description** field, leave the default description "Applies custom Xslt transformation to the input Xml stream" as is, or change it for informational purposes. You can enter up to 500 characters.
   - In the **Conversion Mode** field, leave the default option, **Apply conversion record by record**, to save memory during the import.
3. To get an idea of the contents of the Data Source file, click the **View Sample Input** button.

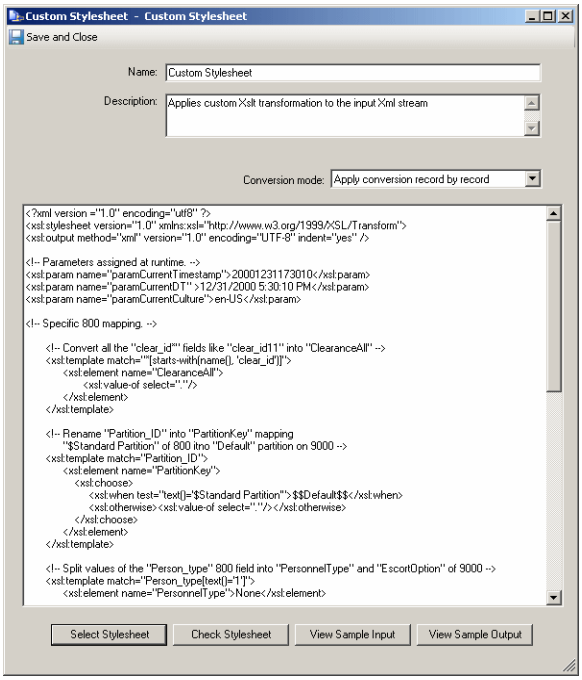
   The system displays the already selected sample for your review, automatically converted from CSV to XML, as partially shown below (Ellipses [...] indicate where entries have been skipped):

```
<CrossFire culture-info=" en-US".>
   <ExternalObject ImportMode=" Default">
      <Access_Facility_Code>0</Access_Facility_Code>
      <Activation_DT>01/01/1990 19:00</Activation_DT>
      <Agency_Code>0</Agency_Code>
      <ADA>0</ADA>
      <Activate_AP_Event>0</Activate_AP_Event>
      ...
      <Card_Num>17205</Card_Num>
      ...
      <Partition_ID>$Standard Partition</Partition_ID>
      <Person_type>1</Person_type>
      ...
   </ExternalObject>
</CrossFire>
```

4. Click the **Select Stylesheet** button. The **Select Stylesheet** dialog box opens.
5. Select an XSLT file from the list, or browse to find the XSLT file you want to use, and click **Open**.

   The XSLT file, a valid style sheet, replaces the default 'dummy' in the **Custom Stylesheet Editor**, as shown partially in Figure 31 on Page 117. (A valid custom stylesheet (XSLT file) that can be used for imports from C•CURE 800 is documented in its entirety in Custom Stylesheet Sample on Page 560.

Figure 31: Custom Stylesheet Editor with Valid XSLT



6. Click **Check Stylesheet** to make sure the style sheet is correct. If the system displays a message saying "No errors were detected in the stylesheet", you know you can proceed.
7. To perform the test conversion, click the **View Sample Output** button. The Custom Stylesheet converts the input sample and displays the result, as partially shown below (Ellipses [...] indicate where entries have been skipped):

```
    <ExternalObject ImportMode=" Default">
        <Access_Facility_Code>0</Access_Facility_Code>
        <Activation_DT>01/01/1990 19:00</Activation_DT>
        <Agency_Code>0</Agency_Code>
        <ADA>0</ADA>
        <Activate_AP_Event>0</Activate_AP_Event>
        ...
        <Card_Num>17205</Card_Num>
        ...
        <PartitionKey>$$Default$$</PartitionKey>
        <PersonType>None</PersonType>
        ...
    </ExternalObject>
</CrossFire>
```

Notice that the Custom Stylesheet has changed only the following items in the sample output file:

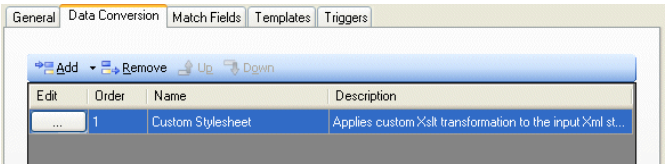
- The original **Partition_ID** field name to **PartitionKey** and its value from **$Standard Partition** to **$$Default$$**.
- The original **Person_type** field name to **PersonnelType** and its value from **1** to **None**.

This is because the default partitions in C•CURE 800 and C•CURE 9000 have different field values as well as different field names, as do personnel types:

However, the custom conversion has not applied the correct C•CURE 9000 naming convention to other fields in the file. As a result, you have to perform another conversion to fix this problem. While you could create and use another Custom Stylesheet for this purpose or modify the one in Figure 31 on Page 117, it is easier to use the Personnel mapping tool as a second data converter placed after the Custom Stylesheet converter.

8. To save this custom conversion, click **Save and Close**.

   The **Data Conversion** tab reappears with the Custom Stylesheet added as the first row in the Data Conversion table.



9. Click the arrow next to the **Add** button and then click **Personnel mapping tool** from the drop-down list.

   The Personnel Mapping tool opens with the remaining CSV data fields mapped as well as the system is able to map them.

   The external file still needs the following changes:

   - The field names must be changed from the external names to the names used by C•CURE 9000 objects.
   - The fields related to the child records, such as 'Credential', must be wrapped with the nested tags.

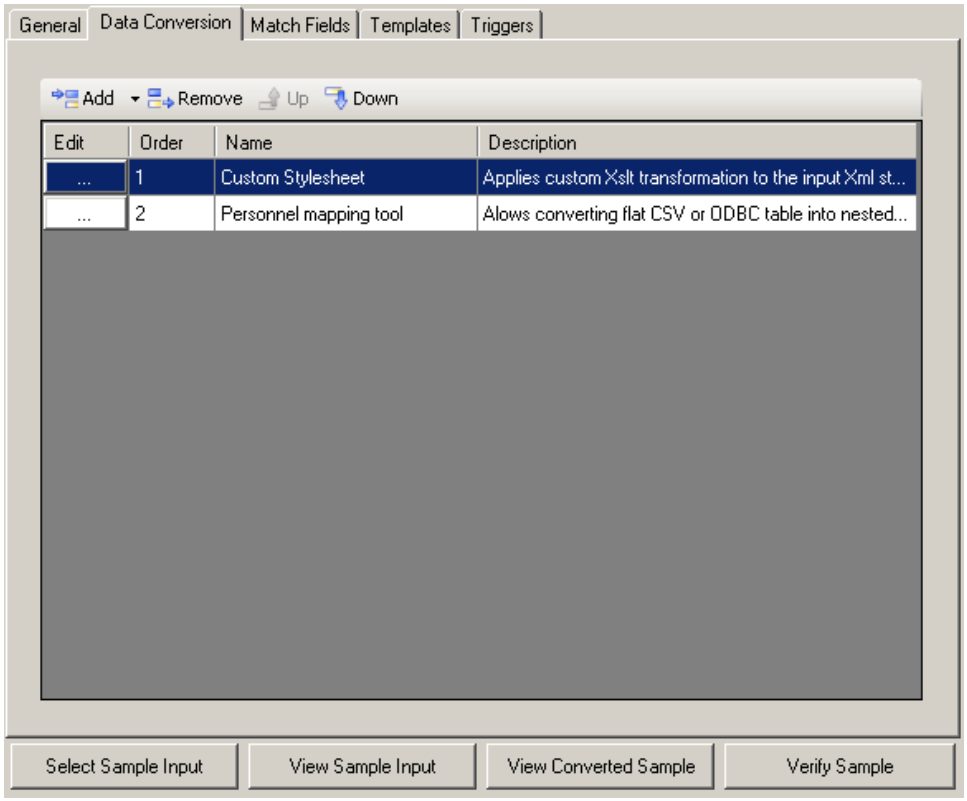
10. Use the down-arrows next to the entries in the **C•CURE 9000 Target Type** and **C•CURE 9000 Target Field** columns to map the external Data Source Fields.

11. To see how the test sample has been further converted by the mapping tool, click the **View Converted Sample** button. The converted file opens for your review.

12. If the sample now seems correct, click **Save and Close** to save this mapping.

    The Data Conversion tab reappears with the Personnel mapping tool added as the second row in the Data Conversion table as shown in Figure 32 on Page 119.

Figure 32: Data Import Editor - Data Conversion Tab with Multiple Converter Rows



13. To check that the Data Source file has been properly converted, click the **Verify Sample** button.
14. If the message confirms that the system recognizes every field in the sample, click **Save and Close**.

Data Import Match Fields Tab

The **Match Fields** tab is populated with object types and fields from a selected sample input, allows you to specify the fields you want to match for an Import Definition—necessary when you are configuring an import that requires records to be updated. (See Figure 35 on Page 125 for an example of the **Match Fields** tab unpopulated because no sample input was selected.)

The **Match Fields** tab is shown in Figure 33 on Page 120 and Figure 34 on Page 121.

This tab must be used when you select either of the import rules for updating records in the **Default Import Mode** box on the **General** tab (see General Tab Definitions on Page 75 and Selecting the Default Import Mode on Page 84.

Figure 33: Data Import Editor - Match Fields Tab with Personnel Object Type

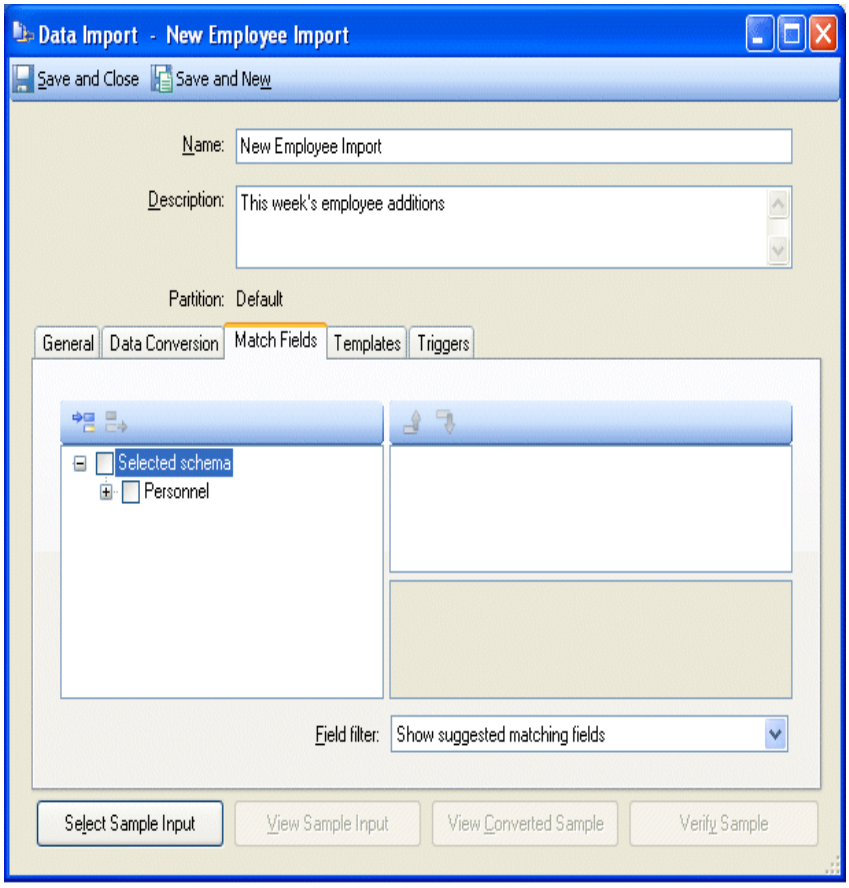
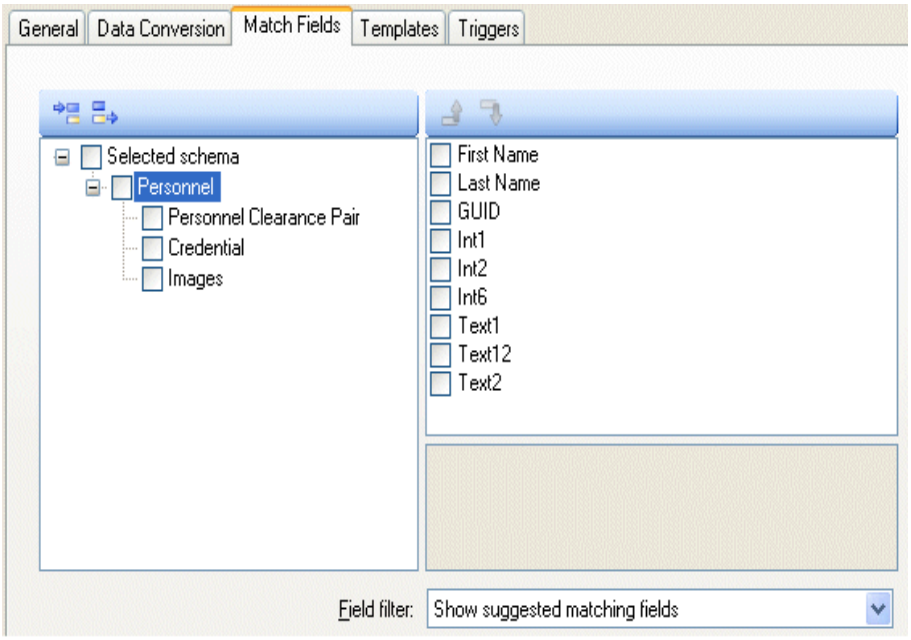


Figure 34: Data Import Editor - Match Fields Tab with Personnel and Three Child Objects



Match Fields Tab Definitions

The Match Fields tab has the fields described in Table 26 on Page 121.

Table 26: Data Import Editor Match Fields Tab Definitions

Fields/Buttons	Description
(Top Level Object Types)	This **left-hand pane** displays a tree with a list of recognized object types (with relations between different object types) once import filters are properly configured and one of the following is true: • The system can recognize some tags in the converted samples as importable entities. • You have manually selected an object type from the Select type dynamic view list. You can click ⊞ or ⊟ to expand and contract the tree. **Example:** See the Personnel type with its child objects in Figure 34 on Page 121. You can click an object type in the tree to display its fields in the right-hand pane (unselected ☐), as well as one of the Field filter options to limit/expand which fields are displayed. To select individual fields as match fields for the import, click any field in the right-hand pane (☑). NOTE: The check box next to the object types in the left-hand pane indicates that match fields are selected for that type.
(Properties of Selected Object[s])	This **right-hand pane** displays the fields associated with the **object type** currently selected, as delimited by the filter option selected in the **Field filter** field. **Example:** If your Import definition is for **Personnel** objects and you click Credential (one of its child object in the **left-hand pane**), the fields for **the Credential** record are listed in this **pane**. To specify one or more match fields for an import, double-click the field name, and a ☑ appears to the left of the name to indicate it is selected; or click the ☐ to the left of the field name. To clear a field so it does not act as a match field, double-click the field name, and a ☐ appears to the left of the name to indicate it is no longer selected; or click the ☑ to the left of the field name. NOTE: Software House recommends choosing as match fields one or more from those displayed by the **Show suggested matching fields** Field filter option

Table 26: Data Import Editor Match Fields Tab Definitions (continued)

Fields/Buttons	Description
Field Filter	Select one of the filter options from the drop-down list to control which fields display in the right-hand pane for the selected object type. • Show suggested matching fields – from the fields listed in the sample XML document, displays only those recommended as matching fields. • Show all fields – displays all the fields recognized by the system that are listed in the sample XML document. (There can be more fields for the selected object type than are displayed.) NOTE: If you did not select a sample input and are configuring the match fields manually: - Show suggested matching fields – displays those fields recommended as matching fields from all the fields in the system for the selected object type. - Show all fields – displays all the fields in the system for the selected object type.
(Field description)	When you select a Field in the **right-hand pane** above, a description of the field displays in the box underneath.

Match Fields Tab Tasks

You use the **Match Fields** tab to specify the fields to use for matching incoming records with records in the C•CURE 9000 database when you are configuring an import that requires records to be updated:

- Specifying Match Fields Using a Sample Input File on Page 124
- Specifying Match Fields Manually on Page 125

Specifying Match Fields

The value of the chosen fields in the source import file must match the value of these fields in a record in the C•CURE 9000 database, or the record will not be updated. Instead, depending on the Import Mode configured, the record will be added or rejected. Typically you would want to choose one field that has a unique value, or one or more fields that in combination would identify a record uniquely. To build a proper matching rule you should select one or more fields for each top level object and each child object that you want to be updated by the import process.

Example:

In Personnel, the Customer tab fields **Int6** and **Text12** must have unique values, so they would be good choices to uniquely identify a Personnel record (providing you have put data values in these fields in your database).

If your C•CURE 9000 is partitioned, object names are unique only within their Partition, not across the entire system. Therefore, when defining Imports that match on **Int6** and **Text12** (or any other unique field)**,** you must take into account that there could be duplicates across the system. Consequently in a partitioned system:

- If the import XML document contains any Partitions, matching should include matching on the Partition field as well.
- If the import XML document does not contain any Partitions and there is more than one record found with the **Int6** or **Text12** value, matching will reject the record.

If you are using either **Update** Import Mode option and you match on a field other than GUID, Software House recommends that GUID **not** be included in the source import file. If GUID is included in the source import file, Software House recommends that you match on GUID.

If the GUID is modified for any record during the update operation, you **will lose the link** to the previous Journal and Audit Log data for the modified records.

NOTE Software House recommends that you **not** use **Card Number** (for matching only) for import matching if you are importing an XML file whose records have more than one credential assigned.

In the left-hand pane you add objects to import. The right-hand pane displays persistent fields associated with the selected object. You select the fields that you want to use for matching.

NOTE If a sample input has been selected, the right-hand pane contains only fields defined in the sample. Consequently, some child types may show no fields in this pane.

The system does not allow you to save an import definition with an update import mode if you have not specified at least one matching criteria.

NOTE If you specified matching for only some of the object types in the Import Definition, the import process will generate an error each time the imported document requests an update for an object for types without matching criteria.

The default Import Mode you choose can be overruled by the imported document on a record-by-record basis. See Attribute 'ImportMode' on Page 548 in Appendix A.

Specifying Match Fields Using a Sample Input File

If a sample input file has not already been selected, the system prompts you to select one. For detailed information, see Selecting the Source Type and Automation Mode on Page 79 and Selecting and Viewing a Sample Input on Page 85.

To Specify Match Fields with a Sample Input File

1. On the **Match Fields** tab populated with the object types and fields from the selected input sample, as shown in the examples in Figure 33 on Page 120 and Figure 34 on Page 121, click the top-level object type in the tree in the left-hand pane, **Personnel** in the example.

   Its associated fields display in the right-hand pane.

2. Select a Field filter option to control the fields displayed in this example:

   - Show suggested matching fields – to display only those fields recommended for matching.

3. In the right-hand pane, double-click a field to select it as the match field for Personnel—for this example, **Text 12** (a field required to have a unique value).

   A ☑ appears to the left of the name to indicate it is selected.

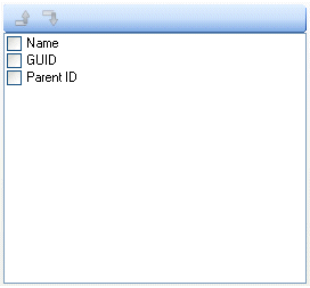
4. In the left-hand pane, click the child object, **Credential** in the example, to display its associated fields in the right-hand pane.

5. In the right-hand pane, double-click a field to select it as the match field for Credential**—**for this example, **Card number**.

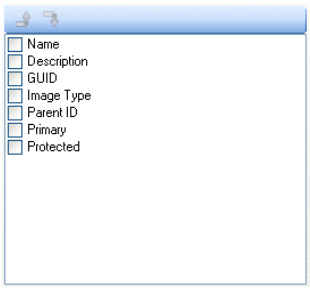
   A ☑ appears to the left of the name to indicate it is selected.

6. In the left-hand pane, click the child object, **Images** in the example, to display its associated fields in the right-hand pane.

   In this case, the field you want to use as the match field for Images is not listed.



   a. To see all the Images fields in the input sample, as shown below, click the down-arrow in the **Field filter** field and select the **Show all fields** option.



   b. In the right-hand pane, double-click a field to select it as the match field for Images**—**for this example, **Image Type**.

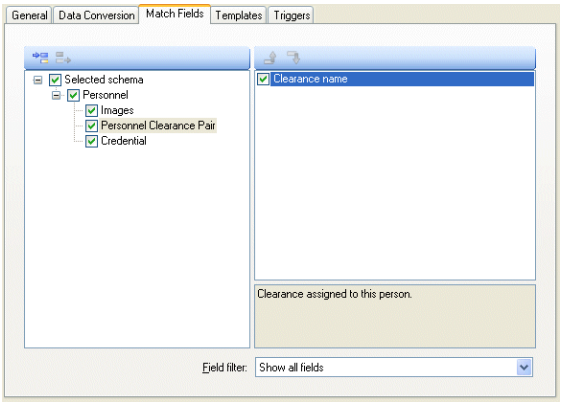
      A ☑ appears to the left of the name to indicate it is selected.

7. In the left-hand pane, click the last child object, **Personnel Clearance Pair** in the example, to display its associated fields in the right-hand pane.

8. In the right-hand pane, double-click a field to select it as the match field for Personnel Clearance Pair—for this example, **Clearance Name**, the only field available.

   A ☑ appears to the left of the name to indicate it is selected.

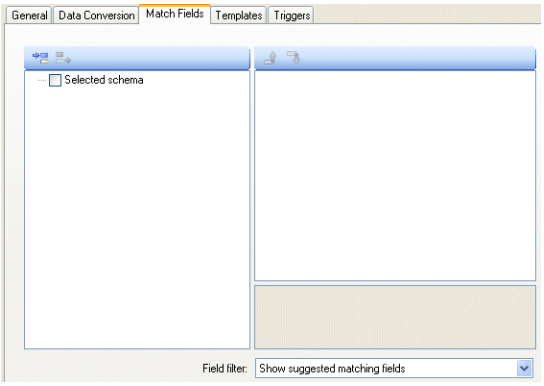
   Now that you have selected match fields for all of the object types in the left-hand pane, each of them has a check mark ☑ next to them.



Specifying Match Fields Manually

When you do select a sample input file before opening the **Match Fields** tab, it displays unpopulated, as shown in Figure 35 on Page 125. You need to select the data objects for your import manually yourself before you can select match fields.

Figure 35: Data Import Editor - Match Fields Tab Unpopulated



NOTE

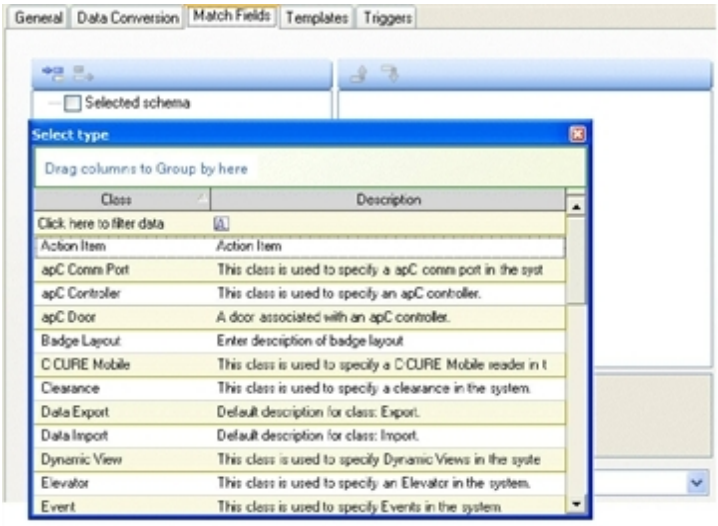
You could still select a sample input at this point and populate the tab automatically by clicking the **Select Sample Input** button.

Once a sample has been selected, clicking the **Verify Sample** button verifies that the **Match Fields** tab contains all the recognized types from the sample input, and appends missing types to the list.

To Specify Match Fields Manually

1. On the **Match Fields** tab, as shown in the preceding figure, click ⇄.

   The system displays a dynamic view that lets you select a top-level data type or object to add to the **Match Fields** tab.



2. From the **Select Type** view, scroll down to select the object you want to add, in this example **Personnel**. The **Match Fields** tab displays as shown in Figure 34 on Page 121 with the Personnel object type and its three child objects listed in the tree in the left-hand pane.
3. Select match fields for each object type as described in Step 2 on Page 124 to Step 8 on Page 125.

NOTE When you are selecting match fields manually without the aid of a sample input, the fields that display in the right-hand pane—depending on which Field filter option you chose—are not limited to only those in the sample. They are either **all** the importable fields for the object type or **all** the suggested match fields for the object type.

4. To add another object type, and its match fields, for this Import Definition click  again.

   From the **Select Type** view, scroll down and select the object you want to add, in this example **Clearance**.
5. Select match fields for the added object type(s).
6. Repeat the preceding steps as many times as needed to add more object types.
7. To remove objects from the **Match Fields** tab, click  .

Data Import Templates Tab

The **Templates** tab is used to configure a list of template rules to be used by this Import Definition. A template rule defines a template to be applied to the record being imported when the record satisfies the query expression configured in the rule.

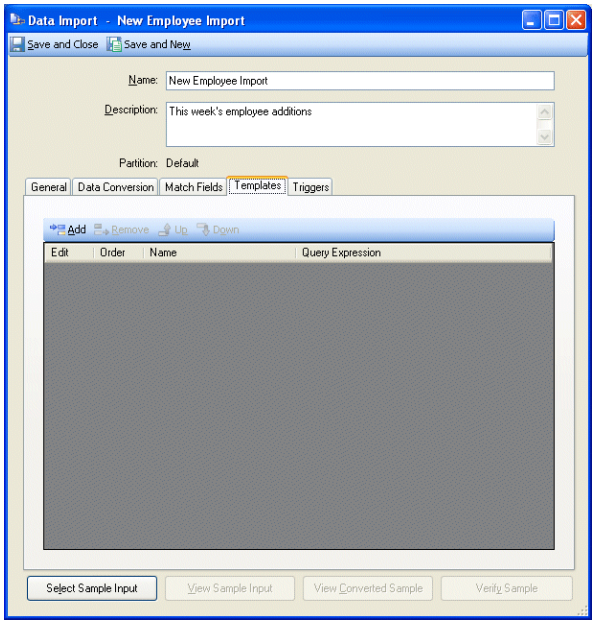
The **Templates** tab is shown in Figure 36 on Page 127.

Example:

You can utilize templates for differing Personnel types (roles) such as Contractors, Employees, and Managers to add clearances to their records or update them.

For more information, see How Template Rules Work in Importing on Page 138.

Figure 36: Data Import Templates Tab

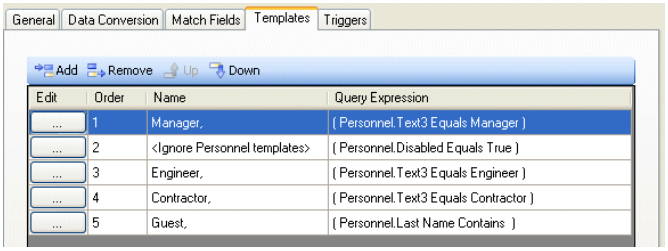


NOTE You must have a sample input selected to use this tab. If a sample was not already selected, clicking **Add** prompts you to select one. For more information, see the note in Templates Tab Buttons on Page 128.

Once configured, the **Templates** tab, as shown in the example in Figure 37 on Page 127, contains a list with the following:

- Reference to existing templates of top-level importable types in the system, such as Personnel templates or Door templates, or an instruction to ignore the temple, such as <Ignore personnel templates>.
- A related query expression.

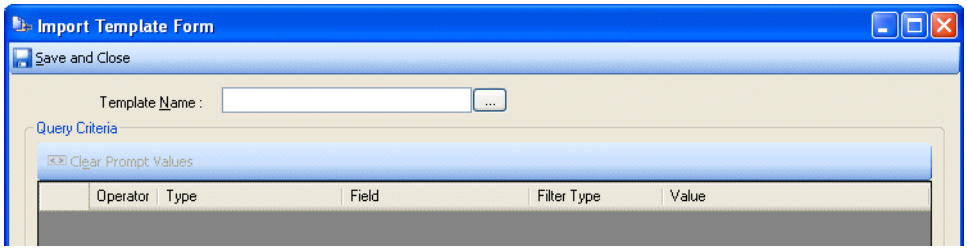
Figure 37: Data Import Editor - Templates Tab Completed



Import Template Form Editor

When you click **Add** on the **Templates** tab, the **Import Template Form Editor** opens, looking as shown in Figure 38 on Page 128. This editor lets you select the template and define its related query expression. Once this editor has been completely configured and saved, a new row is appended to the Templates grid on the **Templates** tab, as shown in Figure 43 on Page 135.

Figure 38: Import Template Form Editor



Once you click ... in the **Template Name** field on the Editor and make your selections from the **Dynamic Selection** dialog box that opens (see Figure 39 on Page 132, the **Import Template Form Editor** displays the Template selection and Query Criteria that you chose (see Selecting a Template Rule for an Import on Page 132.

Template-Related Definitions

The tables below provide definitions for the fields and buttons related to the Import Templates tab.

Templates Tab Buttons

Table 27 on Page 128 describes the buttons on the **Templates** tab (see Data Import Templates Tab on Page 127).

Table 27: Data Import Templates Tab Buttons

Button	Description
Add	Use this button to open the **Import Template Form Editor**, shown in Figure 38 on Page 128, to create and configure a new Template rule; it is then added to the Templates grid. Each row in the table can act as a query filter. Each new row is added after the last. NOTE: When you click this button, if no sample input has yet been selected for this Import Definition, the system opens the **Select File with Sample** dialog box for you to choose one (see Figure 10 on Page 85). Should you click **Cancel** without selecting a sample, **no** new row is appended to the grid.
Remove	Click this button to remove a selected row from the Templates grid. This button is unavailable if there are no rows in the grid.
Move Up	Click this button to move a filter row up in the table. The position of Template rows affects import results. This button is unavailable if the first row in the grid is selected.
Move Down	Click this button to move a filter row down in the table. The position of Template rows affects import results. This button is unavailable if the last row in the grid is selected.

Templates Tab Definitions

The **Templates** tab (see Figure 36 on Page 127) has the fields described in Table 28 on Page 129.

Table 28: Data Import Templates Tab Fields

Field	Description
Edit	Click ... to open the **Import Template Form Editor** for this row of the grid to modify the information.
Order	Displays the number of this row in the grid—1 through n. The Import process examines the template rules in the specified order to find the query expression whose criteria match the imported data in ascending order.
Name	The name of the template to be used if the query expression for the rule matches the incoming data. The system enters this information in the row once you define and save a template rule on the **Import Template Form Editor**. (If you have the necessary Privilege, you can double-click in this field to open the **Template Editor** and make changes to this Template rule.) NOTE: If a template is **not** selected for a row or **neither** the **Apply on Add** or **Apply on Update** options are selected (see Figure 38 on Page 128), this field contains the value '<Ignore 'type' templates>' where 'type' = the name of the selected type. **Example:** <Ignore Personnel templates>
Query Expression	The query expression to be examined against the incoming data. If the query finds a match, the template rule in this row is used by the Import. (If the query expression is too long, it can be viewed in the tool tip.)

Import Template Form Editor Buttons

Table 29 on Page 129 describes the buttons on the **Import Template Form Editor** (see Figure 40 on Page 133). These buttons are not available until you select an Object type and a specific template from the **Dynamic Selection** dialog box. (For information on creating complex queries, see the *C•CURE 9000 Data Views Guide*.)

Table 29: Import Template Form Editor Buttons

Button	Description
Add	Click this button to add a row to the **Query Criteria** table. Each row in the table can act as a query filter. Each new row is added after the current row. To add a new row after a specific existing row, click the row selector ▸ to select a row and then click **Add**.
Remove	Click this button to remove a selected row from the **Query Criteria** table. You must click the row selector ▸ to select a row to remove. If **no** row is selected, this button is **not** available.
Up	Click this button to move a filter row up in the table. The position of filter rows can affect search results. You have to click the row selector ▸ to select a row to move. If **no** row is selected, this button is **not** available.
Down	Click this button to move a filter row down in the table. The position of filter rows can affect search results. You have to click the row selector ▸ to select a row to move. If **no** row is selected, this button is **not** available.
Add Block	For information about this button, see the Query Definition tables in the "Query" chapter in the *C•CURE 9000 Data Views Guide*.
Clear Prompt Values	Click to clear out any values entered in the Value field and return the default value for the criteria, <IGNORED> usually.
▸	Click the Row Selector to select a row before removing it, moving it up or down, or adding another row after it.

Import Template Form Editor Definitions

The **Import Template Form Editor** (see Figure 40 on Page 133) has the fields described in Table 30 on Page 130.

Table 30: Import Template Form Editor Fields

Field	Description
Template Name	Click [...] to open the Dynamic Selection dialog box, shown in Figure 39 on Page 132, where you can select the top-level Object type and an existing template for the selected type. Once you have chosen an Object type and a template, the following changes occur in this Editor: • Template name is entered in this field • **Apply on Add** and **Apply on Update** check boxes appear. (The **Update** check box displays only if the selected Object type is **Personnel**.) • The Query Criteria buttons appear.
Apply on Add	NOTE: This check box appears only after you have selected an Object Type on the **Dynamic Selection** dialog box. Select this option to indicate that the template rule **should be applied** if the Import Definition adds a new object to the database that matches the criteria in the query expression. NOTE: If this option is **not** selected and the Import Definition adds an object matching the specified query expression, the iterative process stops and **none** of the template rules are applied— even if the object matches the query criteria for other template rules further down in the list.
Apply on Update	NOTE: This option is available only for **Personnel** Object types since template rules cannot be applied during Import Update operations to other Object types. The check box appears only after you have selected an Object Type of **Personnel** on the **Dynamic Selection** dialog box. Select this option to indicate that the template rule **should be applied** if the Import Definition updates data in the existing object that matches the criteria in the query expression. NOTE: If this option is **not** selected and the Import Definition updates a **Personnel** Object matching the specified query expression, **none** of the template rules are applied— even if the object matches the query criteria for other template rules further down in the list.
Query Criteria (For information on creating complex queries, see the *C•CURE 9000 Data Views Guide*.)	
Operator	For every row in the table after the first row and for the first row in a block, you must choose a logical Operator (AND or OR) to define the relationship between the current row and the row that preceded it. **Example:** If the first row queries for Personnel with a Last name that begins with 'B' the next row must specify if its criteria is ANDed or ORed with the first row.
Type	This field is automatically entered by the system and is the top-level Object type selected on the **Dynamic Selection** dialog box (see Figure 39 on Page 132).
Field	Select the field for this Query Criteria from the drop-down list of Fields, limited to the fields in the user-defined sample input.
Filter Type	This drop-down list lets you chose a filter type for this Query Criteria. The choices vary depending upon the type of field chosen for this row. **Example:** If the Field is a True/False or On/Off field, the Filter Types are Equals or Not Equals.
Value	Type in or select a Value for the field in this criteria. The allowable Values depend upon the Field chosen and the Filter Type chosen. **Example:** For a True/False field, a check box is displayed in this column. For a text field, an edit box that you can type text into is displayed. NOTE: If <IGNORED> (the default) is left, this row is excluded from the query at runtime. If all rows have a value of <IGNORED>, the query matches any record.

Dynamic Selection Dialog Box Definitions

The **Dynamic Selection** dialog box (see Figure 39 on Page 132) has the fields described in Table 31 on Page 131.

Table 31: Dynamic Selection Dialog Box Fields

Field	Description
Select Type	Click ... to open a selection list of the types of top-level Objects found in the sample input selected for this Import Definition and then click to select an Object type. **Example:** Personnel
Select Object	NOTE: Click ... to open a selection list of existing templates for the Object type specified in the previous field.

Templates Tab Tasks

You use the **Templates** tab to select template rules and configure their related queries for application to security objects by this Import Definition:

Selecting a Template Rule for an Import

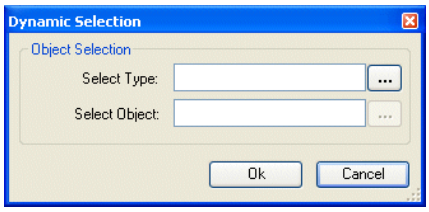
Selecting template rules for importing requires selecting the Object Type that is in the file being imported and a previously created template for that type.

There also may be situations where you do not want any of the template rules you selected for this Import Definition to be applied to some category of the records being imported, such as Personnel records with a Disabled flag. In this case, you need to configure an item to “Ignore the Templates” by leaving the **Select Object** field blank.

To Select a Template Rule

1. Create or modify an Import Definition. See Creating an Import Definition on Page 47 or Modifying a Data Import on Page 71.
2. On the **Data Import Editor**, click the **Templates** tab to open (see Figure 36 on Page 127).
3. Click **Add**. The system opens the **Import Template Form Editor**, looking as shown in Figure 38 on Page 128.
4. Click ... in the **Template Name** field. The system opens the **Dynamic Selection** dialog box, as shown in Figure 39 on Page 132.

Figure 39: Dynamic Selection Dialog Box



5. Click ... in the **Select Type** field to open a selection list of the types of top-level Objects found in the sample input selected for this Import Definition, and then click to select an Object type.

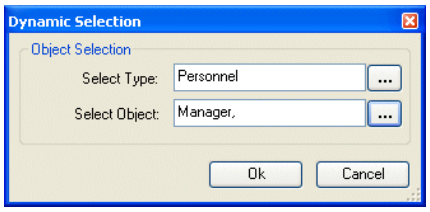
   Example:

   Personnel

   The Object Type you selected is entered in the field.

6. Click ... in the **Select Object** field to open a selection list of the templates in the system for the Object type just selected and click to select a template as a rule.

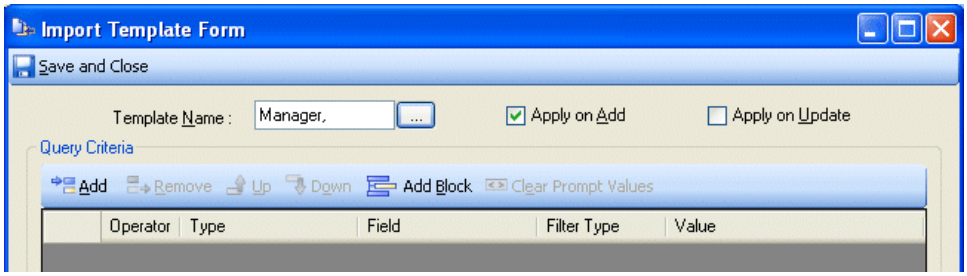
   The **Dynamic Selection** dialog box reappears looking as follows:



— Right-click ... in the **Select Object** field and select **Edit** to open the Editor for the Selected template if you want to review/modify it.

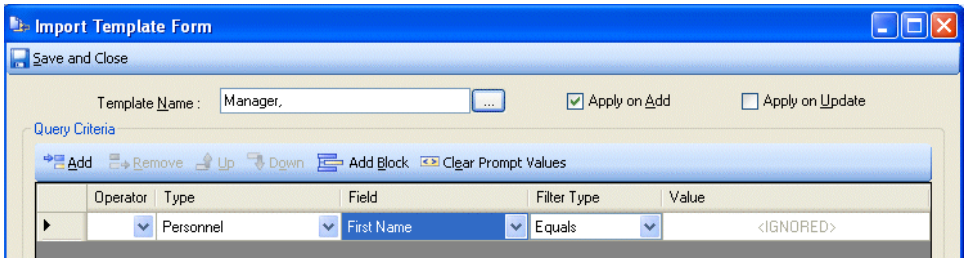
7. Click **OK**. The system enters the Template you selected in the **Template Name** field on the **Import Template Form Editor**, as shown in Figure 40 on Page 133.

Figure 40: Import Template Form Editor with Template Rule Selected



8. Click **Add**. The system enters a new row in the **Query Criteria** box for you to define a query for the selected template rule (described in Configuring a Query Expression for a Template Rule on Page 134). The Editor looks as shown in Figure 41 on Page 133.

Figure 41: Import Template Form Editor – Undefined Query Row

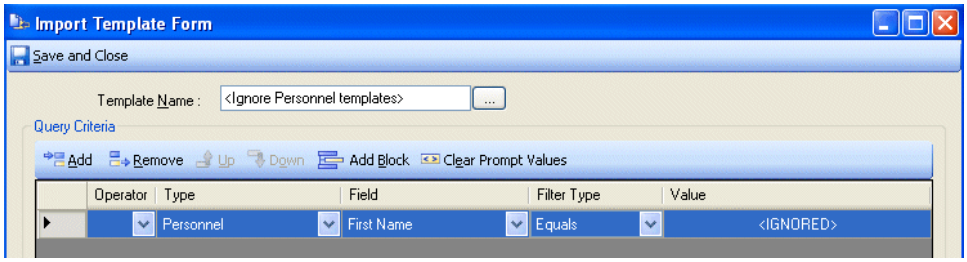


To Ignore a Template Rule

1. Follow Step 3 through Step 5 in To Select a Template Rule on Page 132 to select a top-level Object type.
2. Click **OK** without selecting a template for the **Select Object** field.

   The **Import Template Form Editor** reappears with <Ignore Personnel templates> entered in the **Template Name** field.
3. Click **Add**. The system enters a new row in the **Query Criteria** box for you to define a query for ignoring the template rule. The Editor looks as shown in Figure 42 on Page 134.

Figure 42: Import Template Form Editor – Ignoring a Template Rule



Configuring a Query Expression for a Template Rule

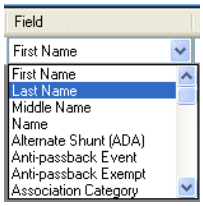
Since the query expression you create will be applied to data being imported, the following is true:

- The system has already entered the value in the Type column of the query expression—the top-level type selected in Step 5 of the procedure, To Select a Template Rule on Page 132.
- The list of fields available for building the query is limited to the fields in the user-defined sample input.
- If a field used in the query is included in the sample input but **not** included in the data being imported, the expression row with that field is evaluated as false.

For detailed information on querying, see the *C•CURE 9000 Data Views Guide*.

To Configure the Query Expression

1. On the **Import Template Form Editor**, as shown in Figure 41 on Page 133, with a Query Criteria row added, pick the field to query by clicking the down-arrow and selecting from the drop-down list.



Example:

Select **Text3**—the Personnel field containing the Personnel type (role) information.

2. Select a **Filter Type**, depending on the type of field you chose.

Example:

Leave the default entry ‘Equals’.

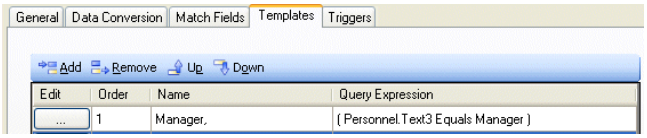
3. For the **Value** field, enter or select a value. (If a value is not entered, the line is ignored during query evaluation.)

Example:

Enter ‘Manager’.

4. Click **Save and Close**. The **Templates** tab re-appears with row 1 added containing the selected template and its related query expression, as shown in the example in Figure 43 on Page 135.

Figure 43: Data Import Editor - Templates Tab with Template Rule Selected



Configuring Multiple Template Rules for this Import Definition

You might want a template from a set of templates to be applied to the Imported Objects during the import operation.

Example:

You are using templates for Personnel types (roles) such as Contractors, Employees, and Managers to add clearances to their records or update them.

To Configure Multiple Template Rules to be Evaluated/Used by the Import

1. Repeat the steps in the procedures Selecting a Template Rule for an Import on Page 132 and/or To Ignore a Template Rule on Page 133.
2. Repeat the steps in the procedure To Configure the Query Expression on Page 134 for each template rule you select.
3. Repeat the preceding steps as many times as times as you need. The Templates tab will appear as shown in the example in Figure 37 on Page 127.

Importing Operator Privileges with Templates

You can use the Templates tab of the Data Import object to import privileges to Operators. Define a Data Import Object to use a chosen field of the Operator (for example: Description) to indicate whether to apply a template when importing, and which template to apply. When you use a template in this manner to create or update Operators, the Privileges in the template are applied to the Operator.

Order for Operator Updates

When you are updating Operators with the template:

1. the existing Privileges for that Operator are removed
2. the Privileges from the Template are applied
3. finally, any privileges added in the XML are applied

For more information, see How Template Rules Work in Importing on Page 138.

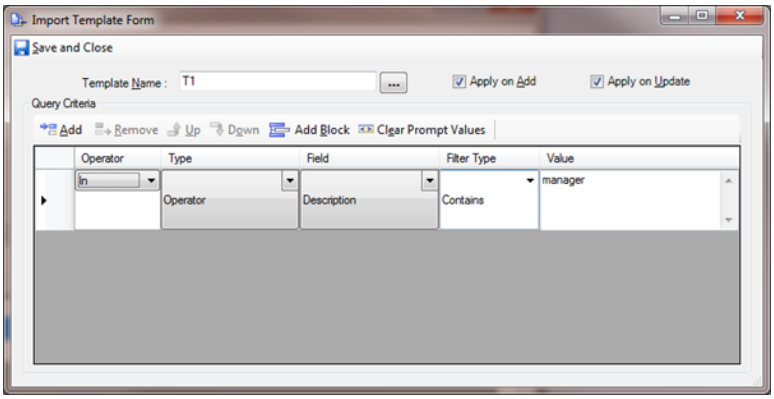
The **Templates** tab is shown in Figure 44 on Page 136.

Example:

Operator templates T1 and T2 have been created. T1 has privileges for managers and T2 has privileges that are at a lower level.

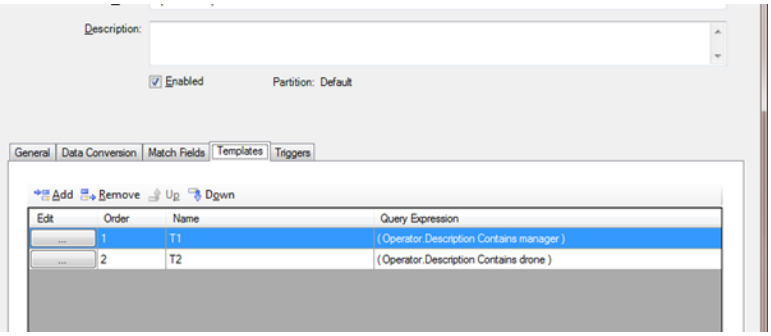
Create the data import with two entries on the Template tab that link the Description field in the imported XML to the appropriate templates. (If the Description field is “manager”, Template T1 is used, and if it is ‘done’, Template T2 is used. The linkages are created by using “Add”, then clicking on ... to define the linkage. See Figure 44 on Page 136

Figure 44: Adding the Linkage to the Templates Tab



Check the **Apply on Add** and/or **Apply on Update** check boxes so that the Template is applied. Click Save and Close. The result is displayed in

Figure 45: Template Tab Linkages Between Description and Templates



When you apply the templates:

1. the Description value in the XML is applied to the Operator
2. the existing Privileges are removed from the Operator
3. the Privileges in the template are added
4. finally, any Privileges in the XML are added

NOTE In an update operation, the template gets applied only if the “Description” field has changed, resulting in the name of a different template.

How Template Rules Work in Importing

When an object is being imported into the system, the Import Definition does the following:

1. Examines the template rules in the list in the specified order.
2. Finds the first line with a query expression whose criteria match the imported data.
3. Applies the template defined by the matched template rule to the object, or skips this step if <Ignore 'type' templates> is configured for this template rule.
4. Applies properties from the external Import source.

NOTE

The Import process only applies template rules once the following has been accomplished:

- Data Conversion – data has been converted so fields from the source file/record are mapped to the C•CURE 9000 fields.
- Field Matching (for Update Import Modes) – fields have been matched, so a matched record from the C•CURE 9000 database has been found (if any exist).

Applying Template Rules During an Import

The way Template Rules apply when you are creating a new object differs from when you are updating an existing object.

Applying Template Rules When Creating New Objects

When data in the imported source matches one of the template rules in the list on the **Templates** tab and no object in the database matches the imported object (or the Add import mode is used), the system operates as follows:

1. Uses the template data to create a new object of the specified type, populating all its fields from this template— including all child objects specified in the template.
2. Copies all the data from the imported record into the new object created from the template in the previous step. This includes updating any child objects created by the template with any child objects being imported.

   Example:

   Clearances

NOTE

If the object being imported contains child objects and template rules are used, Step 2 behaves as an update operation even if a new object is being created: Matching fields must be specified for all child objects being imported even if the import mode is set to 'Add only'.

If you do not specify a matching criteria for a child object being imported when a template rule is used in the Add operation, an error message is generated for that particular object.

3. Adds the newly created record to the C•CURE 9000 database with data combined from the template and the incoming source record.

Applying Template Rules When Updating Existing Objects

NOTE Template rules can be applied during **Import Update** operations solely for **Personnel** records.

When data in the imported source matches one of the template rules in the list on the **Templates** tab and a **Personnel** object in the C•CURE 9000 database matches the imported object, the system operates as follows:

1. Verifies whether or not the template that matches the object being imported differs from the template last used to create (or update) the Matched Personnel object in the database.
   - If the newly matched template is the same as the template used last time, the template is ignored (even if the template's current content differs from the content stored in the database).

     Example:

     The newly matched template is the **Manager** Template and the same as the **Manager** Template that created the Matched Personnel object in the database.
   - If—and only if—the newly matched template is different from the template used last time to create or modify the Personnel object does the following occur:
     - All clearances of the existing Personnel object are deleted.
     - The new clearance list from the newly matched template is assigned.
     - All the other fields in the newly matched template (as well as the Credential records and Images) are ignored.

     Example:

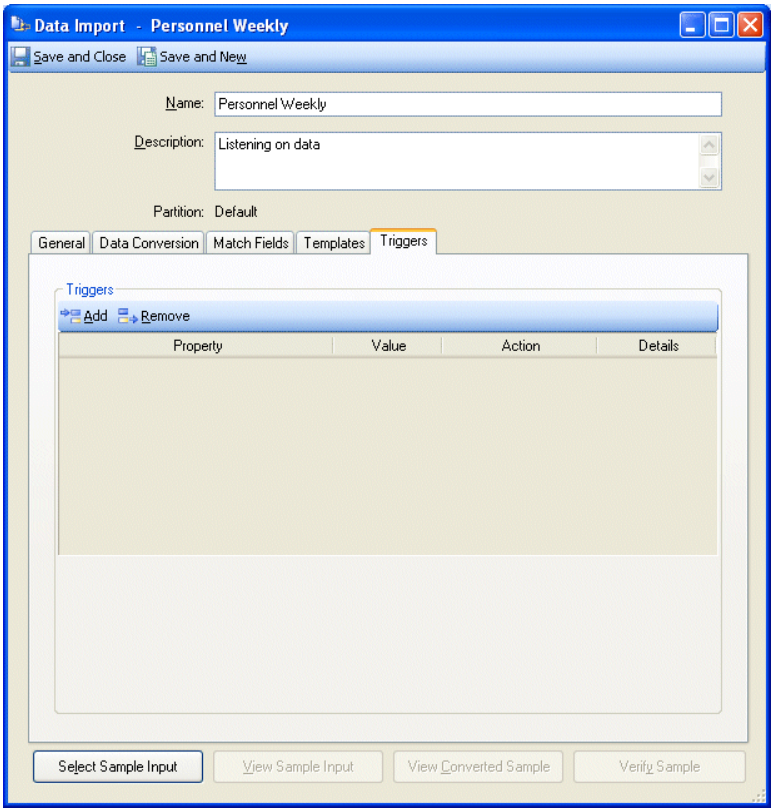
     The newly matched template is the **Engineer** Template and different from the **Manager** Template that created the Matched Personnel object in the database.

     So **Clearances** 01, 03, and 05 (all the clearances assigned to that Personnel record) are deleted from the record in the database, while **Clearances** 02, 07, 08, and 09 are added to the **Personnel** record for the **Engineer** Template.
2. Once the newly matched template is applied (or ignored), the properties from the incoming **Personnel** record (including **Clearances**, if any) are copied over the properties in the existing record and the modified record is saved in the database.

Data Import Triggers Tab

The **Triggers** tab, shown in Figure 46 on Page 140, allows you to set up **Triggers**, configured procedures used by C•CURE 9000 to activate specific actions when a particular predefined condition occurs.

Figure 46: Data Import Editor - Triggers Tab



The tab contains one action, **Activate Event**, that can be linked to a specific Data Import **Status** value and to any event configured in the system. Once the Import's status matches one of these values, the linked **Activate Event** action is triggered and the user-specified event is set to an active state (if allowed by the event, which should be armed at the time). Typically you would use the activated event to send messages to a security guard or administrator when an import has a particular status, such as 'Disconnected' or 'Connectivity Error.' For a list of possible status values and their descriptions, see Data Import Status on Page 70.

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

For more information see:

- Triggers Tab Definitions on Page 140
- Triggers Tab Buttons on Page 141
- Triggers Tab Tasks on Page 142

Triggers Tab Definitions

The **Triggers** tab has the fields described in Table 32 on Page 141.

Table 32: Data Import Triggers Tab Fields

Field	Description
Property	Click in the **Property** field to display ..., and then click this button to select **Status** as the property (the only one available).
Value	Click the down-arrow to select a value from the drop-down list. When the Import's **Status** property matches this value, the event you specify in the **Event** field is activated. For a detailed list of possible status values, see Data Import Status on Page 70. NOTE: The value **Disabled** is not available on this drop-down list for activating an Event.
Action	Click the down-arrow to select **Activate Event** (the only type available) from the drop-down list. This action will be executed when the value of the Import's status matches that selected in the **Value** field.
Details	The name of the event configured for this row (read-only) is entered by the system once you make a selection in the **Event** field.
Event	Click ... in this field to select the event to be activated if the Status for the current row on the grid has the specified value. NOTE: Switching rows in the grid updates this field with the user-selected event so that each row can have its own event to activate.

Triggers Tab Buttons

Table 33 on Page 141 describes the buttons on the **Triggers** tab.

Table 33: Data Import Triggers Tab Buttons

Button	Description
Add	Click this button to create a new row in the Triggers grid. You have to configure all the fields in the row and select an Event to complete the Add operation.
Remove	Click this button to remove a selected row from the Triggers grid.

Triggers Tab Tasks

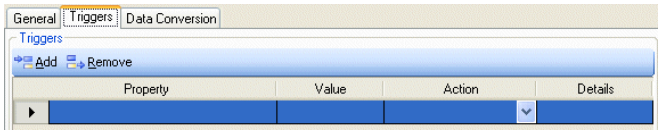
You use the Triggers tab to accomplish the tasks listed below, needed to configure a Data Import object. The procedural steps for each task are detailed in the following subsections.

Configuring Triggers for Data Imports

You can create as many triggers as you wish for any Import Definition.

To Configure Import Triggers

1. Create or modify a Import Definition. See Creating an Import Definition on Page 47 or Modifying a Data Import on Page 71.
2. On the **Data Import Editor**, click the **Triggers** tab to open.
3. Click **Add** to create a new trigger row, as shown in the following figure.



   a. Click in the **Property** field to display [...] and click this button.

      The **Property** selection list opens with one available property, **Status**.

   b. Click **Status** to add it to the row.

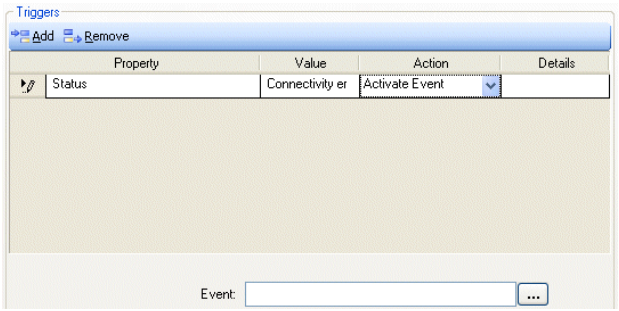
   c. Click the down-arrow in the **Value** field to display a drop-down list of values for the Import's status. Click the **Value** you want to activate the event for this trigger to add it to the row.

      Example:

      Connectivity Error

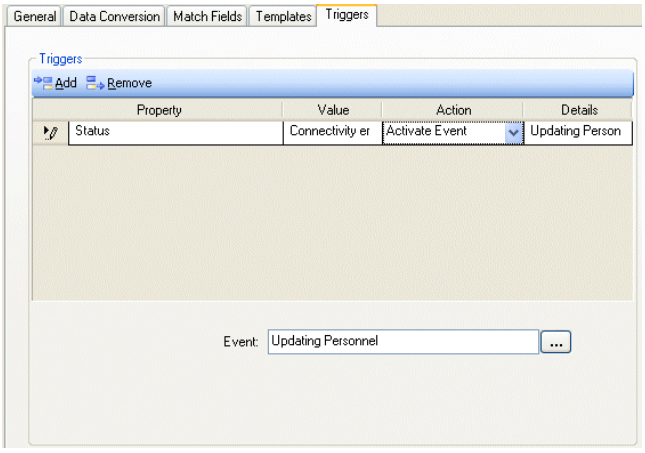
   d. Click the down-arrow in the **Action** field to display a drop-down list containing **Activate Event** as the only available action. Click **Activate Event** to add it to the row as the action that will be executed when the Import's status matches that selected in the **Value** field.

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



4. Click [...] in the **Event** field to display a selection list of all events currently configured in the C•CURE 9000 system, and then click an event to select it. This event will be activated whenever the **Status** for the current row on the grid matches the value specified in that row.

The system enters the name of the Event you select in the **Details** field for the row when you click anywhere outside the **Event** field. The tab now appears.



5. To create more triggers for this Import Definition, repeat Steps 3 through 4 for each trigger you want.

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

Deleting a Trigger from a Data Import

To Delete a Data Import Trigger

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

4

LDAP Data Import

C•CURE 9000 allows you to perform automatic reads from a Lightweight Directory Access Protocol (LDAP) data source to import personnel data directly into the C•CURE 9000 system database. This imported data behaves in the same way as manually entered information.

This chapter provides the background information and configuration procedures specific to LDAP importing. The main documentation for importing data is covered in Chapter 3. It is important that you read the Importing Overview that starts on Page 42 and refer to the following generic importing information and other Chapter 3 information as well as the information in this LDAP chapter:

- Basic Importing Tasks on Page 47
- Data Import Editor on Page 67

In this chapter

LDAP Data Import Overview

C•CURE 9000 supports importing of personnel data from Windows Active Directory or other LDAP servers to the C•CURE 9000 database via LDAP. LDAP Import is a separately licensed feature.

Once configured and set online, the import executes in the background periodically at a user-specified interval. This avoids the need to run the C•CURE 9000 Administration application each time personnel data is to be imported. The import procedure also performs the necessary data validation to prevent corruption of the system personnel table.

LDAP Data Import is configured by using the LDAP Source Configuration Editor on Page 151.

The LDAP import feature is designed to allow connection to any LDAP server. The following LDAP servers are currently supported:

- Oracle 10g - See Oracle LDAP Import Recommendations on Page 160.
- Active Directory 2003
- Active Directory 2008
- Active Directory 2012
- Active Directory 2016
- Active Directory Lightweight Directory Service (AD LDS)
- Active Directory Application Mode (ADAM)

Supported Attribute Types for Active Directory on Page 172 provides a list of the Active Directory Attribute Data Types supported in C•CURE 9000 for LDAP import.

NOTE You can connect to an LDAP server using Secure Sockets Layer (SSL) if you configure your C•CURE 9000 system appropriately. For information, see Connecting the C•CURE 9000 Server to an LDAP Server Using SSL/TLS on Page 173

Benefits of LDAP import include:

- C•CURE 9000 lets you connect to LDAP-compliant data sources including Microsoft® Active Directory for Windows.
- LDAP connection occurs without add-on toolkit or middleware adapter.
- Can retrieve personnel information, credentials, and clearances from external data sources (Windows Active Directory or other LDAP servers) and import information directly into C•CURE 9000 system as new or modified personnel records.
- Customers can link to external directory using an IP address. New employees do not have to wait for long periods of time for all systems to be updated and clearances granted. Updating one database instead of synchronizing multiple systems saves time and costs.
- Supports importing of 100,000 records.
- Can use the Operator Mapping Tool to import operator roles and privilege groups. See Operator Mapping Tool Editor on Page 98.

The LDAP Import allows personnel data to be stored in any desired group of LDAP entries. All data for an individual must be stored in a single LDAP entry. The entries containing personnel data of interest are initially selected from the LDAP directory tree by using a base Distinguished Name (DN) and LDAP search filters.

Use of the LDAP Import feature requires a basic understanding of LDAP, including the DN and search filter syntax, as well as the LDAP server's configuration.

LDAP Import depends on a method for finding records that have changed, since only revised records are imported once the initial import has taken place. Selecting a different method may modify the behavior of the import process.

NOTE If a field in the LDAP database is set to the unknown (not set) value, that value is ignored and not imported at all. Whatever value the field already has in the C•CURE 9000 record being updated is left unmodified.

If the import is creating a new C•CURE 9000 record, fields set to the unknown value in LDAP are left at the default value for the C•CURE 9000 field to which the LDAP field is mapped.

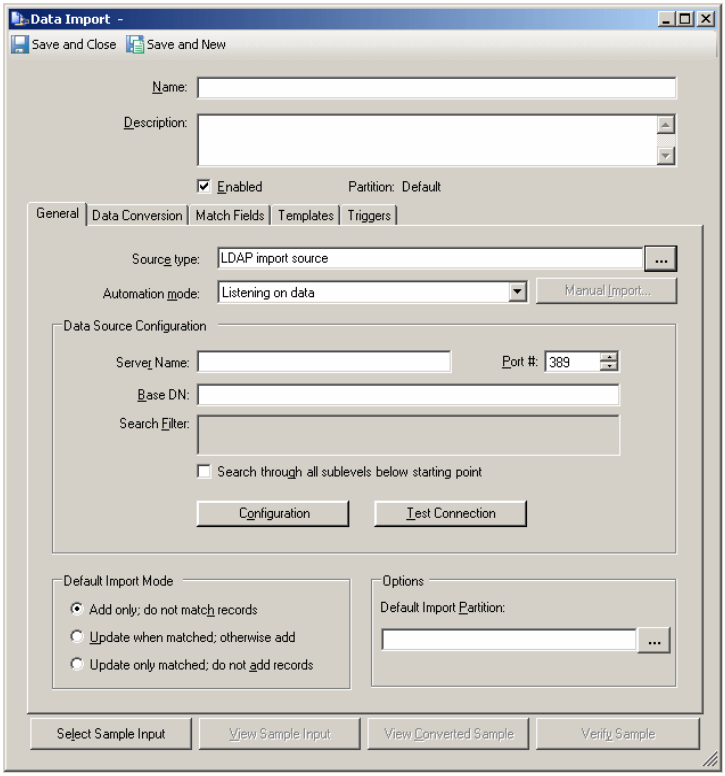
Import Editor General Tab for LDAP

The **General** tab, as shown in Figure 4 on Page 74 in the way in which it displays when you first open it, is used to define the information described in Table 34 on Page 147 specifically for the LDAP Import Definition.

Once you have selected **LDAP import source** in the **Source type** field, two actions occur:

- The **Data Import Configuration General** tab changes, as shown in Figure 47 on Page 147.
- The **LDAP Source Configuration** Editor opens, (see LDAP Source Configuration Authentication Tab on Page 151).

Figure 47: Data Import Editor – General Tab for an LDAP Import



General Tab Definitions for LDAP

For LDAP, the **Data Import General** tab displays the fields and buttons described in Table 34 on Page 147.

Table 34: LDAP Data Import General Tab Definitions

Fields/Buttons	Description
Name	The name of the Import definition. This field is required.
Description	A description of the LDAP Import definition. This field is not required, but if used can make it easier to identify the specific Import definition when you are using it later on.
Enabled	Select this check box to make the Import Definition operational. (The default is selected.)
Partition	A read-only field displaying the Partition to which this Import Definition belongs. (This field is visible only if the C•CURE 9000 system is partitioned.)
General Tab	

LDAP Data Import General Tab Definitions (continued)

Fields/Buttons	Description
Source Type	Click ... to select the LDAP import source from the drop-down list. (The supported types are CSV file, LDAP, ODBC, or XML file.) Once LDAP is selected, the system enters **Listening on data** in the **Automation Mode** field, makes the **Manual Import** button unavailable, and changes the parameters in the **Data Source Configuration** box. NOTE: The LDAP source type is available only if the license for this feature has been validated.
Automation Mode	**Listening on data** is automatically entered as the only mode for LDAP imports. The import source object is initialized by the Import Watcher server component and starts listening for external events. When an external event is received, the import source initiates import of the received data. This is the only mode supported for LDAP Data Import.
Manual Import	**Not** available for LDAP Data Import.
Data source Configuration Box (These are the parameters for the LDAP import source. The values for the LDAP entries are filled in after you complete the entries on the tabs of the **LDAP Source Configuration** dialog box.)	
LDAP Server Name	Valid DSN name or IP Address of the server that runs the targeted LDAP database. This is a required field.
Port #	Number of the port dedicated to communicate with the remote LDAP database. The default value is 389, unless you are connecting to an LDAP server using SSL—in which case the default value is 636.
Base DN	A valid LDAP distinguished name that identifies an object in the LDAP tree containing objects to be imported into the C•CURE 9000 database. Only child objects of the specified node are targeted for import. This is a required field.
Search Filter	This read-only field shows the search filter used for selecting LDAP records. The filter is a combination of the entries in the **Class(es)** list and the **Search Filter** box, both configured in the **LDAP Source Configuration Search** tab.
Search through all sub-levels below starting point	Select this option to indicate that the object specified in the Base DN field plus all the containers in this object be imported into C•CURE 9000. If this option is **not** selected, the containers are not searched and only objects directly owned by the Base DN object are imported.
Configuration	Click this button to open the **LDAP Source Configuration** Editor to continue configuring or to edit the parameters for the LDAP server connection. NOTE: This dialog box opens automatically when you first select LDAP as the source type on this **General** tab.
Test Connection	Click this button to check the specified LDAP server with the current authentication credentials to verify that the remote server runs LDAP and allows the C•CURE 9000 server to connect to the LDAP server.
Default Data Import Mode (**Update when matched, otherwise add** is the only valid import mode for LDAP.)	
Add only; do not match records	**Not** valid for LDAP Data Import. If you select this option, the Import Definition cannot be saved and an error displays.

LDAP Data Import General Tab Definitions (continued)

Fields/Buttons	Description
Update when matched, otherwise add	Select this import rule option to perform matching as follows: • If the import source contains records with match field values that exactly match those field's values in existing records in C•CURE 9000, the records in C•CURE 9000 are updated using imported records. • If C•CURE 9000 does not contain records that exactly match those being imported from the source, the import adds the non-matching records to C•CURE 9000. Selecting this option requires specifying matching fields on the **Match Fields** Tab. See Data Import Match Fields Tab on Page 120 and Match Fields Tab Tasks on Page 123.
Update only matched: do not add records	**Not** valid for LDAP Data Import. If you select this option, the Import Definition cannot be saved and an error displays.
Options Box	
Default Import Partition	Click … to select the Partition in which to place newly imported records when the external records do not include a reference to any C•CURE 9000 partition. (This field is available **only** if the C•CURE 9000 system is partitioned.) Software House recommends that you select a Partition for automated imports to avoid confusion. NOTE: • If this field is left blank in a partitioned system and the records being imported do not refer to any Partition, the Import process will place the files in the 'Default' Partition'. • If the Partition referenced by an Import Definition is deleted from the system, you cannot run the import. The Import Definition cannot be used until you edit it and select another Partition. • The Partition can **only** be updated for a record when it is referenced in the external file, not by its entry in this field.
Buttons	**Description**
Select Sample Input	Click this button to open the **Select Sample Records** dialog box (see Figure 55 on Page 167) that allows you to choose records from the LDAP server. This dialog box includes the same search filter and object classes originally selected in the **Search** tab (see LDAP Source Configuration Search Tab on Page 154). You can use this dialog box to do the following—if necessary for selecting a subset of records that include all the properties designated for import into the C•CURE 9000 database: • Modify the filter to limit/expand which records are selected. • Increase the default number of scanned sample records. The selected sample records should have the same classes and properties to be used later during the import (through the configured Import Definition), though not necessarily the same data. Once you click **OK** in the **Select Sample Records** dialog box, the system reads selected records from LDAP, converts their data into an XML document, and parses the document—stripping off duplicate information, but keeping the structure of the document, **Example:** If 100 Personnel records are selected, the structure will contain a single personnel record, including all the fields defined by the parsed 100 records. NOTE: If you click **Save** in the **Select Sample Records** dialog box, the LDAP Import Definition (in the **LDAP Source Configuration Search**) is updated to reflect changes you made in this dialog box. So unless you actually wish to save your changes here, be sure to simply click **OK**.
View Sample Input	Click this button to open a form with an XML document that represents the structure generated by the system while parsing the sample input records received from the LDAP server. NOTE: This button is unavailable if a sample input has **not** been selected.

LDAP Data Import General Tab Definitions (continued)

Fields/Buttons	Description
View Converted Sample	Click this button to open a form with the XML document that represents the result of the data conversion applied to the selected sample input (configured on the **Data Conversion** tab). NOTE: This button is unavailable if a sample input has **not** been selected or if the list of converters is empty.
Verify Sample Input	Click this button to take the selected sample input converted by the chain of import converters (if any) and verify that each field and each object type in the resulting XML document can be recognized by C•CURE 9000. If the verification fails, the system informs you and suggests creating a proper data conversion. If only some of the fields cannot be recognized by the system, the system can show those fields in a form of XML document. NOTE: This button is unavailable if a sample input has **not** been selected.
Save and Close	Click this button when you have completed any changes to the Import Definition and wish to save those changes. The Import Definition closes.
Save and New	Click this button when you have completed any changes to the Import Definition and wish to save those changes and also create a new Import Definition. The Import Definition that you were editing is saved, and a new Import Definition opens (either blank or including template information if you were using a template to create new Import definitions).
NOTE: When you click **Save...**, the system performs the final validation of the LDAP Import Definition which requires connecting to the specified LDAP Server. If the LDAP server is offline or the Validation cannot be completed for some other reason, you can save the LDAP Import Definition by clearing the **Enabled** check box at the top of the Editor	

LDAP Source Configuration Editor

This Editor opens the first time you select the **LDAP import source** in the Source type field on the General tab of the Data Import editor (see Data Import Editor on Page 67).

To open the LDAP Source Configuration editor subsequently, click the **Configuration** button displayed in the Data Source Configuration box for an LDAP Import, as shown in Import Editor General Tab for LDAP on Page 147.

This Editor allows you to configure the data source for an LDAP import and the parameters required to connect to the LDAP server.

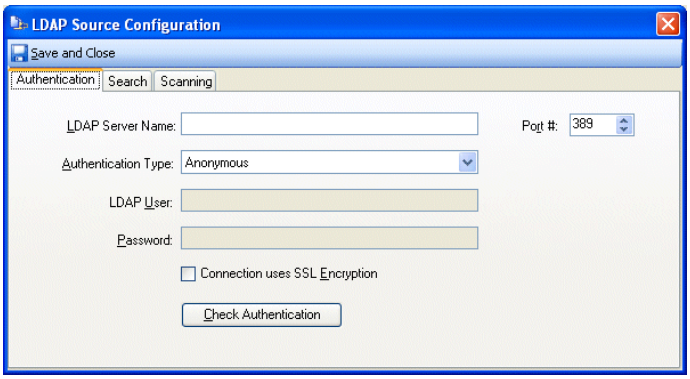
The Editor has the following tabs:

- LDAP Source Configuration Authentication Tab on Page 151
- LDAP Source Configuration Search Tab on Page 154
- LDAP Source Configuration Scanning Tab on Page 160

LDAP Source Configuration Authentication Tab

The **Authentication** tab, as shown in Figure 48 on Page 151, names the LDAP server to which you are connecting and the method by which the connection is authenticated. This tab also provides a means to check the Authentication.

Figure 48: LDAP Source Configuration Editor – Authentication Tab



Authentication Tab Definitions

The **Authentication** tab has the fields and buttons described in Table 35 on Page 151.

Table 35: LDAP Source Configuration Authentication Tab Definitions

Fields/Buttons	Description
LDAP Server Name	Valid DNS name or computer name must be used for the LDAP server name if Kerberos is used (FQDN is preferred). IP address can be used if Microsoft Negotiate is used.
Port #	Number of the port dedicated to communicate with the remote LDAP database. The default value is 389, unless you are connecting to an LDAP server using SSL/TLS—in which case the default value is 636.

Table 35: LDAP Source Configuration Authentication Tab Definitions (continued)

Fields/Buttons	Description
Authentication Type	Select the method by which the connection to the LDAP server is authenticated from the four supported modes: • **Basic** – requires specifying user name and password. User name and password is sent as clear text unless SSL/TLS is used. • **Anonymous** – assumes the LDAP database is configured to accept remote users without any authentication. • **Kerberos**- uses Kerboros protocol to send password in an encrypted form. If user name and password are omitted, it uses the user name and password used to run the C•CURE 9000 Windows services. • **Microsoft Negotiate**- uses Microsoft Negotiate protocol to send password in an encrypted form. If user name and password are omitted, it uses the user name and password used to run the C•CURE 9000 Windows services.
LDAP User	NOTE: This field is available only if you are using the **Basic**, **Kerberos** or **Microsoft Negotiate** Authentication Types. Name of the user for establishing connection between C•CURE 9000 and the remote LDAP server. This is the User ID assigned to the LDAP User by the LDAP server administrator and should have sufficient privileges to read data to be imported from the LDAP server. If you are not using an Active directory LDAP server, this name is a distinguished LDAP object name of a user record with permission to access the LDAP database. **Example:** CN=User,OU=AdamUsers,DC=SWH,DC=Com If you are connecting to an Active Directory LDAP server, the user name should be in the Microsoft "User Principal" form. The associated user must have permission to access the parts of the LDAP database needed for the import. **Example:** JohnDoe@domainName.com
Password	NOTE: This field is available only if you are using the **Basic**, **Kerberos** or **Microsoft Negotiate** Authentication Types. The password assigned to the LDAP user specified in the previous field by the LDAP server administrator. The password is stored in an encrypted form in the database and is decrypted when the LDAP Import object is loaded into memory.
Connection uses SSL Encryption	Select this option to indicate that any communication between the LDAP server and the C•CURE 9000 system should be encrypted using an SSL/TLS certificate installed on the C•CURE 9000 server running the Import Watcher service. Before this option can be used, the system administrator must configure the certificate appropriately. For further information, see Connecting the C•CURE 9000 Server to an LDAP Server Using SSL/TLS on Page 173.
Check Authentication	Click this button to connect to the remote LDAP server to verify that it accepts the credentials specified in this tab.
Save and Close	Click this button when you have completed any changes to the **Authentication**, **Search**, and/or **Scanning** tabs and wish to save those changes. The tab closes and the **Data Import Editor General** tab reappears.

Authentication Tab Tasks

Configuring the Authentication Tab

To Configure the Authentication Tab

1. In the **LDAP Server Name** field, enter either a valid DNS name or an IP Address of the server operating the targeted LDAP database (see Figure 48 on Page 151). This is a required field.
2. Check the **Port #** (number) assignment for connecting to the remote LDAP database:
   - Default value – **389**, generally
   - Default value – **636**, if you are using SSL to connect to the LDAP server

   See Connecting the C•CURE 9000 Server to an LDAP Server Using SSL/TLS on Page 173 for more information.

3. In the **Authentication Type** field, click the down-arrow to display the list of modes for authenticating the connection to the LDAP server:
   - **Basic** requires specifying user name and password. User name and password is sent as clear text unless SSL/TLS is used.
   - **Kerberos** uses Kerboros protocol to send password in an encrypted form. If user name and password are omitted, it uses the user name and password used to run the C•CURE 9000 Windows services.
   - **Microsoft Negotiate** uses Microsoft Negotiate protocol to send password in an encrypted form. If user name and password are omitted, it uses the user name and password used to run the C•CURE 9000 Windows services.
   - **Anonymous** assumes the LDAP database is configured to accept remote users without any authentication.

NOTE Using **Anonymous** authentication mode to connect to an LDAP server is usually **not** allowed by LDAP server administrators. It is also possible that an Anonymous connection succeeds, but returns no data. (The return of 'no data' could also happen if the specified user has limited permissions on the LDAP server.)

4. In the **LDAP User** field, enter the User ID assigned to the LDAP user being designated to import data from the LDAP server through the Basic Authentication Type. (This user establishes the connection between C•CURE 9000 and the remote LDAP servers.)

   The name is a distinguished LDAP object name of a user record with permission to access the LDAP database. Different users can see a different subset of the records stored in the LDAP database.

   Example:

   CN=User,OU=AdamUsers,DC=SWH,DC=Com

NOTE This field is not available for LDAP imports using **Anonymous** Authentication.

5. In the **Password** field, enter the password assigned to the LDAP user specified in the preceding **LDAP User** field for LDAP Imports using the Basic Authentication Type. (The Password is stored in an encrypted form in the database and is decrypted when the LDAP Import object is loaded into memory.)

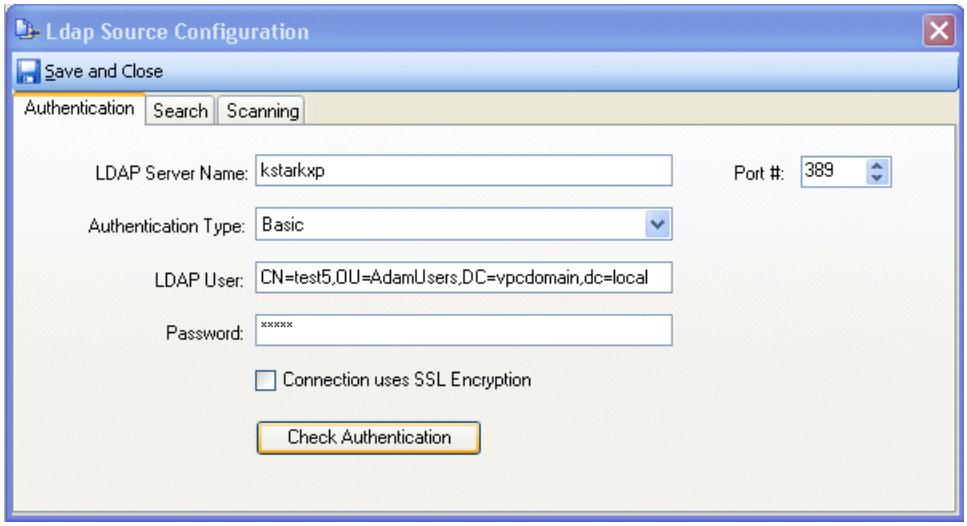
NOTE This field is not available for LDAP imports using **Anonymous** Authentication.

6. Select the **Connection uses SSL Encryption** option to indicate that any communication between the LDAP server and C•CURE 9000 be encrypted using an SSL/TLS certificate installed on the C•CURE 9000 server running the Import Watcher service, or clear the option so SSL/TLS encryption is **not** used.

   For further information, see Connecting the C•CURE 9000 Server to an LDAP Server Using SSL/TLS on Page 173.

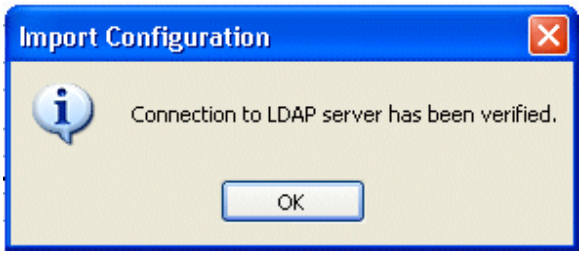
   The completed **Authentication** tab now appears as shown in the example in Figure 49 on Page 154.

Figure 49: LDAP Source Configuration Editor - Authentication Tab Completed



7. To verify that the credentials you specified on this tab are acceptable and allow you to connect to the remote LDAP server, click the **Check Authentication** button. A message box, similar to the following, displays with either success or error information.

NOTE It is possible for other configuration parameters to be improperly set, even though the authentication test is successful.



8. Click **Save and Close** when you have completed any changes to the **Authentication** tab and wish to save those changes. The tab closes and the **Data Import Editor General** tab reappears.

LDAP Source Configuration Search Tab

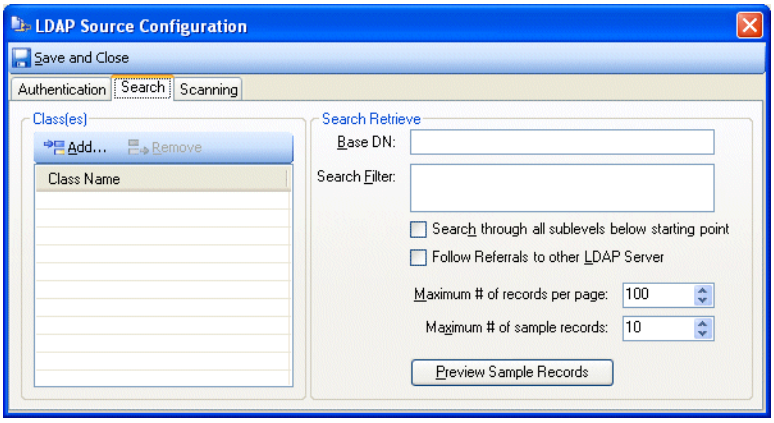
The**Search** tab, as shown in Figure 50 on Page 155, is used to specify parameters that limit the amount of data scanned by the C•CURE 9000 import process in order to:

- Optimize the performance of the data exchange.
- Eliminate LDAP records irrelevant to C•CURE 9000.

NOTE Since some operations available on this tab request information from the remote LDAP database, it should be put online.

In addition, the configuration of this tab can be completed **only** if the parameters on the **Authentication** tab are properly configured. Otherwise you cannot connect to the remote LDAP database.

Figure 50: LDAP Source Configuration Editor – Search Tab



Search Tab Definitions

The **Search** tab has the fields described in Table 36 on Page 155.

Table 36: LDAP Source Configuration - Search Tab Definitions

Fields/Buttons	Description
Class(es)	Use this list box to select object classes from the LDAP server for import. If no Classes are selected, objects of all classes are evaluated for importing. The selected Classes—usually the Class 'user' is selected—are combined with the Search Filter entries and displayed in the **Search Filter** field (read-only) in the **Data Source Configuration** box on the **Data Import General** tab.
Add	Click this button to add an object class from the LDAP server to the **Class(es)** list by selecting it from the list of classes that opens.
Remove	Click this button to remove an object class from the **Class(es)** list.
Base DN	A valid LDAP distinguished name that identifies an object in the LDAP tree containing objects to be imported into the C•CURE 9000 database. Only child objects of the specified node are targeted for import. This is a required field. **Example:** OU=Stuff, DC=Vpdomain, DC=Local
Search Filter	Enter an LDAP Search Filter using valid LDAP search filter syntax. This entry allows you to limit or expand the set of records to be imported from the LDAP server into the C•CURE 9000 database. The maximum length is 1000 characters. **Example:** CountryCode=7 These Search Filter entries are combined with the selected Classes and displayed in the **Search Filter** field (read-only) in the **Data Source Configuration** box on the **Data Import General** tab. NOTE: Using this field requires knowledge of LDAP search filter syntax. If you do not need special filtering, leave this field blank.
Search through all sublevels below starting point	Select this option to indicate that the object specified in the Base DN field plus all the containers in this object be imported into C•CURE 9000. If this option is **not** selected, the containers are not searched and only objects directly owned by the Base DN object are imported.
Follow referrals to other LDAP servers	Select this option to indicate that references to other LDAP servers from this LDAP server, be automatically and transparently resolved. This allows data to be pulled from several LDAP servers. NOTE: This option slows the import and is **not** supported by all server configurations.

Table 36: LDAP Source Configuration - Search Tab Definitions (continued)

Fields/Buttons	Description
Maximum number of records per page	Enter the maximum number of records to return in each page. The Range is 1 to 1000, and the default setting is 100. Returning more records per page is slightly faster, but some LDAP servers have limits on the maximum number of records per page allowed. NOTE: If you are using SSL, the larger the page size, the better the performance. In this case, set the page size as large as possible without incurring LDAP errors.
Maximum number of sample records	Enter the maximum number of records that the C•CURE 9000 server should request when obtaining sample input from the LDAP database. The Range is 1 to 1000, and the default setting is 10. When you use this field in the **Select Sample Records** dialog box, as shown in Figure 55 on Page 167, the first *n* records with all their properties are selected and displayed in the sample records preview, as shown in Previewing Sample Records on Page 158. NOTE: The mapping tools define which properties are available for mapping by examining the content of the records used for the sample (see Personnel Mapping Tool Editor on Page 92). Only the mapped properties are tracked for changes while the LDAP database is being scanned during the import process. Consequently, it is important to make sure that all the properties you want to import are included in the original data sample.
Preview Sample Records	Click this button to retrieve sample LDAP records using values from this tab. (The records retrieved are not actually imported.) The results display in the **Preview Sample Records** dialog box, as shown in Figure 52 on Page 159. Click this button to: • Verify that the values you entered on the tab have good LDAP syntax. • Validate that you are retrieving the records you expected. NOTE: You can increase the maximum number of sample records or change the filter to adjust the results.

Search Tab Tasks

Configuring the Search Tab

To Configure the Search Tab

1. In the **LDAP Source Configuration** dialog box, shown in Figure 48 on Page 151, click the **Search** tab. The tab opens, as shown in Figure 50 on Page 155.
2. The **Class**(**es**) list box allows you to select object classes from the LDAP server for importing. Click **Add** to add classes and **Remove** to delete those that you selected from the list. The use of Classes allows you to limit the Objects selected from LDAP for importing.

   Example:

   'user' is a typical LDAP Class that can be imported into the C•CURE 9000 and converted into **Personnel** records.

   The selected Classes are combined with your Search Filter entries and displayed in the **Search Filter** field (read-only) in the **Data Source Configuration** box on the **Data Import General** tab.
3. Enter the following information in the **Search Retrieve** box to set the search and retrieval methods.
   a. In the **Base DN** field, enter the distinguished name (full path in LDAP syntax) to the location in the LDAP directory where you want the search to begin for records to import into C•CURE 9000.

      Records found beneath this point in the directory are candidates for importing into the C•CURE 9000 database.

      Example:

If you want to retrieve all users in the Houston subfolder of the US folder and the Domain name is test.com then enter the DN as:

OU=Houston, OU=US, DC=Test, DC=Com

b. In the LDAP **Search Filter** field make an entry, in valid LDAP search filter syntax, to:

- Limit or expand which fields are imported.
- Select a subset of records including all the properties designated to be imported into the C•CURE 9000 database.

This field can also include an expression for limiting results to the structural classes you have specified in the **Class(es)** list on this tab.

Example:

- If the search filter “(CN=Te*)” is used, only records with a common name starting with “Te” are considered for importing into the C•CURE 9000 database.
- If the search filter “(1(sn=*a) (sn=Smith))” is used, records with a last name (surname) either ending in “a” or with the value “Smith” are considered for importing into the C•CURE 9000 database.

c. Select the **Search through all sublevels below starting point** option to indicate that all sublevels below the distinguished name specified in the **Base DN** field are scanned for records to import into C•CURE 9000; or clear this option so only records that are immediate subsets of the specified **Base DN** record are scanned.

d. Select the **Follow referrals to other LDAP servers** option to indicate that references from this LDAP server to other LDAP servers are automatically and transparently resolved.

NOTE While this action allows data to be pulled from several LDAP servers, it slows the import, and is **not** supported by all server configurations.

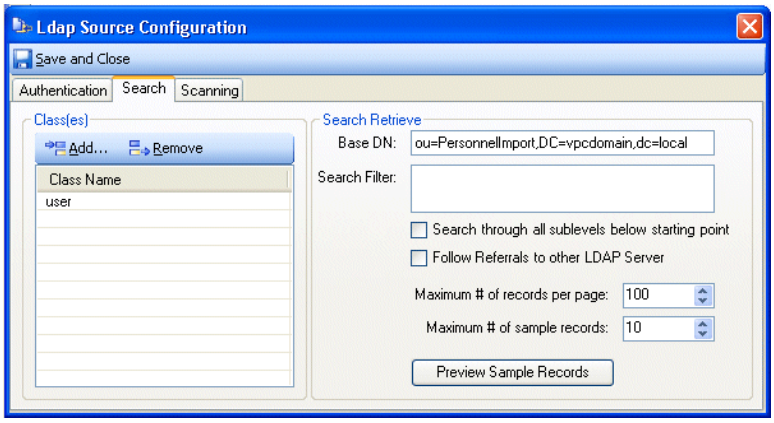
e. In the **Maximum number of records per page** field enter the maximum number of records to return in each page.

- Returning more records per page is slightly faster, but some LDAP servers limit the maximum number of records allowed per page.
- If you are using SSL, the larger the page size, the better the performance. Set the page size as large as you can without incurring LDAP errors.

f. In the **Maximum number of sample records** field enter the maximum number of records for C•CURE 9000 to request when obtaining sample input from the LDAP database.

The completed **Search** tab appears as shown in Figure 51 on Page 158.

Figure 51: LDAP Source Configuration Editor – Search Tab Completed



4. Click **Save and Close** when you have completed any changes to the **Search** tab and wish to save those changes. The tab closes and the **Data Import Editor General** tab reappears.

Previewing Sample Records

Previewing sample records allows you to:

- Verify that the values you entered on the tab have good LDAP syntax.
- Validate that you are retrieving the records you expected.

All parameters on the **Authentication** and **Search** tabs must be correctly configured for the Preview action to be successful in retrieving samples.

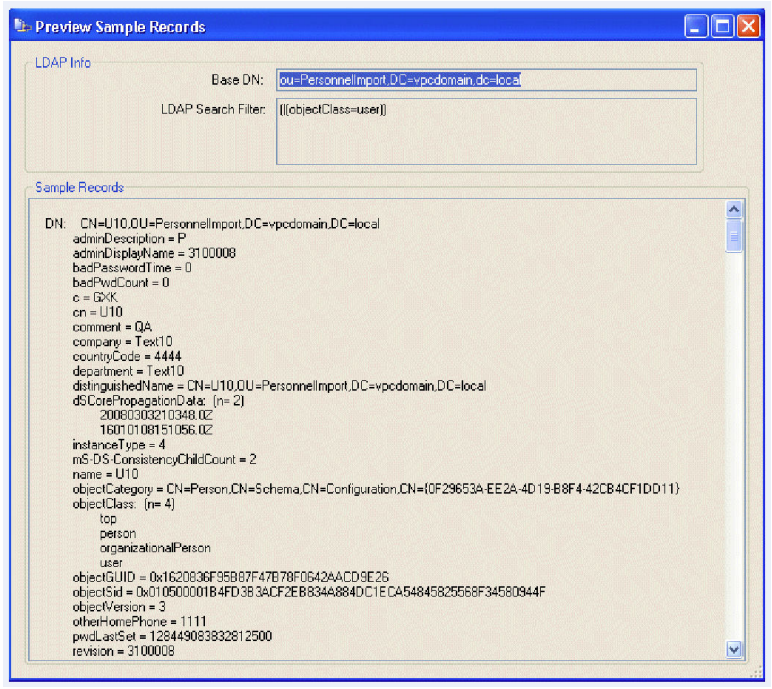
NOTE Software House strongly recommends that you use the **Preview Sample Records** option after any change to the **Search** tab entries.

To Preview Sample LDAP Records

1. To retrieve sample records, click the **Preview Sample Records** button on the **Search** tab.

   The system uses the values you specified on this tab and displays the results in the Preview Sample Records dialog box, as shown in the example in Figure 52 on Page 159.

Figure 52: Preview Sample Records Dialog Box



NOTE Information such as that shown in the sample in Figure 52 on Page 159 indicates that no errors were encountered. If the dialog box is blank, it could mean either of the following:

- The specified LDAP user does **not** have permissions to see records in the specified Base DN.
- The search filter is too restricted.

The **Preview Sample Records** dialog box includes the following information:

- Location of the sample records.
- Search filter used to retrieve the records.
  - Expression for limiting results to the structural classes specified in the **Class(es)** list on the **Search** tab.

The information can be Interpreted as follows:

- The **Base DN** is the Distinguished name selected in the **Search** tab.
- The **LDAP Search Filter** listed is a read-only field displaying the search filter used to select the LDAP records. (It is a combination of the Class list and the Search Filter, both selected either in the **LDAP Source Configuration Search** tab (see Figure 51 on Page 158) or in the **Select Sample Records** dialog box (see Figure 55 on Page 167).
- **Sample Records** box: If the request for the sample data was successful, all retrieved records and their properties are displayed in a scroll-through list.

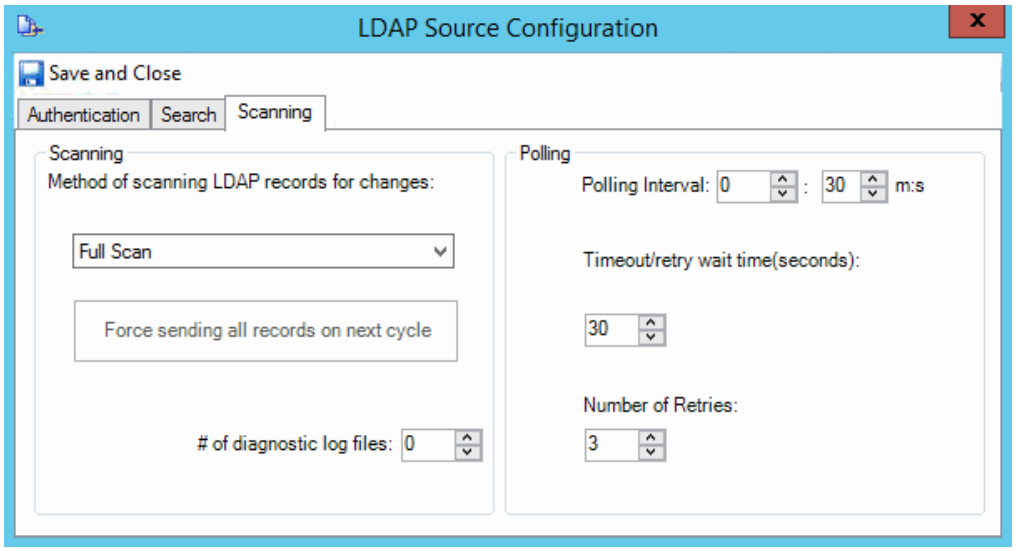
- **Errors** box: If the LDAP server returned an error, error messages display. At a minimum, the messages allow you to tell whether the error was caused by a Base DN, search filter, or authentication problem.

2. Click to close the dialog box.

LDAP Source Configuration Scanning Tab

The **Scanning** tab, as shown in Figure 53 on Page 160, allows you to specify a method to detect changes made to records stored on an LDAP server since the last time the server was checked. This tab specifies parameters that define the way C•CURE 9000 scans the remote LDAP database.

Figure 53: LDAP Source Configuration Editor Scanning tab



Oracle LDAP Import Recommendations

If you are using an Oracle LDAP server to import records into C•CURE 9000, Software House recommends the following (unless you have a 1 GB LAN network and the LDAP server and 9000 server are on the same subnet):

- Change the Oracle LDAP server settings to increase the maximum number of records returned.
- In the Polling box on the LDAP Scanning tab, set the value for the **Before retrying, wait for xx seconds for response** field very high.
  - For 50,000 records, set the value to about 2000 (about 33 minutes).
  - For 100,000 records, set the value to about 4000 (about 66 minutes).
  - For a greater number of records, scale up proportionally.

NOTE

The following conditions apply:

- The maximum number of records you can import is around 250,000.
- Oracle LDAP has a slow import scan performance (30 records/second). This means that if you have 100,000 records, the system can only scan for changes to the records about once/hour--and even less frequently if there are more records.
- With the “retry…” value set so high, certain types of errors will take a very long time to report.

Scanning Methods

For support of a wide range of LDAP servers, the following methods are currently supported to extract changes from the LDAP server:

- **Full Scan Method** – can be used with the widest possible range of LDAP servers. However, it has the slowest performance and puts the most load on the LDAP server. It reads all possible personnel records from LDAP on each cycle, comparing them against a disk copy it has of the records' data, preserved from the last scan. Any records that have changed are sent on to the C•CURE 9000 system. Only properties mapped to C•CURE 9000 properties are received and evaluated.
- **Scan by Microsoft Active Directory Timestamp Method** – uses a timestamp so it can detect which records have changed since the last time it scanned the records. This makes it at least fifty times faster than the Full Scan method. However, this method has restrictions on how deleted records are handled.

Scanning Method Limitations

The following limitations should be considered before selecting a method to use with LDAP.

Full Scan Method

- If more than one entry in LDAP has same matching key, both are updated, but a warning is generated. It is **not** possible to predict which one is processed first; whichever one is processed first is overwritten.
- If you click the **Force sending all records on next cycle** button, the disk file is erased and all knowledge of the existing LDAP records is lost. This means that the next scan will **not** delete any records from the C•CURE 9000 database. There is no way to later ensure that records deleted from the LDAP server, before the forced re-sending is completed, are also deleted in the C•CURE 9000 database.
- If the LDAP server is restored from a backup, a full scan is required to synchronize C•CURE 9000 with the restored LDAP server. Even that may result in records which exist on the C•CURE 9000 server, but **not** on the LDAP server—which is not detected automatically.

Microsoft Active Directory Timestamp Method

- For this method to be used, the LDAP server must keep a timestamp property (attribute in LDAP) for each record, each time it is modified. The LDAP server also needs to allow you to efficiently search only for records changed since a particular timestamp value. For Microsoft Active Directory, the USNChanged attribute satisfies both of these conditions.
- Whenever the LDAP entry changes, even if the change is in a property that is not pertinent, the C•CURE 9000 personnel record is updated.
- If you want LDAP to automatically delete records, you must use the 'objectGUID' property, map it into the GUID field in the target record, and then use the GUID field as your **only** match field. If you do **not** care about LDAP deleting records, you can use any property as your match field. If you want LDAP to automatically delete records but do **not** want to match on GUID, use the Full Scan method instead.

NOTE If you use fields other than 'ObjectGUID' as match fields, whenever you delete an object from LDAP or force a full scan, an error message displays saying that the object is not deleted due to missing match fields.

- If the LDAP server is restored from a backup, a full scan will be required to synchronize the C•CURE 9000 server with the restored LDAP server. Even that may result in records that exist on the C•CURE 9000 server but not on the LDAP server—which is **not** detected automatically.

Microsoft Active Directory Timestamp Method Deleting Limitations

- If an LDAP entry is moved from a part of the directory tree where the LDAP import is looking for it, to another part of the tree **not** in the area of interest to the LDAP server, that LDAP entry will **not** be deleted.

Example:

- The **Base DN** field in the LDAP Import Definition (where the search is to begin) is configured to be: CN=Lexington, CN=users.
- The LDAP entry was previously underneath CN=Lexington, CN=users, but it has now been moved to be under CN=New York, CN=users.
- Even though the LDAP entry will **no longer** be imported, and would **not** be added to a new C•CURE 9000 system, the existing C•CURE 9000 personnel record corresponding to this LDAP entry will **not** be deleted.

- If the **Base DN** field in the LDAP Import Definition is itself changed, any records placed under the old entry, but **not** under the new entry, will **not** be deleted.
- If the **Search Filter** field in the LDAP Import Definition is changed, any records included under the old search criteria, but now excluded, will **not** be deleted.
- If you are including **Computed Fields**, such as MemberOf, the Microsoft Active Directory Timestamp Method will not work correctly because the timestamp will not change when the fields change. If using **Computed Fields**, use the full scan method.

Scanning Tab Definitions

The Scanning tab has the fields and buttons described in Table 37 on Page 162.

Table 37: LDAP Source Configuration - Scanning Tab Definitions

Fields/Buttons	Description
Method of scanning LDAP records for changes	Select the method to use to scan for changes in records stored on an LDAP server: • **Full Scan** – can be applied to all LDAP servers, but is the most time-consuming because it is a full scan. • Microsoft **Active Directory Timestamp** – is the most efficient to use for Active Directory.
Force sending all records on next Cycle	Click this button to have the following take place: • The system deletes all information about the state of records already imported into the C•CURE 9000 system from LDAP • The next scheduled scan through the LDAP records re-imports all LDAP records from the LDAP server to the C•CURE 9000 database. This option is useful when the servers have been restored from a backup. However, it does **not** delete records that exist in C•CURE 9000, but do **not** exist in the LDAP backup.
Polling Interval	Enter the interval in minutes:seconds at which the C•CURE 9000 server checks the LDAP server for changed records within the specified period. The range is 00:10 to 99:59 mm:ss. The default value is 00:30 mm:ss.
Timeout/retry wait time (seconds)	Enter the number of seconds the system waits before determining that the message has timed-out when the LDAP server fails to respond to a message. This is also the amount of time it waits before trying to resend the message. The range is from 1 to 9999 seconds. The default value is 30 seconds. NOTE: This value may need to be set to 1000 seconds or greater when importing from an Oracle LDAP server. See Oracle LDAP Import Recommendations on Page 160.
# of diagnostic log files	Enter the number of log files you want the system to keep. If 0, no log files are kept.

Scanning Tab Tasks

Configuring the Scanning Tab

To Configure the Scanning Tab

1. In the **LDAP Source Configuration** dialog box, shown in Figure 48 on Page 151, click the **Scanning** tab. The tab opens, as shown in Figure 53 on Page 160.
2. In the **Method of scanning LDAP records for changes** box, click the down-arrow to display the list of methods for scanning:
   - **Full Scan** – is the most time-consuming (because it is a full scan), but can be applied to all LDAP servers.
   - Microsoft **Active Directory Timestamp** – is the most efficient to use for Active Directory.

NOTE If you are planning to use **Active Directory Timestamp** to scan for Personnel record changes, see Microsoft Active Directory Timestamp Method on Page 161 and Microsoft Active Directory Timestamp Method Deleting Limitations on Page 161 for information.

3. In the **Polling Interval** fields enter in minutes:seconds the interval within which the LDAP server checks the C•CURE 9000 server for changed records.
4. In the **Before retrying, wait for** xx **seconds for response** field enter the number of seconds the system waits before determining that the message has timed-out when the LDAP server fails to respond to a message. (If importing from an Oracle LDAP server, see Oracle LDAP Import Recommendations on Page 160.)
5. In the **Try** xx **times** field, enter the number of tries you want the system to make to regain polling communications with the LDAP server—before the communications loss is reported.

NOTE If the value for **Before retrying, wait for xx seconds for response**=t, and the value for **Try xx times**=n, then the system waits (n-1) x t seconds before reporting a connectivity problem for the LDAP.

6. Click **Save and Close** when you have completed any changes to the **Scanning** tab and wish to save those changes. The tab closes and the **Data Import Editor General** tab reappears.

Force Sending of All Records

The **Force sending all records on next cycle** button:

- Causes the deletion of all information about the state of the records saved by a previous LDAP import with this Import Definition.
- Causes the next scheduled scan through the LDAP records to re-import all the LDAP records from the LDAP server to the C•CURE 9000.

Consequently, this option is helpful when the servers have been restored from a backup.

NOTE This button is only available after you have completed the configuration of this LDAP Import Definition and run the import.

Causes for Automatic Force Sending of All Records

- For both the **Full Scan** and **Timestamp** methods, automatic re-sending of records occurs when the following changes happen:
  - Whenever the method is changed from **Full Scan** to **Timestamp** or from **Timestamp** to **Full Scan**, because it is likely that the stored data is out-dated for either method.
  - When one certain kind of field mapping change occurs, as described in the following example:

Example:

If the field mapping is changed so that LDAP **field A** which used to be mapped to C•CURE 9000 **field 1** is now mapped to C•CURE 9000
field 2. The LDAP field has not changed; it is still **field A**. However, the target C•CURE 9000 field has changed.

- For the **Full Scan** method only, when the match fields on the C•CURE 9000 server change, re-sending of all records is forced. No other changes to the LDAP Import Definition configuration force an actual full re-send of records. However, any other modification to the mapping fields also results in sending all records again. In the latter case, since the deletion history is **not** lost, it is a more limited type of re-sending.
- For the **Timestamp** method, re-sending all records is forced whenever any of the following change:
  - Field mapping changes
  - Base DN changes
  - Search Filter changes
  - 'Search through all sublevels below starting point' changes (selected or cleared)

NOTE If either the LDAP or C•CURE 9000 databases are restored from backup, you must manually force the re-sending of all records, as described in the following procedure.

To Force Send All Records

1. Click the **Force sending all records on next cycle** button.

   The following confirmation message appears.

2. Click to select one of the two options for the next connection to the LDAP server:
   - Click **Yes** if you want all records of interest in the LDAP server to be imported whether or not they have been imported before. (This causes an increased load on C•CURE 9000 while the record transfer is taking place.)
   - Click **No** if you do not want the records to be re-sent.

   The Scanning tab re-appears.
3. If you click Save and Close on the **LDAP Source Configuration Editor**, the **Data Import Editor General** tab reappears.
4. If you should then click **Save and Close** or **Save and New** on the **Data Import Editor**, the following message displays:

NOTE This message also displays whenever you click to save the Import on the **Data Import Editor** after making a change to the LDAP configuration, such as to the mapping or to the match fields.

5. Click **OK** if you want all records of interest in the LDAP server to be imported whether or not they have been imported before. (This causes an increased load on C•CURE 9000 while the record transfer is taking place.)

   - or -

Click **Cancel** to return to the **Data Import Editor** without saving.

- To close/exit the **Data Import Editor** without forcing a full re-scan, click  .

Configuring an Import Definition for an LDAP Source

The following steps **outline** the basic procedures for configuring a simple LDAP Import Definition. Where a procedural element is **not** LDAP-specific, the step references specific sections in the Data Import chapter.

Ensure that the designated LDAP users have been given sufficient privileges, plus valid user names and passwords by the LDAP server administrator.

NOTE The LDAP Server should be online and available for connection when you are configuring an LDAP Import Definition.

To Configure an LDAP Import Definition

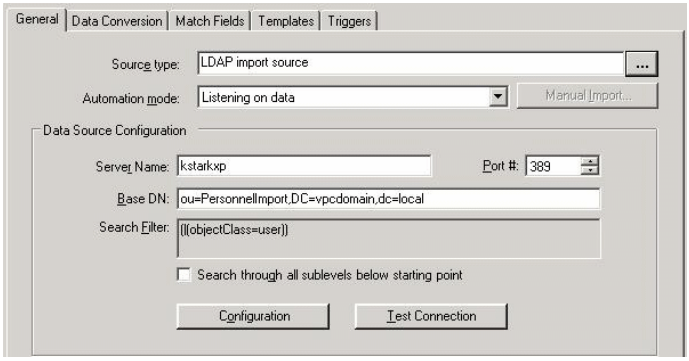
1. Begin creating an Import Definition as detailed in Steps 1 through 4 in Creating an Import Definition on Page 47.
2. On the **Data Import Editor** (see Figure 4 on Page 74), do the following:
   a. Enter a **Name** for the LDAP Import.
   b. Enter a **Description** to distinguish the LDAP Data Import.
3. On the **General** tab in the **Source type** field, click ... and select **LDAP import source** from the list.

   The system automatically opens the **LDAP Source Configuration Editor** (see Figure 48 on Page 151) for you to configure the Import Definition as a connector to a remote LDAP database.

NOTE The system also enters **Listening on data** in the **Automation mode** field and changes the parameters in the **Data Source Configuration** box in the **Data Import General** tab (see Figure 47 on Page 147)—although you cannot see this as the **LDAP Source Configuration Editor** overlays it.

4. Configure all three tabs of the **LDAP Source Configuration Editor** according to the following:
   a. **Authentication** tab – see LDAP Source Configuration Authentication Tab on Page 151 and Authentication Tab Tasks on Page 152.
   b. **Search** tab – see LDAP Source Configuration Search Tab on Page 154 and Search Tab Tasks on Page 156.
   c. **Scanning** tab – see LDAP Source Configuration Scanning Tab on Page 160 and Scanning Tab Tasks on Page 163.
5. Click **Save and Close** when you have finished configuring the parameters on the **LDAP Source Configuration Editor**. The **Data Import Editor General** tab reappears completed, as shown in the example in Figure 54 on Page 166. The **Data Source Configuration** box has the parameters you configured on the tabs of the **LDAP Source Configuration Editor**.

Figure 54: General Tab Data Source Configuration Box Completed for LDAP



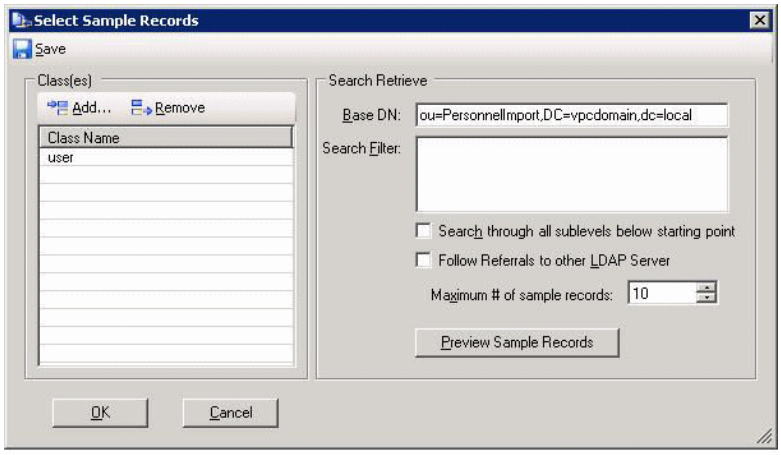
6. Click the **Test Connection** button to check the specified LDAP server with the current authentication credentials. This verifies that the remote server runs LDAP and allows the C•CURE 9000 server to connect to it and read data from the specified Base DN.

The system displays a message informing you whether or not the test was successful.

7. Click the **Select Sample Input** button on the bottom of the **Data Import Editor**.

   The **Select Sample Records** dialog box appears, as shown in Figure 55 on Page 167, already populated with the entries you made in the **LDAP Source Configuration Search** tab (see Figure 51 on Page 158).

Figure 55: LDAP Select Sample Records Dialog Box



Use this dialog box to check that the records selected in the sample have all the properties you want for importing—by default, only the first ten records are included in the preview sample.

a. Click the **Preview Sample Records** button and when the preview opens (see Figure 52 on Page 159), review the records. If the necessary properties are **not** there, do one or both of the following:

   — Increase the number in the **Maximum # of sample records** field.

   — Enter a search criteria in valid LDAP search filter syntax in the **Search Filter** box.

   Example:

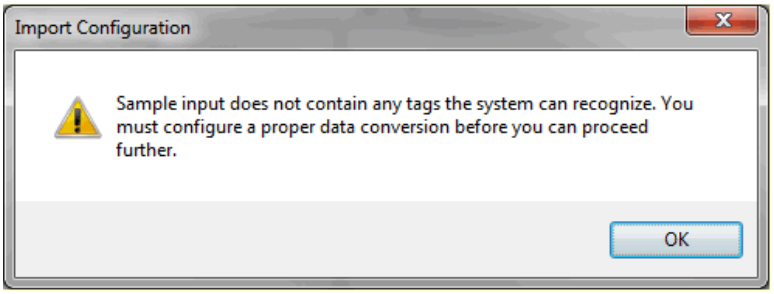
   givenName=John
   sn=Smith

b. Once all the properties you want for import are present, click **OK**.

To ensure that you do **not** change the actual **Search Filter** and **Class(es)** configured for the LDAP Data Import Definition (the parameters on the **LDAP Source Configuration Search** tab) when you alter these fields to select a good sample, click **OK**, not **Save**.

If you click **Save**, these parameters are updated to reflect your changes.

The system reads the data from the LDAP sample, converts it to XML, and tries to map it to the C•CURE 9000 data types. Because the LDAP structure is so different from the C•CURE 9000 database structure, the following message will most likely display.



8. Click **OK** to close the message.

   The **Data Conversion** tab opens for you to set up the conversion. (For information, see Data Import Data Conversion Tab on Page 89, Data Conversion Tab Definitions on Page 90, and Data Conversion Tab Tasks on Page 91.)

9. On the **Data Conversion** tab, click **Add** to open the Personnel Mapping tool.

10. Map the fields in the LDAP data source records to the C•CURE 9000 target fields following Using the Personnel Mapping Tool to Convert Personnel Data on Page 95 for general directions. (The information in Personnel Mapping Tool Editor on Page 92 should also be helpful.)

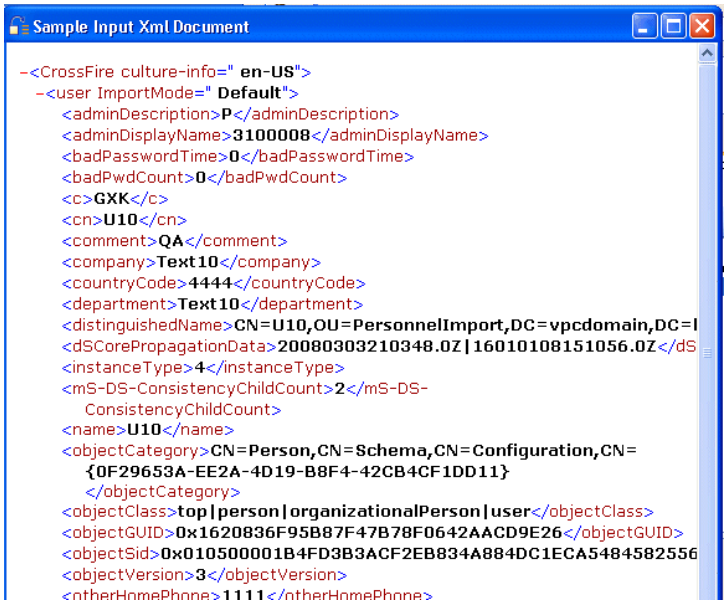
    Software House recommends mapping LDAP source fields as follows:

LDAP Data Source Field	C•CURE 9000 Target Field
objectGUID	GUID
givenName	FirstName
sn	LastName
distinguishedName	Any Text1 throughText20

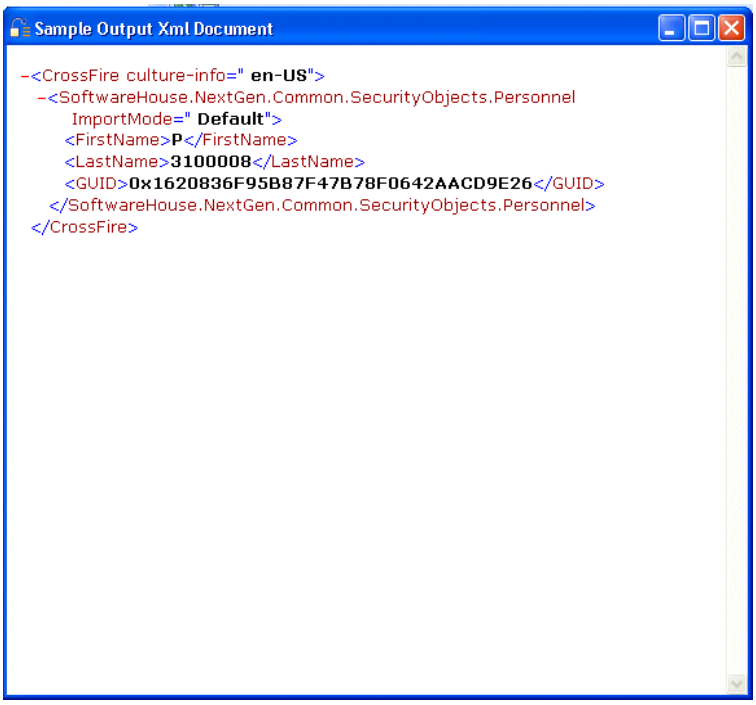
NOTE If you are connected to an Active Directory LDAP Server and the main object class from which you are importing is 'user' or 'computer', a new "virtual" attribute, _AD.UserDisabled, appears. The system treats this virtual attribute like any normal LDAP boolean attribute, and you can successfully import it into a C•CURE 9000 boolean field. If the Active Directory user is disabled, the value of this attribute will be TRUE; otherwise it will be FALSE.

a. To check the conversion of the LDAP **Data Source** records into an XML document, click the **View Sample Input** button. The converted document opens for your review, as shown in Figure 56 on Page 168.

Figure 56: XML Sample LDAP Import Records



b. Once you have mapped all the fields, click the **View Converted Sample** button. The converted file opens for your review, as shown in the following example:



c. To save your mapping, click **Save and Close**.

The **Data Conversion** tab reappears with the Personnel Mapping tool added as the first row in the Data Conversion table Figure 19 on Page 97.

d. To check that the Data Source file has been properly converted, click the **Verify Sample** button. A message displays informing you whether or not every field in the input sample has been recognized.

11. Re-open the **General** tab and select **Update when matched**; **otherwise add** as the **Default Import Mode** option.

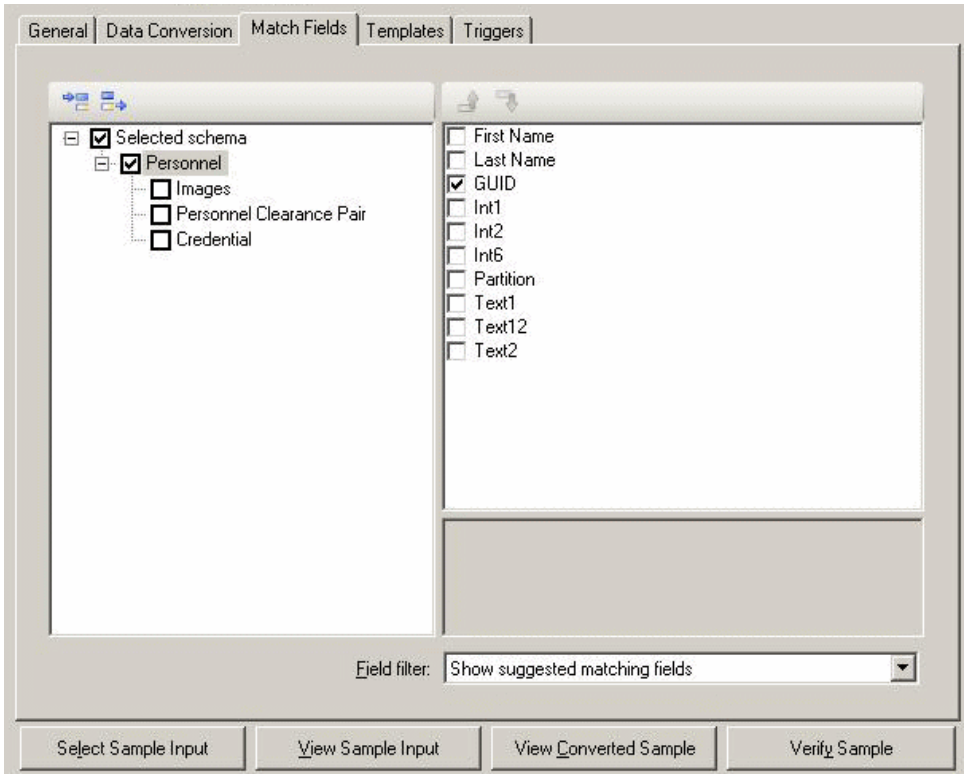
NOTE If you set the mode to **Add only...** or **Update only...** for an LDAP Import, the Import Definition **cannot** be saved, and an error message displays.

12. Click the **Match Fields** tab to open, as shown in the example in Figure 57 on Page 170, to specify the fields on which to match the imported records. (For information about matching, see Match Fields Tab Definitions on Page 121 and Specifying Match Fields on Page 123.)

Software House recommends that you match on the **GUID** field.

NOTE You cannot use virtual attributes, such as _AD.UserDisabled, as match fields for importing. If you do, the system generates an error and aborts the scan. For information about this virtual attribute, see the note in Step 10.

Figure 57: Data Import Editor – Match Fields Tab for LDAP



Once you have finished selecting match fields, the required elements of the configuration for an LDAP Data Import Definition are complete. You could save the LDAP Import Definition now.

However, the **Data Import Editor** has two optional tabs that can provide useful functionality for your import: **Templates** and **Triggers**.

NOTE If you are planning to use any template rules, configure the **Templates** tab before saving the Import Definition because LDAP can start the import process as soon as the Import Definition is saved.

13. Click the **Templates** tab if you want to configure template rules that this LDAP Data Import Definition applies during the import process to the Personnel objects being modified. (Template rules are optional.)

    Template rules can be used for updating information, such as **clearance** assignments, based on different Personnel types (roles) such as **Managers**, **Employees**, and **Contractors**.

    (For complete detailed information about templates, see the Data Import Templates Tab section that starts on Page 127 and ends on Page 139.)

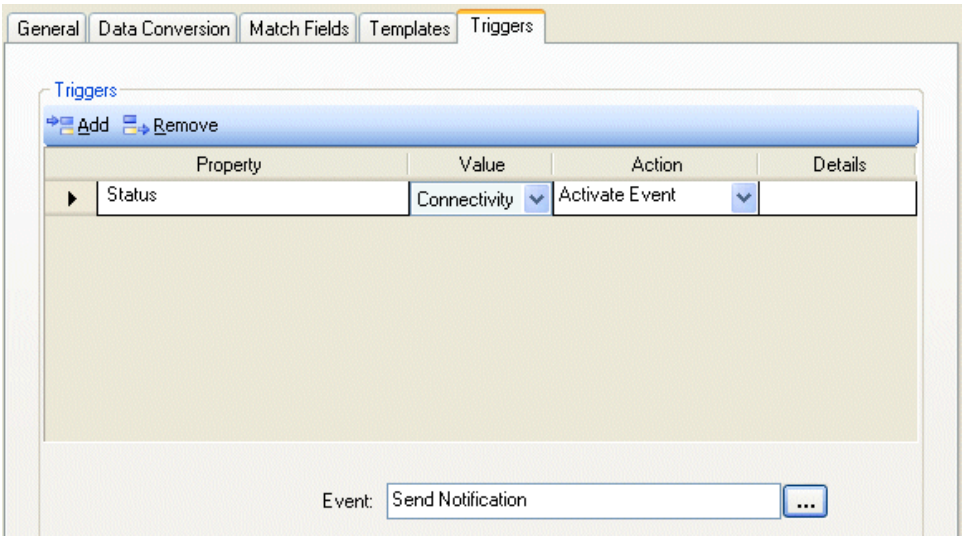
14. Click the **Triggers** tab if you want to configure a trigger to activate an event when this LDAP Data Import Definition has a defined status. (Triggers are optional.)

    A common and important use for a trigger would be notification of the loss of communications between C•CURE 9000 and the LDAP server— **Status** of **Connectivity error**. (For information, see Data Import Editor Tasks on Page 69.)

    (For more information about configuring triggers, see Data Import Triggers Tab on Page 140.)

    See Figure 58 on Page 171 for an example of the **Triggers** tag completed for an LDAP Import.

Figure 58: Data Import Editor Triggers Tab for LDAP Completed



15. Make sure that the **Enabled** check box on top of the **Data Import Editor** is still selected (the default) so the Import Definition is operational.

    You have now completed the configuration of an LDAP Import Definition.

16. To save your Import Definition, click **Save and Close**.

    - or -

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

NOTE When you click **Save...**, the system performs the final validation of the LDAP Import Definition which requires connecting to the specified LDAP Server. If the LDAP server is offline or the Validation cannot be completed for some other reason, you can save the LDAP Import Definition by clearing the **Enabled** check box at the top of the Editor.

Supported Attribute Types for Active Directory

Only the Attribute data types in Table 38 on Page 172 are supported for LDAP data import from Active Directory.

Table 38: Supported Active Directory Attribute Types

Attribute Type	Name in ASDI Editor	9000 Data Type
Boolean	Boolean	Boolean
CaseIgnoreString	Case Insensitive String	String
Case-Sensitive String	Case Sensitive String	String
Integer	Integer	Integer
Object (DN-Binary)	DN-Binary	String
Object(DN-DN)	Distinguished Name	String
Object(DN-String)	Dist. name with String	String
String (Numeric)	Numerical String	Integer
String (Object-Identifier)	Object Identifier	String
String (Octet)	Octet String	String*
String (Printable, IA5)	String (IA5)	String
String(SID)	SID	String
String(Unicode)	Unicode String	String
String(UTC Time)	UTC Time string	Date/time

NOTE ObjectGUID is an exception: it can be imported into the GUID field (type GUID) in the 9000 object.

Connecting the C•CURE 9000 Server to an LDAP Server Using SSL/TLS

This section describes the procedures for configuring the C•CURE 9000 System if you wish to connect to an LDAP Server using Secure Sockets Layer (SSL) and Transport Layer Security (TLS). The following instructions also describes how to use the self-signed root certificate option.

Table 39 on Page 173 lists the order in which the procedures for configuring the C•CURE 9000 System to connect to an LDAP Server using SSL/TLS should be performed.

Table 39: Procedures for Configuring C•CURE 9000 for SSL/TLS Connection with LDAP Server

Order	Task	See...
1	Checking if SSL/TLS is Already Enabled on your Machine.	Checking if SSL/TLS is Already Enabled on your Machine on Page 174
2	Install Microsoft Internet Information Services (IIS), if **not** yet installed on Active Directory.	Installing Microsoft Internet Information Services on Page 174.
3	Install Certificate Authority (CA), if **not** yet installed on Active Directory.	Installing the Certificate Authority on Page 175.
4	Export the CA Certificate from the Active Directory server.	Exporting the Certificate on Page 176.
5	Import the CA Certificate to the computer where the C•CURE 9000 server will run, if **not** on the Active Directory server.	Importing the Certificate on Page 176.
6	Verify SSL Is Enabled on the Active Directory server (Optional).	Verifying SSL is Enabled on Page 177.

Once you have completed the procedures listed in Table 39 on Page 173,
C•CURE 9000 should be able to establish an SSL/TLS connection to the LDAP on the Active Directory server computer.

NOTE For SSL/TLS connection, you must use the Fully Qualified Domain Name (FQDN) of the Active Directory server computer and port **636**, and select the **Connection uses SSL Encryption** check box, on the **LDAP Source Configuration Authentication** tab when configuring an LDAP object.

Overview

In order for SSL/TLS to work the certificate used by the LDAP server must be trusted by the machine running the C•CURE 9000 server. This can be done in one of the three following ways.

- You can purchase a certificate from a trusted SSL Certificate Provider and install it on the LDAP Server machine. Alternatively you can use a free domain-validation certificate from an open-source certificate authority.
- An Active Directory domain containing both the LDAP server and the C•CURE 9000 server may already be set up with trusted certificates. Check this by verifying if SSL/TLS is enabled. For more information see "Verifying SSL is Enabled " on page 177.
- You can create a self-signed Root Certificate authority for the LDAP/Active Directory server and install it on the C•CURE 9000 Server. You must export the Root Certificate authority certificate and install it in Microsoft Certificate manager. For more information see "Installing the Certificate Authority" on page 175.

Requirements

The following requirements must be met before attempting to run LDAP over SSL/TLS.

- The LDAP SSL/TLS certificate must be located in the LDAP server (Domain Controller) Local Computer's Personal certificate store.

- A private key that matches the certificate must be present in the Local Computer's certificate store and must be correctly associated with the certificate.
- The Enhanced Key Usage extension includes the Server Authentication (1.3.6.1.5.5.7.3.1) object identifier. This is shown under the certificate properties in Windows Certificate Authority as Server Authentication Purpose.
- The Active Directory fully qualified domain name of the domain controller/LDAP server (for example, DC01.DOMAIN.COM) must appear in one of the following places:
  - The Common Name (CN) in the Subject field.
  - DNS entry in the Subject Alternative Name extension.
- The SSL/TLS certificate must be issued by a certificate authority that the domain controller and the LDAP SSL clients trust. Trust is established by configuring the clients and the server to trust the root CA to which the issuing CA chains. If you buy a certificate from a trusted certificate authority, this trust should happen automatically.
  - If you use a self-signed certificate, trust is established by importing the self-signed Root Certificate Authority certificate into the "Trusted Root Certification Authorities" section of the Microsoft Certificate manager, on the C•CURE 9000 server machine.

Checking if SSL/TLS is Already Enabled on your Machine

You can configure a test import to check if SSL/TLS is already enabled by following the steps below.

Configuring a Test Import

1. In the **Data Import (Template)** window, select the **General** tab and ensure **Source Type** is set to LDAP import source.
2. Click the **Configuration** button. The LDAP Source Configuration window opens.
   a. Enter the server name in the **LDAP Server Name** field and set the **Port #** to 636.
   b. Select Basic, Kerberos, or Microsoft Negotiate from the **Authentication Type** drop-down menu.
   c. Enter the LDAP user in the **LDAP User** field.
   d. Enter the password in the **Password** field.
3. Select the **Connection Uses SSL Encryption** check box.
4. Click **Check Authentication**.
5. Ensure the correct **BASE DN** is entered.
6. Click **View Sample**. If you can view the sample record SSL/TLS is already enabled.

NOTE If step 4 or step 6 fails begin the process from Installing Microsoft Internet Information Services below.

Installing Microsoft Internet Information Services

Microsoft **Internet Information Services** (**IIS**) is the Web service integrated with Windows Server 2008, Windows Server 2012, and Windows Server 2016. If the Certificate Authority (CA) is **not** already installed, you can install it on your Active Directory server.

When you configure the Server using Windows Server 2008, Windows Server 2012, or Windows Server 2016, you should choose the **World Wide Web Service** option to allow the use of the **Auto-Update Configuration** utility.

Installing IIS on Windows Server 2008, Windows Server 2012, or Windows Server 2016

1. Click **Start**, then **Server Manager**. The **Server Manager** tool starts.

2. Click **Manage** ,then click **Add Roles and Features**. The **Add Roles and Features Wizard** window opens.
3. On the **Before You Begin** page, click **Next**.
4. On the **Installation Type** page, select **Role-based or feature-based installation**. Click **Next**.
5. On the **Server Selection** page, select **Select a server from the server pool**. Click **Next**.
6. On the **Server Roles** page, ensure the Web Server (IIS) checkbox is selected. Click **Next**. The **Add Roles and Features Wizard** window opens.
7. In the **Add Roles and Features Wizard** window, click **Add Features**.
8. On the **Features** page, keep the default selections. Click **Next**.
9. On the **Role Services** page, keep the default selections. Click **Next**. The **Confirmation** page opens. Click **Install**.
10. Open the **Control Panel** and double-click **Administrative Tools**. There is a new icon labeled **Internet Information Services**.

Installing the Certificate Authority

If the Certificate Authority (CA) is **not** already installed, you can install it on your Active Directory server (Windows Server 2008, Windows Server 2012, or Windows Server 2016).

Installing the Certificate Authority

1. Click **Start**, then **Server Manager**. The **Server Manager** tool starts.
2. Click **Manage** ,then click **Add Roles and Features**. The **Add Roles and Features Wizard** window opens. Click **Next**.
3. On the **Installation Type** page, select **Role-based or feature-based installation**. Click **Next**.
4. On the **Server Selection** page, select **Select a server from the server pool**. Click **Next**.
5. On the **Server Roles** page, ensure the **Active Directory Certificate Services** checkbox is selected. Click **Next**. The **Add Roles and Features Wizard** window opens.
6. In the **Add Roles and Features Wizard** window, click **Add Features**.
7. On the **Features** page, keep the default selections. Click **Next**. The **Active Directory Certificate Services** page opens. Click **Next**.
8. On the **Role Services** page, keep the default selections. Click **Next**. The **Confirmation** page opens. Click **Install**.
9. When installation has completed, click **Close**. You must now configure your Certificate Authority.

Configuring the Certificate Authority

You must configure the certificate authority in Server Manager in Windows Server 2008 or Windows Server 2012 after installing the certificate authority.

Configuring the Certificate Authority

1. Click **Start**, then **Server Manager**. The **Server Manager** tool starts.
2. Click on the Navigation flag in the top-right of the **Server Manager** window. Click **Configure Active Directory Certificate Services on the destination server**. The Active Directory Certificate Services Configuration window opens.
3. On the **Credentials** page, verify the correct credentials are inserted. Click **Next**.
4. On the **Role Services** page, check the **Certification Authority** checkbox. Click **Next**.

5. On the **Setup Type** page, select the **Enterprise CA** option. Click **Next**.
6. On the **CA Type** page, select the Root CA option. Click **Next**.
7. Configure **Private Key** settings.
   a. Select the **Create a new private key** option. Click **Next**.
   b. On the **Cryptography** tab, keep the default selections. Click **Next**.

NOTE You can set the hash algorithm to SHA256, SHA384, or SHA512 for increased security.

   c. On the **CA Name** page, keep the default names. Click **Next.**
   d. On the **Validity Period** page, set the required validity period. Click **Next**.
8. On the **Certificate Database** page, click **Next**.
9. The **Confirmation** page opens. Click **Configure**to complete the Certificate Authority configuration.
10. Reboot the machine before continuing to export the certificate.

Exporting the Certificate

You now need to export the certificate from the Active Directory server.

To Export the Certificate from the Active Directory Server

1. Log on as a **Domain Administrator** to the **Active Directory** server.
2. Export the certificate to a file as follows:
   a. Click **Start**>**Control Panel**>**Administrative Tools**>**Certificate Authority** to open the **CA Microsoft Management Console (MMC)** dialog box.
   b. Highlight the **CA** and right-click to select **Properties** for the **CA**.
   c. From the **General** menu, click **View Certificate** button.
   d. Select the **Details** view, and then click the **Copy to File** button on the lower-right corner of the window.
   e. Use the **Certificate Export Wizard** to save the CA certificate in a file.

NOTE You can save the CA certificate in either DER Encoded Binary X-509 format or Base-64 Encoded X-509 format.

Importing the Certificate

After you have exported the CA certificate from the Active Directory server, you must import it to the computer where the C•CURE 9000 server will run. Ensure that the Microsoft Certificate console is added to the server if it is not already available.

Adding the Microsoft Certificate console to your server

1. Click **Start**, then **Run**.
2. Type `mmc` in the **Run** dialog box and click **OK**. The **Console** window appears.
3. On the **Console** window, click **File**, then **Add/Remove Snap-In...**. The **Add or Remove Snap-ins** page is displayed.
4. In the **Available snap-ins** column select **Certificates**. Click **Add**.
5. On the **Certificates snap-in** page, select **Computer account**. Click **Next**.

6. On the **Select Computer** page, select **Local computer: (the computer this console is running on)**. Click **Finish**. **Certificates** will be displayed in the **Selected snap-ins** column.
7. On the **Add or Remove Snap-ins** window, click **OK**. The Microsoft Certificate console is added.

Importing the Certificate on the C•CURE 9000 server.

1. Click **Start**, then **Run**.
2. Type `mmc` in the **Run** dialog box and click **OK**. The **Console** window appears.
3. On the left column, double-click **Certificates (Local Computer)** to expand the folder structure.
4. Right-click the **Trusted Root Certification Authorities** folder, navigate to **All Tasks**, then click **Import**.
5. The **Certificate Import Wizard** window opens. Ensure **Current User** is selected as Store Location. Click **Next**.
6. On the **File to Import** page, browse to the location of your Certificate file and insert into the **File name** dialog box. Click **Next**.
7. On the **Certificate Store** page, select the desired Certificate Store. **Click Next**.
8. On the **Completing the Certificate Import Wizard** page review your settings. Click **Finish**. A dialog box will display to confirm the import was successful.

You can now try to run LDAP, or optionally verify that SSL is enabled.

Verifying SSL is Enabled

This procedure is optional. If you attempt to run LDAP after you have finished importing the Certificate on the LDAP client system and LDAP runs, there is **no need** for the verification procedure.

However, if LDAP does **not** run, the Verification procedure is useful in trouble-shooting the nature of the problem(s). It may also be useful to run this Verification procedure up-front to check that your configuration for SSL is correct.

You need to install an LDAP tool (**ldp.exe**) to test the SSL connectivity.

Installing the LDAP tool (Active Directory Lightweight Directory Services)

1. On Windows Server 2008 or Windows Server 2012:
   a. Click **Start**, then type **Turn Windows Features On and Off** in the search box. Click to open it. The **Add Windows Features** window opens.
   b. On the **Before You Begin** tab click **Next**.
   c. On the **Installation Type** tab, select your installation and click **Next**.
   d. On the **Server Selection** tab, select your server and click **Next**.
   e. On the **Server Roles** tab, select **Active Directory Lightweight Directory Services**. A new **Add Roles and Features Wizard** window opens. Click **Add Features**, then click **Next**.
   f. On the **AD LDS** tab, click **Next**, then click **Install** on the **Confirmation** tab. Active Directory Lightweight Services installs.

Detailed Verification of SSL/TLS on the Active Directory Server

1. Open the **Command Prompt** window from the **Start** menu.
2. Type **ldp** into the command prompt and press **enter**. The **ldp** window opens.

3. Select **Connection**>**Connect** and supply the host name (not IP address) and port number (636). Also select the **SSL** check box.
4. Ensure that you type the fully qualified domain name (FQDN) of the Active Directory server computer correctly.
5. Obtain the **FQDN** of the Active Directory server as follows:
   - Right-click the **My Computer** icon.
   - Click the **Network Identification** tab.
   - Click the **Full Computer Name** field.
6. If the **FQDN** cannot be resolved on the client computer, it is important to add the following entry to the end of the HOSTS file located under **%SystemRoot%\SYSTEM32\DRIVERS\ETC** directory on the client computer:

   FQDN IP

   (Where **FQDN** is the fully qualified domain name of the Active Directory server and **IP** is the IP address of the Active Directory server.) The FQDN and IP address must be separated by a space.

- If this procedure is successful, a window displays listing information related to the Active Directory SSL connection.
- If the connection is unsuccessful, restart your system and repeat this procedure.

5

ODBC Data Import

C•CURE 9000 allows you to perform automatic reads from any Open Database Connectivity (OBDBC) data source to import personnel data directly into the C•CURE 9000 system database. This imported data behaves in the same way as manually entered information.

This chapter provides the background information and configuration procedures specific to ODBC importing. The main documentation for importing data is covered in Chapter 3. It is important that you read the Importing Overview that starts on Page 42 and refer to the following generic importing information and other Chapter 3 information as well as the information in this ODBC chapter:

- Basic Importing Tasks on Page 47
- Data Import Editor on Page 67

In this chapter

ODBC Data Import Overview

C•CURE 9000 supports importing of personnel data from external ODBC-compliant databases to the C•CURE 9000 database

Once configured and set online, the import executes in the background periodically at a user-specified interval. This avoids the need to run the C•CURE 9000 Administration application each time personnel data is to be imported. The import procedure also performs the necessary data validation to prevent corruption of the system personnel table.

The ODBC import feature is designed to allow connection to any ODBC-compliant database. The following ODBC databases are currently supported:

- MS Access 2007
- MS SQL Server 2008 R2, 2012, 2016
- Oracle 10g
- Progress

NOTE ODBC import is not supported for Excel or Text files. You can use an automated Data Import for CSV files with Import Watcher for those cases. For information, see Importing Overview on Page 42.

NOTE ODBC import uses third-party ODBC drivers installed on Windows, independent from the C•CURE 9000 database. Improper installation or configuration of the third-party ODBC drivers can effect the C•CURE 9000 ODBC import

For information about ODBC and C•CURE data types and possible conversion errors, see C•CURE Data Types on Page 558.

Data Import Query Process

C•CURE 9000 automatically generates an external database query based on the external field information and filter criteria you specify in the **ODBC Source Configuration** Editor **Records** tab.

C•CURE 9000 supports three methods for doing this:

- Querying on a “timestamp” field in the external database.
- Reading all the records based on the record constraints (criteria) you specify.
- Querying on both a timestamp field and record constraints.

Timestamp Field in the External Database

This method requires that you designate an external database field as a timestamp field. This field contains a numeric value or date time value that increases in magnitude with each external database update. Whenever the external software changes or adds a personnel record, it must update the timestamp field in the modified record, either from the system time or from a counter that it maintains. Subsequently, whenever C•CURE 9000 queries for new records, it looks for records with timestamp values higher than those in the records previously processed. The C•CURE system itself doesn’t modify the external database. This works in the same way with the update.

Record Constraints on External Database

This method requires that you specify record constraints (query criteria) as field value pairs. C•CURE 9000 then reads each record in the table that meets the constraints and imports it into the C•CURE Personnel database. You can specify more than one field value criteria.

Example:

A field value constraint specified as **EmployeeID > 10** will import all records whose EmployeeID field has a value greater than 10.

Timestamp field and Record Criteria Filters on External Database

This method combines the previous two approaches. You can specify both a timestamp field and record constraints to filter the records for importing.

NOTE If you do not select any of the filter criteria described in the preceding methods, all the records will be considered for import. A proper Delete option must be used in this case. See Records Delete Option on Page 194.

ODBC Automated Import Special Considerations

The following are special considerations for ODBC Automated Import:

Data Field Mismatch

When properly configured, automated imports are characterized by matching field assignments between the source database and destination database.

Example:

A field assignment is established between the **Last Name** field in the source database and the **Last Name** field in the destination database.

Field assignments must always be made between like data types, such as character-to-character, integer-to-integer, and timestamp-to-timestamp. Unpredictable results occur when fields of unrelated types are matched.

Example:

Attempting to match a Last Name field (a character data type) in the source database with a Card Number field (an integer data type) in the destination database yields an unpredictable result. Another common mismatch is the character to timestamp mismatch.

Some data types are not standardized, such as the ENUM data type. Using such data types also causes unpredictable results.

Missing Fields

The external database does not need to contain all the C•CURE 9000 fields in the records being imported. Missing fields are handled as they are for the XML import:

- Fields in existing records are not changed
- Fields in new records are assigned the default value as specified in the $Default record for the partition for the user assigned to the import.

The external database can also contain fields that are not intended for the import operation. If an external field is not mapped with an existing C•CURE 9000 field in the specified record type (see Personnel Mapping Tool Editor on Page 92), the external field is skipped during the import operation.

Non-displaying PINs

If the PIN is set to not display for your C•CURE 9000 and you try to import records with PINs, PINs in new and updated records are set to asterisks. To import records in systems that require hidden PINs, follow one of the following methods:

- Import records and then enter PINs manually through the C•CURE 9000 Administration application.

- Select the **Display PIN** System Variable in the System Variables Personnel Section, change its value to **True**, and then import records with their PINs. PINs are added to new and updated records. After you import the records, you can hide PINs again by setting the **Display PIN** System Variable back to **False**.

Setting Up an ODBC External Data Source

This section describes how to set up a data source for a 64-bit operating system.

As of v2.70, C•CURE 9000 does not support 32-bit Windows Operating Systems. The only time that C•CURE ODBC Import configuration recognizes 32-bit ODBC DSN configurations if the C•CURE 9000 server is installed on a PC that is running a 32-bit Windows OS.

NOTE Field names must not contain spaces. For example, “client name” should be “client_name” or “clientname”. For example, if you create the field name “**client name**”, the field name appears in the C•CURE 9000 as “**client_x0020_name**”.

To Set Up a Data Source for an ODBC Automated Import

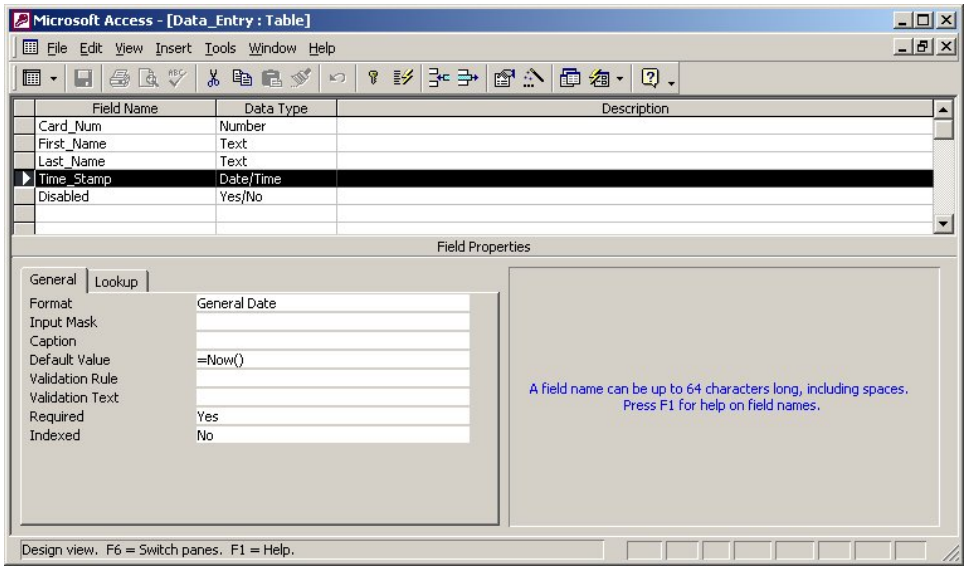
1. Design and implement a database to import from, if necessary. In this example, a small Microsoft Access database is used.

Table 40: Microsoft Access Database Fields

Field Name	Access Type
Card_Num	Number
First_Name	Text
Last_Name	Text
Time_Stamp	Date/Time
Disabled	Yes/No

2. In the **Access** dialog box, notice that the Time_Stamp field is a general date field with a default value set to *=Now()*.

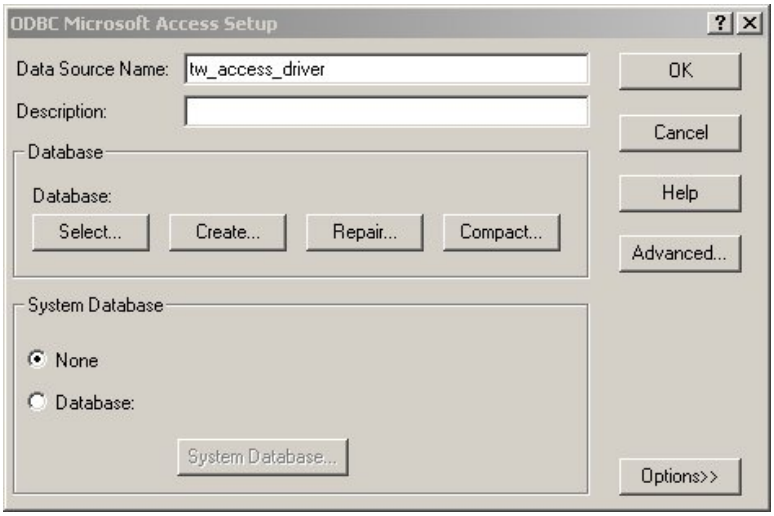
Figure 59: Microsoft Access Dialog Box



3. Go to **Control Panel**>**Administrative Tools**>**ODBC Data Sources (64-bit)**. The **OBDC Data Source Administrator** dialog box opens. Click on the **System DSN** tab.
4. Click **Add**. The **Create New Data Source** dialog box opens.

5. Select **Microsoft Access Driver (*.mdb)** and click **Finish**. The **OBDC Microsoft Access Setup** dialog box opens (see Figure 60 on Page 184).

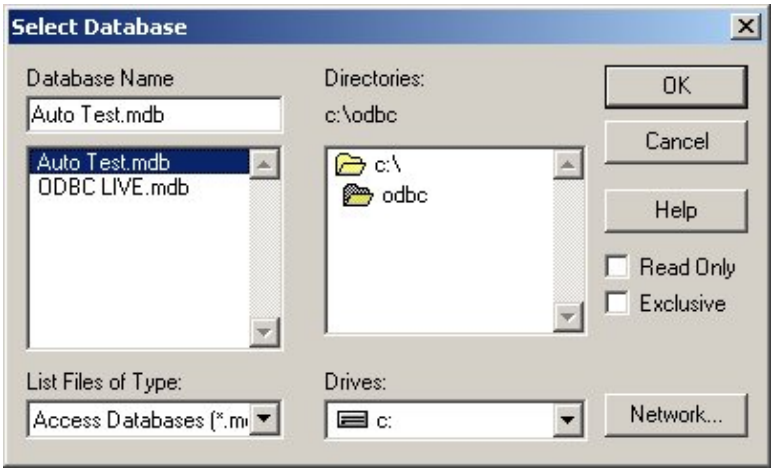
Figure 60: OBDC Microsoft Access Setup Dialog Box



6. Enter a name for the database in the **Data Source Name** (DSN) field and click **Select** in the **Database** box.

   The **Select Database** dialog box opens.

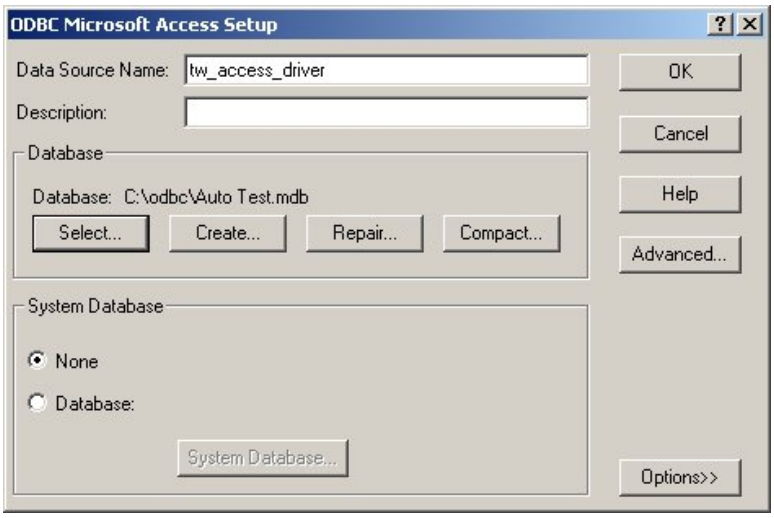
Figure 61: Select Database Dialog Box



7. Select the database created in Step 1 on Page 183. Click **OK**.

   The **OBDC Microsoft Access Setup** dialog box reopens, with the selected database name appearing in the **Database** box, as shown in Figure 62 on Page 185.

Figure 62: OBDC Microsoft Access Setup Dialog Box with Database



8. Click **OK** in the **OBDC Microsoft Access Setup** dialog box.
9. Click **OK** in the **OBDC Data Source Administrator** dialog box.
10. Close the **Control Panel**.

Import Editor General Tab for ODBC

For instructions to access the C•CURE 9000 Data Import Editor, see Accessing the Data Import Editor on Page 47.

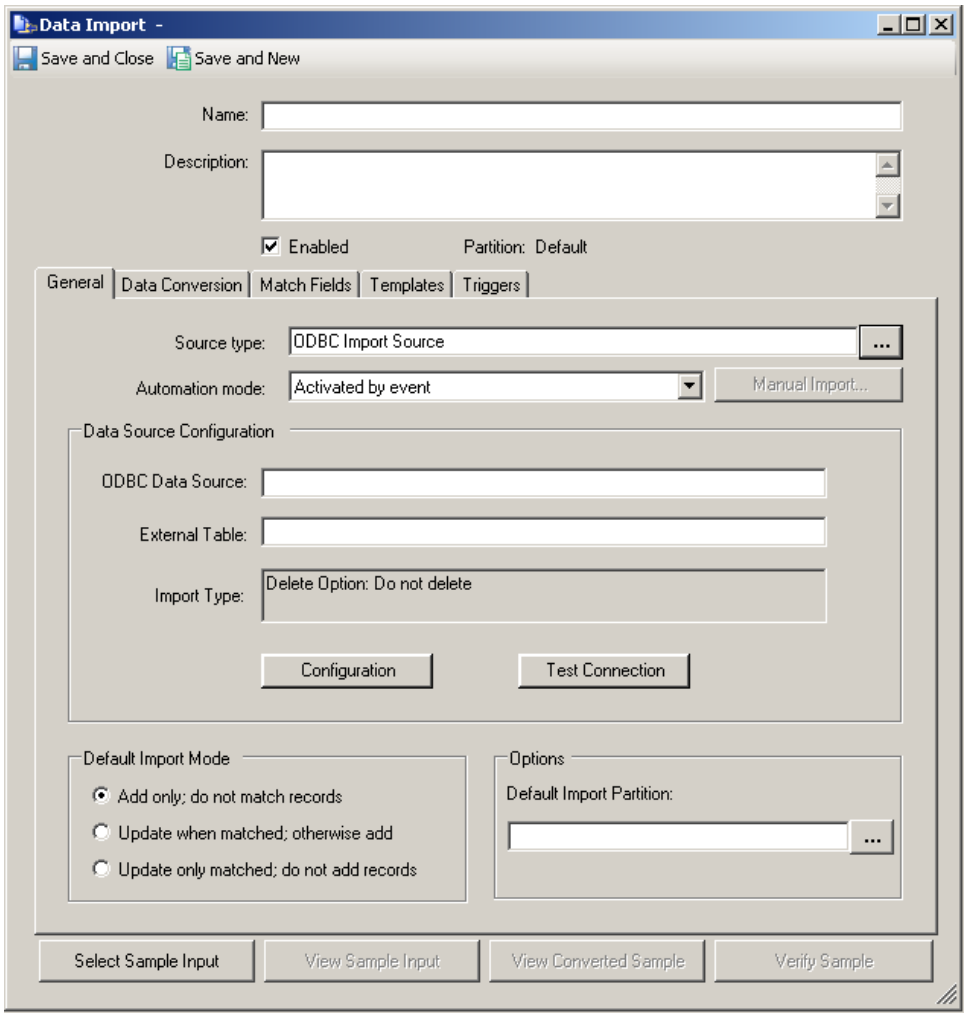
NOTE Data Import Editor General Tab on Page 74 shows the General tab the way it displays when you first open it. The General tab changes when you select an import source.

NOTE See the Data Import Editor on Page 67 for the **Data Conversion** tab, **Match Fields** tab, **Templates** tab, and **Triggers** tab configuration information.

Once you select **ODBC import source** in the **Source type** field, two actions occur:

- The **Data Import Configuration General** tab changes, as shown in Figure 63 on Page 186 described in General Tab Definitions for ODBC on Page 186.
- The ODBC Source Configuration Editor on Page 190 opens, as shown in Figure 64 on Page 190.

Figure 63: Data Import Editor – General Tab for an ODBC Import



General Tab Definitions for ODBC

For ODBC, the **Data Import General** tab displays the fields and buttons described in Table 41 on Page 187.

Table 41: ODBC Data Import General Tab Definitions

Fields/Buttons	Description
Name	The name of the Import definition. This field is required.
Description	A description of the ODBC Import Definition. This field is not required, but if used can make it easier to identify the specific Import definition when you are using it later on.
Enabled	Select this check box to make the Import Definition operational. (The default is selected.)
Partition	A read-only field displaying the Partition to which this Import Definition belongs. (This field is visible only if the C•CURE 9000 system is partitioned.)
General Tab	
Source Type	Click ... to select the ODBC import source from the drop-down list. Once ODBC is selected, the system displays **Activated by event** in the **Automation mode** field, makes the **Manual Import** button unavailable, and changes the parameters in the **Data Source Configuration** box.
Automation Mode	Select either of two modes in which the ODBC import will operate: • Activated by event (automated) – the Import Definition listens for C•CURE 9000 events that trigger the Import Definition to poll its import source for existing data. A new Event activation or explicit execution of" Run on Server" command, is required to rung the import again. • Listening on data (automated) – the import source object is initialized by the Import Watcher server component and starts listening to receive new external data in an ODBC database by running a query on a specified table periodically. When one or more records are detected, the import source initiates import of the records into C•CURE 9000.
Manual Import	**Not** available for ODBC Data Import.
Data source Configuration Box (These are the parameters for the ODBC import source. The values for the ODBC entries are filled in after you complete the entries on the tabs of the ODBC **Source Configuration** dialog box.)	
ODBC Data Source	Valid DSN name of the external ODBC database. This is a required field.
External Table	External ODBC database table from which to import records.
Import Type	The particular record constraints, such as 'Import on time stamp', and Delete option configured for this ODBC Import definition.
Configuration	Click this button to open the **ODBC Source Configuration** Editor to continue configuring or to edit the parameters for the **ODBC** server connection. NOTE: This dialog box opens automatically when you first select **ODBC** as the source type on this **General** tab.
Test Connection	Click this button to verify that the C•CURE 9000 server can connect to the specified ODBC data source.
Default Data Import Mode (**Update when matched, otherwise add** is the only valid import mode for ODBC.)	
Add only; do not match records	**Not** valid for ODBC Data Import. If you select this option, the Import Definition cannot be saved and an error displays.

ODBC Data Import General Tab Definitions (continued)

Fields/Buttons	Description
Update when matched, otherwise add	Select this import rule option to perform matching as follows: • If the import source contains records with match field values that exactly match those field's values in existing records in C•CURE 9000, the records in C•CURE 9000 are updated using imported records. • If C•CURE 9000 does not contain records that exactly match those being imported from the source, the import adds the non-matching records to C•CURE 9000. Selecting this option requires specifying matching fields on the **Match Fields** Tab. See Data Import Match Fields Tab on Page 120 and Match Fields Tab Tasks on Page 123. NOTE: Make sure that the configuration data is complete (ODBC Source Configuration Editor on Page 190), and that Test Connection indicates successful connection to the database prior to selecting this option. Specifying matching fields requires knowledge about the structure of the external table which cannnot be done without proper ODBC connection configuration.
Update only matched: do not add records	**Not** valid for ODBC Data Import. If you select this option, the Import Definition cannot be saved and an error displays.
Options Box	
Default Import Partition	Click ... to select the Partition in which to place newly imported records when the external records do not include a reference to any C•CURE 9000 partition. (This field is available **only** if the C•CURE 9000 system is partitioned.) Software House recommends that you select a Partition for automated imports to avoid confusion. NOTE: • If this field is left blank in a partitioned system and the records being imported do not refer to any Partition, the Import process will place the records in the 'Default' Partition'. • If the Partition referenced by an Import Definition is deleted from the system, you cannot run the import. The Import Definition cannot be used until you edit it and select another Partition. • The Partition can **only** be updated for a record when it is referenced in the external record, not by its entry in this field.
Buttons	**Description**
Select Sample Input	Click this button to open the **Select Sample Records** dialog box (see Figure 71 on Page 204) that allows you to choose records from the ODBC server. This dialog box includes the same external ODBC Data Source, User ID, Password, and Table originally selected in the **Configuration** tab (see ODBC Source Configuration Configuration Tab on Page 190).
View Sample Input	Click this button to open a form with an XML document that represents the structure generated by the system while parsing the sample input records received from the ODBC server. NOTE: This button is unavailable if a sample input has **not** been selected. Make sure the configuration data is completed before calling this function.
View Converted Sample	Click this button to open a form with the XML document that represents the result of the data conversion applied to the selected sample input (configured on the **Data Conversion** tab). NOTE: This button is not available if a sample input was **not** selected, or if the list of converters is empty.

ODBC Data Import General Tab Definitions (continued)

Fields/Buttons	Description
Verify Sample Input	Click this button to take the selected sample input converted by the chain of import converters (if any) and verify that each field and each object type in the resulting XML document can be recognized by C•CURE 9000. If the verification fails, the system informs you and suggests creating a proper data conversion. If only some of the fields cannot be recognized by the system, the system can show those fields in a form of XML document. NOTE: This button is unavailable if a sample input was **not** selected.
Save and Close	Click this button when you have completed any changes to the Import Definition and wish to save those changes. The Import Definition closes.
Save and New	Click this button when you have completed any changes to the Import Definition and wish to save those changes and also create a new Import Definition. The Import Definition that you were editing is saved, and a new Import Definition opens (either blank or including template information if you were using a template to create new Import definitions).

ODBC Source Configuration Editor

This Editor opens the first time you select the **ODBC import source** in the **Source type** field on the **General** tab of the **Data Import Editor**. To open this Editor after that, click the **Configuration** button that displays in the **Data Source Configuration** box for an ODBC Import, as shown in Figure 63 on Page 186.

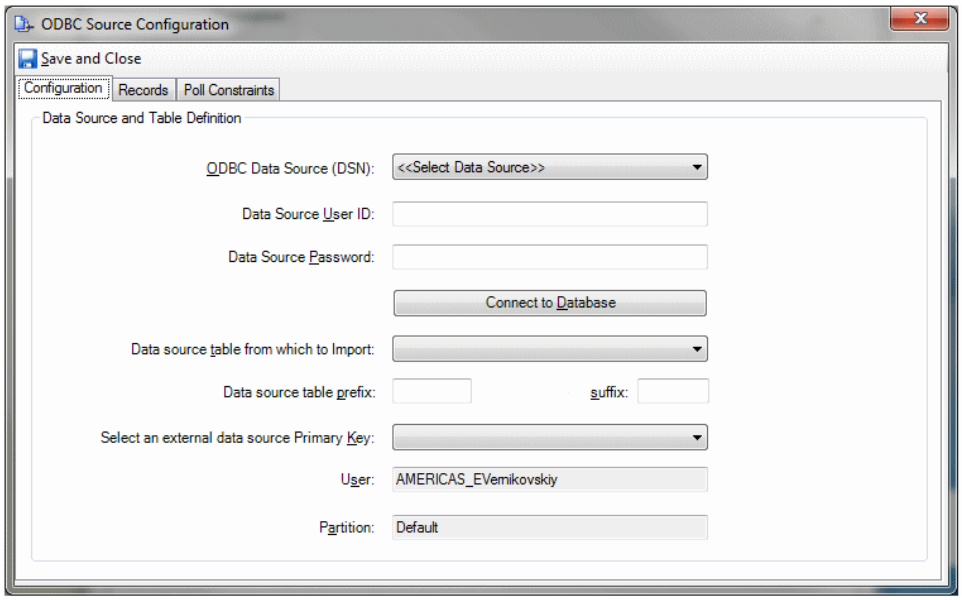
This Editor allows you to configure the data source for an ODBC import and the parameters required to connect to the ODBC server. The Editor has the following tabs:

- ODBC Source Configuration Configuration Tab on Page 190
- ODBC Source Configuration Records Tab on Page 192
- ODBC Source Configuration Poll Constraints Tab on Page 198

ODBC Source Configuration Configuration Tab

The **Configuration** tab, as shown in Figure 64 on Page 190, lets you enter ODBC connection parameters to link to the external data source. This tab also provides a means to validate the connection to the database.

Figure 64: ODBC Source Configuration Editor Configuration Tab



Configuration Tab Definitions

The **Configuration** tab has the fields and buttons described in Table 42 on Page 190.

Table 42: ODBC Source Configuration Configuration Tab Definitions

Fields/Buttons	Description
ODBC Data Source (DSN)	Select a data source from the list of available data sources. This list box displays the System Data Sources that were configured in the ODBC Control Panel on the C•CURE 9000 Server computer.

Table 42: ODBC Source Configuration Configuration Tab Definitions (continued)

Fields/Buttons	Description
Data Source User ID	Enter the user ID or user name needed to establish an ODBC connection to the data source, if the DSN is configured with SQL Authentication. NOTE: The Data Source Password is disabled if the external database uses integrated Windows Authentication. In that case, you must make sure that the CrossFire Framework Service and the SoftwareHouse CrossFire Import Watcher run on behalf of a user account that has authorized access to the external data source.
Data Source Password	Enter the password needed to establish an ODBC connection to the data source, if it is configured with SQL Authentication. NOTE: The Data Source User ID is disabled if the external database uses integrated Windows Authentication. In that case, you must make sure that the CrossFire Framework Service and the SoftwareHouse CrossFire Import Watcher run on behalf of a user account that has authorized access to the external data source.
Connect to Database	Click this button to connect to the database to obtain the list of database table after selecting a data source in the **ODBC Data Source (DSN)** field.
Data Source Table to Import from	From the drop-down list of tables in the external data source, select the table you want to import from. NOTE: The list is disabled until you select a data source in the **ODBC Data Source (DSN)** field and click the **Connect to Database**e button to connect to the data base.
Data Source Table Prefix Suffix	The prefix and the suffix are required if your table name does not meet the configuration requirements (for example, a table name with spaces in the name). If the external database is a known database, then the prefix and suffix used by that database automatically appear in the fields. Known databases and their corresponding suffix and prefix are listed below: • SQL - Prefix: [- Suffix:] • MS Access - Prefix: [- Suffix:] • Progress - Prefix: Pub. NOTE: If your table name does not meet the name requirements, and you delete the known prefix and suffix, you will receive an error message. The prefix varies across databases. You must enter a valid prefix, depending on the external databases you are connecting to. If the external database is not a known database, or you select a table name that does not conform to the configuration requirements, then the prefix and suffix fields are blank. You must enter a valid prefix and suffix, depending on the external database you are connecting to. The following example describes a non-conforming table name. **Example** A prefix and suffix would be required in the case of using SQL, where the valid prefix and suffix are "[" and "]". If you create a table named "Table 1" and did not provide the prefix and suffix in the Configuration tab, and then select Sample input, an error message is displayed. The query "Select * from Table 1" will not work because the table name has spaces. If the Data Source table prefix and suffix were used, then the query will be "Select * from [Table 1]" which provides the proper result.
External Data Source Primary Key	Select a primary key field for the table. Each record in the table must have a unique value for this field. If the selected data source table has a primary key in it, the primary key will be listed. If the table has a composite key, the combination of keys will be shown separated by a ".". If a primary key was not defined, then all the fields of the selected external table are available for selection, if required. NOTE: If you do not select a primary key field, you will not be able to select a **Delete** option on the **Records** tab.
User	Read-only field that displays the name of the user logged in.
Partition	Read-only field that displays the Partition of the user who configured this Data Import definition.

Table 42: ODBC Source Configuration Configuration Tab Definitions (continued)

Fields/Buttons	Description
Save and Close	Click this button when you have completed any changes to the **Configuration**, **Records**, and/or **Poll Constraints** tabs and wish to save those changes. The tab closes and the **Data Import Editor General** tab reappears.

Configuring the Configuration Tab

To Configure the Configuration Tab

1. In the **ODBC Data Source (DSN)** field, select a data source from the list of available data sources configured in the ODBC Control Panel (see Figure 64 on Page 190). This is a required field.
2. If required by the external database. enter the User ID in the **Data Source User ID** field, otherwise leave the field blank.
3. If required by the external database, enter the password n the **Data Source Password** field, otherwise leave the field blank.
4. Click the **Connect to Database** button to make the connection to the data source and also enable the **Data source table from which to Import** list.
5. Select a table from the **Data Source Table to Import from** drop-down list.
6. If necessary for the syntax for this ODBC driver, enter a Data Source table and/ or suffix.
7. Select a primary key field.

NOTE If the selected table has a primary key defined, it is selected automatically. If a primary key was not defined, then all the fields of the selected external table are available for selection, if required.

The primary key of other tables are listed if there are table names with the same name. For example, if you select Table_1 as the data source table, Table.1 and Table 1 are also listed.

The system automatically displays the name and partition of the user logged in.

The Data Source User ID and Data Source Password are disabled if the external database uses integrated Windows Authentication. In that case, you must make sure that the CrossFire Framework Service and the SoftwareHouse CrossFire Import Watcher run on behalf of a user account that has authorized access to the external data source.

8. Click **Save and Close** when you have completed any changes to the **Configuration** tab and wish to save those changes. The tab closes and the **Data Import Editor General** tab reappears.

NOTE If you change the ODBC data source (DSN), the tables of the new database will not appear for 30 to 60 seconds.

NOTE The ODBC Source Configuration Records Tab must be configured before you save the entire configuration.

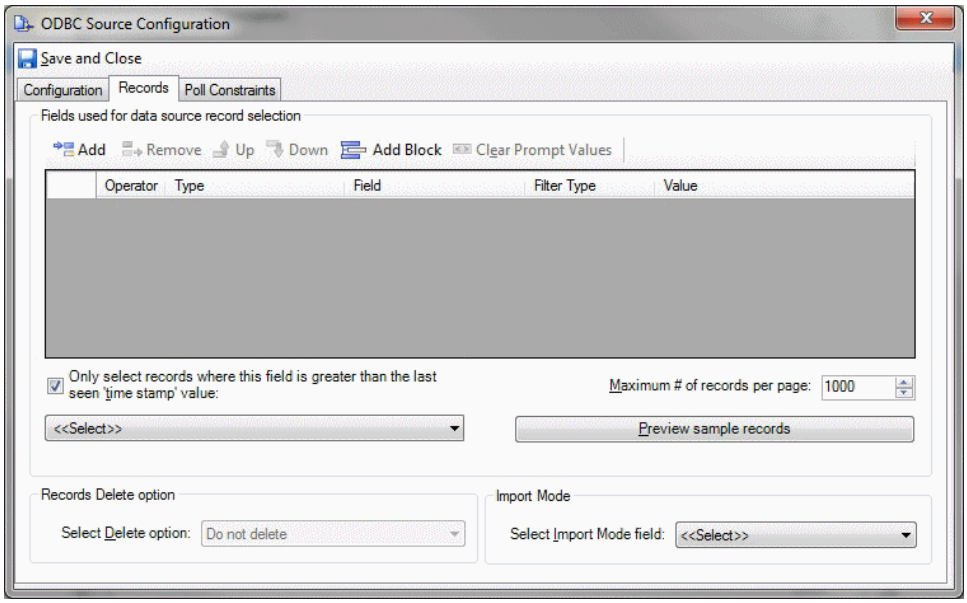
ODBC Source Configuration Records Tab

The **Records** tab, as shown in Figure 65 on Page 193 is used to:

- Set up a query of the data source to select records for import to C•CURE 9000.
- Select additional options for retrieving records from the data source.

NOTE The ODBC Source Configuration Configuration Tab on Page 190 must be completed, and a table for import selected, before the Records tab can be selected.

Figure 65: ODBC Source Configuration Editor Records Tab



Records Tab Definitions

The Records tab has the fields described in Table 43 on Page 193 and the query criteria buttons described in Table 44 on Page 195.

Table 43: ODBC Source Configuration Records Tab Definitions

Fields/Buttons	Description
Fields used for data source record selection (For information on creating complex queries, see the Query chapter in the C•CURE 9000 Data Views Guide.)	
Operator	For every row in the table after the first row and for the first row in a block, you must choose a logical Operator (AND or OR) to define the relationship between the current row and the row that preceded it. **Example:** If the first row queries for Personnel with a Last name that begins with 'B', the next row must specify if its criteria is ANDed or ORed with the first row.
Type	This field is automatically populated by the system with the name of the table from which you are importing.
Field	Select the field for this Query Criteria from the drop-down list of Fields, limited to the fields in the table which you are importing. NOTE: You cannot import a field from an Oracle ODBC source with a name that includes double-quotes (such as "Person_ID"). Oracle allows such fields to be created, but they are not properly recognized by Microsoft SQL, and cause the import to fail. Check the field names in the Oracle source to make sure that none of the fields you intend to import have names enclosed in double-quotes.
Filter Type	This drop-down list lets you chose a filter type for this Query Criteria. The choices vary depending upon the type of field chosen for this row. **Example:** If the Field is a True/False or On/Off field, the Filter Types are Equals or Not Equals.

Table 43: ODBC Source Configuration Records Tab Definitions (continued)

Fields/Buttons	Description
Value	Type in or select a Value for the field in this criteria. The allowable Values depend upon the Field chosen and the Filter Type chosen. **Example:** For a True/False field, a check box is displayed in this column. For a text field, an edit box that you can type text into is displayed. After a new row is appended, <IGNORED> is displayed in the Value column. All rows must have real values, or remove the rows with <IGNORED>, prior to saving the configuration. If you leave an <IGNORED> row in the query and try to **Save and Close**, you will receive an error message.
Other Selection Options	
Only select records where this field is greater than the last seen 'time stamp' value'	Click this option to use a Date Time or Numeric data type field to filter the records for the import. The field's value is combined with the query expression to define the scope of records to be imported from the external table. The value of this field in the ODBC source is used as the starting point for importing records. Choose the field to use from the **<<Select>>** drop-down list. Choose a Date Time field that functions as a time stamp if you wish to identify records updated since the previous import by modification by Date/Time. Choose a Numeric field that is incremented for new rows in the ODBC data source if you wish to identify records updated since the previous import by this value. If you clear the check box for this option, you must change **Select Delete Option** to a value other than **Do not delete** (which is only valid if **Only select records where this field is greater than the last seen 'time stamp' value** is enabled).
Maximum # of records per page	Select the number of records to import at one time. After these records are imported, the next page of records is processed.
Preview sample records	Click this button to open the Preview Sample Records screen containing the actual records with the actual values from the external table. In this case, query is applied on the records.
Records Delete Option	
Select Delete Option	Select one of the Delete options if you want to delete the records from the data source after they have been imported into C•CURE 9000. • **Do not delete** – the default. This option is valid only if 'timestamp mode' (**Only select records where this field is greater than the last seen 'time stamp' value**) is enabled. • **Delete records in chunk** – an entry is created in Import History after importing every chunk (the number of records you configured in the Maximum # of records per page field). • **Delete records in bulk after import** – deletes the records after the entire import has completed.This option is useful i the selected table has no primary index. The entire table is deleted upon import conversion. NOTE: Delete options are not available if you did not select a Primary Key on the ODBC Source Configuration Configuration Tab on Page 190.
Import Mode	

Table 43: ODBC Source Configuration Records Tab Definitions (continued)

Fields/Buttons	Description
Select Import Mode field	The Import Mode values are the default values of C•CURE 9000. The following table lists the import mode values supported.

	String	int	boolean
Default	Default	0	FALSE
Add	Add	N/A	N/A
Set	Set	N/A	N/A
Update	Update	N/A	N/A
Delete	Delete	1	TRUE

Table 44: Records Tab Query Criteria Buttons

Button	Description
Add	Click this button to add a row to the **Query Criteria** table. Each row in the table can act as a query filter. Each new row is added after the last. To add a new row after a specific existing row, click the row selector ▸ to select a row and then click **Add**.
Remove	Click this button to remove a selected row from the **Query Criteria** table. You have to click the row selector ▸ to select a row to remove. If **no** row is selected, this button is **not** available. NOTE: If the selected row is the beginning of a block, the system removes the entire block once you confirm the deletion.
Move Up	Click this button to move a filter row up in the table. The position of filter rows can affect search results. You have to click the row selector ▸ to select a row to move. If **no** row is selected, this button is **not** available.
Move Down	Click this button to move a filter row down in the table. The position of filter rows can affect search results. You have to click the row selector ▸ to select a row to move. If **no** row is selected, this button is **not** available.
Add Block	Click this button to add a block of filter rows to the **Query Criteria** table. Rows that are in a block are resolved (AND/OR conditions evaluated) together, then are evaluated with other table rows in order. **Example:** If you had four rows as below (simplified for example): - **Personnel Last Name** starts with **G [single row]** - **AND [Block rows start]** **Disabled** equals ☑ OR **Logical1** equals ☑ - **[Block rows end]** - AND **Credential Stolen** equals ☐ **[single row]** The query finds **all Personnel** with **Last Name** starting with **G**, then tests those records against both conditions in the **Block filter**, then tests the remaining records for the **Credential Stolen filter**. After you have added the block, click the row selector ▸ to select a row in the block and click **Add** to add more rows to the block. If your added rows are **not** correctly positioned outside or inside the block, select the row and click **Up** or **Down** to correct the positioning.
Clear Prompt Values	Clears out any values entered for a prompt for a criteria and returns the default value for the criteria prompt, <IGNORED> usually. NOTE: All rows must have real values, or remove the rows with <IGNORED>, prior to saving the configuration.

Records Tab Tasks

NOTE The ODBC Source Configuration Configuration Tab on Page 190 must be completed, and a table for import selected, before the Records tab can be selected.

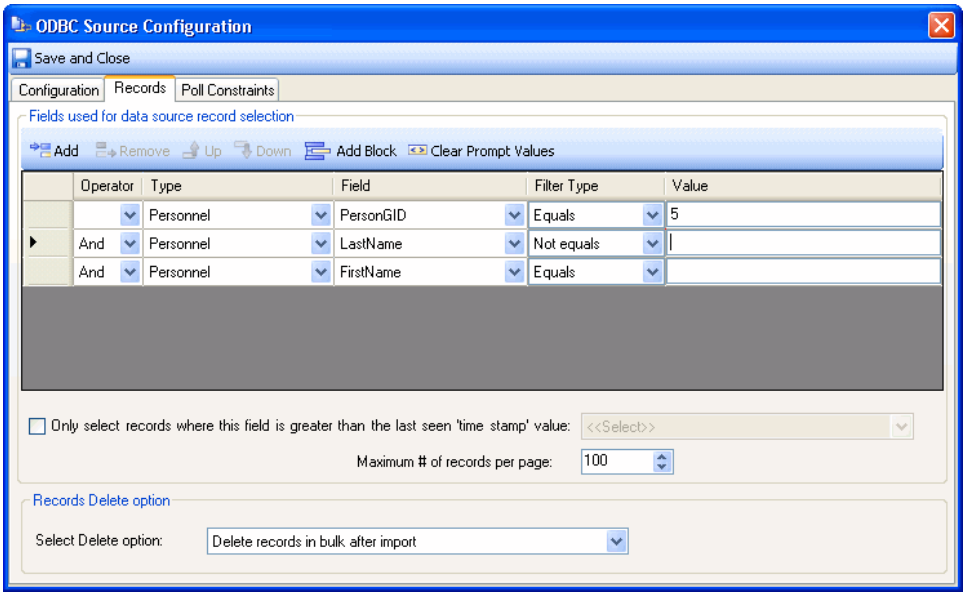
To Configure the Records Tab

1. In the **Data Import Editor General** tab, click **Configuration**.
2. In the **ODBC Source Configuration** dialog box, shown in Figure 64 on Page 190 click the **Records** tab. The tab opens, as shown in Figure 65 on Page 193.
3. Click **Add** . The system enters a new row in the **Fields used for data source record selection** box for you to define a query for retrieving records for import.
4. Select the logical operator (AND or OR) to define the relationship between the current row and the row that precedes it.
5. Select the field for the query criteria.
6. Select, or enter a value for the field.
7. Optionally, select the 'Time Stamp' option and a Time Stamp field so that the import only takes place when the time stamp is updated for changes to the external data source.
8. Select a **Records Delete** option. The default is **Do not delete**.

NOTE The default option, **Do not delete**, is not allowed if the Time Stamp field was not selected in the previous step.

The completed **Records** tab appears as shown in Figure 66 on Page 196.

Figure 66: ODBC Source Configuration Editor – Records Tab Completed



9. Click **Save and Close** when you have completed any changes to the **Records** tab and wish to save those changes. The tab closes and the **Data Import Editor General** tab reappears.
10. See Preview Sample Records on Page 196.

Preview Sample Records

Preview sample records allows you to:

- Verify that the values you entered on the tab have a valid ODBC syntax.
- Validate that you are retrieving the correct records.

All parameters on the **Configuration**, **Records** and **Polling** tabs must be correctly configured for the Preview action to be successful in retrieving samples.

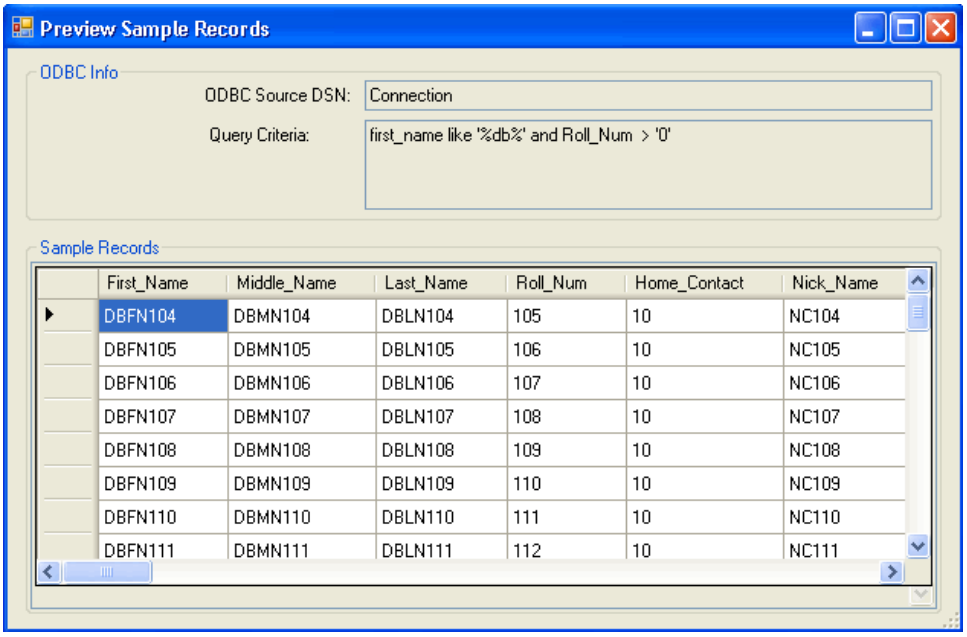
NOTE Software House strongly recommends that you use the **Preview Sample Records** option after any change to the **Configuration** and **Records** tab entries.

To Preview Sample ODBC Records

1. Click the **Preview sample records** button on the **Records** tab.

   The system uses the values you specified on the Records tab, and displays the results in the Preview Sample Records dialog box, as shown in the example in Figure 67 on Page 197.

Figure 67: ODBC Preview Sample Records Screen



NOTE Record information in the dialog box such as that shown in the sample in Figure 67 on Page 197 indicates that no errors were encountered . If the dialog box is blank, it could mean either of the following:

- The specified user does **not** have permissions to see records in the specified ODBC Source DSN.
- The search filter is too restricted.

Table 45: ODBC Preview Sample Records Screen Definitions

Fields	Description
ODBC Source DSN	The ODBC data source name configured for import.
Query Criteria	The criteria applied to search through the sample records.
Sample Records	Displays all the records matching the criteria.

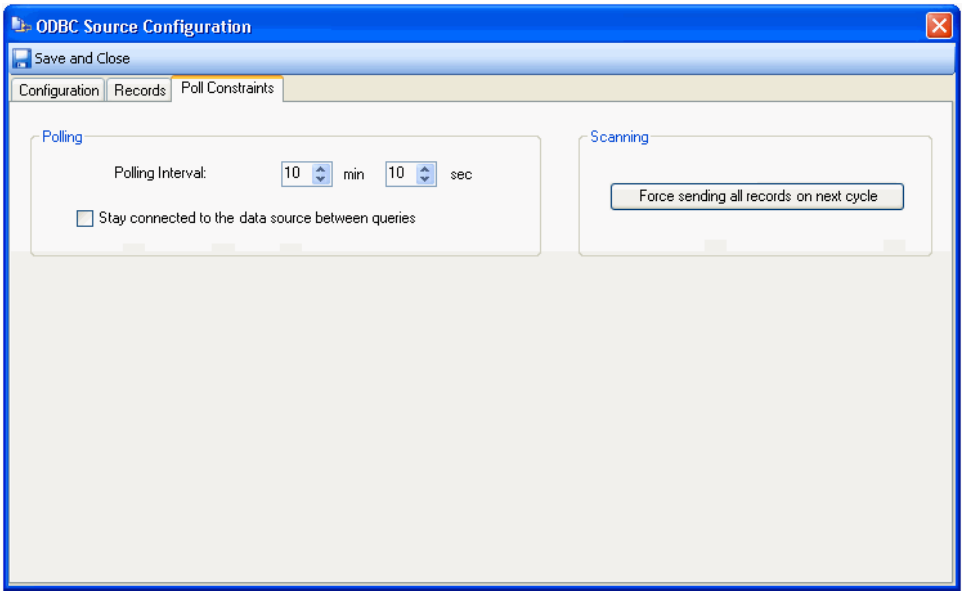
2. Click  to close the dialog box.

ODBC Source Configuration Poll Constraints Tab

The **Poll Constraints** tab, as shown in Figure 68 on Page 198, allows you to specify the parameters for querying the ODBC server for changes and for staying connected to the data source.

NOTE If the Automation mode selected in the General tab is Activated by event, the fields in the Poll Constraints tab are disabled and their values are ignored.

Figure 68: ODBC Source Configuration Editor Poll Constraints Tab



Poll Constraints Tab Tasks on Page 199 for configuration information.

Poll Constraints Tab Definitions

The **Poll Constraints** tab has the fields and buttons described in Table 46 on Page 198.

Table 46: ODBC Source Configuration - Poll Constraints Tab Definitions

Fields/Buttons	Description
Polling Interval	Enter the interval in minutes:seconds at which the C•CURE 9000 Import Watcher checks the ODBC server for changed records within the specified period. The range is 00:10 to 99:59 mm:ss. The default value is 00:30 mm:ss.
Stay connected to the data source between queries	Select this option to keep the ODBC connection open between import queries. Depending on your environment, connecting to an ODBC data source may be relatively slow. As a result, if you are importing frequently, you may want to connect to the data source and then keep the connection open for subsequent imports.
Force sending all records on next cycle	This option is only available if the ODBC import was configured with the 'Timestamp' option. Click this button to have the following take place: • The system deletes all information about the state of records already imported into the C•CURE 9000 system from ODBC. • The next scheduled scan through the ODBC records re-imports all ODBC records from the ODBC server to the C•CURE 9000 database.. This option is useful when the servers have been restored from a backup. However, it does not **delete** records that exist in C•CURE 9000, but do **not** exist in the ODBC backup.

Poll Constraints Tab Tasks

Configuring the Poll Constraints Tab

To Configure the Poll Constraints Tab

1. In the **Data Import Editor General** tab, click **Configuration**.
2. In the **ODBC Source Configuration** dialog box, shown in Table 42 on Page 190, click the **Poll Constraints** tab. The tab opens as shown in Figure 68 on Page 198.
3. In the **Polling Interval** fields enter in minutes:seconds the interval within which the ODBC server checks the C•CURE 9000 server for changed records. This applies only to the **Listening on data** automation mode.
4. Select the **Stay connected to the data source between queries** option to keep the connection open for subsequent ODBC imports
5. Click **Save and Close** when you have completed any changes to the **Poll Constraints** tab and wish to save those changes. The tab closes and the **Data Import Editor General** tab reappears.

Force Sending of All Records

The **Force sending all records on next cycle** button:

- Causes the deletion of all information about the state of the records saved by a previous ODBC import with this Import Definition.
- Causes the next scheduled scan through the ODBC records to re-import all the ODBC records from the ODBC server to the C•CURE 9000.

Consequently, this option is helpful when the servers have been restored from a backup.

NOTE This button is only available after you have selected the Timestamp option, and completed the configuration of this ODBC Import Definition and run the import.

Causes for Automatic Force Sending of All Records

- For both the Full Scan and Timestamp methods, automatic re-sending of records occurs when the following changes happen:
  - Whenever the method is changed from **Full Scan** to **Timestamp** or from **Timestamp** to **Full Scan** , because it is likely that the stored data is out-dated for either method.
  - When one certain kind of field mapping change occurs, as described in the following example:

    Example:

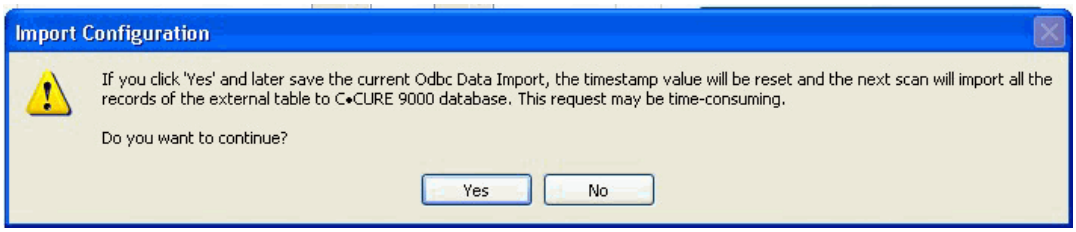
    If the field mapping is changed so that ODBC **field A** which used to be mapped to C•CURE 9000 **field 1** is now mapped to C•CURE 9000 **field 2**. The ODBC field has not changed; it is still **field A** . However, the target C•CURE 9000 field has changed.
- For the **Full Scan** method only, when the match fields on the C•CURE 9000 server change, re-sending of all records is forced. No other changes to the ODBC Import Definition configuration force an actual full re-send of records. However, any other modification to the mapping fields also results in sending all records again. In the latter case, because the deletion history is not lost, it is a more limited type of re-sending.
- For the **Timestamp** method, re-sending all records is forced whenever any of the following change:
  - Field mapping
  - Query Criteria
  - Timestamp field selection

NOTE If either the ODBC or C•CURE 9000 databases are restored from backup, you must manually force the re-sending of all records, as described in the To Force Send All Records on Page 200 procedure.

To Force Send All Records

1. Click the **Force sending all records on next cycle** button.

   The following Import Configuration message is displayed:



2. Click to select one of the following options for the next connection to the ODBC server:
   - Click **Yes** and the last timestamp value will be dropped/cleared. When the next import takes place, the entire external table is scanned and records are imported to the C•CURE 9000.
   - Click **No** if you do not want the records to be re-sent

   The Scanning tab re-appears.
3. If you click **Save and Close** on the **ODBC Source Configuration Editor**, the **Data Import Editor General** tab reappears.
4. If you should then click **Save and Close** or **Save and New** on the **Data Import Editor**, the following Import Configuration message is displayed:

NOTE This message is also displayed when you click to save the Import on the Data Import Editor after making a change to the ODBC configuration, such as to the mapping or to the match fields.

5. Click **OK** if you want all records of interest in the ODBC server to be imported whether or not they have been imported before. (This causes an increased load on C•CURE 9000 while the record transfer is taking place.)

   - or -

   Click **Cancel** to return to the **Data Import Editor** without saving.
6. To close/exit the **Data Import Editor** without forcing a full re-scan, click  .

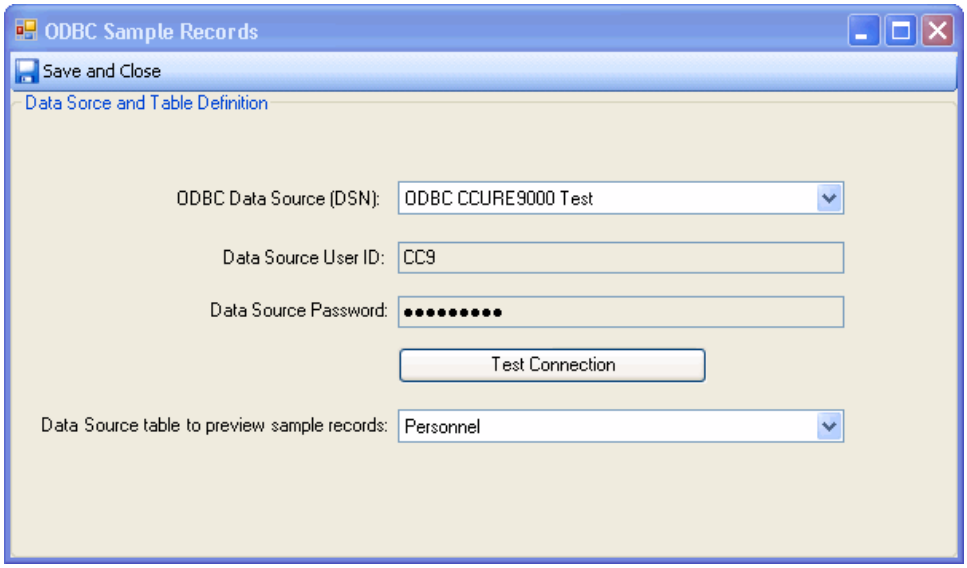
ODBC Sample Records Dialog Box

The ODBC Sample Records dialog box, shown in Figure 69 on Page 201, appears already populated with the entries you made in the Figure 64 on Page 190. The ODBC Sample Records dialog box allows you to check that the sample record created using the ODBC schema has all the properties you want for importing.

The system reads the data from the ODBC sample, converts it to XML, and tries to map it to the C•CURE 9000 target types. The fields of the ODBC sample will be listed in the Data Conversion tab.

Click **Select Sample Input** button on the Data Import Editor to access the ODBC Sample Records Dialog Box.

Figure 69: ODBC Sample Records Dialog Box



ODBC Sample Records Dialog Box Field/Button Descriptions

Table 47: Sample Records Dialog Box Field/Button Description

Fields/Buttons	Description
Data Source Password	Read-only field. The password used to establish an ODBC connection to the data source, if it is configured with SQL Authentication.
ODBC Data Source (DSN)	Select a data source from the list of available data sources. This list box displays the System Data Sources that were configured in the ODBC Control Panel on the C•CURE 9000 Server computer.
Data Source User ID	Read-only field. The user ID or user name used to establish an ODBC connection to the data source, if it is configured with SQL Authentication.
Data source table from which to preview sample records	Select the table you want to preview from the drop-down list of tables in the data source.
Test Connection	Click this button to verify that the C•CURE 9000 server can to connect to the ODBC data source.
Save and Close	When you click this button, you will receive an Import Configuration message. Click OK to open the Data Conversion Tab for you to set up the conversion.

ODBC Sample Records Dialog Box Tasks

To Configure the ODBC Sample Records Dialog Box

1. Click the **Select Sample Input** button on the bottom of the Data Import Editor.

   The ODBC Sample Records Dialog Box appears already populated with the entries you made in the ODBC Source Configuration Editor.

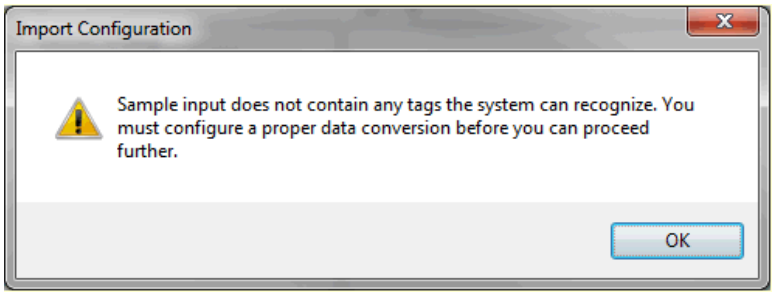
2. Select the ODBC Data Source (DSN), and click the **Test Connection** button.

   The system displays a message informing you whether or not the test was successful.

3. Select the data source table from the Data Source table to preview sample records drop-down list.

4. Click **Save and Close.**

   You will receive the following Import Configuration message:



5. Click **OK** to close the message.

   The Data Conversion tab opens for you to set up the conversion. For information, see:

   - Data Import Data Conversion Tab on Page 89,
   - Data Conversion Tab Definitions on Page 90
   - Data Conversion Tab Tasks on Page 91

Configuring an Import Definition for an ODBC Source

The following steps outline the basic procedures for configuring a simple ODBC Import Definition. Where a procedural element is **not** ODBC-specific, the step references specific sections in the Data Import chapter.

To Configure an ODBC Import Definition

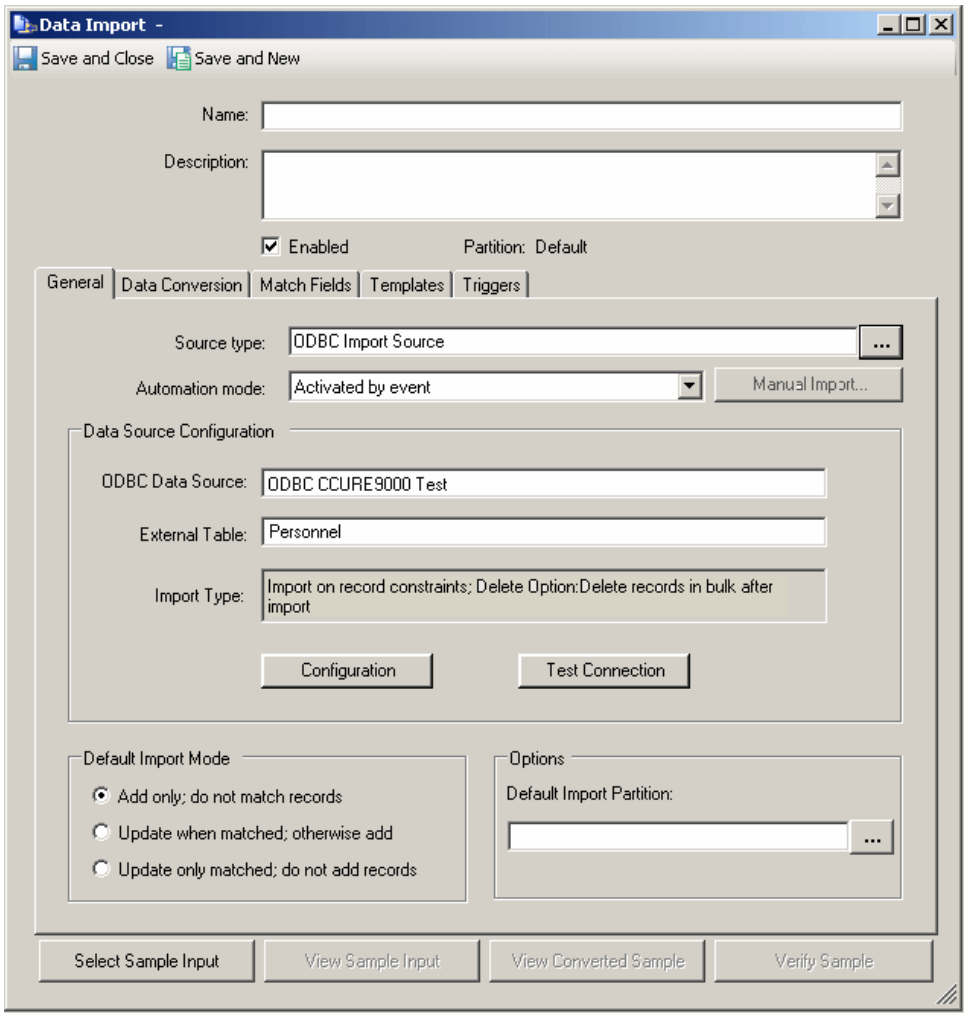
1. Begin creating an Import Definition as detailed in Steps 1 through 4 in Creating an Import Definition on Page 47.
2. On the **Data Import Editor** (see Figure 4 on Page 74), do the following:
   a. Enter a **Name** for the ODBC Import.
   b. Enter a **Description** to distinguish the ODBC Data Import.
3. On the **General** tab in the **Source type** field, click [...] and select **ODBC import source** from the list.

   The system automatically opens the **ODBC Source Configuration Editor** (see ODBC Source Configuration Editor Configuration Tab on Page 190) for you to configure the Import Definition as a connector to an external ODBCdatabase.

NOTE The system also enters **Activated by Event** in the **Automation mode** field and changes the parameters in the **Data Source Configuration** box in the **Data Import General** tab (see Import Editor General Tab for ODBC on Page 186)—although you cannot see this as the **ODBC Source Configuration Editor** overlays it.

4. Configure all three tabs of the **ODBC Source Configuration Editor** according to the following:
   a. **Configuration** tab – see ODBC Source Configuration Configuration Tab on Page 190 and Configuring the Configuration Tab on Page 192.
   b. **Records** tab – see ODBC Source Configuration Records Tab on Page 192 and Records Tab Tasks on Page 196.
   c. **Poll Constraints** tab – see ODBC Source Configuration Poll Constraints Tab on Page 198 and Poll Constraints Tab Tasks on Page 199.
5. Click **Save and Close** when you have finished configuring the parameters on the **ODBC Source Configuration Editor**. The **Data Import Editor General** tab reappears completed, as shown in the example in Figure 70 on Page 204. The **Data Source Configuration** box has the parameters you configured on the tabs of the **ODBC Source Configuration Editor**.

Figure 70: General Tab Data Source Configuration Box Completed for ODBC



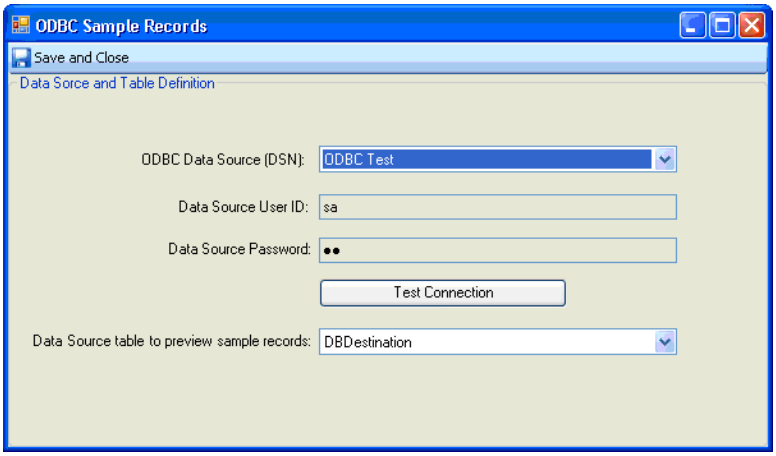
6. Click the **Test Connection** button to check data source connectivity.

   The system displays a message informing you whether or not the test was successful.

7. Click the **Select Sample Input** button on the bottom of the **Data Import Editor**.

   The **Select Sample Records** dialog box appears, as shown in Figure 71 on Page 204, already populated with the entries you made in the **ODBC Source Configuration Configuration** tab.

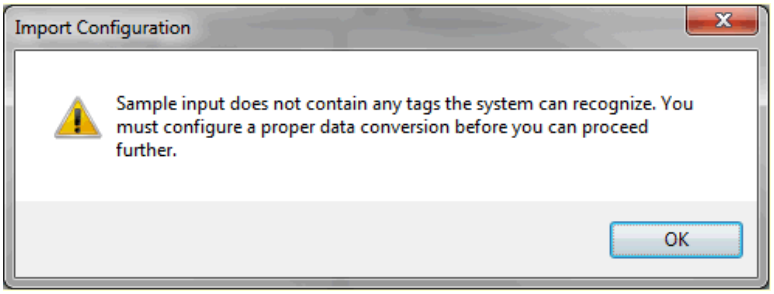
Figure 71: ODBC Select Sample Records Dialog Box



Use this dialog box to check that the sample record created using the ODBC schema has all the properties you want for importing.

The system reads the data from the ODBC sample, converts it to XML, and tries to map it to the C•CURE 9000 data types. The fields of the ODBC sample are listed in the Data Conversion tab.

Figure 72: Import Configuration Message



8. Click **OK** to close the message.

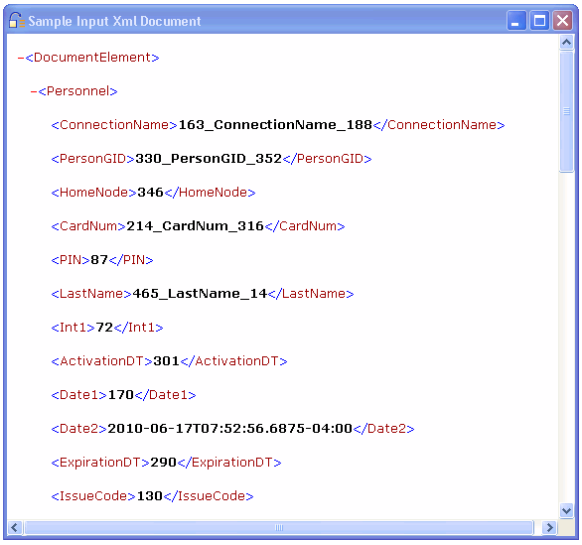
   The **Data Conversion** tab opens for you to set up the conversion. (For information, see on Page 89, Data Conversion Tab Definitions on Page 90, and Data Conversion Tab Tasks on Page 91.)

9. On the **Data Conversion** tab, click **Add** and then click **Personnel mapping tool** from the drop-down list to open the Personnel Mapping tool.

10. Map the fields in the ODBC data source records to the C•CURE 9000 target fields following Using the Personnel Mapping Tool to Convert Personnel Data on Page 95 for general directions. (The information in Personnel Mapping Tool Editor on Page 92 should also be helpful.)

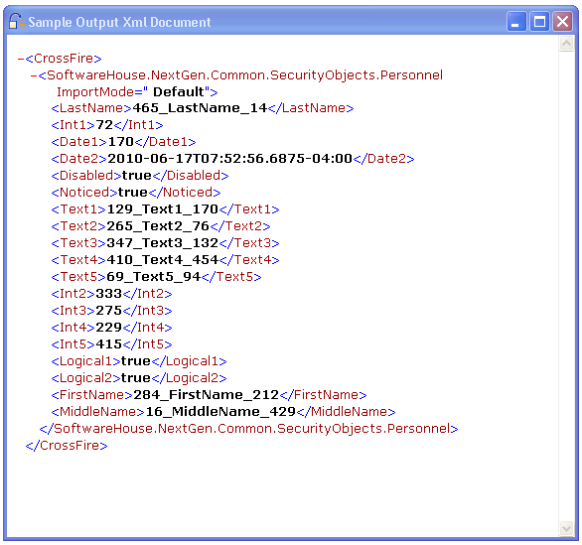
    a. To check the conversion of the ODBC **Data Source** records into an XML document, click the **View Sample Input** button. The converted document opens for your review, as shown in Figure 73 on Page 205.

Figure 73: XML Sample ODBC Import Records



    b. Once you have mapped all the fields, click the **View Converted Sample** button. The converted file opens for your review, as shown in Figure 72 on Page 205.

Figure 74: Sample Output XML Document



c. To save your field mapping, click **Save and Close**.

   The **Data Conversion** tab reappears with the Personnel Mapping tool added as the first row in the Data Conversion table, as shown in Figure 19 on Page 97.

d. To check that the Data Source file has been properly converted, click the **Verify Sample** button. A message displays informing you whether or not every field in the input sample has been recognized.

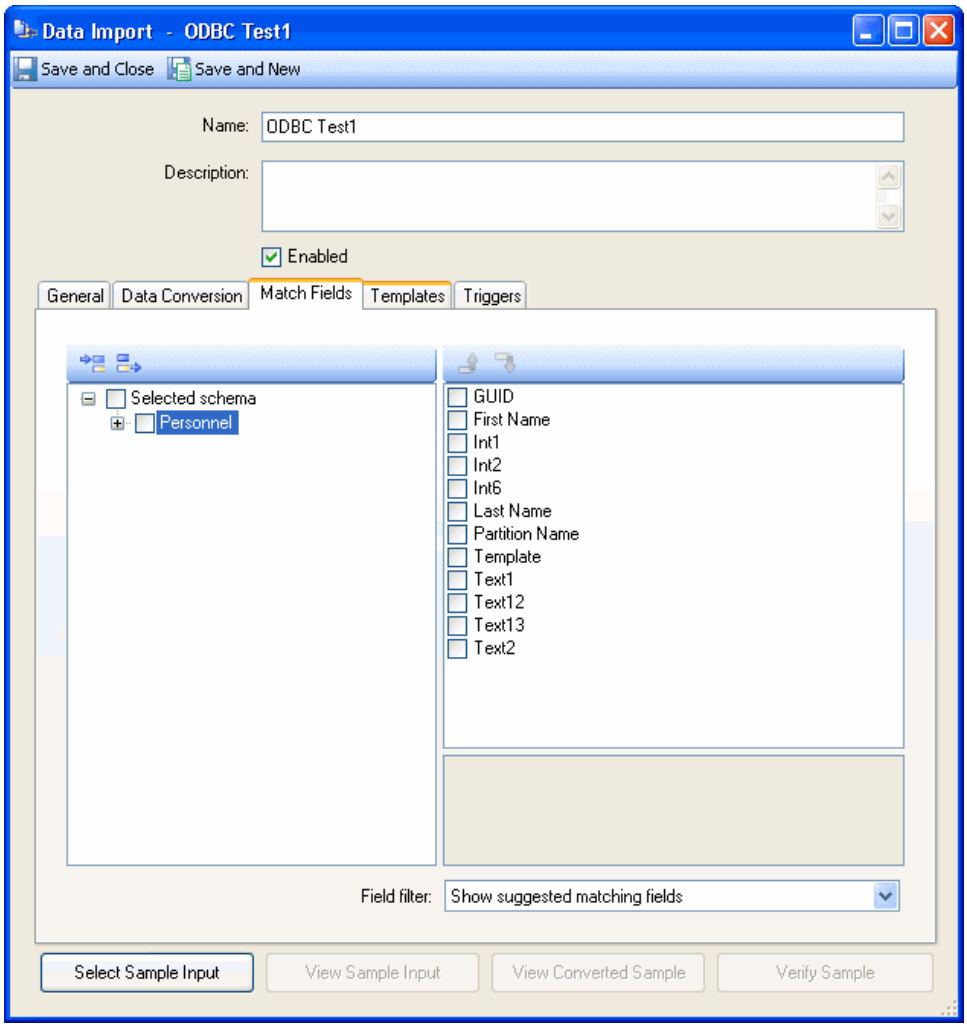
11. Re-open the **General** tab and select **Update when matched**; **otherwise add** as the **Default Import Mode** option

NOTE If you set the mode to **Add only...** or **Update only...** for an ODBC Import, the Import Definition **cannot** be saved, and an error message displays.

12. Click the **Match Fields** tab to open, as shown in the example in Figure 75 on Page 207, to specify the fields on which to match the imported records. (For information about matching, see Match Fields Tab Definitions on Page 121 and Specifying Match Fields on Page 123.)

    Software House recommends that you match on the **GUID** field.

Figure 75: Data Import Editor Match Fields Tab for ODBC



Once you have finished selecting match fields, the required elements of the configuration for an ODBC Data Import Definition are complete. You could save the ODBC Import Definition now.

However, the **Data Import Editor** has two optional tabs that can provide useful functionality for your import: **Templates** and **Triggers**.

NOTE

If you are planning to use any template rules, configure the **Templates** tab before saving the Import Definition because ODBC starts the import process as soon as the Import Definition is saved if the import definition was configured with **Listening on data**.

The import process does not start when the import object is saved if the Import Definition is configured with **Activated by event** Automation mode. The import process starts when the event associated with the import objects becomes active. You can also right-click on the configured import object and select **Run on Server** so start the import process.

13. Click the **Templates** tab if you want to configure template rules, that this ODBC Data Import Definition applies during the import process to the Personnel objects being modified. (Template rules are optional.)

    Template rules can be used for updating information, such as **clearance** assignments, based on different Personnel types (roles) such as **Managers**, **Employees**, and **Contractors**.

    (For complete detailed information about templates, see the Data Import Templates Tab section that starts on Page 127 and ends on Page 139.)

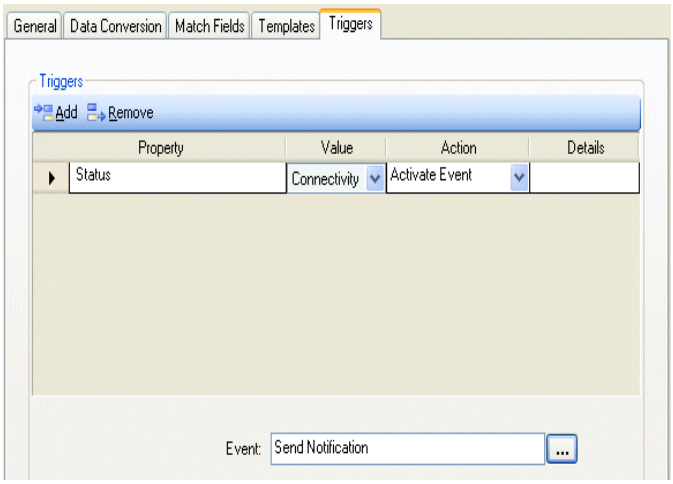
14. Click the **Triggers** tab if you want to configure a trigger to activate an event when this ODBC Data Import Definition has a defined status. (Triggers are optional.)

    A common and important use for a trigger would be notification of the loss of communications between C•CURE 9000 and the ODBC server— **Status** of **Connectivity error** or **Disconnected**. (For information, see Data Import Editor Tasks on Page 69.)

    (For more information about configuring triggers, see Data Import Triggers Tab on Page 140.)

    See Figure 76 on Page 208 for an example of the **Triggers** tag completed for an ODBC Import.

Figure 76: Data Import Editor Triggers Tab for ODBC Completed



15. Make sure that the **Enabled** check box on top of the **Data Import Editor** is still selected (the default) so the Import Definition is operational.

    You have now completed the configuration of an ODBC Import Definition.

16. To save your Import Definition, click **Save and Close.**

    - or -

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

6

Data Export

C•CURE 9000 lets you export records from C•CURE 9000 databases to an export file that can be used to import the records into external databases and other C•CURE 9000 databases. You can export records at any time, schedule exports to run at predetermined intervals, or export records in response to events monitored by the system.

This chapter provides an overview of the export process and describes how to create export definitions, run exports, and examine the results of exporting.

In this chapter

Exporting Overview

C•CURE 9000 manages export information as objects. In C•CURE 9000, the term 'Object' is used to refer to the collection of definable properties that are saved in a database to describe elements of the system (such as readers and controllers), and the activities and individuals that are monitored by the system. You can export C•CURE 9000 Objects and properties to an external database using parameters contained in uniquely named Export Definitions, that are themselves Objects managed by C•CURE 9000.

When you create an Export Definition, you define a collection of C•CURE 9000 Objects and their associated properties to be exported. The result of the export process is an XML file that can be used by the import function of an external target database to import the records taken from C•CURE 9000. The Export Definition can also specify a confirmation file that identifies how many records were exported. C•CURE 9000 maintains a record of exports from the system and provides a means to let you review the export history at any time.

Using a unique name to identify each Export Definition allows you to create multiple Export Definitions, each containing a unique set of records to be exported, depending on your needs. You can also save Export Definitions as templates, to simplify the creation of multiple Export Definitions.

You can use C•CURE 9000 Export to do the following:

- Export data to be imported by another C•CURE 9000 database or an HR or other external database.
- Export files in both manual and automated modes.
- View historical logs for all exports.
- Convert the internal C•CURE 9000 data schema into an external XML document.

For more information, see:

- Data Export Editor on Page 213
- Exportable Objects on Page 210
- The Export Process on Page 211
- Basic Exporting Tasks on Page 216
- Data Export Editor Tasks on Page 222

Exportable Objects

All C•CURE 9000 Objects are exportable, but not all export files are re-importable into another C•CURE 9000system.

Exporting Objects from a Dynamic View

From an Object's Dynamic View, you can export one or more exportable Objects of the same type into an XML or CSV file. You do this by selecting the Object(s) and then clicking **Export selection** on the right-click Context menu. This functionality allows you to quickly and easily create XML/CSV reports on selected C•CURE 9000 data. For information and detailed procedures, see the Dynamic Views chapter in the *C•CURE 9000 Data Views Guide*.

For exporting Configuration pane objects see Exporting an Object on Page 24.

The export creates a special Export Result record in the Import/Export History log for the export operation. For information, see Viewing Export Results History on Page 226.

Exporting Portraits

From the Personnel Dynamic View, you can export Badge images separately as .jpg graphic files. You do this by selecting the Personnel Object(s) and then clicking **Export selected Portraits** on the right-click Context menu. For more information, see

the *C•CURE 9000 Personnel Configuration Guide*.

Hardware Objects

You can export a Hardware tree from one C•CURE 9000 system and then import that tree into another C•CURE 9000 system. To be re-importable in this way, the Hardware Folder and the entire tree from its top-level Object down must be exported and then imported in the following correct sequence:

- iSTAR Hardware
  a. Hardware Folder
  b. iSTAR Cluster with the rest of the tree
- apC Hardware
  a. Hardware Folder
  b. Comm Ports
  c. ISC or apC Controller with the rest of the tree

The exported Tree includes inputs/readers/outputs, but **not** doors. Doors should be exported as separate Objects—each Door type (apC Door or iSTAR Door) with a different Export Definition.

NOTE Custom Card Formats may cause problems when re-importing Readers.

Event/Action Objects

You export Events and Actions as separate Objects. In this way you can export them from one C•CURE 9000 system and re-import them into another C•CURE 9000 system.

NOTE Make sure to import Hardware and Schedules prior to importing Events/Actions.

The Export Process

In C•CURE 9000, successfully exporting records requires a specific sequence of preparation, execution, and review. The process depends on a set of parameters referred to as an Export Definition that you configure in advance. In addition, you must complete other system configuration tasks even before you can begin to create an Export Definition and export data. The configuration tasks depend on whether you are exporting data manually or automatically.

Requirements for Manual Exports

Before you can create an Export Definition for the type of records you want to export into C•CURE 9000, you must:

- Establish appropriate access privileges. For more information about how to determine and update your access permissions, see Privilege Overview on Page 416.

Requirements for Automatic Exports

Before you can create Export Definitions to run exports automatically—either according to a Schedule or in response to an Event, you must complete the preceding requirement for running an export manually. Then you must do the following:

- To export by Schedule, configure an Event and associate a Schedule with the Event. For details about scheduling an Export, see Scheduling Exports on Page 220.
- To export in response to an Event, configure the Event.

(For details about configuring Events, see Understanding Events on Page 237.)

The Export starts running as soon as the Event is activated and keeps running until the operation is complete.

The Export Definition

The Export Definition specifies parameters that the system will follow when creating an export file. The Export Definition provides the option to include a custom query that you can create to filter exported records.

In general, to export records from C•CURE 9000, do the following:

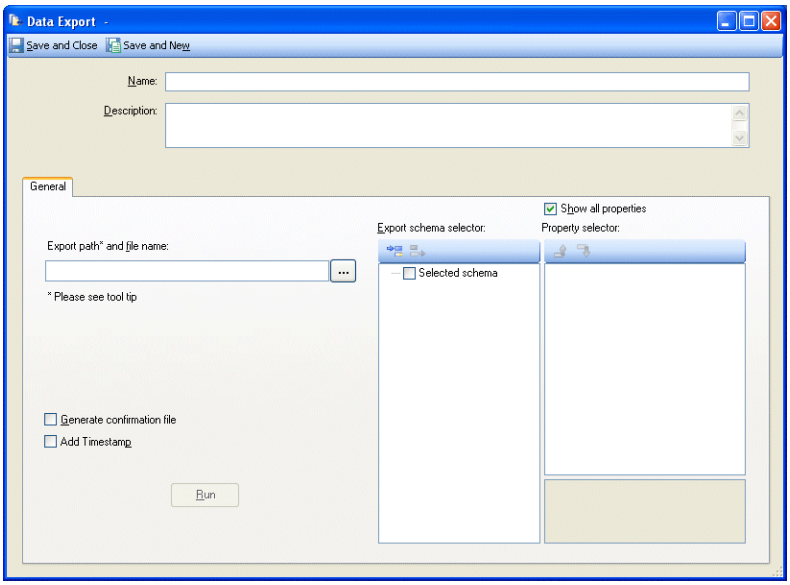
1. Configure an Export Definition that describes the objects and properties that you want to export. Save the Export Definition as a named object in C•CURE 9000. For details, see Creating an Export Definition on Page 216 and Configuring an Export Definition on Page 218.
2. Run the pre-configured Export manually or have the system run it automatically. For details, see Data Export Editor Tasks on Page 222.
3. Examine the results of the export to confirm how many records exported properly. For details, see Viewing Export Results History on Page 226.

Data Export Editor

The Data Export Editor in C•CURE 9000 lets you create multiple Export Definitions for exporting records from the C•CURE 9000 database to files that can be imported into external databases. From the Data Export Editor, you can specify the objects and properties you want to export, as well as other parameters for the export operation.

The Data Export editor has one tab: **General** Tab – see Data Export General Tab Definitions on Page 213 for definitions of the fields and buttons on the General tab.

Figure 77: Data Export Editor



The following topics give more information about the Data Export object and how to use it.

- Exporting Overview on Page 210
- Basic Exporting Tasks on Page 216
- Data Export Editor Tasks on Page 222
- Accessing the Data Export Editor on Page 216

Data Export General Tab Definitions

The Data Export Editor General tab has the buttons described in Table 48 on Page 213.

The Data Export Editor General tab has the fields described in Table 49 on Page 214.

Table 48: Data Export Editor Buttons

Button	Description
Save and Close	Click this button when you have completed any changes to the Export Definition and wish to save those changes. The Export Definition closes.
Save and New	Click this button when you have completed any changes to the Export Definition and wish to save those changes and also create a new Export Definition. The Export Definition you were editing is saved, and a new Export Definition opens (either blank or including template information if you were using a template to create new Export definitions).

Table 48: Data Export Editor Buttons (continued)

Button	Description
	Click this button when you want to close the **Export Definition 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 49: Data Export Editor General Tab Fields/Buttons

Fields/Buttons	Description
Name	The name of the Export Definition. This field is required.
Description	A textual description of the Export Definition. This field is **not** required, but if used can make it easier to identify a specific Export Definition.
Partition	A read-only field displaying the Partition to which this Export Definition belongs. NOTE: This read-only field is visible **only** if the C•CURE 9000 system is partitioned.
General Tab	
Export path* and file name *Please see tool tip	Indicates the name of the XML file that will receive the records you want to export. Click ... to select the location and filename for your export XML file. *The manual export path is relative to the client's machine. Automated export paths are relative to the server's machine. To avoid confusion, always use UNC (Universal Naming Convention) paths. **Example:** \\Computer Name\Program Files\Tyco\CrossFire\Export
Query	Click ... to select a C•CURE 9000 Query to further filter the records to be included in this export. NOTE: This field is available only if you are exporting a single top-level object type—only one top-level object is selected in the **Export schema selector**.
Generate confirmation file	Select this option to indicate that once the export process has completed, the system will create a confirmation file named ExportfileName + ".confirm". The confirmation file is useful for automated exports since it details the number of records exported and its filename indicates the completion date/time. **Example:** If the selected export file is "c:\People.xml', the confirmation file name would be "c:\People.confirm.xml". If you also selected the **Add Timestamp** option, the confirmation file name would be "c:\People.2008-03-29.46.48.confirm.xml".
Add Timestamp	Select this option to indicate that a timestamp will be added to the export filename. This facilitates multi-file exports. **Example:** If the selected export file is "c:\People.xml", the output file name would be "c:\People.2008-04-28.34.28.xml".
Run	Click this button to run the Export. The **Run** button is not available until you save and close the Export Definition, and then reopen it.

Table 49: Data Export Editor General Tab Fields/Buttons (continued)

Fields/Buttons	Description
Show all properties	Select this option to display all exportable properties of the Object type selected in the **Export schema selector** on the left in the **Property selector** on the right. If you clear this option, only exportable user-selectable properties display and are available for selection for exporting. "User-selectable" indicates properties that can be displayed for an Object type in a Dynamic View. **Example:** The selected Object type is **Personnel Clearance Pair**: - If the **Show all properties** option is selected, the properties displayed are: **Clearance ID**, **Clearance name**, **Object ID**, and **Personnel ID**. - If this option is cleared, the only property displayed is **Clearance name**. The default for this option is Selected.
Export schema selector	The **schema selector** displays a tree showing the top-level Object types and their child Objects available for exporting. You use both the **schema selector** and the **Property selector in the right-hand pane** to specify the Objects and properties to be exported by this Export Definition. You can click ⊞ or ⊟ to expand/contract the tree. To include every field in a group of data fields in the export, click the ☐ next to the branch (it becomes a ☑, and every field in the branch is displayed in the **Property selector** with a ☑). To select individual fields to include in the export, click the branch name, and the individual field names appear in the **Property selector** (unselected ☐). You can then click any field to select it (☑).
Add	Click this button to open the Select Type Dynamic View where you can select a new Object type to add to the Export schema.
Remove	Click this button to remove the selected Object type in the tree from the Export schema.
Property selector	The Property **selector** displays the properties associated with the Export **schema selector** branch currently selected. **Example:** If your Export is for **Personnel** objects and you click the branch name **Personnel** in the **schema selector**, the fields that are part of the **Personnel** record are listed in the **Property selector**. To choose a **Property** for exporting, double-click the **Property** name, and a ☑ appears to the left of the name to indicate it is selected for the Export; or click the ☐ to the left of the **Property** name. To clear a **Property** so it is not included in the Export, click the **Property** name, and a ☐ appears to the left of the name to indicate it is no longer selected; or click the ☑ to the left of the **Property** name.
(Property description)	When you select a Property in the **Property selector**, a description displays in the box underneath.
Up	Click this button to move a selected property up in the Property list. This button is unavailable if the first row is selected.
Down	Click this button to move a selected property down in the Property list. This button is unavailable if the last row is selected.

Basic Exporting Tasks

The primary tasks related to the exporting of data that the C•CURE 9000 Data Export Editor allow you to accomplish are:

- Accessing the Data Export Editor on Page 216
- Creating an Export Definition on Page 216
- Creating an Export Definition Template on Page 217
- Configuring an Export Definition on Page 218
- Running an Export on Page 219
  - Running Exports Manually on Page 219
  - Running Exports Automatically on Page 220

Data Export Editor Tasks

- Selecting Objects for Export on Page 222
- Viewing a List of Data Exports on Page 224
- Deleting an Object on Page 25
- Modifying a Data Export on Page 225
- Viewing the Confirmation File on Page 226
- Viewing Export Results History on Page 226

Accessing the Data Export Editor

You can access the **Data Export Editor** from the C•CURE 9000 **Configuration** Pane of the **Navigation** Pane of the Administration Client.

To Access the Data Export Editor

1. Click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Data Export**.
3. Click **New** to create a new Export Definition.

   - or -

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

The **Data Export Editor** opens.

Creating an Export Definition

You create a new export definition using the **Data Export Editor**. For information on export prerequisites, see The Export Process on Page 211.

To Create an Export Definition

1. In the **Navigation** Pane of the Administration Client, click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Data Export**.

3. Click **New**to create a new Export Definition. The **Data Export Editor** opens, as shown in Figure 77 on Page 213.
4. You can now configure the Export Definition—specifying the objects and object properties you want to export; indicating whether or not you want a confirmation file generated when the export is completed and/or a timestamp added to the export; and if only one top-level Object is being exported, selecting a query to filter the records included in the export operation.
   - Generating viewable confirmation files allows you to ensure that the export file was created and when (completion date/time) and with how many records. This is useful information when you are exporting automatically.
   - Adding the date and time the export finished to the file name of the completed export can help to distinguish specific export files when you are creating multiple export files.
   - Using a query helps to control which records are included in the export operation. You create the query using the C•CURE 9000 Query Editor. See the *C•CURE 9000 Data Views Guide* for more information on Queries.
5. To save your new Export Definition, click **Save and Close**.

   - or -

   Alternatively, if you want to save the Export Definition and then create a new one, click **Save and New**. The current Export Definition is saved and closed, but the **Data Export Editor** remains open ready for a new Export Definition (either blank or including template information if you were using a template to create the saved Export definition).

Creating an Export Definition Template

An Export template can save time and effort if you are creating multiple Export Definitions with similar characteristics.

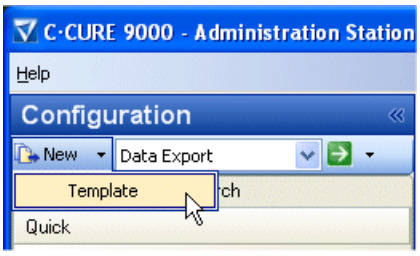
Example:

If you want multiple Export Definitions to export the same Object and its child Objects—**Personnel** and **Personnel Clearance Pair**, **Images**, and **Credential**—but include different object properties, you can create a template that specifies the selected Objects. Then use the template to create multiple Export Definitions that you modify as necessary, and then save as new definitions.

Creating a New Export Definition Template

To Create an Export Template

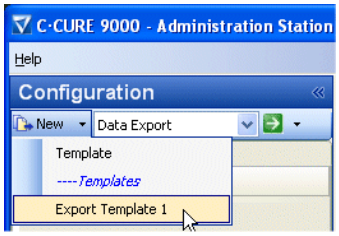
1. In the **Navigation** pane of the Administration Client, click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Data Export**.
3. Click the down-arrow on the **New** button, and click **Template**.



The **Data Export Editor** where you can configure the export template opens.

4. Configure the template to meet your requirements. Any fields for which you configure values become part of the template; then when you subsequently create a new Export Definition from that template, these field values are already filled in.
5. In the **Name** field, enter the name you wish to use for the template (**Export Def 1**, for example).
6. To save the template, click **Save and Close**.

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



Configuring an Export Definition

Configuring an Export Definition is the process of specifying the Objects and properties you want to export; indicating whether or not you want a confirmation file generated once the export is finished and/or a timestamp added to the export; and if only one top-level Object is being exported, selecting a Query to filter the records to be included in the export.

To Configure an Export Definition

1. Open an existing Export Definition using the **Data Export Editor**, or create a new one.
2. In the **Data Export Editor**, do the following:
   - In the **Name** field, enter a unique name to identify the Export Definition when you run the export. You can enter up to 100 characters.
   - In the **Description** field, describe the Export. You can enter up to 500 characters.
3. On the **General** tab, do the following:
   a. In the **Export file name** field, identify the XML file to receive the records you want to export. Click ... to locate the file. C•CURE 9000 creates this file automatically when the data export is created, and names the file based on the name of the Export Definition.

NOTE If there is a space in the filename selected for this field, the entire filename may not *display* in the field, although the file you selected is entered. To see the complete filename, place the cursor in the field and press the right-arrow key, or "hover" the cursor over the field to display the tooltip.

   b. Select the **Generate confirmation file** option to have the system create a confirmation file when the export completes by appending ".confirm" to the Export file name. This is useful for automated exports.
   c. Select the **Add Timestamp** option to have the system add the date and time the export is completed to the Export file name.
4. Using the **Export schema selector** and the **Property selector**, select the Objects and properties that you want to export. Click the  icon to add Objects to the **schema selector** pane. For details, see Data Export Editor Tasks on Page 222.
5. In the **Query** field, click ... to select a pre-defined Query from a Select List to filter the data to be exported.

NOTE The Query field is not available until you have selected the export schema and only if one top-level Object type was selected.

Example:

If your Export schema includes both **Personnel** and **iSTAR Clusters**, the **Query** field is not available.

6. To save your Export Definition and close the editor, click **Save and Close**.

- or -

Alternatively, if you want to save the Export Definition and then create a new one, click **Save and New**. The current Export Definition is saved and closed, but the **Data Export Editor** remains open ready for a new Export Definition (either blank or including template information if you were using a template to create the saved Export Definition).

To run the Export Definition you have just created, you must save the Export Definition.

NOTE The **Run** button is **not** available until you save and close the Export Definition. When you re-open the Export Definition, the **Run** button is available.

Running an Export

You can run exports manually or automatically. When using either method, you must specify a pre-configured Export Definition. When running an export automatically, you must also consider how you want to initiate the export.

You can launch an export according to a schedule, or in response to a pre-determined event that can be monitored by C•CURE 9000. Because they run independently, executing automatic exports requires that you ensure in advance that the export file you specify in the Export Definition is available when the export attempts to start.

You can run exports in several ways:

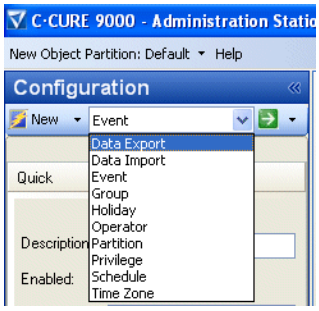
- Manually, at any time. See Running Exports Manually on Page 219.
- Scheduled at a specified time. See Scheduling Exports on Page 220.
- In response to an Event monitored by the system. See Running an Export in Response to an Event on Page 221.

Running Exports Manually

You can run a pre-configured Export Definition at any time. You must configure and save an Export Definition before you can use it to export data from C•CURE 9000.

To Run an Export Manually

1. In the Administration Client, on the Navigation pane, select **Configuration**.
2. On the **Configuration** pane, in the drop-down menu, select **Data Export**.

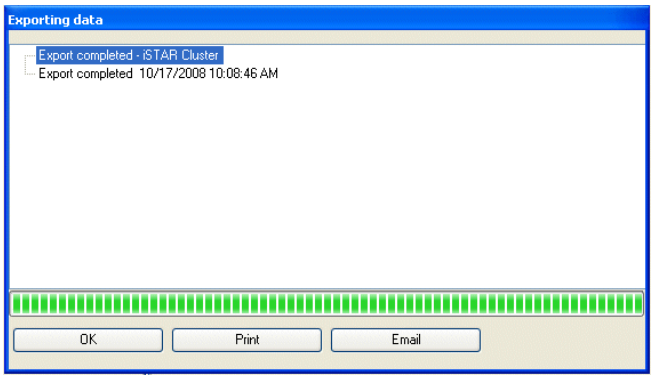


3. On the Search pane, in the **Name** field, enter the name of the Export Definition you want to open, or search for Export Definitions by clicking . From the search results displayed in the right pane as a dynamic view, select the Export Definition you want to run.
4. Do one of the following:
   - In the dynamic view, right-click the selection and click **Run** on the context menu.
   - In the dynamic view, double-click the selection and click **Run** in the **Data Export Editor** that opens.

The progress of the export displays in the **Exporting data** dialog box, shown in Figure 78 on Page 220. A message displays in this dialog box to indicate when the export of each object is complete and to indicate when the entire export finishes.

To cancel the export, click **Cancel** while the export is running.

Figure 78: Exporting Data Dialog Box



5. When the export is complete, do one of the following:
   - To close the **Exporting data** dialog box, click **OK**.
   - To print a copy of the information about this export, click **Print**.
     - On the standard Windows **Print** dialog box, click **OK**.
     - On the **Print Preview** dialog box that displays, click  .
   - To transmit a copy of the information by email, click **Email**.
6. If the Export Definition was configured to generate a confirmation file, review the confirmation file. By default, confirmation files are created in the folder where the export file is saved. For more information, see Viewing the Confirmation File on Page 226

Running Exports Automatically

In C•CURE 9000, you can run Exports automatically according to a Schedule, and in response to an Event. Automated exports run in the context of a specified Operator, the one who created or last edited the Event Action. The Operator must have the appropriate permissions to run the export. Only Objects this Operator has Privileges to access are exported. For details, see Privilege Overview on Page 416. In all cases, you must have previously configured an Export Definition to implement an automated export. For details, see Creating an Export Definition on Page 216 and Configuring an Export Definition on Page 218.

Scheduling Exports

To schedule an export, you must configure an Event that is associated with a pre-defined Schedule and runs the export as an Action.

To Run an Export on Schedule

1. Open an existing Export Definition on the **Data Export Editor**, or create a new one.
2. Configure your Export Definition appropriately according to the directions in this chapter.
3. Save the Export Definition by clicking **Save and Close**.
4. Configure the Event to run the Export by Schedule as follows:

a. Assign the Event a unique name.

b. On the **General** tab of the **Event Editor**, select a schedule that you want to use to determine when the export runs.

   You can select from Schedules already defined in C•CURE 9000. To run the export at a time different from those configured in the available Schedules, you must create and save a new Schedule. For details about how to create a schedule, see Schedule Overview on Page 466.

c. On the **Action** tab of the **Event Editor**, specify **Run Export** as an Action for the Event and select the Export Definition you want to run from the Exports currently saved in the system.

NOTE The system automatically enters the name of the Operator who is configuring/modifying the Event Action (and in a partitioned system, their Partition) indicating that the 'Run Export' Action is occurring with their Privilege. (This Operator's name [and Partition, if existing] will be entered in the Journal message and Export History that record the running of this export at its scheduled times.)

   You can configure other aspects of the Event, such as:

   — Priority of the Event

   — Messages sent when the Event runs the export

   — Acknowledgement requirements

   — Messages or secondary Events triggered if this Event is deactivated.

d. Make sure that the Event is both **enabled** and **armed**.

   For details about configuring Events, see Understanding Events on Page 237.

Running an Export in Response to an Event

To run an export automatically in response to an Event, you configure an Event that runs the export. The export runs when the system detects the trigger action for the event. You can also configure a separate Event that triggers the Event that runs an export.

To configure an Event to run an export, follow the previous procedure (with the exception of Step 4b).

Data Export Editor Tasks

You can perform the following tasks to export data from C•CURE 9000.

- Selecting Objects for Export on Page 222
- Viewing a List of Data Exports on Page 224
- Modifying a Data Export on Page 225
- Deleting an Object on Page 25
- Viewing Export Results History on Page 226

Selecting Objects for Export

When you configure an Export Definition, you must specify the Objects and the Properties that you want to export. You accomplish these tasks with the **Export schema selector** and **Property selector** provided as two panes on the right side of the **Data Export Editor General** tab, as shown in Figure 77 on Page 213 and Figure 79 on Page 224.

Using the Export Schema and Property Selectors

- The **Export Schema selector** allows you to select the Object Types and any child Objects for your Export Definition, and also to quickly select or clear the Properties to include in the export.
- The **Property selector** allows you to select the Properties of the Object you want to export. By default, all Properties are selected for export. To prevent an Object Property from being included in the export, you can clear the check box for the property.

The **Export Schema selector** displays a tree showing the Object Type(s) you have chosen for your Export Definition, as well as any child Objects related to the selected type.

Example:

If you choose an Object type of **Personnel**, the **Export Schema Selector** displays **Personnel** and its child Objects—**Personnel Clearance Pair**, **Images**, and **Credential**.

If you click  to select () the Object type or child Object branches of the tree, you cause all the Properties of that Object type or child Object to be selected in the **Property selector**, as well as all Properties in its child Objects (if there are any).

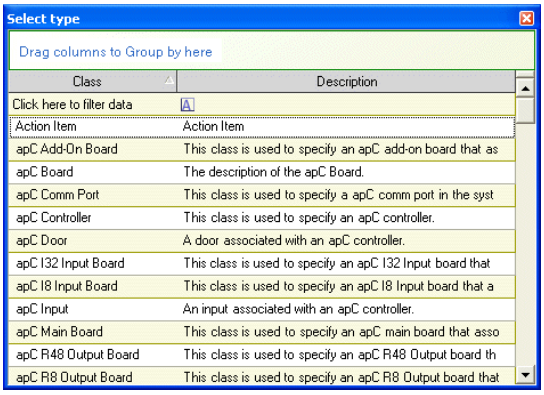
If you click the Object type or child Object name in the tree, you cause all Properties of that Object type or child Object to appear in the **Property selector**, without being selected. You can then select () individual Properties to be included in the Export Definition.

NOTE Once you select a Property for an Object type or child Object in the **Property selector**, the related Object, any Object(s) higher in the Export Schema hierarchy, and the Selected Schema appear selected in the tree, with  next to their name. The Properties in the top-level Object types are not selected, however.

To Use the Export Schema Selector and the Property Selector

1. Create or modify an Export Definition. See Creating an Export Definition on Page 216 and Configuring an Export Definition on Page 218.
2. In the **Export schema selector** pane, click  to add Objects to the Export.

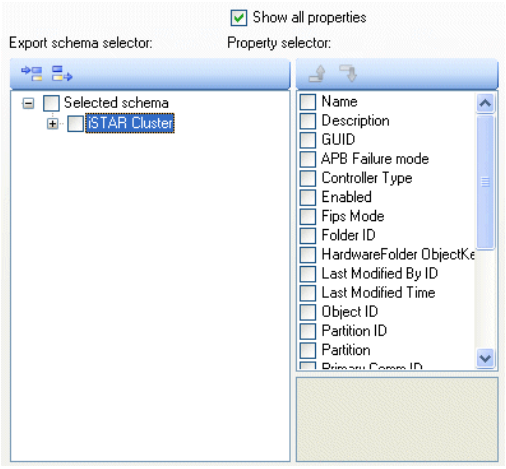
   The system displays the **Select Type** dynamic view where you select Objects types (one at a time) for your Export Definition.



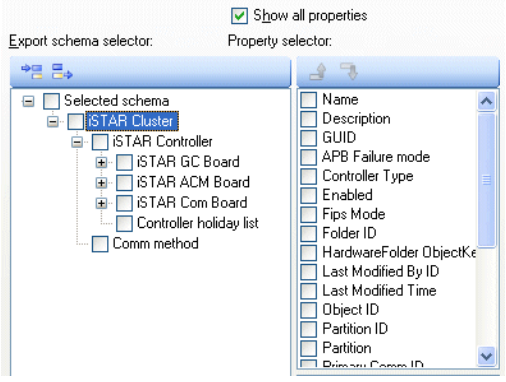
3. Click to select the Object type you want to export and add it to the **Export schema selector**.

   (To remove Object types from the **Export schema selector**, select the Object, and click Remove object.)

   The **Export schema** and **Property selectors** now appear.

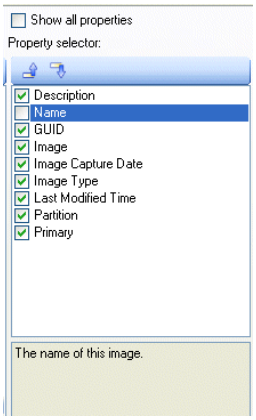


4. Click to expand the tree (or to contract it).



5. In the **Export schema selector** Tree:
   - Select next to an Object Type or child Object to select all Properties of that type and all its sub-types.
   - Click an Object Type or child Object name to display all its Properties. (You can then act on individual Properties to select/remove them from inclusion in the Export.)
6. To display all the exportable properties for an Object Type, select **Show all properties**. To display only user-selectable exportable properties, clear **Show all properties**.

7. In the **Property selector**, choose the Properties you want to include in the export—either by double-clicking the field name or by clicking to the left of the field name. A appears in the check box. Clear the check boxes of the Properties you do not want to export.
   - To see information about a Property, highlight it and a description displays in the box at the bottom of the **Property selector**.



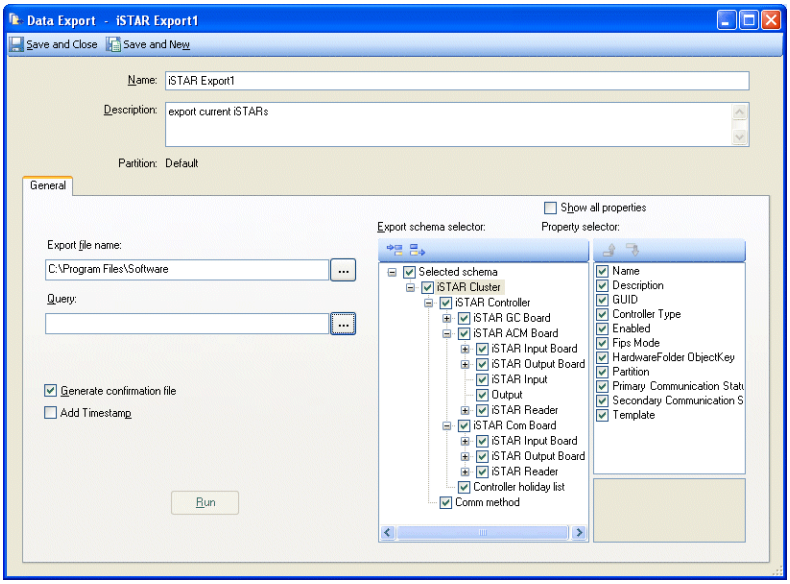
If the selections you make are not valid, a red information icon flashes next to the pane or field that needs correction.

a. Move the cursor over the icon to display the tooltip of information on the selection.

b. Correct the selection.

The completed Export Definition appears as shown in the example in Figure 79 on Page 224.

Figure 79: C•CURE 9000 Export Editor completed



Viewing a List of Data Exports

You can display a list of the Data Export Definitions you have created by opening a Dynamic View of Data Exports. See Viewing a List of an Object Type on Page 22.

Data Export List Context Menu

The context menu that opens when you right-click a Data Export in the Data Export Dynamic View includes the selections described in Using the Object List Context Menu on Page 23.

Context menu options specific to Data Export are described in Table 50 on Page 225.

Table 50: Data Export List Right-Click Context Menu Options

Menu Selection	Description
Set property	Click this menu selection to change the value of the selected properties in the selected Data Export(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 this property. The following properties can be changed. • **Add Timestamp** – You can determine whether or not this Data Export should have a timestamp added to the export filename by selecting this property and selecting/clearing the **Value** check box. • **Description** – You can change the textual description of the Data Export(s) by selecting this property and typing in a new value. • **Generate Confirm file** – You can determine whether or not this Data Export should have a confirmation file created by the export operation by selecting this property and selecting/clearing the **Value** check box. • **Show All Properties** – You can determine whether or not the **Property selector** on the Data Export Editor should display all exportable properties of the selected Object type or only exportable user-selectable properties by selecting this property and selecting/clearing the **Value** check box.
Run	Click this menu selection to cause the selected Export Definition to start exporting files. See Running Exports Manually on Page 219.
Change Partition	Click to open a dialog box that allows you to change the Partition to which the Export Definition belongs. For information see, Changing the Partition of an Object on Page 395. NOTE: Changing the Partition of a Data Export Object can prevent some automatic Exports from running—if the new Partition is not included in the Privileges of the Operator who owns the Event Action.

Modifying a Data Export

You can modify an existing Data Export by editing it using the **Data Export Editor**.

To Modify a Data Export

1. In the **Navigation** pane of the Administration Client, click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Data Export**.
3. Click  to open a **Dynamic View** showing a list of all Data Export Objects.
4. Right-click the Data Export you want to change and click **Edit** from the context menu that appears.

   - or -

   Double-click the Data Export you want to change.
5. The **Data Export Editor** opens for you to edit the Export making changes as you wish.
6. To save your modified Data Export, click **Save and Close**.

   - or -

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

Viewing Export Results History

After the export completes, you can review the export results by reviewing the confirmation file, if you configured the Export Definition to generate one.

C•CURE 9000 also provides a function that allows you to review the export history for the entire C•CURE 9000—the **Data Import/Export History** option on the **Options and Tools** pane.

The **Export history** tab includes the following information:

Name	Unique name that identifies the export in the system. **Not** the name of the file containing data being exported.
Description	Description given to the export when configured. No more than 500 characters.
Operator Name	Name of the operator performing the export. (For an automated export or any export initiated by an Event, this is the name of the Operator who configured the Event—and its Action, or last modified it.)
Export Filename	Name of the file containing the XML data being exported.
Created at time	Time when the export was started.
End at time	Time when the export finished.
Status	The current status of the export. **Example:** **Completed**
# Exported	Number of records that were exported from the system.
Confirm File	Name of the file that confirms the completion of the export. Specifies the export filename and the date and time the export finished.
Partition	Name of the Partition of the export. (If your system is non-partitioned, 'Default' is entered.)

For more information, see the *C•CURE 9000 System Maintenance Guide*.

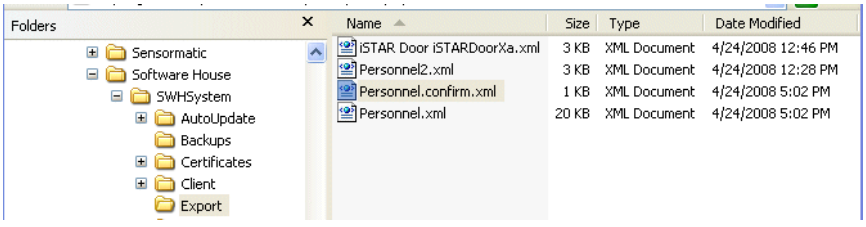
Viewing the Confirmation File

The confirmation file is an XML file that indicates the date/time when the export completed and how many records were exported.

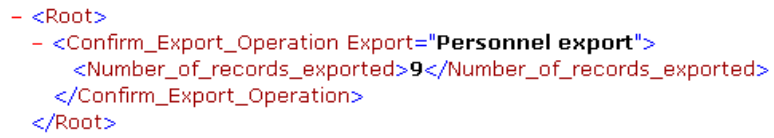
By default, the confirmation file is created automatically in the same folder as the export file specified in the Export Definition, and based on the name of the Data Export Definition with a .confirm file extension.

To View the Confirmation File

1. In Windows, open the folder that contains the export file generated by the export.



2. In a browser or text editor, open the confirmation file.



7

Document

This chapter describes how to add Document objects to C•CURE 9000.

In this chapter

Document Overview

You can add Document objects to C•CURE 9000 using the Document editor. You can then link these Document objects to other C•CURE 9000 objects.

You can add Documents to the following:

- Personnel records – to supplement the information in the record—with procedures for the employee's department or parking regulations, for example. You do this on the Personnel Documents tab. For information, see the *C•CURE 9000 Personnel Guide.*
- Events (for Event Assessment) – to provide a Document that opens when the Event is assessed and gives the operator information specific to that Event, such as a procedure to follow or a URL to a web page showing a map of the facility. You do this on the Events Editor Assess Event tab. For information, see the Assess Event Overview on Page 271.

To be able to add Documents to the system and to remove them, you must have full Permissions for Documents. For more information, see the Privilege Editor on Page 423.

NOTE The system uses Adobe Reader in conjunction with the web browser to display many of the Document objects. Therefore, you must make sure that Adobe Reader is installed.

For more information on using the Document editor and creating document objects, see:

- Document Editor on Page 230
- Document Object Tasks on Page 233

Document Editor

The Document editor allows you to add Document objects to C•CURE 9000. You can then use these Documents within the application, attaching them to:

- Personnel records to provide additional information.
- Events as part of the Assess Events feature.

For information about the Document object and editor see:

- Document Overview on Page 229
- Document Editor Definitions on Page 232
- Document Object Tasks on Page 233

Adding Documents to C•CURE 9000

You create a document object in the C•CURE 9000 database by:

- Importing any one of many different file types that are then stored in the database:
  - PDF, TXT, XML, DOC, XML, or XLS.
  - An Image file such as a JPG, GIF, PNG, TIF, or other type.
- Specifying the target URL of a web page. The URL (not the actual web page) is stored in the database.

NOTE You can only import Document files smaller than 500K.

When you select and import a URL or a PDF, TXT, or XML file, or an Image File whose Viewer is supported by the browser, the Document contents display for viewing in the browser in the bottom half of the **Documents** editor.

When you select another type of file, such as a DOC or XLS file, a **File Download** dialog box appears asking "Do you want to open or save this file?" When you click **Open**, the file appears in an external window in its native format. (Image files whose viewer is not supported by the browser, TIF files, for example, open in whichever Graphics application format you have on your system—such as Paint Shop Pro or Paint.)

Figure 80 on Page 231 shows the Document Editor as it appears for selecting Files (the default). Figure 81 on Page 231 shows the Document Editor as it appears for selecting URLs.

Figure 80: Document Editor for Importing Files

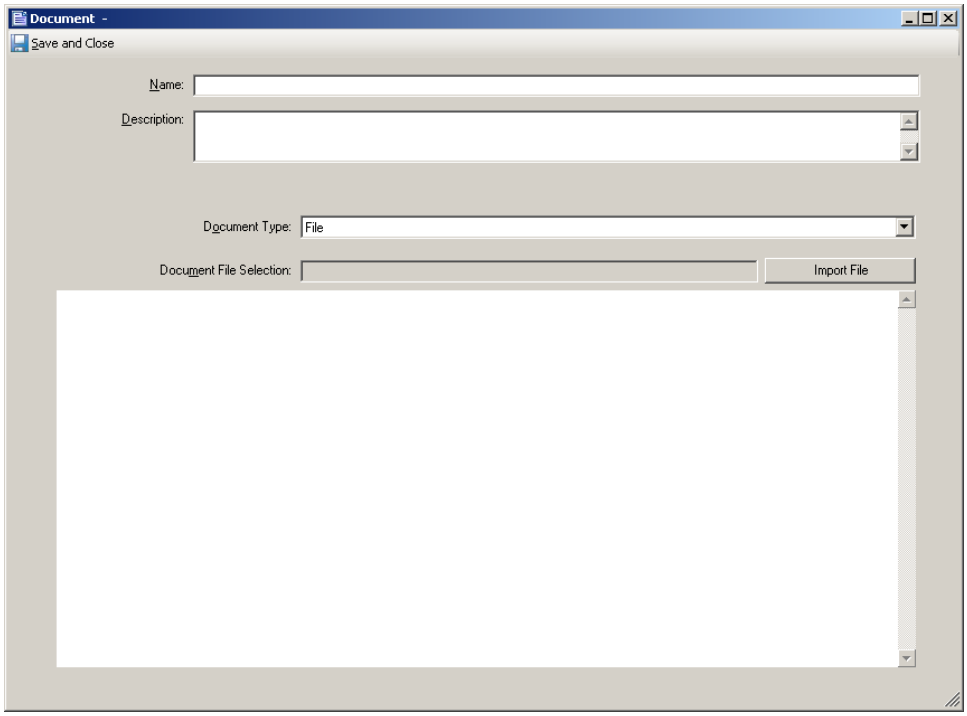


Figure 81: Document Editor for Importing URLs

Accessing the Document Editor

You access the Document Editor from the C•CURE 9000 Configuration pane.

To Access the Document Editor

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

   - or -

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

   The **Document Editor** opens, as shown in the example in Figure 80 on Page 231.

Document Editor Definitions

Definitions for the fields and buttons in the Document editor are described in Table 51 on Page 232.

Table 51: Document Editor Definitions

Field/Button	Description
Name	Enter the name you want to assign this document in C•CURE 9000.
Description	Enter a textual description for this document.
Document Type	This drop-down list lets you select the type of Document you want for this object and the Document selection field changes accordingly. (The default type is **File**.) • If you select **File**, the next field becomes the **Document File Selection** field, and an **Import File** button appears on the right. • If you select **URL**, the next field becomes the **Document URL** field, and a **View URL** button appears on the right.
Document File Selection - or - Document URL	This field changes depending on the Document Type you selected in the previous field. • **Document File Selection** – Select the PDF, TXT, or other type of file that you want to import into C•CURE 9000 for this Document object by clicking the **Import File** button. • **Document URL** – Type the URL that you want this Document object to contain. If you don't start the URL with http://, the system adds it when you click **View URL**.
Import File	Click this button to open a Windows file dialog box for locating the file you want to import into the system. When you click the down-arrow on the **Files of type** field, three file types drop down that you can use to filter your options: • Documents (*.pdf; *.txt) • Image Files (*.bmp; *.jpeg; *.gif; *.png) • All Files (*.*) Select a file and click **Open**. (The document can be no larger than 500K or an error message displays.)
View URL	Once you have entered a URL into the **Document URL** field, click this button to view it in the Content area.
Content Area	The Document you've imported into C•CURE 9000 displays in this area if it is a PDF, TXT, XML, or image file whose viewer is supported by the browser, or a URL. If the Document is another type of file, such as a DOC or XLS file, a **File Download** dialog box appears asking "Do you want to open or save this file?" When you click **Open**, the file appears in an external window in its native format. Image files whose viewer is not supported by the browser—TIF files, for example—open in whichever Graphics application format you have on your system—such as Paint Shop Pro or Paint. (Depending on how the application settings for opening in a browser are set, the DOC, PPT, or XLS file may open in the Content area.) NOTE: Although the external window has buttons that seemingly allow you to edit the file and save changes, these changes are **not** saved in the C•CURE 9000 database. To change a Document, you would have to edit it outside C•CURE 9000 and then re-import it.
Save and Close	Click to save your settings and close the Document editor.

Document Object Tasks

You can perform the following tasks using the Document editor.

- Adding a File as a Document on Page 233.
- Adding a URL as a Document on Page 234.

You can perform the following task with the Document Objects:

- Viewing a List of Documents on Page 235.

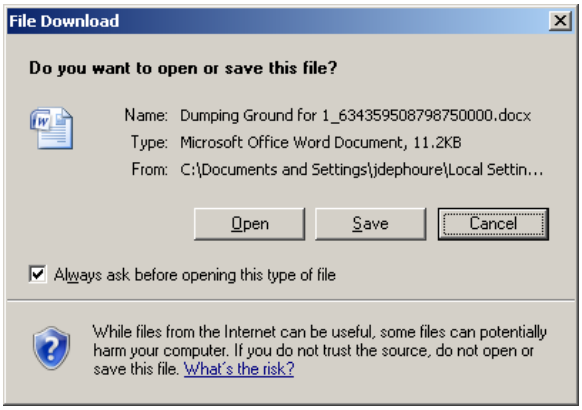
Adding a File as a Document

Files of many different types can be added to the C•CURE 9000 database. The main requirement is that the file be no larger than 500k.

To Add a File as a Document

1. In the Navigation Pane of the Administration Client, click the Configuration pane button.
2. Click the Configuration drop-down list and select **Document**.
3. Click **New** to create a new Document. The Document Editor opens.
4. Type a Name and Description for the Document that sufficiently identifies it and its purpose.
5. In the **Document Type** field, click the down-arrow and select File.
6. In the **Document File Selection** field, either enter a file name or click the **Import File** button to the right of the field.

   A standard Windows file dialog box opens. The **Files of type** field on the bottom reads Documents (*.pdf; *.txt) which filters the files lists to only those two types. Clicking the down-arrow opens a drop-down with further file type filters: Image Files (*.bmp; *.jpeg; *.gif; *.png) and All Files (*.*).
7. Navigate to the file you want to add to the system, select it, and click **Open**.
   - If the file you selected is a PDF, TXT, HTM, or XML file or a BMP, GIF, JPG, or PNG graphics file, it opens in the Content area of the Document Editor.
   - If the file you selected is a DOC, PPT, or XLS file or an Image file whose viewer is not supported by the browser such as a TIF file, a **File Download** dialog box appears asking "Do you want to open or save this file?"



   - Click **Open** and the file appears in an external window in its native format with buttons that allow you to edit the file. (Image files whose viewer is not supported by the browser open in whichever Graphics application format you have on your system—such as Paint Shop Pro, Paint, or a Preview window.)

NOTE Depending on the way your browser is set up, the DOC, PPT, or XLS file may open in the Content area.

8. If the content you are viewing is what you want for your Document, click **Save and Close**.

Adding a URL as a Document

To add a URL as a Document

1. Follow Steps 1 through 4 in the procedure above.
2. In the **Document Type** field, click the down-arrow and select **URL**.
3. In the **Document URL** field, enter the URL you want.
4. Click **View URL** and the URL you chose displays in the Content area of the Document Editor.
5. If the content you are viewing is what you want for your Document, click **Save and Close**.

Viewing a List of Documents

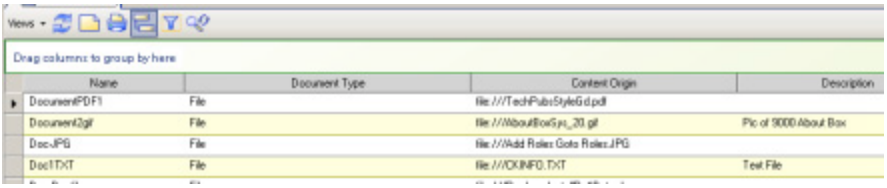
You can display a list of the Documents you have created by opening a Dynamic View of Documents. See Viewing a List of an Object Type on Page 22 for more information.

NOTE Only Documents added to the system with the Document Editor—"shared Documents"—can be viewed in a Dynamic View. "Private Documents" added to a Personnel record cannot be displayed in a Dynamic View.

To View a List of Documents

1. In the Navigation Pane of the Administration Workstation, click the Configuration pane button.
2. Click the Configuration drop-down list and select **Document**.
3. Click  to open a Dynamic View listing all Documents, as shown in Figure 82 on Page 235. (You can also click the down-arrow of this button to view the list in the current tabbed view).

Figure 82: Document List



You can sort, filter, and group items in the list. You can right-click a Document in the list to open the Document Context menu and perform any functions on the menu.

Document List Context Menu

The context menu that opens when you right-click a Document in the Document Dynamic View includes the selections described in Using the Object List Context Menu on Page 23 the Overview chapter of the *C•CURE 9000 Software Configuration Guide*. Context menu options specific to Documents are described in Table 52 on Page 235.

Table 52: Document List Right-Click Context Menu Options

Menu Selection	Descriptions
View	Click this menu selection to display the selected Document in a new tab in the Content pane.
Popup View	Click this menu selection to display the selected Document in a new free-floating window.
View in Current Tab	Click this menu selection to display the selected Document in the current tab replacing the current display.

8

Events

This chapter describes how to configure Events in C•CURE 9000.

In this chapter

Understanding Events

An event is a software definition that you can create using C•CURE 9000 dialog boxes and options. An event is an object that lets you link security objects, actions, annunciations, and time activations into a single software component. Events are triggered by state changes, such as environmental fluctuations, forced doors, or rejected access requests. C•CURE 9000 manages events using a **cause and effect** strategy. Anything that C•CURE 9000 can monitor can be used to generate an event, and the event can trigger any action.

Events are a critical component of C•CURE 9000 because they define security violations and initiate actions that the system and security personnel will take. Events can also control routine activities, such as unlocking entry doors and turning on lights. You can also create events that perform complex functions, such as arming, disarming, and monitoring an Intrusion Zone. You can link an event directly to a single action or you can link it to multiple events and actions. You can schedule events to occur or repeat at specific times.

There are three broad categories of events:

- Time-based events - activated by Schedule (For example - to open doors during the day shift)
- Industrial control events - activated by inputs to cause actions such as activate outputs.
- Events that respond to error situations - Door Held and Door Forced and other alarms

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 (see the *C•CURE 9000 System Maintenance Guide* chapter on Event Priorities).

As of v2.70SP1, you can configure Events to remain Active in the Event Viewer of the Monitoring Station after you disarm them. You can configure Events to remain Active after you disarm them by setting **Keep Disarmed Event Active** to **True** in the **Event Handling** section of system variables. This Active status means that Actions of an Event are still in effect and other objects, which depend on the Event, keep their states until you render the Event Inactive. This variable controls the behavior of Events in the Monitoring Station.

A potential use case of this feature occurs when there is building that has a door with an output of an alarm. This door is opened and the alarm triggers. The guard wants the alarm to stop, but wants to investigate the incident in further detail at a later time. The guard can do this by setting the system variable to **True** and configuring the Event to require acknowledgement.

If you select the **This event requires acknowledgement check box** on the **Acknowledgement** tab of the Event editor and this system variable is set to **True**, you can disarm the Event and it remains in the Event Viewer until you or the Monitor formally acknowledges the Event. If you do not select the acknowledgement check box and you disarm the Event, the Event leaves the Event Viewer. Table 53 on Page 237 provides the behaviors of Panel Events and Host Events during the different configurations

Table 53: Behaviors of disarming Panel and Host Events

Configuration	State	Panel Event Behavior	Host Event Behavior
System Variable = False			

Configuration	State	Panel Event Behavior	Host Event Behavior
• Event configured to require Acknowledgement • Acknowledge not allowed while Event is active • Activate Event	Armed	• Active • Displays in the Event Viewer • Associated Actions in effect	• Active • Displays in the Event Viewer • Associated Actions in effect
	Disarmed	• Active • **Not** displayed in the Event Viewer • Associated Actions in effect	• Inactive • Not displayed in the Event Viewer • Associated Actions **not** in effect
• Event configured to require Acknowledgement • Acknowledge is allowed while Event is active • Activate Event • Acknowledge Event (Causes still Active)	Armed	• Active • Displays in the Event Viewer	• Active • Displays in the Event Viewer
	Disarmed	• Inactive • Not displayed in the Event Viewer • Associated Actions **not** in effect	• Inactive • Associated Actions **not** in effect
	Armed again or Disarm cancelled	• Active • Displays in the Event Viewer • Associated Actions in effect NOTE: This re-triggers momentary actions again as if the Event is going Active	• Active • Displays in the Event Viewer • Associated Actions in effect
Event not configured to require Acknowledgement	Armed	• Active • Displays in the Event Viewer	• Active • Displays in the Event Viewer
	Disarmed	• Inactive • **Not** displayed in the Event Viewer • Associated Actions **not** in effect	• Inactive • **Not** displayed in the Event Viewer • Associated Actions **not** in effect
System Variable = True			
• Event configured to require Acknowledgement • Acknowledge not allowed while Event is active • Activate Event	Armed	• Active • Displays in the Event Viewer • Associated Actions in effect	• Active • Displays in the Event Viewer • Associated Actions in effect
	Disarmed	• Active • Displays in the Event Viewer • Associated Actions in effect	• Active • Displays in the Event Viewer • Associated Actions in effect
• Event configured to require Acknowledgement • Acknowledge is allowed while Event is active • Activate Event • Acknowledge Event (Causes still Active)	Armed	• Active • Displays in the Event Viewer • Associated Actions in effect	• Active • Displays in the Event Viewer • Associated Actions in effect
	Disarmed	• Inactive • **Not** displayed in the Event Viewer • Associated Actions **not** in effect	• Inactive • **Not** displayed in the Event Viewer • Associated Actions **not** in effect

Configuration	State	Panel Event Behavior	Host Event Behavior
Event not configured to require Acknowledgement	Armed	• Active • Displays in the Event Viewer • Associated Actions in effect	• Active • Displays in the Event Viewer • Associated Actions in effect
	Disarmed	• Inactive • **Not** displayed in the Event Viewer • Associated Actions **not** in effect	• Inactive • **Not** displayed in the Event Viewer • Associated Actions **not** in effect
NOTE: The icon color for C•CURE 800 Active Disarmed Events in the Event Viewer is gray (disarmed state). For C•CURE 9000, it is the Current Active/Requires Acknowledgement/Requres Clear/Acknowledgement-Overdue/Clear-Overdue color.			

To create and configure Events, see Event Editor on Page 280.

For more information about how Events work in C•CURE 9000, see:

- Event Causes and Actions on Page 239
- Event Actions on Page 241
- Event Cause List on Page 251
- Straightforward Events on Page 255
- Complex Events on Page 259
- Latch and Unlatch for Events on Page 261
- Toggle an Event on Page 267
- Pulse an Event on Page 269
- Assess Event Overview on Page 271

Event Causes and Actions

Events initiate actions based on an Event Action, **Trigger**, a Schedule, a Keypad Command, or a manual action. The Trigger is the C•CURE 9000 object (an input, output, reader, door or elevator) that activates the Event. The C•CURE 9000 dialog boxes that you use to configure Events also provide options, such as door forced or held, that control how the Event is activated.

Various hardware components have Triggers or Alarms associated with them. When TRUE (when a state change defined in the Trigger/Alarm occurs), these Triggers/Alarms can activate certain Event actions. Event actions can activate Events that have full access to all of the event actions.

Host and Panel Events

An Event can reside and be activated on the C•CURE 9000 server (host Event) or an Event can be downloaded to an iSTAR controller, and be activated on the controller (called a panel Event. The Event Actions that are available for an Event are determined by whether the Event is a host Event or a panel Event.

There are situations where an Event performs differently depending upon whether it is a host or panel Event.

Example:

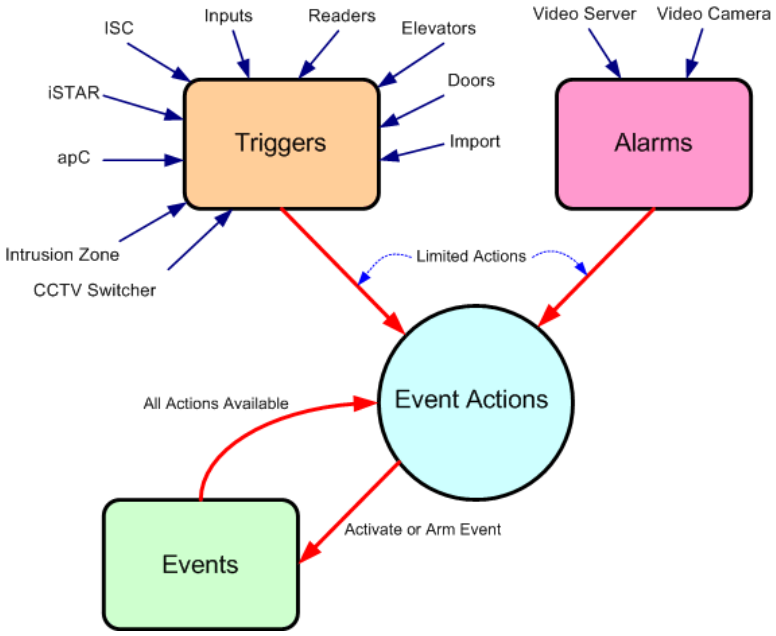
A Door trigger is configured to activate an Event when the **Admit Status** property changes to **Noticed Reject**. However, if the Event is a panel Event, it will not be triggered by Lost, Stolen or Disabled credentials, because these credentials are not downloaded to an iSTAR controller. If the Event is a host event, the Event is triggered correctly by a **Noticed Reject**.

Event Causes

Causes for an Event are displayed in a Cause List, which can be accessed from the Monitoring Station or from a Dynamic View of Events in the Administration Station. See Event Cause List on Page 251 and Viewing a List of Events for more information about Cause Lists.

Figure 83 on Page 240 shows the relationship between Triggers, Alarms, and Events.

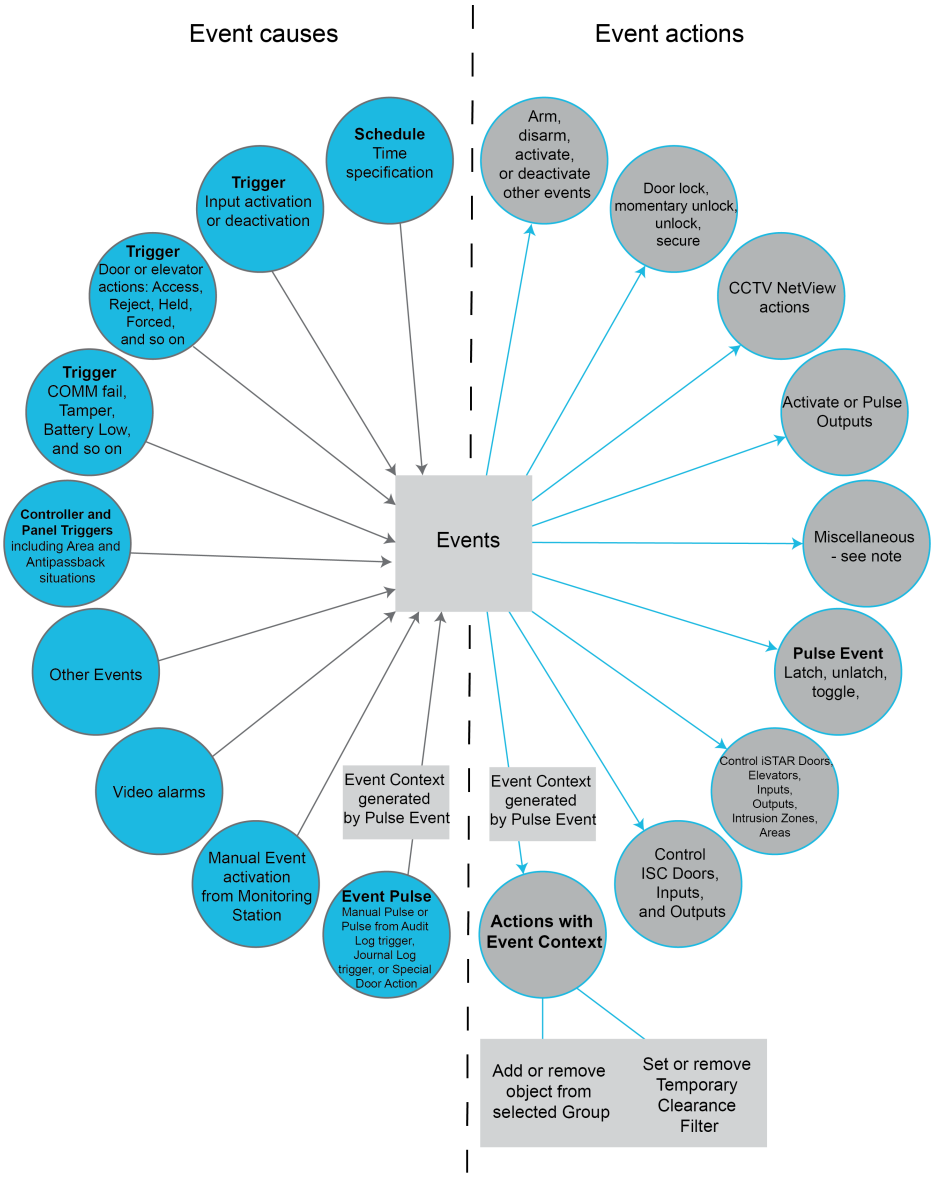
Figure 83: Triggers, Alarms, and Events



Event Actions

Figure 84 on Page 241 shows the Event causes (left) and actions (right) available with C•CURE 9000 software.

Figure 84: Diagram of Event Capability



The tables in this section provide descriptions of the available event actions that can be configured for Events. Many of these actions are also available for objects that support Triggers.

- Host Only Event Actions on Page 242
- apC Event Actions on Page 243
- Event Actions that Affect iSTARs on Page 244
- Event Actions for iSTAR Intrusion Zones and Clearance Filters on Page 246
- Device Trigger Actions and Video Alarm Actions on Page 247
- JCI Controller Event Actions on Page 250

Host Only Event Actions

This table lists event actions which are executed by Events on the host (C•CURE 9000 server), and that affect the host only.

Table 54: Event Actions Affecting Host Only

Action	Description
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. Examples - Call up camera, Call up camera with preset, etc.
De-muster Area	Select an Area to de-muster. Personnel currently in this Mustering Area(s) are moved to their de-mustering Area. The system updates the Area counts to reflect the number of Personnel being moved from the Mustering Area(s) to the de-muster Area. You can only select Areas that are configured as Mustering Areas.
Display Message Display as Feedback	Causes a message to appear in a pop-up text box on the Monitoring Station when the Event is activated. The lower section of this tab displays a text box where you can type the message that you wish to appear. Select **Display as Feedback** to have message displayed only on the Workstation that activated the event. See Workstation on Page 528 for more information on Workstations.
Display Viewer	Select an object type and object that you wish to display when this Event is activated. For example, you can choose Map for the object type, then select a specific map to display as a pop-up window in the Monitoring Station. Select **Display as Feedback** to have object displayed only on the Workstation that activated the event. See Workstation on Page 528 for more information on Workstations.
Play Sound	Select a WAV sound file to play from a list of Sounds that have been imported into the C•CURE 9000 database. The sound can be played at an interval or just once. See the Sound Editor on Page 491 for more information about importing and using Sound files.
Remove Expired Custom Clearance from Personnel	The action has no parameters. When executed, it selects Custom Clearances that are past their expiration date/time and deletes them from their associated Personnel record(s).
Remove Reports Results	The action has no parameters. When executed, it selects Reports Result objects in the database with the flag **Delete automatically** set to true and the date value in the field **Delete after** in the past and deletes these obsolete results permanently. C•CURE 9000 has a pre-configured Event called **Remove Obsolete Results** which executes this action daily at 2:17 AM.
Remove Import Results	The action has no parameters. When executed, it selects Import Result objects in the database with the flag **Delete automatically** set to true and the date value in the field **Delete after** in the past and deletes these report results permanently. C•CURE 9000 has a pre-configured Event called **Remove Obsolete Results** which executes this action daily at 2:17 AM.
Run Export	Select a Data Export object to run when this Event is Activated. The action allows selection of a predefined Export object. Executing the action runs the selected Export object, producing an XML file in the specified export folder.
Run Import	Select a Data Import object to run when this Event is Activated. The Automation mode of the Import must be **Activated by event**. Executing the action starts the import object for a single import.
Run Personnel Portrait Export	You can export one or more Personnel Portraits by selecting a Personnel Query to execute when this Event is Activated. Portraits associated with the Personnel records returned by this query are exported to the folder you specify in **Output folder on the server**. Exported portraits are named according to the pattern in **Portrait name pattern**. The default pattern - Personnel {Name} ({Object}).jpg - result in filenames such as **Personnel Last, First (5001).jpg**. If you choose Rename existing files, any files that exist in the folder that would have been overwritten by an exported portrait are instead renamed with a .bak extension (in the example above, **Personnel Last, First (5001).jpg.bak**).

Event Actions Affecting Host Only (continued)

Action	Description
Run Report	Select a Report to **Run on Server** when the Event is activated. The action allows selecting a single report record. Executing the action runs the selected report on the server and saves the result in a new Report Result object. The Export Results flag indicates that once the report result record is created, it can be exported to an external file and optionally printed or sent by e-mail.
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.
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. See Configure an Event to Display Recorded Video on Page 304 for more information. • **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. See the *C•CURE 9000 Video Guide* Video Action chapter for more information.

apC Event Actions

The apC differs from the iSTAR in that Events and Triggers cannot be downloaded to the apC. The Host controls Event activity in the apC. The iSTAR cluster is designed to continue to operate even if the Host communication is lost.

The apC has no concept of priority levels of actions like the iSTAR does. The apC will obey orders from the Host in a serial way.

What happens when Host communications is lost? The apC has a memory of card holders and their clearances for the readers (doors) that are implemented on that particular apC. The access control decisions will continue to be made and the doors will function but the monitor station data is buffered until the connection is reestablished.

With a few exceptions, the Host event/trigger actions will not operate. The exceptions are Time-Based actions that are in the apC memory. *Time-Based* means either a Schedule induced Event or a Manual action.

Timed actions are supported for the following:

- Set Reader in Secured Mode
- Set Reader in Unlocked Mode
- Set Reader in Locked Mode
- Set PIN required
- Set PIN not required
- Arm Input
- Disarm Input
- Pulse Output
- Activate Output
- Deactivate Output

Example:

- Unlock Door (Reader) from 8 AM to 5 PM,

- Activate Output from 2:30 to 2:32, etc.

Event Actions that Affect iSTARs

This table describes event actions affecting iSTARs that can be executed by Events on the host or downloaded to the iSTAR. Many of these actions are also available for objects that support Triggers and Alarms.

Table 55: Event Actions that Affect iSTARs

Action	Opposite Action	Description
Activate Event	Deactivate Event	Select an Event to activate when this status occurs. The Activate Event action in conjunction with the Arm Event action provide an AND gate for basic logic operations (see Boolean Event Situation on Page 259).
Activate Output	Deactivate Output	Select an Output to activate when the Event or Trigger containing this action occurs. Outputs can be Normally Off or Normally Energized, to provide for Fail-Secure or Fail-Safe.
Arm Event	Disarm Event	Select an Event to arm. An armed Event can be activated; a disarmed Event cannot be activated. The Arm Event action in conjunction with the Activate Event action provide an AND gate for basic logic operations (see Boolean Event Situation on Page 259).
Arm Input	Disarm Input	Select an Input to arm. An armed Input can be activated. A disarmed Input cannot be activated. Arming and Disarming an input can selectively allow alarms at different times, such as a motion detector that is only active from 9 PM to 6 AM.
Arm Intrusion Zone	Disarm Intrusion Zone	Select an Intrusion Zone to Arm. An example of an Intrusion Zone could be the Jewel room of a museum, with are many motion sensors and glass break sensors within the room. After hours, the zone is armed and the sensors are monitored. When the Museum opens the next morning the zone is set to disarmed and most of the sensors are disarmed. The IZ can cause events when there is a violation or when the zone is armed or disarmed. See **Event Control** in the *C•CURE 9000 Area and Zones Guide* for information about controlling iSTAR Intrusion Zones with Events.
Backup iSTAR Database		Select an iSTAR controller on which to backup the controller's database. This action is performed by the controller firmware. The backup is a Configuration backup, not a complete data backup.
Clear Area Counts		Return the Personnel count for all Areas to 0 (zero), including in Area Personnel Groups.
Control Access	Uncontrol Access	Select an Elevator Button which you want the Action to set for controlled access Controlled access means that you have to swipe a card to access the floor represented by the button.
Deactivate Event	Activate Event	Select an Event to be deactivated. If the Event is Active when this action occurs, the action deactivates the Event.
Deactivate Output	Activate Output	Select an Output to be deactivated. If the Output is Active when this action occurs, the action deactivates the Output.
Disable Keypad Commands	Enable Keypad Commands	Select an iSTAR Reader on which to disable Keypad Commands. See the *C•CURE 9000 Areas and Zones Guide* Keypad Commands chapter for more information.
Disable PIN	Enable PIN or PIN Required	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	Arm Event	Select an Event to disarm. A disarmed Event cannot be activated; an Event must be armed to be activated.

Event Actions that Affect iSTARs (continued)

Action	Opposite Action	Description
Disarm Input	Disarm Event	Select an Input to disarm. A disarmed Input cannot be activated; an Input must be armed to be activated.
Disarm Intrusion Zone	Arm Intrusion Zone	Select an Intrusion Zone to Disarm. An example of an Intrusion Zone could be the Jewel room of a museum with many motion sensors and glass break sensors n the room. After hours, the zone is armed and the sensors are monitored. When the Museum opens the next morning the zone is set to disarmed and most of the sensors are disarmed. The intrusion zone can cause events when there is a violation or when the zone is armed or disarmed. See **Event Control** in the *C•CURE 9000 Area and Zones Guide* for information about controlling iSTAR Intrusion Zones with Events.
Enable Counting for Access Restriction		Select the Area (or Area Group) for which you want to enable personnel counting for access restriction. The various counting actions allow you to set up an N Man Rule area or a parking garage that will not overfill. The concept of N Man Rule is used when you want to set a maximum number of people or cars that will be allowed into an area. There are other times when you want to set a minimum number of people in an area for safety reasons. There are events available at the min-max limits that can be used to control the entrance reader. See the *C•CURE 9000 Areas and Zones Guide* iSTAR Areas chapter for more information.
Enable Counting for Event		Select the Area (or Area Group) for which you want to enable personnel counting for Events. The various counting actions allow you to set up an N Man Rule area or a parking garage that will not overfill. See the *C•CURE 9000 Areas and Zones Guide* iSTAR Areas chapter for more information.
Enable Counting Only		Select the Area (or Area Group) for which you want to enable personnel counting. The various counting actions allow you to set up an N Man Rule area, or a parking garage that will not overfill. See the *C•CURE 9000 Areas and Zones Guide* iSTAR Areas chapter for more information.
Enable Keypad Commands		Select an iSTAR Reader on which to enable Keypad Commands. Keypad commands allow events to be executed from readers that have keypads. Examples are turning lights on and off in a room, arming or disarming Intrusion Zones, etc. See the *C•CURE 9000 Areas and Zones Guide* Keypad Commands chapter for more information.
Enable PIN	Disable PIN	Set the Reader you select to require that a cardholder perform a card swipe, then enter a PIN to be granted access. This provides a second level of security to protect against lost or stolen cards.
Force Arm Intrusion Zone		Select an Intrusion Zone to Force Arm (Arm Zone before Zone is **Ready to Arm**). An Intrusion Zone will not arm if any of the sensors are in alarm. This action is for the case where there is a faulty sensor, but you need to arm the IZ for the night. In effect, the IZ ignores the bad sensor. See **Event Control** in the *C•CURE 9000 Area and Zones Guide* for information about controlling iSTAR Intrusion Zones with Events.
Latch Event	Unlatch Event	Select an Event to be Latched. The Event named in the Latch action is activated, and it will stay activated until it is the subject of an Unlatch or Toggle Event action (with an equal or higher priority). The Latch action is added to the Cause list for the Event. If the Event is already Latched, the Latch Event action has no effect. Upon system restart, host and panel Events retain their Latch state.
Lock Door	Unlock Door	Select a Door to Lock from the Door field in the Details area. Locked means you must badge in. This differs from Secure Door in that a Secure Door is disabled and cannot be badged through. Issuing a Lock Door action will cause a Secure Door to change to a Locked Door.
Momentary Unlock Door		Select a Door to Momentarily Unlock from the Door field in the Details area. The Unlock time defaults to 5 seconds and is defined in the Door configuration editor. Note that this is the proper way to let someone through a door. Do not use the Manual Action Unlock Door.

Event Actions that Affect iSTARs (continued)

Action	Opposite Action	Description
PIN Required	Disable PIN	PIN Required is a redundant action;. It is the same as Enable PIN. If you use the PIN Required action, it will be converted to Enable PIN by the software when you save the Event.
Pulse Event		Select an Event to be Pulsed. A Pulse is a momentary activation of an Event. If the minimum activation time is configured in the Event, that value is used as the duration of the Pulse; otherwise the duration of the Pulse is one second.
Pulse Output		Select an Output to activate for the duration specified in the Output's **Pulse Duration** field. The pulse duration is in tenths of a second. The Output can be normally off or normally energized.
Remove All Personnel From Area		Select an Area from which to remove all Personnel. WARNING: The Area ID for Personnel removed from the Area is set to NULL and all counts for the Area are set to 0 (zero).
Secure Door	Unlock or Lock Door	Select a Door that you want to secure. This action inhibits the reader associated with the Door. It is used to shut down an area or perhaps to service the door. The only way to change the state of Secure is to either Unlock the door or Lock the door.
Set Clearance Filter to Level 1 ... Level 6		Set the Clearance Filter value for an iSTAR Reader or Reader Group to the specified Level. Level 1 is the lowest and Level 6 is the highest These event actions are used to vary the Clearance Filter Level either manually or automatically using Events. Each cardholder is assigned a Clearance Filter Level and they can only pass through doors that have an equal or lower level than is assigned to them. See Clearance Filter Events on Page 255 for more information.
Toggle Event		Select an Event to be Toggled. The Event named in the Toggle action is Latched if it is currently Unlatched, or Unlatched if it is currently Latched. The Latch action is added to the Cause list for the Event. If the Event is Inactive, the Toggle Event action Latches the Event. See Latch and Unlatch for Events on Page 261 for more information about Latching and Unlatching, and Toggle an Event on Page 267 for more information about Toggling an Event.
Toggle Intrusion Zone Mode		Toggle the Intrusion Zone mode between the **Armed** and **Disarmed** states. Commonly used as a Keypad Command event action. Toggle in the morning to Disarm and then toggle again in the evening to Arm the Intrusion Zone.
Uncontrol Access	Control Access	Select an Elevator Button which you want the Action to set for uncontrolled access. Uncontrolled access means that all cardholders have free access to the floor represented by the button.
Unlatch Event	Latch Event	Select an Event to be Unlatched. The Event named in the Unlatch action is deactivated if the Event is currently Latched, and it will stay deactivated until it is the subject of a Latch or Toggle Event action (with an equal or higher priority). The Unlatch action is added to the Cause list for the Event. If the Event is already Unlatched, the Unlatch Event action has no effect. Upon system restart, host and panel Events retain their Unlatched state.
Unlock Door	Lock Door	Select a Door to unlock from the Door field in the Details area. Will also allow a Secure Door to be re-activated.

Event Actions for iSTAR Intrusion Zones and Clearance Filters

This table provides descriptions of actions that are only available when an Event is configured to be downloaded to the iSTAR that has the Intrusion Zone or Clearance Filter.

These actions are not visible in the list of Actions until the Event is declared to be downloaded to an iSTAR. These actions are usually associated with Keypad commands - The Keypad Command is configured to activate the Event containing the Action.

The reason that they are referred to as Local is that you must enter the Keypad command from a reader associated with the iSTAR to which the Event is downloaded.

Table 56: Event Actions for iSTAR Intrusion Zones and Clearance Filters

Action	Opposite Action	Description
Arm Local Intrusion Zone	Disarm Local Intrusion Zone	Set the Local Intrusion Zone to Armed. An example of an Intrusion Zone could be the Jewel room of a museum. There are many motion sensors and glass break sensors within the room. After hours, the zone is armed and the sensors are monitored. When the Museum opens the next morning the zone is set to disarmed and most of the sensors are disarmed. The Intrusion Zone can cause events when there is a violation or when the zone is armed or disarmed.
Disarm Local Intrusion Zone	Arm Local Intrusion Zone	Set the Local Intrusion Zone to Disarmed. An example of an Intrusion Zone could be the Jewel room of a museum. There are many motion sensors and glass break sensors within the room. After hours, the zone is armed and the sensors are monitored. When the Museum opens the next morning the zone is set to disarmed and most of the sensors are disarmed. The Intrusion Zone can cause events when there is a violation or when the zone is armed or disarmed.
Force Arm Intrusion Zone		Select an Intrusion Zone to Force Arm (Arm Zone before Zone is **Ready to Arm**). An Intrusion Zone will not arm if any of the sensors are in alarm. This action is for the case where there is a faulty sensor, but you need to arm the Intrusion Zone for the night. In effect, the Intrusion Zone ignores the bad sensor. See **Event Control** in the *C•CURE 9000 Area and Zones Guide* for information about controlling iSTAR Intrusion Zones with Events.
Show Clearance Filter Causes		The LCD of the reader where the Keypad Command was entered displays the Clearance Filter level changes.
Show Local Intrusion Zone Off Normal Points		The LCD of the reader where the Keypad Command was entered displays any sensors, or monitoring points that are not normal (in alarm) in the local Intrusion Zone
Show Local Intrusion Zone Status		The LCD of the reader where the Keypad Command was entered displays the Arm and Disarm status of the local Intrusion Zone.
Toggle Intrusion Zone Mode		Toggle the Intrusion Zone mode between the **Armed** and **Disarmed** states. This is a Keypad Command event action. Toggle in the morning to Disarm and then toggle again in the evening to Arm the Intrusion Zone.

Device Trigger Actions and Video Alarm Actions

This table provides descriptions of Trigger or Alarm Actions that are available at the device editors. All Devices can execute an Event Action which provides access to all of the various Event actions. Doors, Readers, Inputs and Elevators can also Activate Outputs and Events outside Schedule. Readers can directly use many Event Actions, as indicated.

Table 57: Device Triggers and Alarms - Resultant Actions

Trigger or Alarm Action	Devices	Description
Activate Event	Doors, Readers, Inputs, Elevators, Video Server, Video Camera, Comm. Port, CCTV Switch, IZ, Area, apC, iSTAR, Cluster	Select an Event to activate when the cause occurs. The Activate Event action in conjunction with the Arm Event action provide an AND gate for basic logic operations.
Activate Event Outside Schedule	Doors, Readers, Inputs, Elevators	Select an Event to activate when the cause occurs and the associated Schedule is False. The Activate Event action in conjunction with the Arm Event action provide an AND gate for basic logic operations. (Trigger Action Only)
Activate Output	Doors, Readers, Inputs, Elevators	Select an Output to activate when the Event or Trigger containing this action occurs. Outputs can be Normally Off or Normally Energized, to provide for Fail-Secure or Fail-Safe.
Arm Event	Readers	Select an Event to arm. An armed Event can be activated; a disarmed Event cannot be activated. The Arm Event action in conjunction with the Activate Event action provide an AND gate for basic logic operations.
Arm Input	Readers	Select an Input to arm. An armed Input can be activated. A disarmed Input cannot be activated. Arming and Disarming an input can selectively allow alarms at different times, such as a motion detector that is only active from 9 PM to 6 AM.
CCTV Action	Readers	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. Examples - Call up camera, call up camera with preset, etc. This is useful if there is an alarm at a Reader.
Control Access	Readers	Select an Elevator Button which you want the Action to set for controlled access. Controlled access means that you have to card swipe to access the floor represented by the button.
Deactivate Event	Readers	Select an Event to be deactivated. If the Event is Active when this action occurs, the action deactivates the Event.
Deactivate Output	Readers	Select an iSTAR Reader or Reader Group on which to disable Keypad Commands. See the C•CURE 9000 Areas and Zones Guide Keypad Commands chapter for more information.
Disable PIN	Readers	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	Readers	Select an Event to disarm. A disarmed Event cannot be activated; an Event must be armed to be activated.
Disarm Input	Readers	Select an Input to disarm. A disarmed Input cannot be activated; an Input must be armed to be activated.
Enable Keypad Commands	Readers	Select an iSTAR Reader on which to enable Keypad Commands. Keypad commands allow events to be executed from readers that have keypads. Examples are turning lights on and off in a room, arming or disarming Intrusion Zones, etc.
Enable PIN	Readers	Set the Reader you select to require that a cardholder perform a card swipe, then enter a PIN to be granted access. This provides a second level of security to protect against lost or stolen cards.

Device Triggers and Alarms - Resultant Actions (continued)

Trigger or Alarm Action	Devices	Description
Latch Event		Select an Event to be Latched. When the Event is activated, the Event named in the Latch action is activated, if the Latch action has the highest or same priority with later time than other actions. The Event stays activated until it is the subject of an Unlatch or Toggle Event action (with an equal or higher priority). The Latch action is added to the Cause list for the Event. If the Event is already Latched, the Latch Event action has no effect. Upon system restart, host and panel Events retain their Latch state. See Latch and Unlatch for Events on Page 261 for more information about Latching and Unlatching.
Lock Door	Readers	Select a Door to Lock from the Door field in the Details area. Locked means you must badge in. This differs from Secure Door in that a Secure Door is disabled and cannot be accessed. Issuing a Lock Door action will cause a Secure Door to be Locked, and usable.
Momentary Unlock Door	Readers	Select a Door to Momentarily Unlock from the Door field in the Details area. The Unlock time defaults to 5 seconds and is defined in the Door configuration editor. Note that this is the proper way to let someone through a door. Do not use the Manual Action Unlock Door.
Pulse Event		Select an Event to be Pulsed. When the Event is activated, the Event named in the Pulse action is activated. A Pulse is a momentary activation of an Event. If the minimum activation time is configured in the Event, the value will be used as the duration of the Pulse; otherwise the duration of the Pulse will be 1 second.
Pulse Output	Readers	Select an Output to activate for the duration specified in the Output's Pulse Duration field. The pulse duration is in tenths of a second. The output can be normally off or normally energized.
Secure Door	Readers	Select a Door that you want to secure. This action inhibits the reader associated with the Door. It is used to shut down an area or perhaps to service the door. The only way to change the state of Secure is to either Unlock the door or Lock the door.
Send Email	Readers	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.
Toggle Event		Select an Event to be Toggled. When the Event is activated, the Event named in the Toggle action is Latched if it is currently Unlatched, or Unlatched if it is currently Latched. The Latch action is added to the Cause list for the Event. If the Event is Inactive, the Toggle Event action Latches the Event. See Latch and Unlatch for Events on Page 261 for more information about Latching and Unlatching, and Toggle an Event on Page 267 for more information about Toggling an Event.
Uncontrol Access	Readers	Select an Elevator Button which you want the Action to set for uncontrolled access. Uncontrolled access means that all cardholders have free access to the floor represented by the button.
Unlatch Event		Select an Event to be Unlatched. When the Event is activated, the Event named in the Unlatch action is deactivated if the Event is currently Latched, and it will stay deactivated until it is the subject of a Latch or Toggle Event action (with an equal or higher priority). The Unlatch action is added to the Cause list for the Event. If the Event is already Unlatched, the Unlatch Event action has no effect. Upon system restart, host and panel Events retain their Unlatched state. See Latch and Unlatch for Events on Page 261 for more information about Latching and Unlatching.

Device Triggers and Alarms - Resultant Actions (continued)

Trigger or Alarm Action	Devices	Description
Unlock Door	Readers	Select a Door to unlock from the Door field in the Details area. Will also allow a Secure Door to be re-activated.
Video Camera Action	Readers	Link a Camera to a Video Server and initiate the Camera to Record, initiate a Camera Preset Command, or a Camera Pattern Command.

JCI Controller Event Actions

The event actions listed in the table apply to Johnson Controls CK721A and S321-IP controllers.

Table 58: JCI Controller Event Actions

Action	Description
Fast Flash Output	Flash output quickly.
Slow Flash Output	Flash output slowly for several seconds.

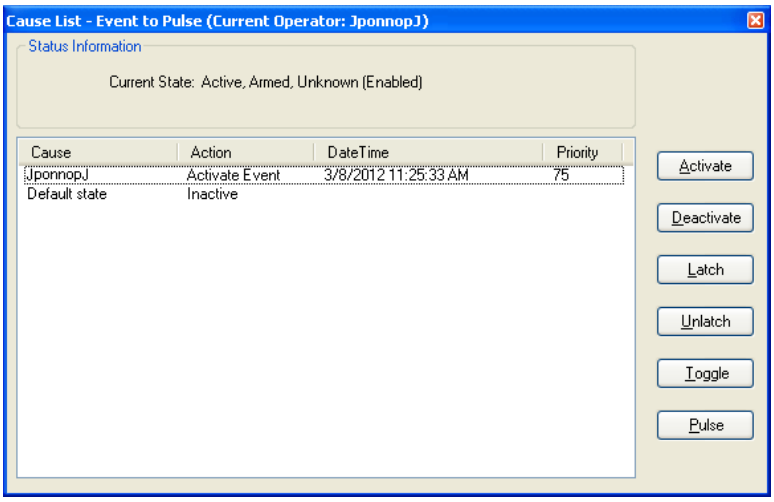
Event Cause List

Causes for an Event are displayed in a Cause List, which can be accessed from:

- Monitoring Station Event Viewer
- Monitoring Station Explorer Bar Status List

An example of the Cause List dialog box is shown in Figure 85 on Page 251.

Figure 85: Cause List Dialog Box



The Cause List shows the current state of the object, the settings or actions that cause the current state, sorted by Priority, and includes buttons that allow you to perform manual actions on the object.

Cause List Definitions

The fields and buttons that appear on the Cause List are defined in Table 59 on Page 251.

Table 59: Cause List Definitions

Field/Button	Description
Status Information	Lists the current state of the Event.
Cause	This column lists the Event Causes (the reasons that an Event is activated or deactivated, and other actions or conditions that affect the Event).
Action	This columns lists the actions that are currently affecting the state of the Event.
Date/Time	This column lists the date and time of each cause.
Priority	This column lists the priority assigned to each cause.
Activate	Click to open a **Manual Action Edit** dialog box with parameters for activating the selected Event. If the Event is disarmed, the **Activate** button is not available.
Deactivate	Click to open a **Manual Action Edit** dialog box with parameters for deactivating the selected Event. If the Event is disarmed, the **Deactivate** button is not available.

Cause List Definitions (continued)

Field/Button	Description
Latch	Click this menu selection to Latch the Event. When you Latch an Event, the Event is activated, and it will stay activated until it is the subject of an Unlatch or Toggle Event action (with an equal or higher priority). The Latch action is added to the Cause list for the Event. If the Event is already Latched, the Latch Event action has no effect. Upon system restart, host and panel Events retain their Latch state. If the Event is disarmed, the **Latch Event** button is not available.
Unlatch	Click to Unlatch the Event. When you Unlatch an Event, the Event is deactivated if the Event is currently Latched, and it will stay deactivated until it is the subject of a Latch or Toggle Event action (with an equal or higher priority). The Unlatch action is added to the Cause list for the Event. If the Event is already Unlatched, the Unlatch Event action has no effect. Upon system restart, host and panel Events retain their Unlatched state. If the Event is disarmed, the **Unlatch Event** button is not available.
Toggle	Click to Toggle the Event. The Event you Toggle is Latched if it is currently Unlatched or inactive, or Unlatched if it is currently Latched. The Latch action is added to the Cause list for the Event. If the Event is disarmed, the Toggle Event button is not available.
Pulse	Click to Pulse the Event. The Event you Pulse is activated. A Pulse is a momentary activation of an Event. If the minimum activation time is configured in the Event, the value is used as the duration of the Pulse; otherwise the duration of the Pulse will be one second. If the Event is disarmed, the **Pulse Event** button is not available.

Events and Time Zones

An Event can be associated with a specific Time Zone by configuring the **in Time Zone** field on the Event General tab (see Event General Tab on Page 281).

By default, an Event and any Schedule configured in the Event are activated using the local time of the C•CURE 9000 server. However, you can configure the Event to be activated in a different Time Zone from the server, using the **In Time Zone** field on the Event General tab.

However, if the Event is configured to be downloaded to an iSTAR controller, the iSTAR controller's Time Zone is configured as the Event Time Zone, and cannot be changed

Example:

An Event can be assigned to Pacific Time (GMT -08:00) and configured to be activated when a Schedule becomes active. If the C•CURE 9000 Server is in the Pacific Time Zone, or the Event is downloaded to a controller that is in the Pacific Time Zone, any Schedule associated with the Event becomes active according to Pacific time.

Time Zone Mismatch

If you add a Time Zone to an Event that is associated with an apC or iSTAR controller that resides in a different Time Zone, a warning is displayed when you attempt to save the Event to let you know that there is a Time Zone mismatch between the server time zone and the Time zone of the controller. You can still save the Event.

If you configure an Event and get a Time Zone Mismatch warning, it indicates that if the apC controller is offline from the server, the Event is activated on the server, but the apC hardware based action does not occur.

Example:

Time Zone mismatch message: "This event has actions on an apC hardware in another time zone."

When you configure an Event that affects objects that reside in different Time Zones, a Time Zone Mismatch warning is displayed when you save the Event:

"This event has actions on a hardware in another time zone."

Example:

You configure an Event and on the Options tab you configure the Event to be downloaded to an iSTAR that resides in the Eastern Time Zone (GMT -5:00). You create an action to activate an Output on another Controller that resides in the Pacific Time Zone (GMT -8:00). When you attempt to save the Event, a Time Zone Mismatch warning message box is displayed.

The Time Zone Mismatch warning for a panel Event alerts you that the action you configured occurs based on the Time Zone of the controller rather than the Time Zone of the C•CURE 9000 server (host).

When you see a Time Zone Mismatch warning, you can either click:

- **OK** to save the Event.
- **Cancel** to cancel saving the Event and return to the Event editor.

Event Time Zones and Groups

When you configure an Event to perform an action on a Group object, you should consider making sure that all of the objects in the Group are in the same Time Zone to avoid unintended circumstances.

Example:

A host Event on a C•CURE 9000 server in the Eastern Time Zone is configured to unlock the Doors in a Door Group at a scheduled time. However, the Doors in the Door Group are in different Time Zones:

- Door1 is in the Eastern Time Zone
- Door2 is in the Pacific Time Zone.

When the Event is activated at 9:00 AM in the Eastern Time Zone, it is only 6:00 AM in the Pacific Tim Zone, and Door2 will also unlock.

For this reason, in most cases you will want to avoid configuring Events with Group objects in different Time Zones. You could instead configure two Door Groups; one for each controller, and separate Events, one for each controller, and download each Event to the respective controller, to ensure that the Doors unlocked at the intended time.

Straightforward Events

You can configure straightforward events to perform simple functions, like unlocking a door or turning on lights. This section contains examples of these types of events and gives an overview of the steps you need to take to create them.

Sample Unlock Door Event

The event in this example unlocks the lobby door when a daytime security officer manually activates an event from the Monitoring Station. The officer can also unlock the door by pressing a switch.

To Create this Event

1. Create an event that activates an unlock door action and specify the door that is unlocked.
2. Link the event that activates the unlock door action with the input switch at the Monitoring Station.
3. Link the event that activates the unlock door action with a time specification. The time specification defines the time (in this case, daytime) that the guard can activate the event and unlock the door.

Sample Door Forced Event

The event in this example activates the output to a siren, sends a message, and activates a sound at the Monitoring Station if the lobby door is forced after normal business hours. If an officer fails to acknowledge the event, a second event activates. The second event sends a page to the security supervisor.

To Configure this Event

1. Create an event that activates the output to the siren, and specify a door forced event on the lobby door.
2. Specify officer acknowledgments, Monitoring Station sounds and subsequent events:
   a. Send the event to the Monitoring Station.
   b. Specify the sound that plays at the Monitoring Station.
   c. Require acknowledgement.
   d. If the event is unacknowledged within a specific time, activate a subsequent event (the event in this example sends a page).
3. Link the event with a schedule. This specifies the time that the event is active (in this case, after business hours).

Clearance Filter Events

Clearance filters can be used to regulate access at iSTAR readers. C•CURE 9000 events can be configured to set a clearance filter value at iSTAR readers or reader groups. The event to be associated with a particular reader can be linked to a cardholder by a comparison of the clearance filter level of the cardholder with that of an iSTAR reader.

Once a clearance filter is set at an iSTAR reader or reader group, cardholders with equal or greater clearance filter value are allowed access at the reader or reader group while the event is active. Conversely, cardholders with lesser clearance filter levels are not allowed access at such iSTAR readers until the triggered event is deactivated or the cardholder's clearance filter level is increased.

There are six reader and personnel clearance filters available:

- Clearance Filter value 6 (the highest value)
- Clearance Filter value 1 (the lowest and default value)

Personnel Clearance Filters allow you to control personnel access to the system. Clearance Filters describe the locations (readers) and situations for which a person's access card is valid. With clearance Filters, you can associate readers controlling the following objects with Events that set a Clearance Filter level, determining which cardholders are allowed access.

- Doors or door groups
- Elevators or elevator groups
- Floors or floor groups

The default personnel (or cardholder) Clearance Filter Level is 1. To configure clearance filter values for cardholders, go to the Configuration pane, select Personnel and go to the Clearances tab. The Clearance Filter Level can be selected at the lower right-hand corner of the Clearances dialog box. See Chapter 2 of the *C•CURE 9000 Personnel Guide* for more information.

To Configure an Event Using Clearance Filters

1. Select **Clearance Filter Levels** for applicable cardholders, using the Personnel editor Clearances tab.
2. Click **Configuration** to open the Configuration pane.
3. Select **Event** from the Configuration pane drop-down list.
4. Click **New** to create a new Event.

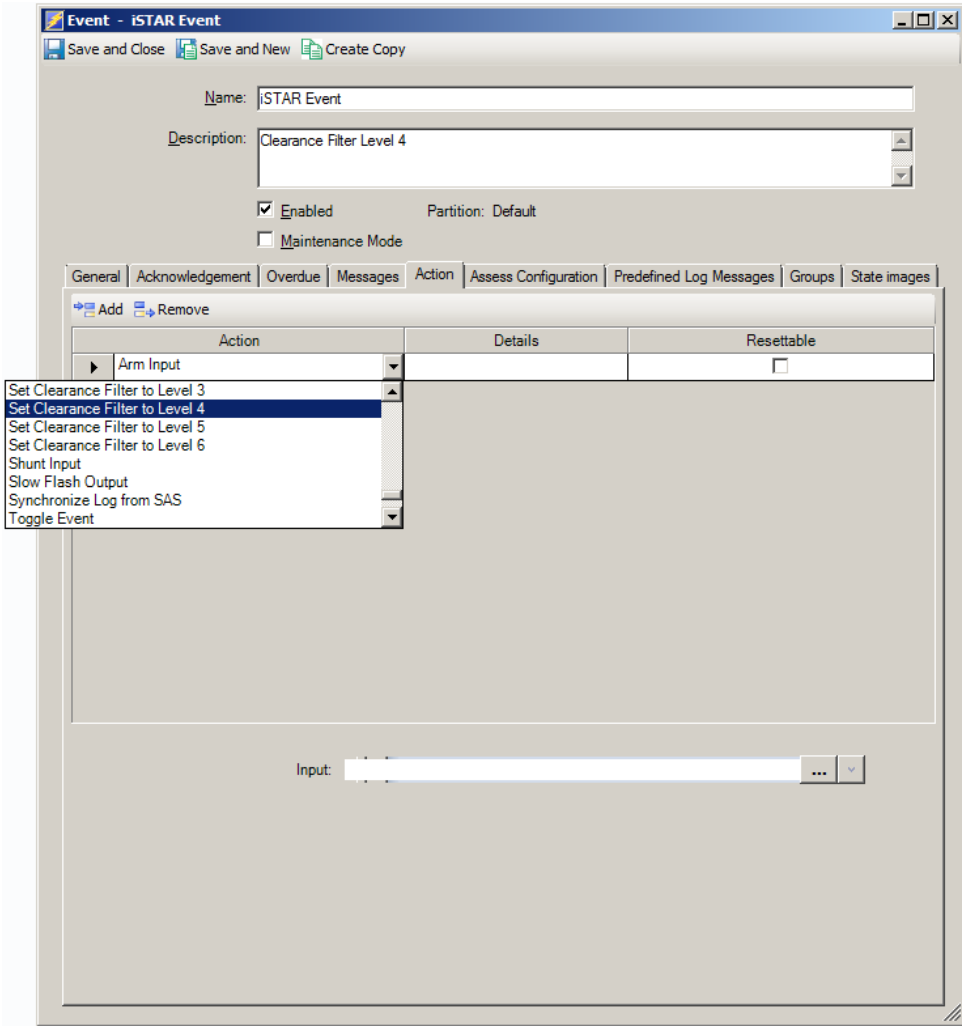
   -or-

5. Click and a dynamic view listing existing **Events** appears in the content area.
6. Click to select the **Event** you wish to modify in the dynamic view and right-click to display the context menu and select **Edit**.

   The Event editor opens, as shown in Figure 92 on Page 282.
7. Arm the Event by selecting the **Armed** check box in the **Default state** box of the General tab.
8. Change any of the default settings for the Event in the General tab such as:
   - **Priority** - this parameter can be set numerically (from 0-200) or from **Very Low** to **Critical** in the drop-down selection field. The default value is Medium low (75).
   - **Timing** - the **Activation delay time** and **Minimum activation time** can be set within a range of 0 (the default) to 999 hours, 59 minutes and 59 seconds.
   - **Scheduling** - the event can be scheduled for activation and for arming when you click ... and select from existing schedules.

     You can also edit an existing schedule by selecting **Edit** from the context menu in the **Schedule** selection window.
9. Also be sure to select the **Enabled** check box when you want to set it online.
10. Click the **Action** tab (see Figure 86 on Page 257).

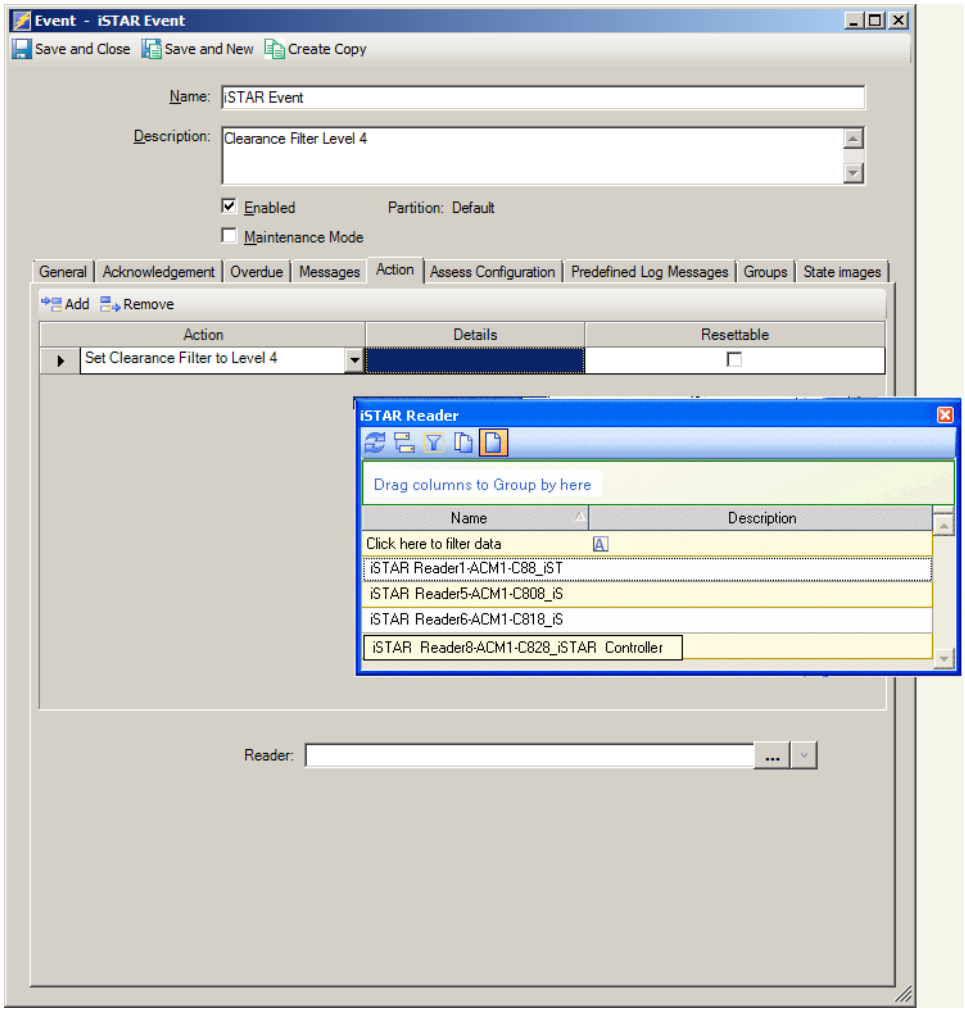
Figure 86: Event Editor Action Tab - Select Clearance Filter



11. Click **Add** to select an **Action**. When you click within the **Action** field, a drop-down list is displayed from which you can choose the **Clearance Filter Level** that you want the reader to set when the Event is activated at the door.
12. To select a reader, click [...] in the **Reader** field and select from existing readers. See Figure 87 on Page 258.

    In this example, when the iSTAR Event is activated, the reader you have selected will allow only those cardholders with a Clearance Filter Level of 4 or greater to enter through the associated door(s).

Figure 87: Event Editor Action Tab - Select Reader



In the **Options** tab you can also configure the Event to require acknowledgement, configure a second event to be activated if acknowledgment is not forthcoming, and select a compatible controller to which the event is to be downloaded.

Applicable instructions for Monitoring Station personnel can also be included in the **Messages** tab.

13. To save the Event, click **Save and Close**.

Complex Events

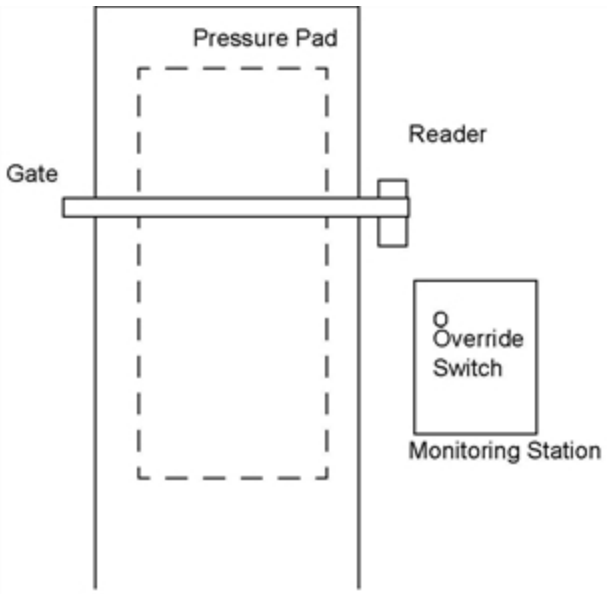
If your site requires it, you can configure events that perform complex functions, including events configured for Boolean situations.

Boolean Event Situation

Example:

The following shows how events are configured for Boolean (AND/OR) situations. The site is a parking garage that controls vehicle exit with a card reader, a pressure pad, and a Monitoring Station override switch.

Figure 88: Boolean Event Example



AND Operation

To configure the gate to open when a vehicle activates the pressure pad and a card is presented (AND operation):

1. Configure the events:
   a. Configure Event A to raise gate.
   b. Configure Event B to arm Event A.
   c. Configure Event C to activate Event A.
2. Configure the triggers:
   a. Link Event B to the pressure pad input by creating an Input trigger that Activates Event B when **Active Status** = **Active**.
   b. Link Event C to the door by creating a Door trigger that Activates Event C when **Admit Status** = **Admit**.

OR Operation

To configure the gate to open if the override switch is pressed or a card is read (OR operation):

1. Configure the events:

a. Configure Event A to raise gate.

b. Configure Event B to arm Event A.

c. Configure Event C to activate Event A.

2. Configure the triggers:

a. Link Event C to the override switch input by creating an Input trigger that Activates Event C when **Active Status** = **Active**.

b. Link Event B to the door by creating a Door trigger that Activates Event B when **Admit Status** = **Admit**.

Boolean Operators and Combinations

The C•CURE 9000 supports the following Boolean operations:

Table 60: Boolean Operations for Events

Operation	Function	Description
f = A • B	**(A and B)**	Input A > Event A >Activate Event f Input B > Event B >Arm Event f
f = A + B	**(A or B)**	Input A > Event A > Activate Event f Input B > Event B > Activate Event f
f = A ⊕ B	**(A exclusive or B) (Either one but not both)**	Input A > Event A > Activate Event f > Activate Event C Input B > Event B > Activate Event f > Arm Event C Event C > Disarm Event f
f = A and Not I	**[f = A • Î]**	Input A > Event A > Activate Event f Input I > Event I > Disarm Event f
f =A and (B or C)	**[f = A •(B+C)]**	Input A > Event A > Activate Event f Input B > Event B > Arm Event f Input C > Event C > Arm Event f
•f = A and a Time Spec		Input A > Event A > Activate Event f Time Spec >Arm Event f or Time Spec > Event B > Arm Event f

Latch and Unlatch for Events

You can cause an Event to activate and remain activated by performing a Latch action on the Event.

Similarly, you can cause an Event to deactivate and remain deactivated by performing an Unlatch action on the Event.

You can Latch or Unlatch an Event manually by:

- Activating an Event that includes a Latch or Unlatch Event action targeted toward another Event (see Configure a Latch or Unlatch Event Action on Page 263).
- Using the **Latch**, **Unlatch**, or **Toggle** actions on the Event context menu (see Latch or Unlatch an Event from the Event Context Menu on Page 263).
- Using the **Latch**, **Unlatch**, or **Toggle** actions on the Event Cause list (see Event Cause List on Page 251).

The ability to Latch an Event allows you to persist a state for a period of time, and use that state to allow or not allow an Event action. A subsequent Event can Unlatch the same Event, ending the state manually or according to a Schedule.

Example:

A vault door can only be opened if Joe Jones or Sam Smith are present in the building and it is before 5:00 PM. One solution is to:

1. Configure Joe Jones and Sam Smith as 'Noticed' in their Personnel records.
2. Define an event (A) to occur when either Joe or Sam are "noticed" using an access card to enter the building. Event A Latches another event (B).
3. Event B (with a **Door Entrance Reader Enabled** action) enables the vault door to be opened or accessed via badge.
4. Another event (C) would be caused by a Schedule activation at 5:00 PM and would then Unlatch event (B), causing the door reader to no longer be enabled.

Latch and Unlatch Priority

Latch and Unlatch actions have a priority rating that determines how multiple actions are handled. You can set the Priority for an Event that performs a Latch/Unlatch action when you configure the action in the Event editor, or you can set the Priority for a Latch/Unlatch action when you manually Latch or Unlatch an Event from the context menu or from the Cause list.

- If an Event is currently Latched, any further Latch actions have no effect, unless the new Latch action has an equal or higher priority than the current Latch action, in which case the new Latch action replaces the current Latch Action.
- If an Event is currently Unlatched, any further Unlatch actions have no effect, unless the new Unlatch action has an equal or higher priority than the current Unlatch action, in which case the new Unlatch action replaces the current Unlatch Action.

Latch and Unlatch on the Event Cause List

A Latch action is placed into the Event Cause list based on its priority, so the Latch action might not affect the current state of the Event, depending on the Latch action's place in the Cause list. This also means that the Latch cause can be intermixed with other causes (e.g., Activate/Deactivate/Arm/etc.).

NOTE Typically Latch and Unlatch actions are configured with the default Priority of 75. However, if you need to create Latch or Unlatch actions with a higher or lower priority to control interactions with other Event causes, the Priority level is adjustable.

Example:

You could create a Latch Event action with the highest Priority level available if you wanted to ensure that the Latch Event action could not be overridden by another action.

The Cause list of an Event contains only one active Latch cause. Any subsequent Latch cause is discarded if it has lower priority or older start time than a Latch action currently in the Cause List (see Event Cause List on Page 251).

The Latch cause in the Cause list is updated if a new Latch action with a higher priority and later time occurs.

If multiple Unlatch actions occur, they are ignored if the Event is not currently latched.

A new Latch (or Unlatch/Toggle) cause is treated as present time. You cannot set a Start Time for a Latch/Unlatch/Toggle Event action.

The Latch, Unlatch, and Toggle actions do not have an ending time. Thus, a Latch cause remains in the Event cause list until it is removed by an Unlatch cause.

When an Unlatch action is issued on an Event, the Unlatch cause can only affect the Event when specific conditions are present.

- If the priority of an Unlatch cause is equal to or higher than the Latch cause, or the time of the Unlatch cause is newer than the Latch cause, the Latch cause is removed. This is the only method to cancel a Latch action that is not the top cause in the cause list.
- If the priority of an Unlatch cause is lower than the Latch cause, or its time is not newer than the Latch cause, the Unlatch cause is ignored
- If the Unlatch cause is first in the Cause list and the target Event is currently Latched, the Event becomes Unlatched – meaning the Latched state is cleared or canceled.
- If the Unlatch cause is first in the Cause list and the target event is not currently latched, the event retains its current state. Regardless, the existing Latch cause (if any) in the Cause list is removed and the Unlatch cause is placed in the cause list.

Effect of Server Restart on Latched and Unlatched Events

The Latched/Unlatched state of Events is retained in the database, and if the C•CURE 9000 server is restarted, the Event Latch, Unlatch, and Acknowledgement state is restored.

- For host Events, the host restores the Events to the correct Latch state based on the property in the Event object upon driver restart.
- For panel Events, the host needs to retrieve each Event's Latch states from the Event object. Upon iSTAR controller restart, the host sends the active Latch causes for these Events to the controller, and the controller restores these Events to the correct Latch state.

Latching or Unlatching Events from Maps

You can add an Event icon to a Map object, and then configure the Event icon to allow Latch/Unlatch from:

- A left-click Icon action.
- A context menu selection.

See the Chapter on Maps in the *C•CURE 9000 Data Views Guide* for more information.

The icon displayed for the Event during a Latch/Unlatch action is **Activate**.

Privilege for Latch and Unlatch

To use the Latch and Unlatch actions, an Operator must have Permission granted for Latch and Unlatch in the Event class.

If the Latch permission is granted, the Operator can latch an Event; if the permission is not granted, the Operator cannot latch an Event.

If the Unlatch permission is granted, the Operator can to unlatch an Event; if the permission is not granted, the Operator cannot unlatch an Event.

By default, these permissions are not granted for a newly created Privilege.

Existing Privileges are not updated to include permission for Latch and Unlatch when C•CURE 9000 is upgraded; the Grant value for Latch and Unlatch is not enabled ( ).

If an Operator has permission for Latch Event or Unlatch Event, but has an exception for the specific Event that has that type of action, the Operator cannot perform an Event action to that Event.

Latch and Unlatch Event Tasks

- Configure a Latch or Unlatch Event Action on Page 263
- Latch or Unlatch an Event from the Event Context Menu on Page 263
- Latch or Unlatch an Event from the Cause List on Page 264

Configure a Latch or Unlatch Event Action

You can configure a Latch Event action that causes another Event to be armed (if currently disarmed), activated, and Latched (kept active until unlatched). When this action is executed, the Event is shown in the Event Cause List as Latched, and the Event stays Latched until an Unlatch or a Toggle action is executed.

You can configure an Unlatch Event action that causes another Event to be Unlatched, if the Event is currently Latched. When this action is executed, the Event is shown in the Event Cause List as Unlatched, and the Event stays Unlatched until a Latch or a Toggle action is executed.

The Priority for a Latch or Unlatch action is that of the Event that contains the Latch or Unlatch action.

To Configure an Event Action to Latch (or Unlatch) an Event

1. From the Event editor (see Accessing the Event Editor on Page 300), click the Event Action tab.
2. Click **Add** to add an Event Action.
3. Select **Latch Event** (or **Unlatch Event**) from the **Action** drop-down list.
4. In the **Event** field near the bottom of the tab, select the Event that you want to Latch (or Unlatch).
5. Click **Save and Close** to save the Event.

Latch or Unlatch an Event from the Event Context Menu

You can Latch or Unlatch an Event from the context menu of the Dynamic View of Events.

If you Latch an Event from the context menu, it causes that Event to be armed (if currently disarmed), activated, and Latched (kept active until unlatched). When this menu item is executed, the Event is shown in the Event Cause List as Latched, and the Event stays Latched until an Unlatch or a Toggle action is executed.

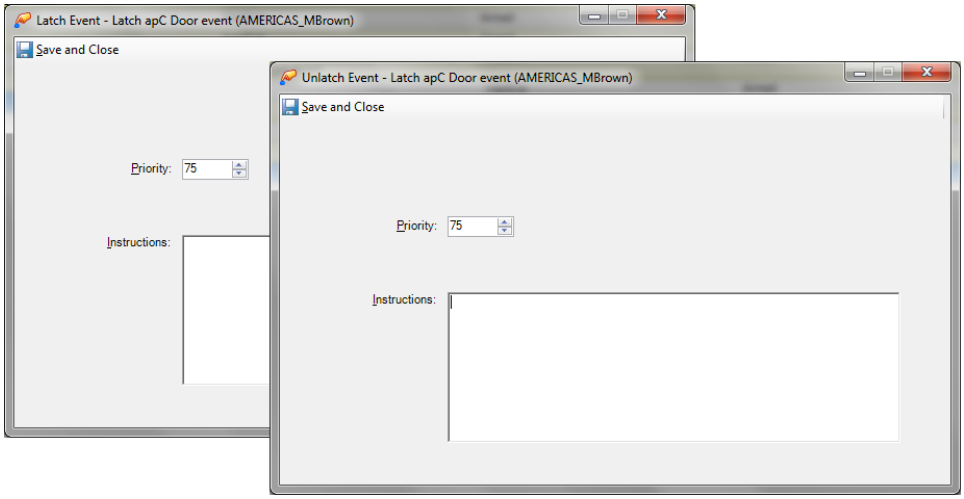
If you Unlatch an Event from the context menu, it causes that Event to be Unlatched, if the Event is currently Latched. When this menu item is executed, the Event is shown in the Event Cause List as Unlatched, and the Event stays Unlatched until a Latch or a Toggle action is executed.

You can set the Priority of the Latch or Unlatch action so that it takes precedence over an existing cause - if the Priority of the Event is higher than the Priority of the Latch or Unlatch action, the Latch or Unlatch action is ignored.

To Latch (or Unlatch) an Event from the Event Context Menu

1. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Event** from the Configuration pane drop-down list.
3. Click  to open a Dynamic View showing all Events.
4. Right click on the Event in the list that you want to Latch (or UnLatch) and select **Latch Event** (or **Unlatch Event**) from the context menu.
5. The Latch Event (or Unlatch Event) dialog box opens (see Figure 89 on Page 264).

Figure 89: Latch Event and Unlatch Event Dialog Boxes



6. You can use the spinner control () to set the Priority of the action (default: 75, minimum: 1, maximum: 200).
7. You can enter a textual message in the **Instructions** field to explain the action. (The **Instructions** text appears on the Event Details dialog box when you view Event Details.)
8. Click **Save and Close** to execute the Latch Event (or Unlatch Event) action.

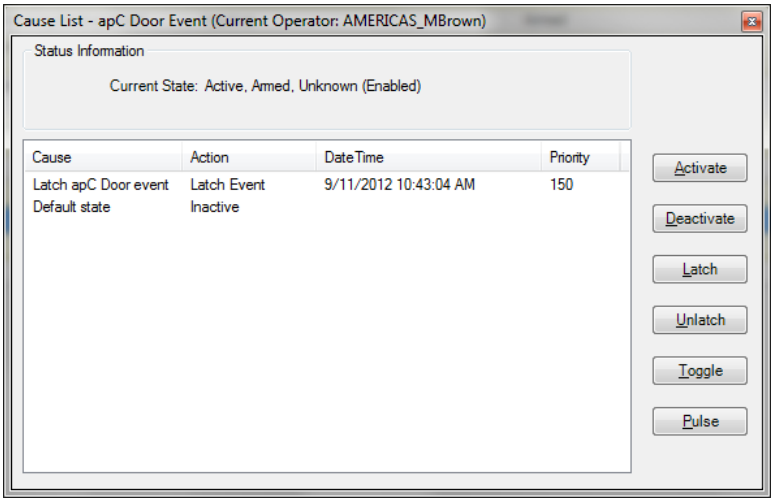
Latch or Unlatch an Event from the Cause List

You can Latch an Event from the Event Cause List by clicking **Latch**.

You can Unlatch a Latched Event from the Event Cause List by clicking **Unlatch**.

These buttons are shown in Figure 90 on Page 265.

Figure 90: Event Cause List



If you attempt to Latch an Event that is already Latched, your Latch action replaces the Latch Event cause only if your Latch action has a higher Priority and a more recent Date/Time than the current Latch cause.

If you attempt to Unlatch an Event that is Latched, your Unlatch action replaces the Latch Event cause only if your Latch action has an equal or higher Priority and a more recent Date/Time than the current Latch cause.

You can access the Cause List to Latch/Unlatch an Event from the following locations:

Location	See...
Dynamic View of Events	To Access the Event Cause List from the Dynamic View of Events on Page 265.
Monitoring Station Event Viewer	To Access the Event Cause List from the Monitoring Station Event Viewer on Page 265.
Monitoring Station Explorer Bar	To Access the Event Cause List from the Monitoring Station Explorer Bar on Page 265.

To Access the Event Cause List from the Monitoring Station Event Viewer

1. From the Monitoring Station, Right-click the Event you want to Latch, Unlatch, or Toggle from the Event Viewer.
2. Select **Show Active Causes**.
3. The Cause List appears. See To Latch (or Unlatch) an Event from the Event Cause List on Page 266.

To Access the Event Cause List from the Monitoring Station Explorer Bar

1. From the Monitoring Station, select Non-Hardware Status from the Explorer Bar.
2. Click **Events** to open the Status List for Events.
3. Right-click on the Event for which you want to view the Cause List and chose **Show Active Causes**.
4. The Cause List appears. See To Latch (or Unlatch) an Event from the Event Cause List on Page 266.

To Access the Event Cause List from the Dynamic View of Events

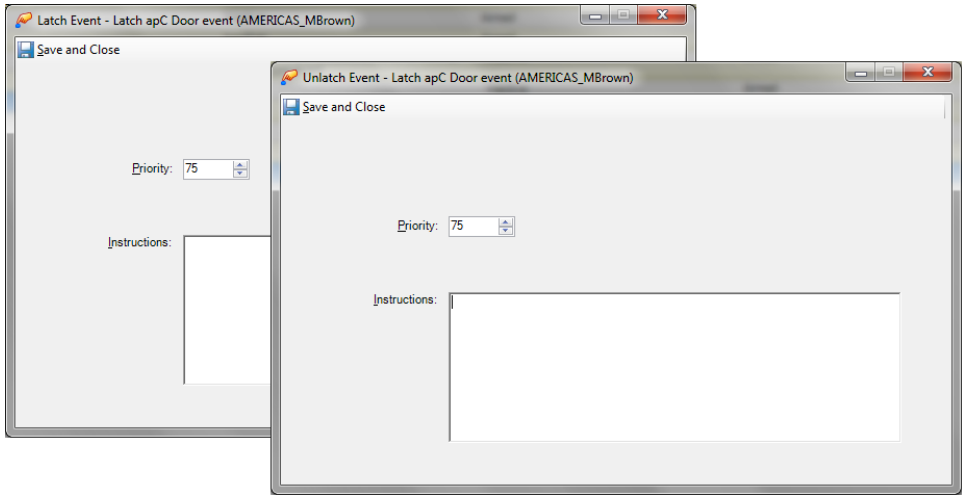
1. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Event** from the Configuration pane drop-down list.

3. Click to open a Dynamic View showing all Events.
4. Right click on the Event in the list that you want to Latch (or Unlatch) and select **Show Active Causes** from the context menu.
5. The Cause List appears. See To Latch (or Unlatch) an Event from the Event Cause List on Page 266.

To Latch (or Unlatch) an Event from the Event Cause List

1. Form the Event Cause List, click **Latch** or **Unlatch** to perform that action on the Event.
2. The Latch Event (or Unlatch Event) dialog box opens (see Figure 91 on Page 266).

Figure 91: Latch Event and Unlatch Event Dialog Boxes



3. You can use the spinner control ( ) to set the Priority of the action (default: 75, minimum: 1, maximum: 200).
4. You can enter a textual message in the **Instructions** field to explain the action. (The **Instructions** text appears on the Event Details dialog box when you view Event Details.)
5. Click **Save and Close** to execute the Latch Event (or Unlatch Event) action.

Toggle an Event

You can use the **Toggle** Event action to reverse an Event's Latch/Unlatch state.

Toggle switches a Latched Event to an Unlatched Event, or switches an Unlatched Event to a Latched Event.

- If the Event is currently Latched, the Toggle action acts like an Unlatch action.
- If the Event is not Latched, the Toggle action acts like a Latch action; if the Event is not currently Activated, it becomes Activated because of its Latched state.

Toggle Priority

Toggle actions have a priority rating that determines how multiple actions are handled. You can set the Priority for a Toggle action when you configure the action in the Event editor or manually Toggle an Event from the context menu or from the Cause list.

- If an Event is currently Latched, a Toggle action with a lower priority has no effect. If the Toggle action has an equal or higher priority than the current Latch cause, the Event becomes Unlatched.
- If an Event is currently Unlatched, a Toggle action with a lower priority has no effect. If the Toggle action has an equal or higher priority than the current UnLatch cause, the Event becomes Latched.

A Toggle action is useful in configuring a single Event that activates or deactivates another Event.

Example:

Event B is configured to Latch Event C, which activates an Output (a warning light). Event A is configured to Toggle Event B based on the state change of an Input (a push button).

When the button is pushed once, Event A toggles Event B, which Latches Event C, and the warning light is activated (and stays on).

When the button is pushed again, Event A toggles Event B, which Unlatches Event C, and the warning light is deactivated (the light turns off and stays off).

Toggling Events from Maps

You can add an Event icon to a Map object, and then configure the Event icon to allow the Toggle action from:

- A left-click Icon action.
- A context menu selection.

See the chapter on Maps in the *C•CURE 9000 Data Views Guide* for more information.

The icon for the Event during a Toggle action is **Activate**.

Privilege for Toggle Event

To use the Toggle Event action, an Operator must have Permission granted for Toggle in the Event class.

If the Toggle permission is granted, the Operator can toggle an Event; if the permission is not granted, the Operator cannot toggle an Event.

By default, this permission is not granted for a newly created Privilege.

Existing Privileges are not updated to include permission for Toggle Event when C•CURE 9000 is upgraded; the **Grant** value for Toggle is not enabled (☐) during upgrade.

If an Operator has permission for Toggle Event but has an exception for a specific Event, the Operator cannot perform an Event action to that Event.

Toggle Event Tasks

To Configure an Event Action to Toggle an Event

1. From the Event editor (see Accessing the Event Editor on Page 300), click the Event Action tab.
2. Click **Add** to add an Event Action.
3. Select **Toggle Event** from the **Action** drop-down list.
4. In the Event field near the bottom of the tab, select the Event that you want to Toggle.
5. Click **Save and Close** to save the Event.

To Toggle an Event from the Event Context Menu

1. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Event** from the Configuration pane drop-down list.
3. Click  to open a Dynamic View showing all Events.
4. Right click on the Event in the list that you want to Toggle and select **Toggle Event** from the context menu.
5. The Toggle Event dialog box opens.
6. You can use the spinner control () to set the Priority of the action (default: 75, minimum: 1, maximum: 200). (The priority must be set to equal to or greater than the Event's current priority, or the Toggle action has no effect.)
7. You can enter a textual message in the **Instructions** field to explain the action. (The **Instructions** text appears on the Event Details dialog box when you view Event Details.)
8. Click **Save and Close** to execute the Toggle Event action.

To Toggle an Event from the Event Cause List

1. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Event** from the Configuration pane drop-down list.
3. Click  to open a Dynamic View showing all Events.
4. Right click on the Event in the list that you want to Toggle and select **Show Active Causes** from the context menu. The Cause List dialog box opens.
5. Click **Toggle Event**. The Toggle Event dialog box opens.
6. You can use the spinner control () to set the Priority of the action (default: 75, minimum: 1, maximum: 200). (The priority must be set to equal to or greater than the Event's current priority, or the Toggle action has no effect.)
7. You can enter a textual message in the **Instructions** field to explain the action. (The **Instructions** text appears on the Event Details dialog box when you view Event Details.)
8. Click **Save and Close** to execute the Toggle Event action.

Pulse an Event

An Operator can cause an Event to be momentarily activated (Pulse).

An Operator can only pulse an Event that is Armed. The Operator must have the Event Privilege **Pulse** to Pulse an Event. Both host and panel Events can be Pulsed.

An Operator can Pulse an Event in the following ways:

To Pulse an Event...	See...
Event action	To Configure an Event Action to Pulse an Event on Page 270
Event context menu	To Pulse an Event from the Event Context Menu on Page 270
Event Cause List	To Pulse an Event from the Event Cause List on Page 270.

When a Pulse action is issued on an Event, the Event is activated for the amount of time specified in the Minimum Activation Time of the Event. If the Minimum Activation Time is 0, then the Event is pulsed for one second.

NOTE Pulse Event is not available on the context menu for Event Groups.

If multiple Pulse actions are issued for the same event, the state of the event is dependent on the priority and start time of the actions.

If two Pulse actions are issued at the same time at the same priority for the same Event, the Event is activated for the specified Activation Time and then the Pulse is repeated.

Pulsing Events from Maps

You can add an Event icon to a Map object, and then configure the Event icon to allow a Pulse from:

- A left-click Icon action.
- A context menu selection.

See Configure an Event Icon on a Map for more information.

The icon for the Event during a Pulse action is the same as **Activate**.

Pulse Action in the Event Cause List

If an Event is Pulsed, the Pulse action appears in the Event Cause list if you select **Show Active Causes** from:

- The Event Dynamic View context menu in the Administration Client.
- The Event Viewer context menu in the Monitoring Station.

The Cause List dialog box for an Event has a button for **Pulse** that allows you to manually Pulse an Event. For more information, see Event Cause List on Page 251.

Privilege for Pulse Event

To use the Pulse Event action, an Operator must have the Permission for Pulse granted in the Event class of their Privilege.

If the Pulse permission is granted, the Operator can pulse an Event; if the permission is not granted, the Operator cannot pulse an Event.

By default, this permission is not granted for a newly created Privilege.

Existing Privileges are not updated to include permission for Pulse Event when C•CURE 9000 is upgraded; the Grant value for Pulse is not enabled ( ).

If an Operator has permission for Pulse Event but has an exception for the specific Event that does not allow a Pulse action, the Operator cannot Pulse the Event.

Pulse Event Tasks

To Configure an Event Action to Pulse an Event

1. From the Event editor (see Accessing the Event Editor on Page 300), click the Event Action tab.
2. Click **Add** to add an Event Action.
3. Select Pulse Event from the **Action** drop-down list.
4. In the Event field near the bottom of the tab, select the Event that you want to Pulse.
5. Click **Save and Close** to save the Event.

To Pulse an Event from the Event Context Menu

1. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Event** from the Configuration pane drop-down list.
3. Click to open a Dynamic View showing all Events.
4. Right click on the Event in the list that you want to Pulse and select **Pulse Event** from the context menu.

To Pulse an Event from the Event Cause List

1. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Event** from the Configuration pane drop-down list.
3. Click to open a Dynamic View showing all Events.
4. Right click on the Event in the list that you want to Pulse and select **Show Active Causes** from the context menu.
5. Click **Pulse** on the Cause List to Pulse the Event.

Assess Event Overview

The Assess Event capability allows you to configure an Event so that a Monitoring Station Operator with the correct Privileges can use an Assess Event Application Layout to:

- View documents associated with the Event.
- View live video associated with the Event.
- View recorded video associated with the Event.
- View Event details.
- View a Map associated with the Event.
- View a Journal Replay of the event, based on a query associated with the Event.
- Use an Event Details Viewer with additional quick action buttons to process the Event.

The Operator can launch the Application Layout and view the objects from the Event Viewer by selecting the Event in the list, right-click and select **View** and **Assess Event** from the context menu.

To configure the Assess Events capability, you need to:

- Provide your Monitoring Station Operators with the correct Privileges to assess Events. See Configuring Privileges for Event Assessment on Page 272 and Configuring Operators for Event Assessment on Page 273.

Assess Events Configuration

To use the Assess Event capability, you need to define the information and objects you want to add to your Assess Events Application Layout: and to the Events that will be assessed using this Application Layout (see Table 61 on Page 271).

Table 61: Assess Events Configuration Process

Step	Action	See...
1.	Determine the types of information and objects your Operators need to assess Events.	Your site's policies and procedures.
2.	Design one or more Assess Event Application Layouts that include Viewers for the information (such as a document) and objects (such as a Map or Video camera) that you want your Operators to be able to see when assessing an Event.	C•CURE 9000 Data Views Guide chapter on Application Layout.
3.	Use the Event editor **Assess Configuration** tab to configure the Events that you want to be assessed so that the information and objects that Operators need are associated with the Event. The Event should have an object configured for every viewer that is included in the Assess Event Application Layout.	Adding an Assess Event Object on Page 274.
4.	Configure your Operators to have the Assess Event Privileges that allow them to assess Events using the Privilege editor.	Configuring Privileges for Event Assessment on Page 272
5.	Configure your Operators with access to your Assess Event Application Layouts using the Operator editor.	Configuring Operators for Event Assessment on Page 273

To configure an Event for assessment, you use the Event Assess Configuration tab in the Event Editor. See Event Assess Configuration Tab on Page 295.

Example

In your site policies and procedures, you have documents that provides step-by-step instructions for your Operators to deal with the following Event types:

- Door Forced Events
- Door Held Events
- Duress Events
- Glass Break Events

You could then design one or more **Application Layouts** that include viewers for the objects related to these Events. If your procedures require an Operator to look at live and recorded video for the areas where the event occurred, you can provide an Application Layout that contains:

- A viewer display your procedure document for that Event type.
- A viewer for live video of that area.
- A viewer for recorded video that was triggered by an Event Action for that area.

In the Event itself, you can use the **Event editor** to specify objects related to the Event:

- Attach a specific procedure document on the Event Assess Configuration tab.
- Identify a specific live video View of the Event area on the Event Assess Configuration tab.
- Configure an video camera Event Action to record video from a specific camera on the Event Action tab.

When an Event occurs and the Operator clicks Assess Event in the **Monitoring Station** Event Viewer, the Assess Event Application Layout you configured opens, displaying:

- Your procedure document for that Event type.
- A live video viewer for the Event vicinity.
- The recorded video created by your Event Video camera action.

Thus the Operator has this information immediately, rather than manually searching for a document, opening camera views, and trying to find recorded video.

Configuring Privileges for Event Assessment

The operator(s) who configure the Assess Event Application Layouts for your system, if they do not have the System All Privilege, need to have a Privilege assigned that gives them access to configure the Assess Event Application Layouts, as well as configure the Events for Event Assessment.

Also, If your Monitoring Station Operators do not have the System All Privilege, you need to set up a Privilege that gives them the correct access to Assess Events.

Granting Privileges for Assess Event Configuration

For an Operator to configure Events for assessment, and create/edit Assess Event Application Layouts, the Operator must have the following **minimum** Privileges (you can assign higher levels of these privileges if desired):

- Edit permission for Application Layouts.
- Edit permission for Events.
- Read and View permissions for Documents (if included in assessments).

NOTE For a C•CURE 9000 System that is upgraded from a previous version, existing Operator Privileges are set with these Privileges **not** enabled, so that Operators do not gain unintended access to a new feature.

This means that an Operator who does not have System All Privilege needs to have these Privileges enabled in order to Assess Events.

To Configure Privileges for Assess Events Application Layouts

1. Create a new Privilege or edit an existing Privilege that you wish to modify. See Creating a Privilege on Page 442.
2. If you are creating a new Privilege, enter a name in the **Name** field, and select the **Enabled** field check box.
3. On the **Default** tab in the Classes list, click **Application Layout**.
4. In the **Permissions** list, select the **Grant** check box for the **Edit** Privilege.
5. On the **Default** tab in the Classes list, click **Document**.
6. In the Permissions list, select the **Grant** check box for the **Read** Privilege.
7. On the **Default** tab in the Classes list, click **Event**.
8. In the **Permissions** list, select the **Grant** check box for the **Edit** Privilege.
9. Click **Save and Close** to save your settings.

Granting Privileges for Monitoring Station Operators to Assess Events

For a Monitoring Station Operator to perform Event Assessment, the Operator must have the following minimum Privileges:

- Read permission for Application Layouts.
- Read permission for Event Assess in Events.
- Read and View permissions for Documents (if included in assessments).
- On the **Viewable Message Types** tab, Event Assess Message should be enabled.

NOTE For a C•CURE 9000 System that is upgraded from a previous version, existing Operator Privileges are set with these Privileges **not** enabled, so that Operators do not gain unintended access to a new feature.

This means that an Operator who does not have System All Privilege needs to have these Privileges enabled in order to Assess Events.

To Configure Privileges for Monitoring Station Operators to Assess Events

1. Create a new Privilege or edit an existing Privilege that you wish to modify. See Creating a Privilege on Page 442.
2. If you are creating a new Privilege, enter a name in the **Name** field, and select the **Enabled** field check box.
3. On the **Default** tab in the Classes list, click **Application Layout**.
4. In the **Permissions** list, select the **Grant** check box for the **Read** Privilege.
5. On the **Default** tab in the Classes list, click **Document**.
6. In the **Permissions** list, select the **Grant** check box for the **Read** and **View** Privileges.
7. On the **Default** tab in the Classes list, click **Event**.
8. In the **Permissions** list, select the **Grant** check box for the **Assess an Event** Privilege.
9. Click the **Viewable Message Types** tab.
10. Select the check box for Event Assess Message.
11. Click **Save and Close** to save your settings.

Configuring Operators for Event Assessment

After you have configured Privileges for your Operators who will be designing Assess Event Application Layouts and using those layouts in the Monitoring Station to Assess Events, you have to assign these Privileges to your Operators using the

Operator editor.

You also need to give access to the Assess Event Application Layouts you have created to the Operators who will be performing Event assessment using the Monitoring Station.

NOTE This procedure is intended for Operators who do not have the System All Privilege. Operators with System All Privilege do not need to be assigned additional Privileges to be able to configure Assess Events or perform Event Assessment.

To Enable an Operator to Configure Event Assessment

1. Use the Operator editor to edit the Operator record for the Operator you want to enable to configure Event Assessment.
2. Click **Add** in the Privileges and Schedules table.
3. Click in the **Privilege** column of the new row, then click ... .
4. Select the Privilege you created for this Operator to configure Event Assessment from the list. The Privilege is added to the Operator record.
5. Click **Save and Close**to save your settings.

To Enable an Operator to Perform Event Assessment in the Monitoring Station

1. Use the Operator editor to edit the Operator record for the Operator you want to enable to perform Event Assessment with the Monitoring Station.
2. Click **Add** in the Privileges and Schedules table.
3. Click in the **Privilege** column of the new row, then click ... .
4. Select the Privilege you created for this Operator to perform Event Assessment from the list. The Privilege is added to the Operator record.
5. Click the Layout tab.
6. Click **Add** in the **Application Layout with Tab Order** table.
7. Select the Application Layouts you want to assign to this Operator for assessing Events, then click OK.
8. Click **Save and Close** to save your settings.

Adding an Assess Event Object

From the Event editor **Assess Configuration** tab, you can add objects that you want to be associated with the Event in the Monitoring Station.

NOTE On the Event Acknowledgement Tab on Page 284, you must select **Send State Changes to Monitoring Station** so that the Event will be visible to be assessed by a Monitoring Station Operator.

You need to select an Assess Event Application Layout for the Event. This Application Layout is used in the Monitoring Station to display the objects that your select.

You should only add one of each type of object to the Event.

You should only add an object if that object is included an Assess Event Application Layout chosen for the Event (because only objects included in the Application Layout are displayed).

See the *C•CURE 9000 Data Views Guide* chapter on Application Layouts for instructions for creating an Assess Event Application Layout.

Example

You select an Assess Event Application Layout called Door-Held which contains viewers for a document, video, and a report. You should not add a Query Assess Event object to this Event because the Assess Event Application Layout does not include a Query Viewer.

To Add an Assess Event Object

1. In the Event Editor, click the **Assess Configuration** tab.
2. Click ... in the **Select Application Layout for Assess Event** field. The Name selection dialog box opens, showing the Assess Event Application Layouts that are available. Click an Application Layout to select it.

   Or, click the down arrow and select **New** to create a new application layout or click **Edit** to edit an existing application layout.
3. Under Assessment Parameters, click **Add**. A Name Selection dialog box opens.
4. Click ... in the **Select Type** field.
5. Select an object type from the list. A list of objects of that selected type appears in the Name Selection dialog box.
6. Select an object from the list in the Name Selection dialog box.

   Example:

   If you selected Document from the Select Type list, a list of available Document objects appears. Select a Document from the list.
7. Click **Add** to add more objects to the Assess Events configuration, or click **Save and Close** to save your new settings for the Event.

Dual Phase Acknowledgement Overview

An Event can be configured so that a Monitoring Station Operator with the correct Privileges uses Dual Phase Acknowledgement. Dual Phase Acknowledgement manages events by requiring that an event remain active after it is acknowledged until it is cleared. Events are configured individually to use Dual Phase Acknowledgement in the Event Editor.

From the Monitoring Station, you can select the event requiring acknowledgement and click the **Acknowledge** button. If the event is configured for a log message, a log message is required at the time the event is acknowledged. If the acknowledged event requires clearing, the event is moved from the Acknowledge state and displayed as Pending Clear. You select the event and click the **Clear** button to clear the event. If the event is configured for a log message, a log message is required at the time you clear the event.

- If an Event is configured as "Requires Clearing", it will by default require Acknowledgement.
- Event Requires Clearing will only be available after the Event has been Acknowledged by an Operator.
- An Event which" Requires Clear" will not be removed from the Event Viewer until an Operator Clears the Event.
- Operators can be configured to only Acknowledge Events, only Clear Events, or Acknowledge and Clear Events.
- Operators with the Acknowledge and Clear privilege can Acknowledge and Clear Events in a single action.
- If an Event pending clear displayed in the Event Viewer is edited and changed to not require Clear, then its state is automatically updated and removed from the viewer.
- Predefined log messages can selected to use when Acknowledging, Clearing, or both.
- A time duration can be configured to activate a second Event if acknowledgement of an Event, or clearing an Event, does not take place within a time frame. The time frame starts when the Event is activated.

Table 62 on Page 276 lists the Dual Phase Acknowledgement configuration sequence, and where to find the configuration procedures.

Table 62: Dual Phase Acknowledgement Configuration Process

Step	Action	Where...	See...
1.	Create a Dual Phase Acknowledgement Application Layout.	Application Layout Editor	Creating a Dual Phase Application Layout on Page 276
2.	Configure Event Permissions and Privileges.	Privilege Editor	Configuring Event Permissions for Dual Phase Acknowledgement on Page 443
3.	Assign the Event Privileges and Application Layout to the operators.	Operator Editor	Assigning the Event Privileges and Application Layout to the Operator on Page 278
4.	Configure an existing event, or a new event, to use Dual Phase Acknowledgement.	Event Editor	Configuring Events to Use Dual Phase Acknowledgement on Page 279

Creating a Dual Phase Application Layout

This section describes how to set up the Application Layout to use Dual Phase Acknowledgement using the sample layout, and also how to create a new layout.

The template contains three panes:

- Event Viewer (top pane) - contains events requiring no action and events that require acknowledgement.
- Event Viewer (bottom pane) - contains events requiring clearing.
- Activity Viewer - contains all activity.

See the *C•CURE 9000 Data Views Guide* for detailed procedures and field descriptions.

To Create the Application Layout Using the Dual Phase Acknowledgement Sample Layout

1. In the Navigation Pane of the Administration Workstation, click the **Data Views** pane button.
2. Click **the Data Views** drop-down list and select **Application Layout**.
3. Click  to display a list of pre-configured application sample layouts in the Dynamic View.
4. Double-click on **Dual phase event acknowledgement layout** template.
5. Click **Create Copy**.
6. Enter a Name and Description for the layout.
7. If desired:
   - Right-click on the Event Viewer tab and select **Properties** to edit the configuration. See the *C•CURE 9000 Data Views Guide* "Application Layout" chapter for more information.
   - Right-click on the Activity Viewer pane tab and select **Properties** to edit the configuration. See the *C•CURE 9000 Data Views Guide* "Application Layout" chapter for more information.
8. Click **Save and Close**.

To Create a New Dual Phase Acknowledgment Application Layout

1. In the Navigation Pane of the Administration Workstation, click the **Data Views** pane button.
2. Click **the Data Views** drop-down list and select **Application Layout**.
3. Click 

to open the Application Layout Editor.
4. Enter a Name and Description for the Dual Phase Acknowledgement layout.
5. Drag **Event Viewer** onto the layout to display the Event Viewer Editor.
6. Select the Buttons and Event actions for the Event Viewer. See the *C•CURE 9000 Data Views Guide* "Application Layout" chapter for more information.
7. Repeat Step 5 through Step 6 to add a second Event Viewer pane for Events Acknowledged Pending Clear.
8. To add other viewer types to the layout. See the *C•CURE 9000 Data Views Guide* "Application Layout" chapter for more information.
9. Click **Save and Close**

Configuring Event Permissions for Dual Phase Acknowledgement

This procedure only describes the Event permissions that need to be configured to use Dual Phase Acknowledgement. See Creating a Privilege on Page 442 for detailed procedures and field descriptions.

Table 63: Dual Phase Acknowledgement Permissions

Permission	Grant Meaning
Acknowledge	Selecting the **Acknowledge** check box, and not the Clear check box, allows the Operator to only acknowledge Events.
Clear	Selecting the **Clear** check box, and not the Acknowledge check box, allows the Operator to only clear Events.

Acknowledge Clear	Selecting the **Acknowledge** check box and the **Clear** check box allows the Operator to Acknowledge Events, and if required, Clear the Event.
Acknowledge and Clear	Selecting the **Acknowledge and Clear** check box allows the Operator to acknowledge and clear Events individually, or in one step. NOTE: The **Acknowledge** check box and the **Clear** check box must also be selected.

To Configure the Event Permissions for Dual Phase Acknowledgement

1. In the Navigation Pane of the Administration Workstation, click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Privilege**.
3. Click  to display a list of privileges in the Dynamic View, or click **New** to create a new privilege. The **Privilege Editor** opens.
4. Click on the **Defaults** tab.
5. Click on **Event** located in the **Classes** list.
6. In the **Permission** list, select the Permissions for the privilege. Ensure that the correct permission for Dual Phase Acknowledgement is selected, see Table 63 on Page 277
7. Click **Save and Close**.

Assigning the Event Privileges and Application Layout to the Operator

This procedure describes only how to assign the operator pre-configured privileges and application layouts to use Dual Phase Acknowledgement. See Creating a Privilege on Page 442 for detailed procedures and field descriptions.

This task assumes that the operator and the application layout are already configured.

To Assign the Event Permissions and Privileges to the Operator

1. In the Navigation Pane of the Administration Workstation, click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Operator**.
3. Click  to display a list of pre-configured operators in the Dynamic View.
4. Double-click on an operator in the list to open the Operator editor.
5. In the **General** tab under **Privileges**, click **Add**.
6. Click in the blank row under **Privilege**, and then click on the  selection button to open the Name Selection dialog box.
7. Click on the privilege that you configured for the operator for dual phase acknowledgement.
8. Click on the **Layout** tab.
9. Click **Add** to open the Name Selection dialog box.
10. Click in the check boxes next to the pre-configured application layouts to select them for the operator.
11. Click **OK** to close the Name Selection dialog box.
12. Click **Save and Close** to save the operator configuration.

Configuring Events to Use Dual Phase Acknowledgement

This procedure only describes how to configure an event to use Dual Phase Acknowledgement. See Event Editor on Page 280 for detailed procedures and field descriptions.

To Configure an Event to Use Dual Phase Acknowledgement

1. In the Navigation Pane of the Administration Workstation, click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Event**.
3. Click  to display a list of events in the Dynamic View. Double-click on the event you want to configure for Dual Phase Acknowledgement to open the Event Editor.

   Alternately, you can click **New** to configure a new event.
4. Click on the **Acknowledgment** tab and select the options required for the event. See Event Acknowledgement Tab on Page 284 for descriptions of the available options.
5. Click on the **Overdue** tab and select the overdue time durations and the event to activate for the overdue Acknowledgement and/or Clearing. See Event Overdue Tab on Page 289 for descriptions of the available options.
6. Ensure that the **Enabled** check box is selected.
7. Click **Save and Close**.

Event Editor

A C•CURE 9000 Event is used to define the way C•CURE 9000 responds to state changes that occur to objects in the system. You can use events to perform actions when a state change occurs.

Example:

You can configure an Event to unlock a door and activate an output when an input becomes active.

You can create events that perform simple functions, like unlocking a door, or a complex functions, like arming, disarming, and monitoring an area. You can link an event directly to a single action, or you can link it to multiple events and actions.

The following topics give more information about the Event object and how to use it.

- Understanding Events on Page 237
- Event Causes and Actions on Page 239
- Event Actions on Page 241
- Event Cause List on Page 251
- Events and Time Zones on Page 253
- Straightforward Events on Page 255
- Complex Events on Page 259
- Latch and Unlatch for Events on Page 261
- Toggle an Event on Page 267
- Pulse an Event on Page 269
- Assess Event Overview on Page 271
- Dual Phase Acknowledgement Overview on Page 276
- Event Tasks on Page 300
- Clearance Filter Events on Page 255
- Assess Events Configuration on Page 271

The Event editor includes eight tabs:

- General (see Event General Tab on Page 281)
- Acknowledgement (see Event Acknowledgement Tab on Page 284)
- Overdue (see Event Overdue Tab on Page 289)
- Messages (see Event Messages Tab on Page 291)
- Actions (see Event Action Tab on Page 293)
- Assess Event (see Event Assess Configuration Tab on Page 295)
- Predefined Log Messages (see Event Predefined Log Messages Tab on Page 297)
- Groups (see Object Editor Groups Tab on Page 26)
- State Images (see Event State Images Tab on Page 298)

(The Groups tab only appears if you have previously defined a Group object that includes Events.)

The Event editor includes basic Identification fields and toolbar buttons, as defined in Table 64 on Page 281.

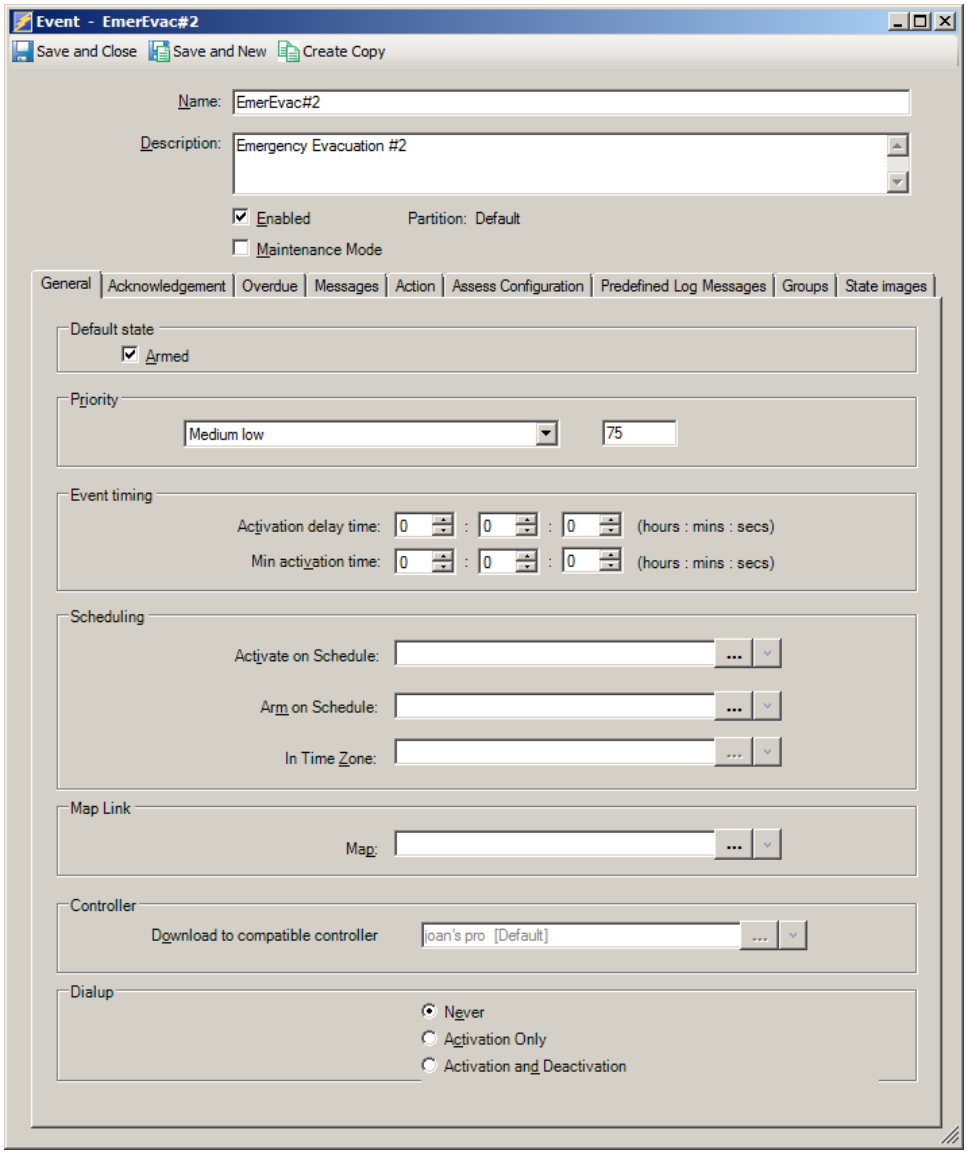
Table 64: Event Configuration Identification Fields

Field	Description
Name	Enter a unique name, up to 50 characters long, to identify the Event. NOTE: The Event name cannot contain non-printable characters. An error message appears if you attempt to save an Event with non-printable characters in the **Name** field.
Description	Enter a description, of up to 500 characters, to identify the Event.
Enabled	Select the Enabled check box to make the Event operational. The default is Disabled (unchecked).
Maintenance Mode	Click to put the Event into Maintenance Mode. See the *C•CURE 9000 Hardware Configuration Guide* "Maintenance Mode" chapter for more information.
Partition	A read-only field displaying the name of the Partition to which this Event belongs. (This field is visible only if the C•CURE 9000 system is partitioned.)
Save and Close	Click this button when you have completed your editing changes to the Event. The Event editor closes.
Save and New	Click this button when you have completed any changes to the Event and wish to save those changes and also create a new Event. The Event you were editing is saved, and a new Event opens (either blank or including template information if you were using a template to create new Event).
Create Copy	Click to save your changes, close that Event, and keep the Event editor open with a copy of the Event you saved. You can use the copy to name and save a new Event using the same settings as the Event you previously saved. If your original Event was downloaded to a controller, the copied Event also has **Download to Compatible Controller** selected, but the controller field is not filled in, so you can select a different controller from the one specified in the original saved Event.

Event General Tab

The Event Editor General tab, shown in Figure 92 on Page 282 lets you define the basic characteristics of an Event.

Figure 92: Event Editor General Tab



The Event Configuration editor includes the fields defined in Table 65 on Page 282 in the **General** tab.

Table 65: Event General Tab Definitions

Field/Box	Description
Default state	
Armed	Select this check box to arm the Event. The default is unarmed (unchecked).
Priority	
Event Priority	Indicates the priority level the system uses for sorting when displaying on the Monitoring Station and prioritizing actions associated with the event. The default priority is 75, Medium Low. Select a value from the drop-down list or type an integer from 0 to 200 to assign a priority to the Event. The lowest value is 0; the highest is 200.

Event General Tab Definitions (continued)

Field/Box	Description
Event Timing	
Activation delay time	The amount of time the system waits to after the Event is initially activated to perform the actions configured in the Event. When event is activated, it would not be active until after the specified period of time. Use the up or down arrows to assign an activation delay for the Event. The maximum value is 99 hours, 59 minutes. If an Event is configured for a Delayed Activation Time, and the Event is activated by an other cause (such as a Manual Action), a new cause (**Delayed Activation**) is added to the Cause list to explain that the Event is not active because of the Activation Delay Time. this cause stays in the Cause list until the delay time is up. When the delay is over, the Event is activated and the **Delayed Activation** cause is removed from the Cause list. If the Event cause does not remain active for the entire delay time, the Event does not activate. **Example:** If an Input state change that activates an Event lasts two minutes, but the Event's Activation Delay time is set to 10:00, the Event never activates.
Min Activation Time	Once the event is active, it remains active for at least the specified period of time. Use the up or down arrows to assign a minimum activation time for the Event. The maximum value is 99 hours, 59 minutes. If an Event is configured for a Minimum Activation Time, and all other Event causes are resolved before the Min Activation Time has elapsed, the Event stays active for the Min Activation Time, and the Cause list displays **Minimum Activation** as the highest priority in the Cause list.
Scheduling	
Activate on Schedule	Click ... to select a Schedule on which the Event will activate. Schedules can be created in the Configuration Pane. See Schedule Editor on Page 473 for more information.
Arm on Schedule	Click ... to select a Schedule on which the Event will be armed.
in Time Zone	Click ... to select a Time Zone for the Event Schedule. The Event can be activated based on the C•CURE 9000 server (host) Time Zone (the default value), the Time Zone of the controller to which the Event is downloaded (**Download to compatible controller**, or a different Time Zone. If you select a Time Zone manually, but then on the Options tab select a controller in a different Time Zone for **Download to compatible controller**, the Time Zone field value is adjusted to be the Time Zone of the controller. The field then becomes read-only, and cannot be changed.
Map Link	
Map	Click ... to select a Map so you can link a map to the Event. Maps are created in the Data Views Pane.

Event General Tab Definitions (continued)

Field/Box	Description
Controller	
Download to compatible controller	Events that are downloaded to an iSTAR controller operate despite a communication failure with the C•CURE 9000. Click ... to select an iSTAR controller to which to download the Event. If you choose to download an Event to an iSTAR Controller, that Event cannot be activated by a trigger defined in an apC object. If you download an event to an iSTAR in a cluster, the event will continue to function even if communication is lost to the host. This includes sensing inputs, activating outputs, activating other events, and performing any door operations throughout the cluster. Activity during the communication fail is buffered and uploaded to the host when communication is re-established. If the event is not downloaded to an iSTAR, the event is host based, and may not fully function if communication is lost to the host. After you select a Controller to which to download the Event, and save the Event, you cannot edit this field again to change the Controller. If you want to discontinue downloading this Event to the Controller, you must delete the Event. If you want to download this Event to another Controller, you need to create a new Event with the same options defined. You can export this Event, then import it with a new name if you need to replace the Event or add additional copies of the Event. You may need to edit the exported XML file to modify the Event so that you can re-import it. For example, you cannot import an Event that has the same name or Object ID (GUID) as an existing Event. If you select this option, the Time Zone field on the General tab of this Event is set to the Time Zone of the iSTAR controller, and cannot be changed.
Dialup (only visible if the controller selected is associated with a cluster that supports dialup)	
Never	if selected, the Controller will not dial the host and not report event changes.
Activation Only	If selected, the controller will only dial the host and report event activation only.
Activation and Deactivation	If selected, the controller will dial the host and report event changes on activation and deactivation.

Event Schedules

An Event can be activated or deactivated, armed or disarmed through the use of Schedules or via another Event.

Example:

An Event can be configured to be activated when a Schedule becomes active (using **Activate on Schedule**). The Schedule is active from 17:00 – 06:00. When the Schedule becomes active at 17:00 (5:00 PM), the Event is activated. When the Schedule becomes inactive the following morning at 06:00, the Event is deactivated, causing the Event to return to the inactive state.

Time Zones for Events

An Event can be associated with a specific Time Zone by configuring the **in Time Zone** field on the Event General tab. See Events and Time Zones on Page 253 for more information.

Event Acknowledgement Tab

The Event Acknowledgement tab allows you to configure the way an Event is reported in C•CURE 9000:

- Including an event in the Journal
- Displaying an event on the Monitoring Station

- Acknowledging an event
- Dual Phase Acknowledgement, which includes Acknowledgment and also Clearing of the event

The Event Acknowledgement tab includes the fields defined in Table 67 on Page 288.

As of v2.70SP1, you can configure Events to remain Active in the Event Viewer of the Monitoring Station after you disarm them. You can configure Events to remain Active after you disarm them by setting **Keep Disarmed Event Active** to **True** in the **Event Handling** section of system variables. This Active status means that Actions of an Event are still in effect and other objects, which depend on the Event, keep their states until you render the Event Inactive. This variable controls the behavior of Events in the Monitoring Station.

A potential use case of this feature occurs when there is building that has a door with an output of an alarm. This door is opened and the alarm triggers. The guard wants the alarm to stop, but wants to investigate the incident in further detail at a later time.

If you select the **This event requires acknowledgement check box** on the **Acknowledgement** tab of the Event editor and this system variable is set to **True**, you can disarm the event and it remains in the event viewer until you or the Monitor formally acknowledges the Event. If you do not select the acknowledgement check box and you disarm the Event, the Event leaves the Event Viewer. Table 66 on Page 286 provides the behaviors of Panel Events and Host Events during the different configurations.

Table 66: Behaviors of disarming Panel and Host Events

Configuration	State	Panel Event Behavior	Host Event Behavior
System Variable = False			
• Event configured to require Acknowledgement • Acknowledge not allowed while Event is active • Activate Event	Armed	• Active • Displays in the Event Viewer • Associated Actions in effect	• Active • Displays in the Event Viewer • Associated Actions in effect
	Disarmed	• Active • **Not** displayed in the Event Viewer • Associated Actions in effect	• Inactive • Not displayed in the Event Viewer • Associated Actions **not** in effect
• Event configured to require Acknowledgement • Acknowledge is allowed while Event is active • Activate Event • Acknowledge Event (Causes still Active)	Armed	• Active • Displays in the Event Viewer	• Active • Displays in the Event Viewer
	Disarmed	• Inactive • Not displayed in the Event Viewer • Associated Actions **not** in effect	• Inactive • Associated Actions **not** in effect
	Armed again or Disarm cancelled	• Active • Displays in the Event Viewer • Associated Actions in effect NOTE: This re-triggers momentary actions again as if the Event is going Active	• Active • Displays in the Event Viewer • Associated Actions in effect
Event not configured to require Acknowledgement	Armed	• Active • Displays in the Event Viewer	• Active • Displays in the Event Viewer
	Disarmed	• Inactive • **Not** displayed in the Event Viewer • Associated Actions **not** in effect	• Inactive • **Not** displayed in the Event Viewer • Associated Actions **not** in effect
System Variable = True			
• Event configured to require Acknowledgement • Acknowledge not allowed while Event is active • Activate Event	Armed	• Active • Displays in the Event Viewer • Associated Actions in effect	• Active • Displays in the Event Viewer • Associated Actions in effect
	Disarmed	• Active • Displays in the Event Viewer • Associated Actions in effect	• Active • Displays in the Event Viewer • Associated Actions in effect

Configuration	State	Panel Event Behavior	Host Event Behavior
• Event configured to require Acknowledgement • Acknowledge is allowed while Event is active • Activate Event • Acknowledge Event (Causes still Active)	Armed	• Active • Displays in the Event Viewer • Associated Actions in effect	• Active • Displays in the Event Viewer • Associated Actions in effect
	Disarmed	• Inactive • **Not** displayed in the Event Viewer • Associated Actions **not** in effect	• Inactive • **Not** displayed in the Event Viewer • Associated Actions **not** in effect
Event not configured to require Acknowledgement	Armed	• Active • Displays in the Event Viewer • Associated Actions in effect	• Active • Displays in the Event Viewer • Associated Actions in effect
	Disarmed	• Inactive • **Not** displayed in the Event Viewer • Associated Actions **not** in effect	• Inactive • **Not** displayed in the Event Viewer • Associated Actions **not** in effect
NOTE: The icon color for C•CURE 800 Active Disarmed Events in the Event Viewer is gray (disarmed state). For C•CURE 9000, it is the Current Active/Requires Acknowledgement/Requres Clear/Acknowledgement-Overdue/Clear-Overdue color.			

Figure 93 on Page 288 shows the Event **Acknowledgement** tab.

Figure 93: Event Acknowledgement Tab

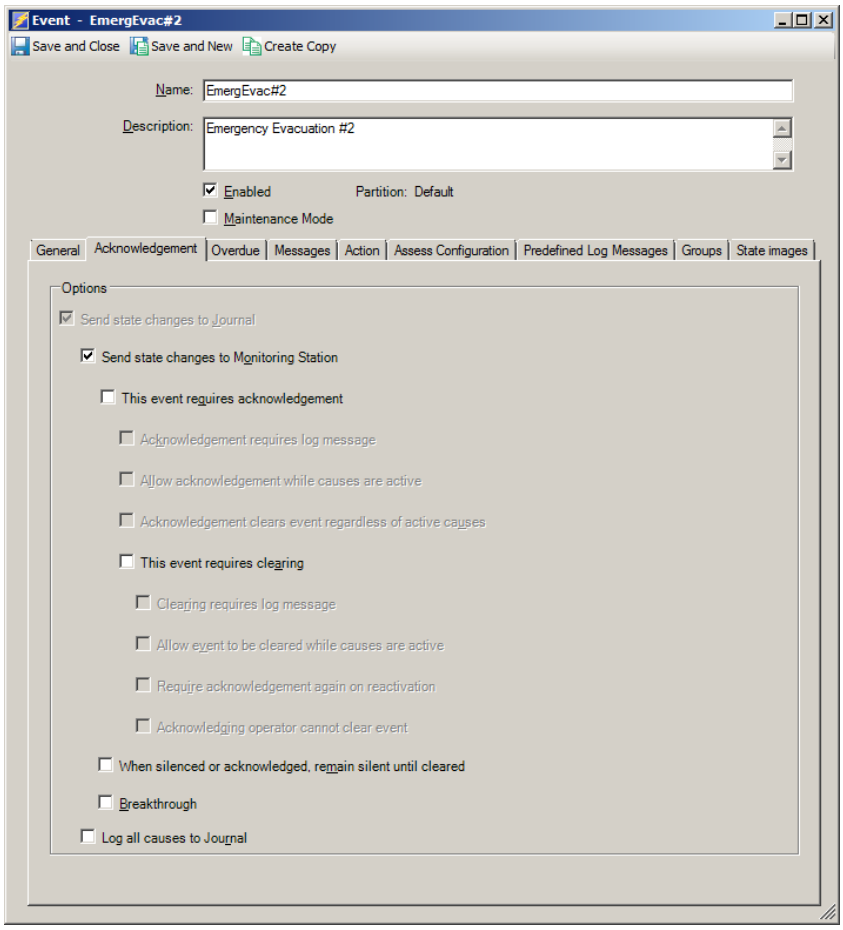


Table 67: Event Acknowledgement Tab Field Definitions

Field/Box	Description
Send state changes to Journal	Select this check box to send a Message to the Activity Journal when this Event is Activated.
Send state changes to Monitoring Station	Select this check box to send activity to the Monitoring Station. This option must be selected for Events that are configured for Event Assessment, otherwise the Event will not be available for assessment in the Monitoring Station. When you select this option, **Send state changes to Journal** is also selected, because an Event sent to the Monitoring Station must be also sent to the Journal.
This event requires acknowledgement	Select this check box to require acknowledgement for the Event, clearing the event following acknowledgement by personnel. Selecting this check box prevents this Event from deactivating until operator has acknowledged it. Normally, an Event deactivates when there are no causes activating it. When you select this option, **Send state changes to Journal** and **Send state changes to Monitoring Station** are also selected because an Event that requires Acknowledgement must be sent to the Monitoring Station and a message must be sent to the Activity Journal. Selecting this check box does not allow acknowledgment if the cause is active. If you attempt to acknowledge the event while the cause is active, all acknowledgement buttons will be disabled. Often configured with "If Event is unacknowledged for longer than the following duration" in the Overdue tab. This selection allows you to activate a secondary event (such as a paging action or additional alarm) if personnel does not respond within a specific time frame. See Event Overdue Tab on Page 289 NOTE: For Proprietary Alarm applications, the Acknowledgement feature must be selected.

Event Acknowledgement Tab Field Definitions (continued)

Field/Box	Description
Acknowledgement requires log message	Select this check box to require that a log message be entered by personnel responding to the event when the Event is acknowledged.
Allow acknowledgement while causes are active	Select this check box to enable personnel to acknowledge an event before all the objects that caused it have reset. Normally, an event cannot be acknowledged until all objects activating the event have reset. Selection is allowed only if the “This event requires acknowledgement” is checked, otherwise the option is unavailable.
Acknowledgement clears event regardless of active causes	Select this check box to clear the Event from the active list on the Monitoring Station as soon as personnel have acknowledge it, even if causing objects are still active. If you do not select this check box, the event does not clear until it deactivates. Selection is allowed only if the “Allow acknowledgement while causes are active” is checked, otherwise the option is unavailable. NOTE: This option is not available if the "This event requires clearing" option is selected.
This event requires clearing	Selecting this option requires the event to be cleared.
Clearing requires log message	Selecting this option requires a log message before the event can be cleared, if the event is configured to require a log message.
Allow event to be cleared while causes are active	Selecting this option allows the event to be cleared even though causes may still be active.
Require acknowledgement again on reactivation	Selecting this options requires acknowledgement if a new event cause is activated. **Example:** If an event is configured to require clearing and has been activated and acknowledged, the event may or may not have still have active causes. If a new cause is activated (added to the event's cause list), then the new cause will require acknowledgement.
Acknowledging operator cannot clear event	Selecting this option overrides permissions assigned to the operator who acknowledges the event, and does not allow the operator who acknowledges the event to clear the event.
When silenced or acknowledged, remain silent until cleared	Selecting this option prevents the sound from restarting if a new cause is activated. Once an event is silenced, it remains silent until it is returned to the Armed (inactive) state, then it will sound again if it is activated.
Breakthrough	Select this check box to allow the Event to function with the breakthrough feature of the monitoring station and mark an event as important. This indicator can be used for high priority events, to mark them for immediate user-intervention.
Log Subsequent Causes to Journal	Selecting this option logs all event causes to the journal database.This includes subsequent causes and logs causes for disarmed Events to the Journal. This feature is intended for limited use. NOTE: This setting can impact system performance if you use it for a large number of Events.

Event Overdue Tab

The Event editor Overdue tab is used to set a duration to activate a second event if acknowledgement of an event, or clearing an event, does not take place within a time frame. The time frame starts when the event is activated. The Overdue tab is shown in Figure 94 on Page 290.

Figure 94: Event Overdue Tab

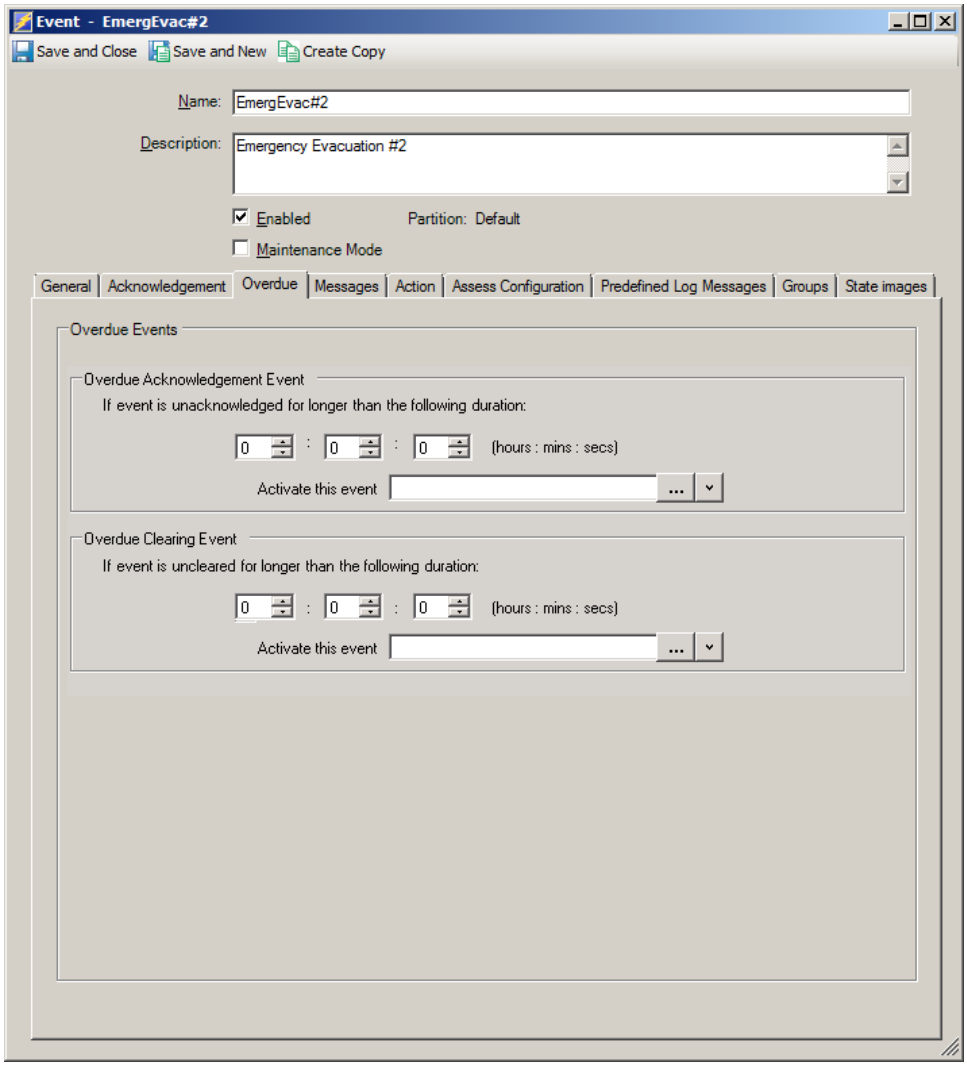


Table 68: Event Overdue Tab Field Definitions

Overdue Events	Description
Overdue Acknowledgement Events	
If Event is unacknowledged for longer than the following duration	Use the up or down arrows to assign an unacknowledged duration for the Event, specifying the time when security personnel must acknowledge the event. Selection is allowed only if the "This event requires acknowledgement" is selected in the Acknowledgement tab, otherwise the option is unavailable. The default is 0. The maximum value is 99 hours, 59 minutes, 59 seconds.
Activate this Event	Click ... to select another Event to activate if the current Event remains unacknowledged for more than the time that you have specified. This secondary event is activated if security personnel have not acknowledge the current Event within the period of time specified in the "If event is unacknowledged for longer than the following duration" field. Selection is allowed only if the "This event requires acknowledgement" is selected, otherwise the option is unavailable.

Event Overdue Tab Field Definitions (continued)

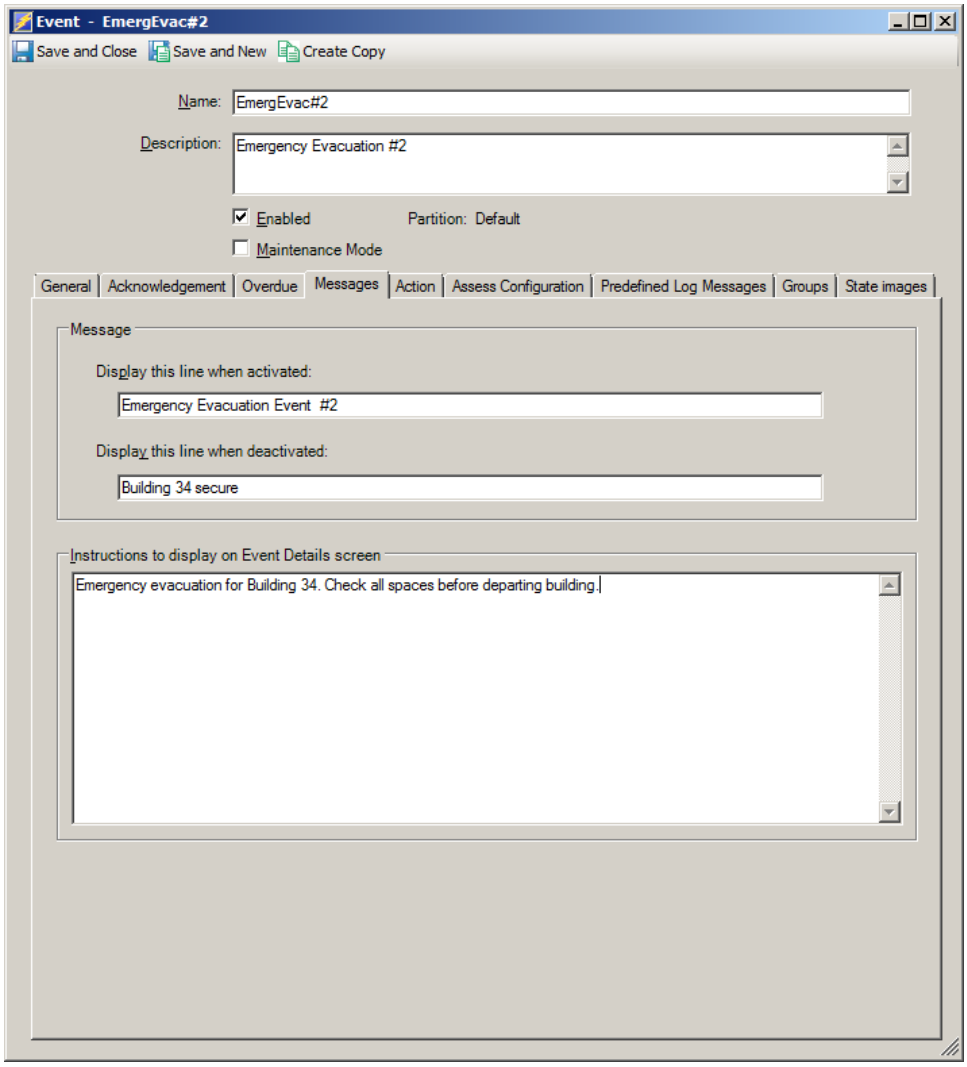
Overdue Events	Description
Overdue Clearing Event	
If Event is uncleared for longer than the following duration	Use the up or down arrows to assign an clearing duration for the Event, specifying the time when security personnel must clear the event. The overdue clear timer starts when the Event is acknowledged. Selection is allowed only if the "This event requires clearing" is selected on the Acknowledgement tab, otherwise the option is unavailable. NOTE: For Panel Events, there is only one timer which starts when the Event is activated. The Event must be acknowledged and cleared (if clear is required) before the time expires, or the Event will become overdue. Default: 0 Maximum value: 99 hours, 59 minutes, 59 seconds.
Activate this Event	Click ... to select another Event to activate if the current Event remains uncleared for more than the time that you have specified. This secondary event is activated if security personnel have not cleared the current Event within the period of time specified in the "If event is not cleared for longer than the following duration" field. Selection is allowed only if the "This event requires clearing " is selected on the Acknowledgement tab, otherwise the option is unavailable.

Event Messages Tab

The Event messages tab allows you to define the messages that are displayed on the Monitoring Station when an Event is Activated or Deactivated, and the instructions for the Event that are displayed on the Event Details dialog box.

The Event Messages tab is shown in Figure 95 on Page 292.

Figure 95: Event Editor Messages Tab



Event message configuration includes the fields defined in Table 69 on Page 292 on the Messages tab.

Table 69: Event Messages Tab Definitions

Field	Description
Display this line when activated	Enter a description, of up to 50 characters, to display when the Event is activated.
Display this line when deactivated	Enter a description, of up to 50 characters, to display when the Event is deactivated.

Event Messages Tab Definitions (continued)

Field	Description
Instructions to display on Event Details screen	Enter a description, of up to 500 characters, to identify the Event Activation. In addition to regular text, you can enter a: • Website address • UNC address • Local file path. These appear as blue underscored hyperlinks in the Monitoring Station, and if they point to a valid location, a Monitoring Station Operator can click the link and open a webpage, a file location, or a specified file. If the link contains any blank spaces, enclose the link in angle brackets ('<' and '>' as in the examples below). **Examples:** www.swhouse.com \\servername\Tyco\CrossFire file:///c:\Windows\notepad.exe <file:///c:\Program Files (x86)\Tyco\CCURE Client\Help\MainHelp.chm>

Event Action Tab

The Event Action tab, shown in Figure 96 on Page 294 includes the fields defined in Table 70 on Page 294on the Action tab.

Figure 96: Event Action Tab

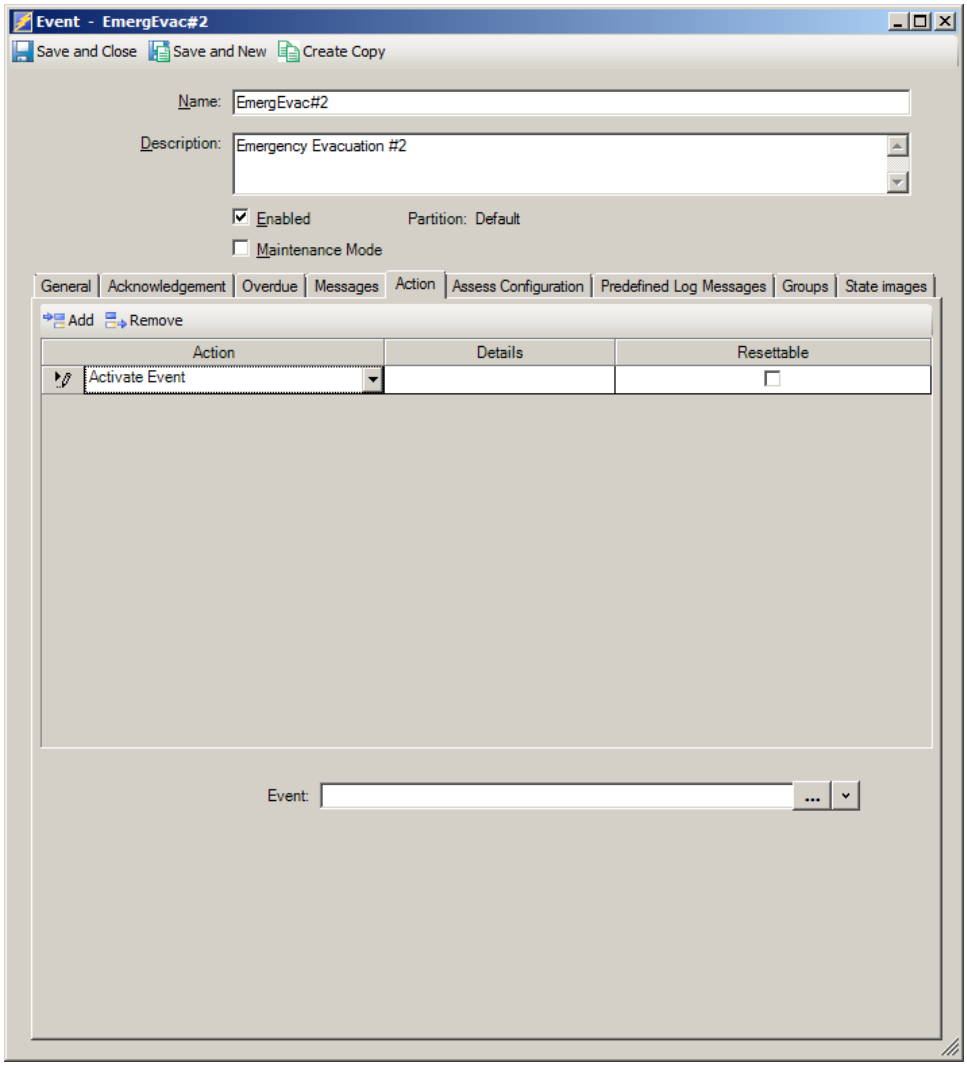


Table 70: Event Action Tab Definitions

Field/Button	Description
	Adds a row for event action configuration.
	Removes the selected event action configuration row.
Action	Add or Remove system-defined Actions using the drop-down list. Click in the **Action** column to display a drop-down list of valid actions. Click an **Action** you want to include as a parameter to add it to the column. As you select an **Action**, a corresponding entry field or group of entry fields, appears at the bottom of the dialog box. Event Actions on Page 241 provides descriptions of the available Event Actions. Click ... to select or type entries in these fields. NOTE: If you want to display a Recorded Video Viewer for Event Assessment, you need to add a **record camera** action for the appropriate camera. See Configure an Event to Display Recorded Video on Page 304 for more information.

Table 70: Event Action Tab Definitions (continued)

Field/Button	Description
Details	This read-only field displays Action details. Depending upon the Action selected, the lower portion of the screen displays the fields needed to specify the details of the Action. Details can include fields such as an Object type and specific object, configuration for a Video action, or an email address to deliver a notification of the Event.
Resettable	Select this check box to indicate that an operator responding to the Event can reset an Action **without acknowledging the Event**. This allows Monitoring Station personnel to manually reset the action caused by the event. Used to turn off output, such as a siren, activated by the event. Reset actions do not require event acknowledgement.

Event Assess Configuration Tab

Event Assess Configuration lets you define the elements that are available to an Operator who initiates the Assessment of an Event in the Monitoring Station. See Adding an Assess Event Object on Page 274 for detailed instructions.

The Event Assess Configuration tab, shown in (see Figure 97 on Page 295, includes the fields defined in Table 71 on Page 296

Figure 97: Event Assess Configuration Tab

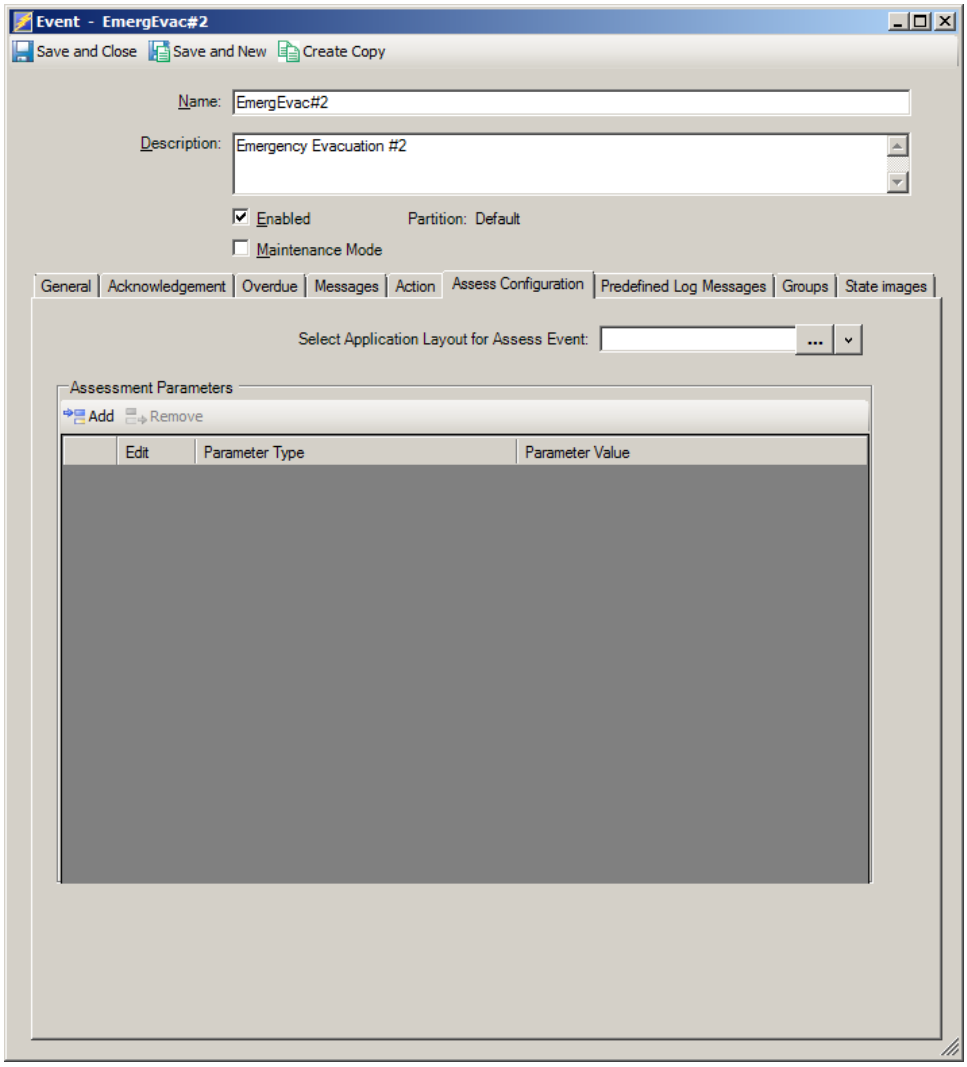


Table 71: Event Assess Configuration Tab Definitions

Field /Button	Description
	Adds a row for event access configuration.
	Removes the selected event access configuration row.
Select Application Layout for Assess Event	Click ... to select an Assess Event Application Layout to use when assessing this Event.
Add	Click add to add a an object to use when assessing an event. A selection dialog box opens to allow you to choose the type of object you want to add, and the specific object of that type. See Adding an Assess Event Object on Page 274.
Remove	Select a row in the Assessment Parameters table and Click **Remove** to remove that row. The row you selected is removed from the table and when you **Save and Close** the object the removal becomes permanent.
Parameter Type	This field displays the type of object you have added to the Event assessment.
Parameter Value	This field displays the object you have added to the Event assessment. **Example**: If you selected **Document** as the Parameter Type, the value shows the Documents that you chose. The following objects can be added to an Event for assessment: • Document - You can add a Document object that you imported into C•CURE 9000. See Document Overview on Page 229. • Query - You can add a Query object (typically related to the object involved in the Event). • Report - You can add a Report object (typically related to the object involved in the Event). • Video View - You can add a Video View object that presents live video (typically of the area where the Event occurred).

Event Predefined Log Messages Tab

The Event Predefined Messages tab allows you to assign Predefined Log Messages and Predefined Log Message Groups to an Event.

The Predefined Log Messages you assign to the Event become available to a Monitoring Station Operator who performs the Log Message action on an Event. See Assigning Predefined Log Messages to Events on Page 413.

The Event Predefined Messages Tab, shown in Figure 98 on Page 297, are described in Table 72 on Page 297.

Figure 98: Event Predefined Log Messages Tab

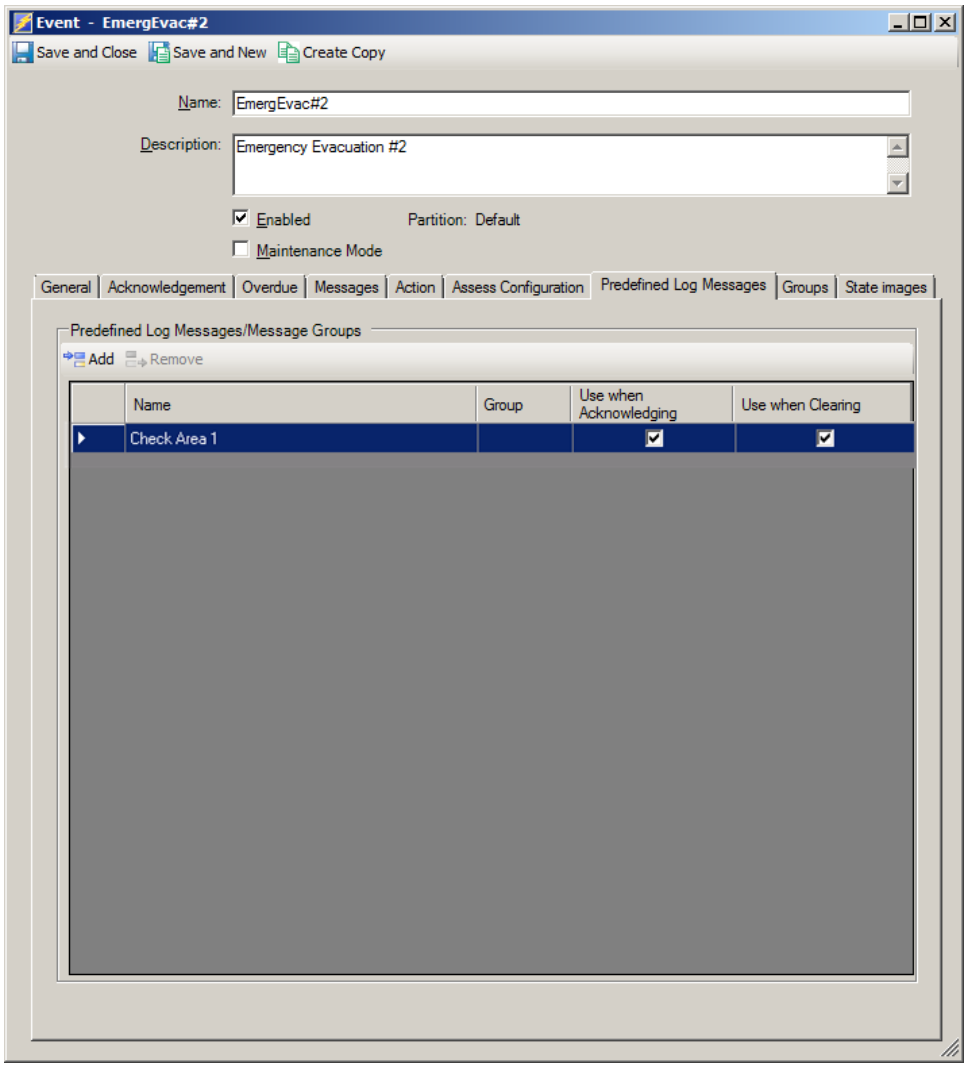


Table 72: Event Predefined Log Messages Tab Definitions

Field/Buttons	Description
	Opens the Name Selection dialog box for selection of Predefined Log Messages or message Groups to assign to the event.
	Removes the selected Predefined Log Message, or Predefined Log Message Group, from the event.
Name	The names of the Predefined Log Messages or Groups assigned to this event.

Table 72: Event Predefined Log Messages Tab Definitions (continued)

Field/Buttons	Description
Group	Displays Group if the Predefined Log Message is a Group of log messages.
Use when Acknowledging[1]	If selected (checked), then the predefined log message is assigned when the event requires acknowledgement.
Use when Clearing[1]	If selected (checked), then the predefined log message is assigned when the event requires clearing.
[1]**Use when Acknowledging** and **Use when Clearing** can both be selected requiring a log message for Acknowledgment and then for Clearing.	

Event State Images Tab

The Event editor State Images tab includes the icons described in on Page 298.

The Event State Images tab is shown in Figure 99 on Page 298.

Figure 99: Event State Images Tab

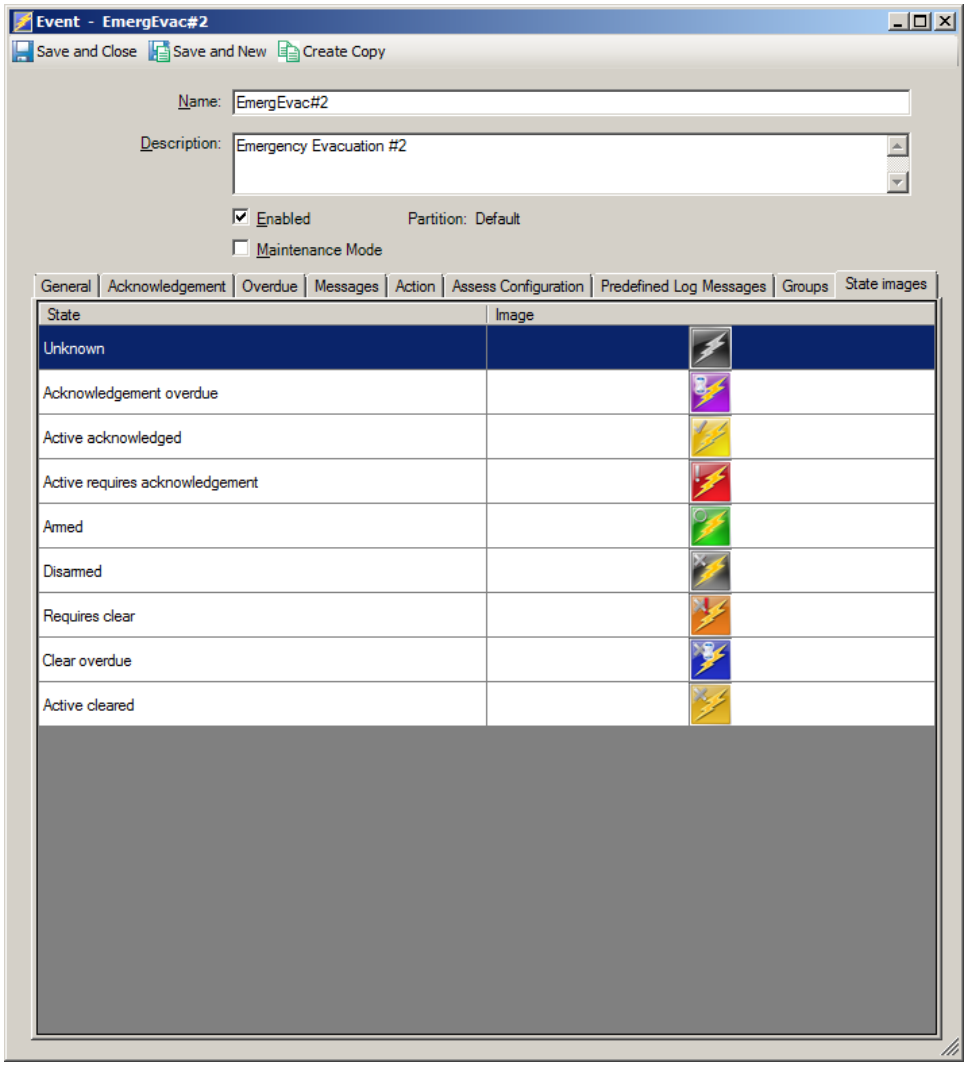


Table 73: Event -State Images Tab Default Images

Name	Description
	Unknown
	Acknowledgement overdue
	Active acknowledged
	Active requires acknowledgement
	Armed
	Disarmed
	Active requires clear
	Clear overdue
	Active cleared

Event Tasks

You can perform the following tasks with Event objects.

Accessing the Event Editor

You access the Event Editor from the C•CURE 9000 Configuration pane.

To Access the Event Editor

1. Click on the **Configure** pane button.
2. Click on the Configure drop-down list and select **Event**.
3. Click  to open a Dynamic View showing all Event objects.
4. Double-click on the Event in the list that you want to edit, and the Event Editor opens.

Creating an Event

You can create Events that perform simple functions, like unlocking a door, or a complex functions, like arming, disarming, and monitoring an area. You can link an event directly to a single action, or you can link it to multiple events and actions.

To Create an Event

1. In the Navigation Pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Event** from the Configuration pane drop-down list.
3. Click **New** to create a new Event. The Event Editor opens, and you can configure the Event.
4. To save your new Event, click **Save and Close**.

   Alternatively, if you want to save the Event and then create a new one, click **Save and New**.

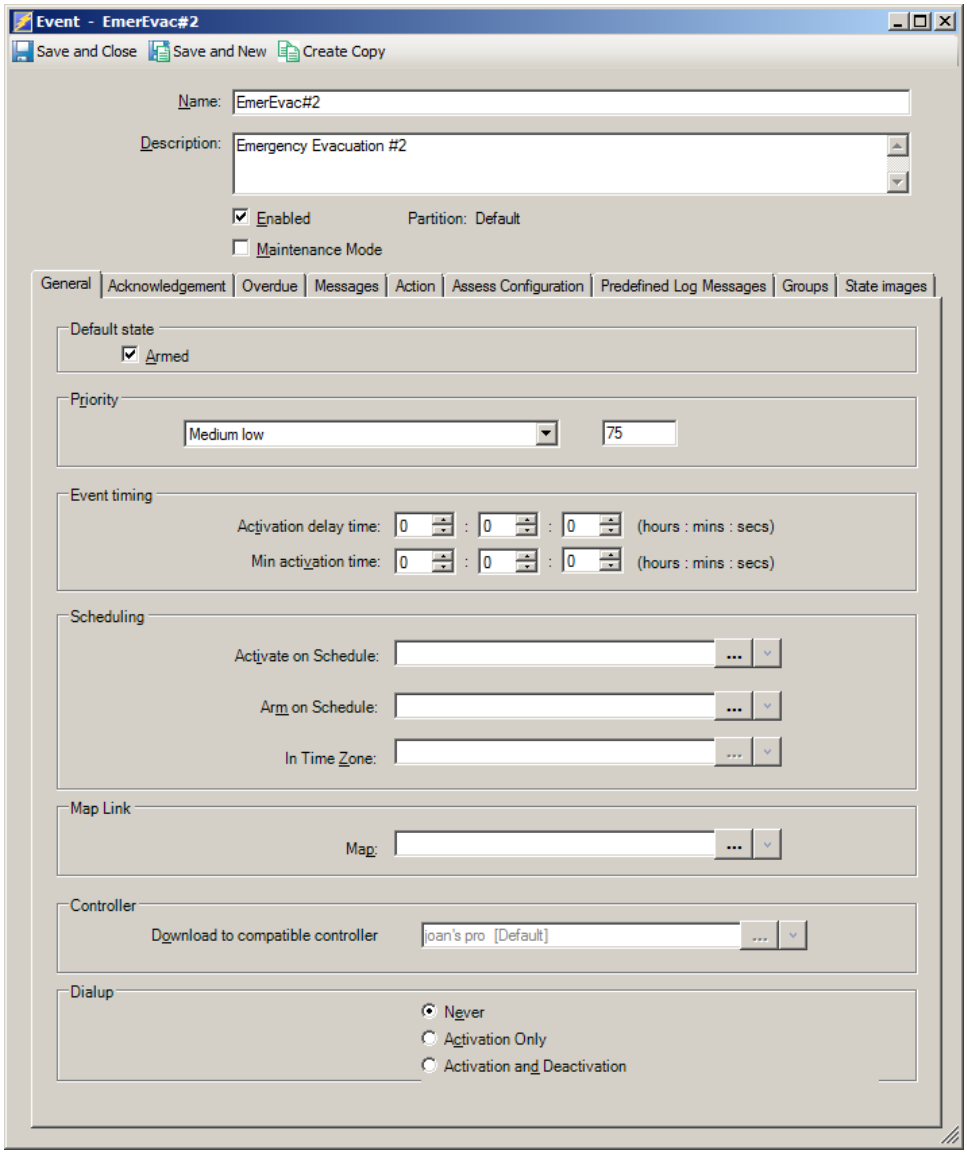
   The current Event is saved and closed, but the Event Editor remains open to allow you to create a new Event.

Configuring an Event

You can configure most C•CURE 9000 objects to cause events. Use the event features, on various C•CURE 9000 dialog boxes, to specify the event cause.

Figure 100 on Page 301 shows the Event Configuration General tab.

Figure 100: Event Configuration General Tab



To configure an Event, you open the Event Editor and adjust the settings for the event based on what you want the Event to accomplish, and how you want the Event to behave.

To Configure an Event

1. Click **Configuration** to open the Configuration pane.
2. Select **Event** from the Configuration Pane drop-down list.
3. Click **New** on the **Configuration** Pane. The **Event** editor opens (see Event General Tab on Page 281).
4. Type in a name for this **Event** in the **Name** field.
5. Type in a **Description** for this Event in the Description field.
6. Click **Enabled** to make the Event available to C•CURE 9000 operators.
7. On the Event **General** tab, choose the General settings that you want for the Event. See Event General Tab Definitions on Page 282 for more information.

8. On the Event **Acknowledgement** tab and the **Overdue** tab (used for Dual Phase Acknowledgement configuration), choose the settings that you want to use for the Event. See Event Acknowledgement Tab on Page 284 and Event Overdue Tab on Page 289 for more information.
9. On the Event **Overdue** tab, set a duration to activate a second event if acknowledgement of an event, or clearing an event, does not take place within a time frame. See Event Overdue Tab on Page 289
10. On the Event **Messages** tab, choose the Messages settings that you want to use for the Event. See Event Messages Tab on Page 291 and Event Messages Tab Definitions on Page 292 for more information.
11. On the Event **Action** tab, choose the Action settings that you want to use for the Event. See Event Action Tab on Page 293 and Event Actions on Page 241 for more information.
12. On the Event **Assess Configuration** tab, select the objects that you want to make available to an Operator who initiates an Event Assessment from the Monitoring Station. See Event Assess Configuration Tab on Page 295 for definitions of the fields.

NOTE When you create a host event with an action type of **Display Message**, a second activation of the event will not display a new message.

13. On the Event **Predefined Log Messages** tab, click  to open the Name Selection dialog box, and select the messages that you want to use for the event. See Event Predefined Log Messages Tab on Page 297.
14. On the Event **State Images** tab, choose the State Images settings that you want to use for the Event. See Event State Images Tab on Page 298, and Table 73 on Page 299 for more information.
15. Click **Save and Close** to save the Event.

Viewing a List of Events

You can display a list of Events by opening a Dynamic View of Events. See Viewing a List of an Object Type on Page 22 for more information.

Event List Context Menu

The context menu that opens when you right-click an Event in the Event Dynamic View includes the selections described in Using the Object List Context Menu on Page 23.

Context menu options specific to Events are described in Table 74 on Page 302.

Table 74: Event List Right-Click Context Menu Options

Menu Selection	Description
Find in Audit Log	This selection displays a Query parameter window with the chosen Event as a parameter for a search in the Audit Log. Click **Run** to perform the query in the Audit Log. The results appear in a Query window.
Find in Journal	This selection displays a Query parameter window with the chosen Event as a parameter for a search in the Journal. Click **Run** to perform the query in the Journal. The results appear in a Query window.
Configuration	
Set property	This selection displays the set property executor where you can change the properties and values of the Event.
Add to group	This selection displays the **Group** window that you can associate the chosen Event with a Group.
Export selection	This selection saves the Event information to either a XML or CSV file. When you click this option, a Windows folder location opens and you can save as the file extension you want, either XML or CSV.

Table 74: Event List Right-Click Context Menu Options (continued)

Menu Selection	Description
Set GIS Location	This selection opens the **Geographic Information System (GIS) Map** window where you can apply a location that corresponds to the chosen Event.
Associate Tag	This selection associates the Event with an existing Tag in the **Tag Manager**. Applying a Tag to the Event categorizes it with metadata in a broad hierarchy that you can view in the Tag Manager from the **Options & Tools** pane.
Assign Predefined Log Message	This selection associates a pre-configured Predefined Log Message with the chosen Event. The Predefined Log Messages you assign to the Event become available to a Monitoring Station Operator who performs the Log Message action on an Event.
Actions	
Activate	Click this menu selection to open a **Manual Action Edit** dialog box with parameters for activating the selected Events.
Deactivate	Click this menu selection to open a **Manual Action Edit** dialog box with parameters for deactivating the selected Events.
Arm	Click this menu selection to open a **Manual Action Edit** dialog box with parameters for arming the selected Events.
Disarm	Click this menu selection to open a **Manual Action Edit** dialog box with parameters for disarming the selected Events.
Latch Event	Click this menu selection to Latch an Event. When you Latch an Event, the Event is activated, and it will stay activated until it is the subject of an Unlatch or Toggle Event action (with an equal or higher priority). The Latch action is added to the Cause list for the Event. If the Event is already Latched, the Latch Event action has no effect. Upon system restart, host and panel Events retain their Latch state. If the Event is disarmed, the Latch Event selection does not appear.
Unlatch Event	Click this menu selection to Unlatch an Event. When you Unlatch an Event, the Event is deactivated if the Event is currently Latched, and it will stay deactivated until it is the subject of a Latch or Toggle Event action (with an equal or higher priority). The Unlatch action is added to the Cause list for the Event. This menu selection only appears if the Event is Latched. Upon system restart, host and panel Events retain their Unlatched state. If the Event is disarmed, the Unlatch Event selection does not appear.
Toggle Event	Click this menu selection to Toggle an Event. The Event you Toggle is Latched if it is currently Unlatched, or Unlatched if it is currently Latched. The Latch action is added to the Cause list for the Event. If the Event is neither Latched or Unlatched, the Toggle Event action has no effect. If the Event is disarmed, the Toggle Event selection does not appear.
Pulse Event	Click this menu selection to Pulse an Event. The Event you Pulse is activated. A Pulse is a momentary activation of an Event. If the minimum activation time is configured in the Event, the value is used as the duration of the Pulse; otherwise the duration of the Pulse will be one second. If the Event is disarmed, the Pulse Event selection does not appear.
Turn Maintenance Mode On	This selection puts the Event into Maintenance Mode and displays the associations that are affected. While it is selected and enabled, activity from that object is not shown in Monitoring Station. It is used when hardware is being added to or being replaced in the system or hardware is being tested. When this mode is enabled, guards are not inundated with “fake” activity from hardware that is being maintained while new objects are being tested that they are configured properly.
View	

Table 74: Event List Right-Click Context Menu Options (continued)

Menu Selection	Description
Details	Click this menu selection to open a **Details** dialog box with detailed information about the Event and buttons that let you acknowledge/clear/silence the selected Event, reset actions triggered by the Event, and/or enter a log message about the Event. You can see Active and Armed Causes from this window.
Monitor	This selection displays a list of objects on the left-hand side starting with the Event being monitored. The activity associated with the listed objects displays on the right-hand side.
Assess Event	This selection appears on the context menu for Events. Click to open the Assess Event Application Layout for the Event.
Associations	This selection displays the objects associated with the Event. Click **Display Dynamic View** to view all types in a Dynamic View with more information.

Modifying an Event

You can modify an Event for use with C•CURE 9000.

To Modify a Event

1. Click **Configuration** to open the Configuration pane.
2. Select **Event** from the Configuration pane drop-down list.
3. Click to view a list of existing Events.
4. Click to select the Event you wish to modify.
5. Right-click on the selected Event and choose **Edit** from the context menu.
6. The Event editor opens, and you can change any of the settings for the Event.
7. To save your modified Event, click **Save and Close**.

Configure an Event to Display Recorded Video

You can configure an Event with an action that records video from a specified camera when the Event is triggered. A Monitoring Station Operator can then view this recorded video from the Event Details dialog box by clicking on Display Recorded Video in the Event Details Toolbar.

If the Event is configured for Assess Event, one or more recorded Video viewers can be included on the Assess Event Application Layout to show the most recent recorded video clips that were recorded as a result of the Event Actions configured on this tab.

To Configure an Event to Display Recorded Video

1. Create an Event (see Creating an Event on Page 300.)
2. Click the Event Action tab.
3. Click **Add**.
4. Select **Video Camera Action** from the Action drop-down list.
5. In the Details section at the bottom of the tab, select the Server and Camera from which you wish to record video.
6. Click the Action Type tab, and select the **Record Camera** action type.

7. Configure the time period in minutes and seconds for Pre Alarm video recording (video recorded prior to the Event activation time).
8. Configure the time period in minutes and seconds for Post Alarm video recording (video recorded after the Event activation time).
9. You can click **Add** again to configure additional Video Camera Actions, if desired.
10. Click **Save and Close** to save the Event.

NOTE If you configure multiple Video Actions for an Event that is configured for Event Assessment, only the four most recent recorded video clips can be displayed. The system collects all the recorded video clips for the server/camera pairs identified in the Video Actions and chooses only the most recent four clips, regardless of server/camera pair. The number of recorded video clips actually displayed in the Monitoring Station for the Event depends upon the number of recorded video viewers configured in the Assess Event Application Layout for the Event.

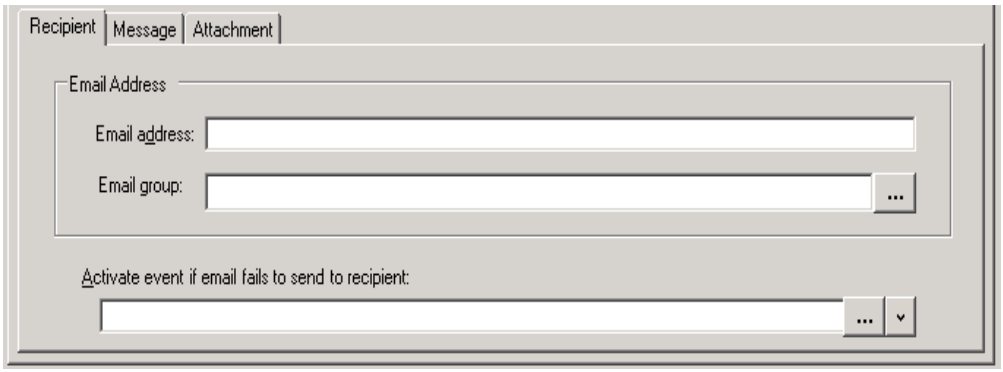
Configuring an Event to Send Email

You can configure an Event with an action that sends Email to individuals or to a Group when the Event is triggered. You can configure Emails to contain custom message text and you can insert various event details, such as the time of Event occurrence, within the text using embedded tags.

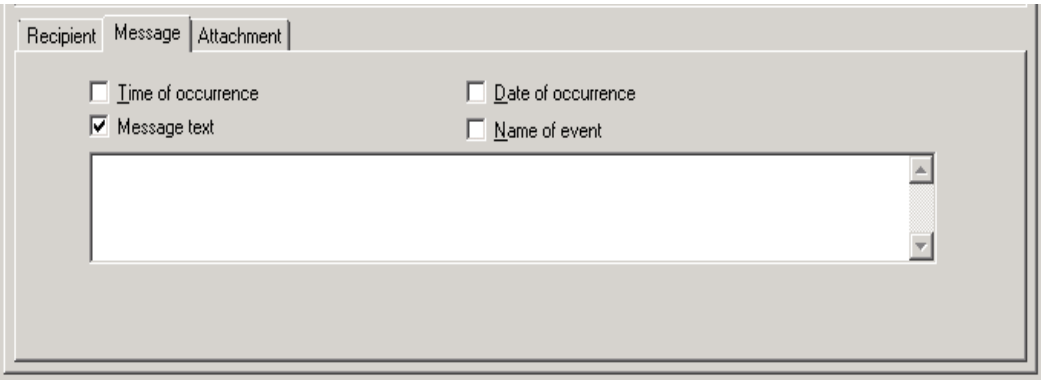
Configuring an Event to Send Email

1. Create an Event (see Creating an Event on Page 300).
2. Click the Event **Action** tab.
3. Click **Add**.
4. Select **Send Email** from the Action drop-down list.
5. In the **Recipient** tab at the bottom of the **Action** tab, enter the email addresses to which you wish to send email.

NOTE If you are including multiple email addresses, you must separate each address by a comma, or a semi-colon.



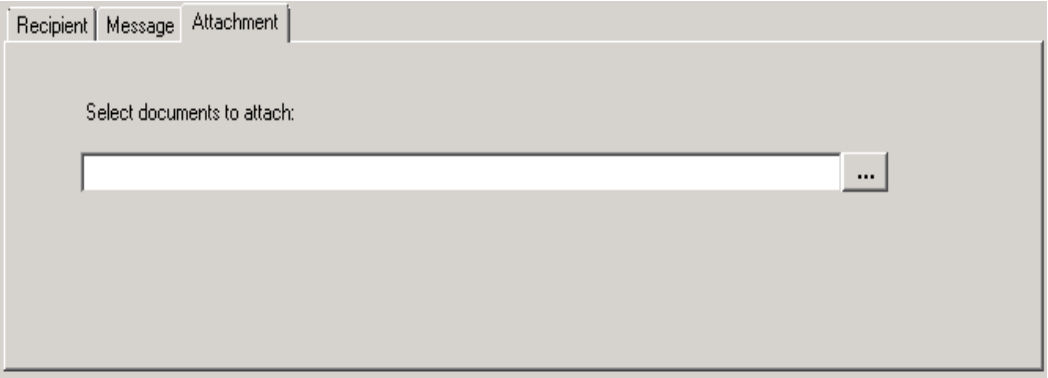
6. You can also select one or more Personnel Groups by clicking ... in the **Email group** field. A selection dialog box opens and you can select Personnel Groups. Personnel in these groups will receive the Event email if their Personnel record contains a valid email address.
7. You can click ... in the Activate event if email fails to send to recipient field to select an Event to activate if any email failures occur.
8. Click the **Message** tab on the Action tab to configure the email message.



a. You can type in a message in the text field on this tab.

b. You can select check boxes to include the **Name of event**, **Time of occurrence** and **Date of occurrence** for the Event, and the Event **Message text**.

9. Click the **Attachment** tab on the Action tab to select documents to attach to the email message.



10. You can click ... in the **Select documents to attach** field to select Document objects to attach to the Event email. A selection dialog box opens and you can select Document objects that you have previously created in C•CURE 9000. Click **OK** to accept the Documents you selected.
11. Click **Save and Close** to save the Event.

Configure an Event Icon on a Map

You can add an icon to a Map that represents an Event. From this icon, you can perform several Event context menu actions such as Activate/Deactivate, show Event Details, and Latch/Unlatch to Event.

You can also configure an Event to display the Map when the Event is activated, so that your Operators can view the map and choose which actions to take.

To Configure an Event Icon on a Map

1. Create or Edit a Map. See the Chapter on Maps in the *C•CURE 9000 Data Views Guide* for more information.
2. Click **Add an Icon** ( ). The Map Icon Properties dialog box opens.
3. Click in the **Type** field to open a Select Type dialog box, and choose **Event**.
4. Click in the **Object** field to open a dialog box that allows you to select an object of the same type as the icon.
5. Choose the Event that you want the icon to represent. The expanded Maps Icon Properties dialog box appears.

6. Under Runtime Options, Click the **Action to run on left-click** drop-down arrow and select an action, such as Latch, Unlatch, Toggle, or Pulse.
7. You can type a tooltip in the **Tooltip to Display on hover** field if you want to display a tooltip message about the icon.
8. If you want the icon to have a context menu enabled for the user to perform additional actions, select **Show context menu on right-click**.
9. Click **Save and Close**. The icon that you have configured appears on your Map.
10. Click and drag the icon into the position that you want it on the Map. Use the selection handles on the icon to resize it if necessary.
11. You can right-click the icon to save it to the Map, or perform any other functions that appear on the context menu.
12. Click **Save and Close** to save the icon changes you made to the Map.

To Configure an Event to Display a Map

1. Create an Event (See Creating an Event on Page 300.
2. Click the Action tab.
3. Click **Add** to add an Action.
4. Select **Display Viewer** from the Action drop-down list.
5. Click in the **Type** field and choose Map from the Select type dialog box.
6. Click in the **Object** field and choose theMap you want to display.
7. Click **Save and Close**. When this Event is activated, the Map you selected appears in the Map View, and you can right-click the Event icon to access the Event context menu.

Event Context

If an Event has context-dependent actions, you can specify the Event Context. Event Context is an additional set of data attached to a Trigger or Special Door Action that pulses an Event. Depending on the Action that is executed by the Event, the data set is either used or ignored. The Activate Event or Pulse Event actions take any existing Event Context and pass it to the Event that they activate. Other actions ignore the context.

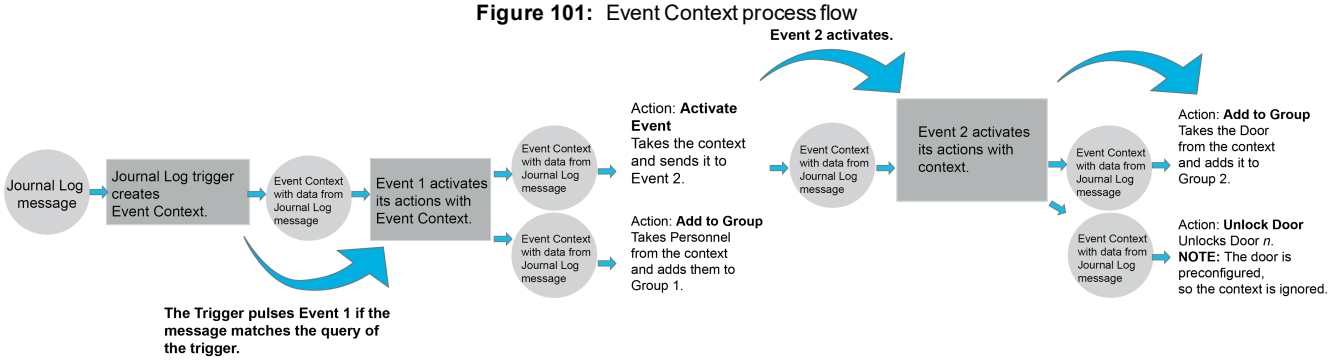
It is optional to specify an Event Context for a Journal Trigger or Audit Log Trigger. However, you must specify an Event Context for a Special Door Action.

The Temporary Clearance Filter and Modify Group Actions do not work properly if an Event Context is not defined for them.

NOTE: Event Context is not available for Panel Events.

Figure 101 shows an example of Event Context transferring between two Events.

Figure 101: Event Context process flow



Enabling Event Context

To add context for an Event, enable the Define Event Context parameter on the Journal Trigger, Audit Trigger, or Special Door Action windows.

For Event Context to work as intended, you need to create two Events. Create one Event to add to the Group and another Event to remove from the Group. You also need two Triggers. Create one Trigger to add to the Group and another Trigger to remove from the group.

1. Create a new Audit Trigger, Journal Trigger, or Special Door Action.
2. Select the **Define Event Context** check box.
3. Click **Save and Close**.
4. Navigate to the **Events** tab and create a new Event.
5. On the **Event** window, select the **Modify Group** action.
6. From the **Group to Modify** field, click the ... browse icon.
7. From the **Name Selection** window, select the Group to modify.
8. Select **Add to Group**.
9. Click **Save and Close**.
10. Repeat Steps 1 to 7. Select the same Group to modify as before.
11. Select **Remove from Group**.

12. In the **Audit Trigger** tab, navigate to the Events that you created.
13. Right-click an Event and click **Edit**. For the Event that you added to the Group, check that the **Value** field contains **Reference Added**. For the Event that you removed from the Group, check that the **Value** field contains **Reference Removed**.

9

Groups

This chapter explains how to create groups for a variety of objects such as Doors, Elevators, Floors, Readers, Inputs, Outputs and Events.

In this chapter

Group Editor Overview

The Group Editor lets you create, and edit, groups made up of same type objects (such as doors). You can configure objects that activate groups, such as inputs activating output groups, or events that specify actions for groups.

Example:

If you want to arm certain inputs for specific times, you can group them together and apply the desired schedule for them once (using an event), rather than setting up schedules for each input separately.

NOTE When you arm or activate a group, you are arming or activating the individual objects listed in the group, not the group itself. A group has no status, but the objects that compose it do.

For more information about Groups, see:

- Group Editor General Tab on Page 312
- Group Editor Tasks on Page 313
- Object Editor Groups Tab on Page 26

Group Rule

Use the Group editor to select a group rule, which sets a criteria to a group of objects. The group rule available for selection is Support Expiring Clearances after you select the **Door** from the **Group Type** drop down menu. Select this rule if you want to create a group of doors and elevators that support expiring clearances per person.

Example:

If you select Support Expiring Clearances as the group rule, then only clearances with the expiring clearances per person option will be available for selection.

Note

- The Support Expiring Clearances rule only supports for iSTAR Ultra doors and elevators.
- You cannot edit a door or elevator group with support expiring clearances if it is assigned to a clearance with expiring clearances per person.

Group Editor General Tab

The Group Editor General tab, shown in Figure 102 on Page 312, lets you create a name and description for a new group, or edit these fields for an existing group. You choose a group type using the browse button. You can add or delete objects from the group using the **Add** or **Remove** buttons.

- Group Editor field definitions are explained in Table 75 on Page 312
- Group Editor Tasks on Page 313

Figure 102: Group Editor

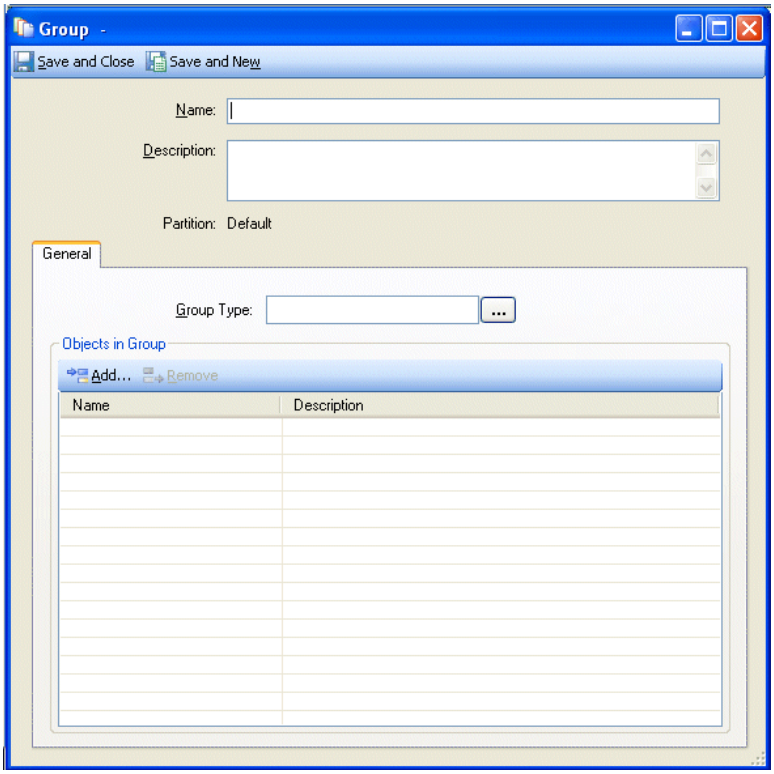


Table 75: Groups Tab Definitions

Field/Button	Description
Name	Enter a unique name, up to 50 characters long, to identify the group.
Description	Enter a description, up to 255 characters, to identify the group.
Partition	A read-only field displaying the name of the Partition to which this group belongs. (This field is visible only if the C•CURE 9000 system is partitioned.)
Group Type	When you click the ... browse button, the Select Type browser appears, allowing you to select a Group Type.
	When you click the Add button, the Object Selection browser appears, allowing you to add objects to the new or existing group. Select an object that you want to add and click the browser's OK button to add the object.
	Select the object that you want to delete and click the Remove button.

Group Editor Tasks

You can perform the following tasks using the Group editor:

- Accessing the Group Editor on Page 313
- Creating Configuration Pane Objects and Templates on Page 21
- Creating a Group Template on Page 314
- Viewing a List of an Object Type on Page 22
- Using the Object List Context Menu on Page 23
- Modifying a Group on Page 315
- Deleting an Object on Page 25
- Setting a Property for an Object on Page 25

Accessing the Group Editor

You access the Group Editor from the C•CURE 9000 Configuration pane.

To Access the Group Editor

1. Click the **Configuration** pane button.
2. Click the Configuration drop-down list and select **Group**.
3. Click **New** to create a new Group.

   - or -

   Click  to open a **Dynamic View** showing all existing Group object, right-click the group you want to change, and click **Edit** from the context menu that appears.

   The Group Editor General Tab on Page 312 opens.

Viewing a List of Groups

You can display a list of Groups by opening a Dynamic View of Groups. See Viewing a List of an Object Type on Page 22 for more information.

Using the Group View Context Menu

The context menu opens when you right-click a Group in the Dynamic View. See Using the Object List Context Menu on Page 23 for information about using the context menu.

NOTE Pre-defined Groups (such as All Doors Group and All Events Group) do not have a right-click context menu.

Creating a Group

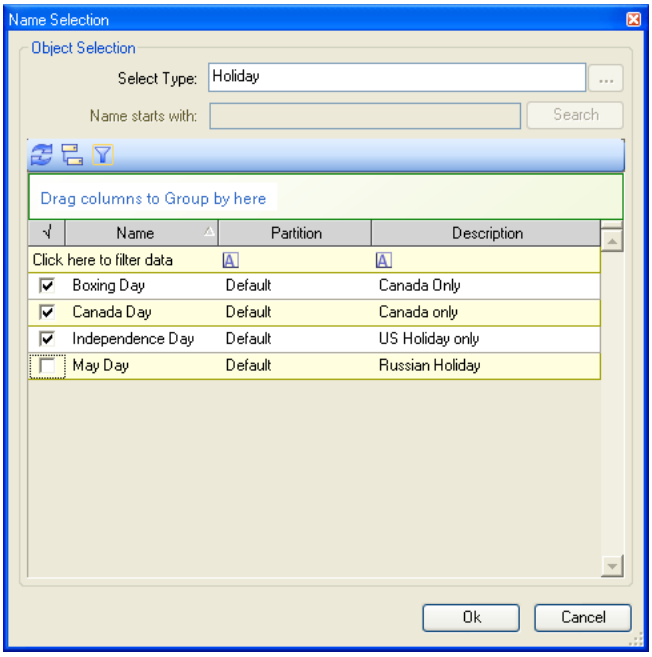
You can create a new Group.

To Create a Group

1. In the Navigation Pane of the Administration Client, click the **Configuration** pane button.
2. Select **Group** from the Configuration pane drop-down list.
3. Click **New** to create a new Group. The Group Editor opens and you can configure the Group.
4. Click ... to open the **Select Type** dialog box.
5. Scroll down and select the object class.

   The object class appears in the Group Type field of the Group Editor.
6. Click **Add** to add security objects to the Group. The Name Selection dialog box showing a list of objects of the same type appears (see Figure 103 on Page 314).

Figure 103: Adding Objects to a Group



7. Select ( ) the objects you wish to add to the Group and click **OK** to add them.
8. To save your new Group, click **Save and Close**.

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

Creating a Group Template

You can create a new template for a Group. A Group template saves you time because you can reuse the same configuration repeatedly.

To Create a Group Template

1. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Group** from the Configuration pane drop-down list.
3. Click the drop-down arrow next to **New** and select **Template**. The Group Template opens.

4. Configure the Group template.
5. To save your new Group Template, click **Save and Close**.

The new Group template appears under Templates in the Template drop down list.

To Select a Group Template

1. In the Navigation Pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Group** from the Configuration pane drop-down list.
3. Click the drop-down arrow next to **New** and select **Template**.
4. Select the template you want to use under Templates.

Modifying a Group

You can change the Name, Description, and Add or Remove objects in the group.

To Modify a Group

1. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Group** from the Configuration pane drop-down list.
3. Click  to open a Dynamic View showing all Group objects.
4. Right-click on the Group in the list that you want to modify and select **Edit** from the context menu.

Configuring a Group Rule to Support Expiring Clearances

Use the Group editor to configure a door or elevator group with the support the expiring clearances rule.

Note

- Group Rule is only available if you select **Door** or **Elevator** as the Group Type in the **General** tab.
- You can only assign the support expiring clearances rule to iSTAR Ultra door groups or iSTAR Ultra elevator groups.

To configure group rule to support expiring clearances group rule

1. In the navigation pane of the Administration Station, select **Configuration**.
2. Click **Group** from the drop-down menu.
3. Click **New**

   OR

   Click  to open a Dynamic View with a list of groups and select the group you want to edit.
4. Type a name for the group.
5. Type a description for the group.
6. Click  in the Group Type field.
7. Select **Door**.

   OR

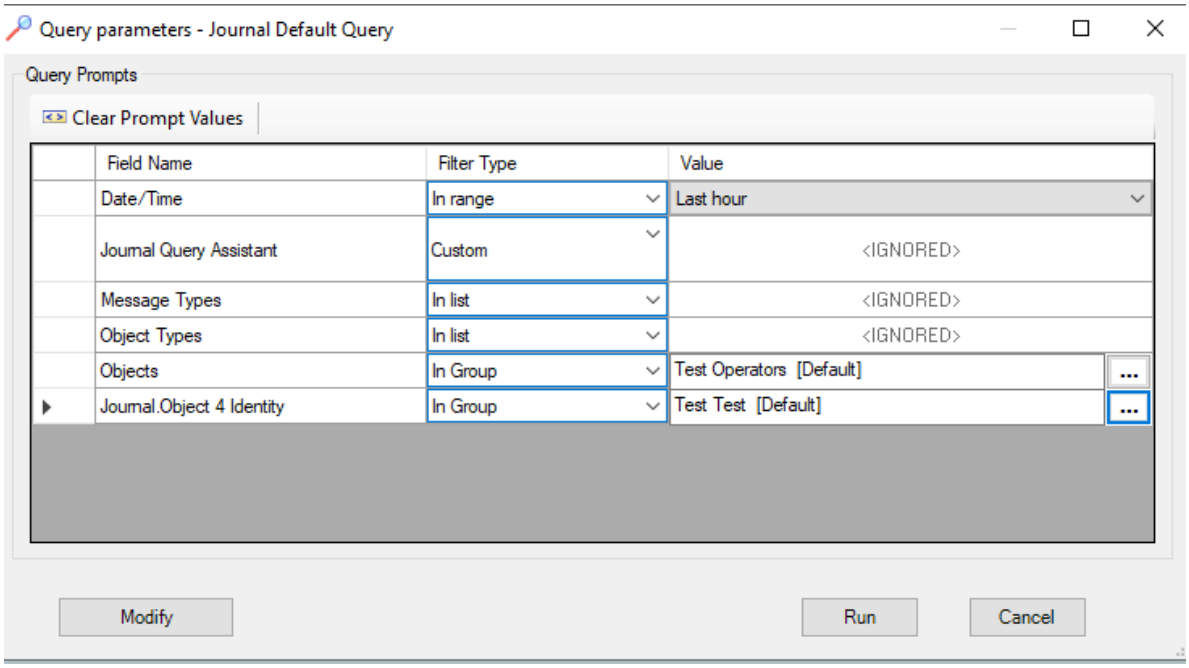
   Select **Elevator**.

8. Click the drop-down menu in the Group Rule field and select **Support Expiring Clearances**.
9. Click **Add** to select the doors you want to add to the group.
10. Click **Save and Close**.

Searching the Journal with the In Group Filter

Using a query with the In Group filter, you can find all the Journal Log or Audit Log records that reference objects from a particular C•CURE 9000 Group. You can use the In Group filter on Object fields in Journal or Audit Log-related queries.

Figure 104: The In Group filter



To search the Journal Log with the In Group filter

1. In the Administration Station, click **Options & Tools** > **Journal**.

Or

   a. Click **Configuration**. From the drop-down menu, select **Group**.
   b. Click the green arrow.
   c. On the **Groups** tab, right-click a Group.
   d. From the context menu, click **Find in Journal...**

2. On the **Query parameters - Journal Default Query** window, in the **Field Name** column, select an object field name.
3. In the **Filter Type** column, click the drop-down menu for the object.
4. Click **In Group**.
5. In the **Value** column, click the three-dot menu.
6. In the **Name Selection** window, click the Group that you want to search.
7. **Optional:** To refine the query, on the **Query parameters - Journal Default Query** window, click **Modify**. For more information, see Configuring a Journal Trigger Advanced Query on Page 348.

8. To run the query, on the **Query parameters - Journal Default Query** window, click **Run**.

The results open in a Dynamic View, which shows all the records where the object in the Object 1 Type column, Object 2 Type column, and so on, reference an Object in the Group.

To search the Audit Log with the In Group filter

1. In the Administration Station, click **Options & Tools** > **Audit Log**.
2. On the **Query parameters - Audit Log for <group name> Group** window, in the **Field Name** column, select an object field name.
3. In the **Filter Type** column, click the drop-down menu for the object.
4. Click **In Group**.
5. In the **Value** column, click the three-dot menu.
6. In the **Name Selection** window, click the Group that you want to search.
7. **Optional:** To refine the query, on the **Query parameters - Audit Log Default Query** window, click **Modify**.
8. To run the query, on the **Query parameters - Audit Log for <group name> Group** window, click **Run**.

The results open in a Dynamic View, which shows all the records where the object in the Object 1 Type column, Object 2 Type column, and so on, reference an Object in the Group.

10

Holidays

This chapter explains how to configure C•CURE 9000 Holidays.

In this chapter

Holiday Overview

A Holiday is an object you configure to specify a day, part of day, or set of days to provide system and access control variations to scheduled events and to the usual lock and unlock times.

You create and configure Holidays using the Holiday editor. See:

- Holiday Editor on Page 321
- Configuring Holidays on Page 326

A Holiday specifies a time period during which an Active Schedule is treated specially. Typically, normally scheduled events and access do not occur on a Holiday.

Example:

You can create a Holiday called New Year's Day, and configure it to occur once per year on the same date.

- You have configured a 'Daily' Schedule as Active every day from 8:00 AM to 5:00 PM.
- You have configured a Holiday called **New Years Day** as the first day of January every year, and included it in a Holiday Group that is downloaded to your controllers.
- You have configured the Schedule to respect the Holiday Group that includes **New Years Day**.
- Consequently, on January 1, the 'Daily' Schedule is treated as Inactive.
- As a result, a Person with a Clearance that uses that Schedule would be unable to gain access on that day.

Holidays can be configured as partial days, can span multiple days, or can recur on various intervals ("every Friday", "Second Monday of every month", "January 1 to January 4"…). The typical holiday is a single 24-hour day.

You can define the following holiday types:

- Non-recurring - a holiday that starts on a particular date and time and ends on a particular date and time (day, month, year, hour, minute).
- Monthly/Yearly - a holiday that occurs once per year or in selected months, either on a specific date or a relative date (the second weekend of July).
- Weekly - a holiday that occurs on a specific day or days (every Thursday).

Guidelines for Configuring Holidays

There is no practical limit to the number of holidays that the C•CURE 9000 supports. There is a maximum of 256 Holidays per Holiday Group (or List).

- Each apC is limited to 256 Holidays across as many as 8 Holiday Lists.
- The holiday lists are selectable per apC. There is no limit to the number of holidays configured; however, the limit is how many holidays you can have in a list (256).
- The other limit is how many lists you can send to a panel (24 for iSTAR or 8 for apC).
- The iSTAR itself does not have a limit on holidays in a list, but the host limits is 256.
- Selective downloading is only available on apC's in the 9000. You can selectively download the apC lists on the 9000, so you can send the first 256 to one apC and the next 256 to the next apC, etc.
- If you attempt to send more than 256 holidays to an apC, in any number of lists, it will accept only the first 256.
- You're limited to 24 holiday lists (groups) on an iSTAR. There is an additional limit of 256 holidays per Holiday list (group). So for practical purposes, you are limited to 24 * 256 = 6144 holidays. You can download all 6144 holidays to all iSTARs.

Holiday Groups and Schedules

You can include a Holiday in a Holiday Group and include a Holiday Group in a Schedule. Holidays are only downloaded to an apC or iSTAR Controller when they are included in a Holiday Group.

If a Schedule includes a Holiday Group in the **When These Holiday Groups Are Active, do not Activate Schedule** grid, the Holidays in the Holiday Group are evaluated by the controllers to which the Holiday Group is downloaded. If one of the Holidays in the Holiday Group is active, the Schedule is treated as Inactive.

You can also create exceptions to Holidays when you define a Schedule by adding a Holiday Group to the **When These Holiday Groups Are Active, Activate Schedule Only During Times Specified Below** grid. You add the Holiday Group to the Schedule and specify the hours during which you want the Schedule to ignore an active Holiday and operate normally.

For more information see:

- Adding Holiday Groups to the Schedule on Page 476.
- Schedule with Overrides on Page 483

apC Controller Holidays

The apC Controller uses Holidays that are in the Holiday Groups you specify on the apC Controller editor Holiday Groups tab. You need to add any Holidays that you want to affect an apC Controller to one of the Holiday Groups defined for that apC Controller. See Schedules and Holidays on the apC Controller on Page 468 for more information.

Holidays in Holiday Groups that are not specified in the apC Controller editor have no effect on Schedules downloaded to an apC. However, **all** Holiday Groups that are downloaded to the apC affect **all** Schedules on the apC. An apC Controller can support a maximum of 256 Holidays.

C•CURE 9000 Server and iSTAR Controller Holidays

Schedules that are used on the server itself (typically for activating server-based Events and functions like Reports) and the iSTAR Controller are only affected by Holiday Groups explicitly added to the Schedule.

Holiday Editor

The Holiday Editor in C•CURE 9000 lets you create a Holiday object, which is a Schedule type for configuring holidays.

The following topics give more information about the Holiday object and how to use it.

- Holiday Overview on Page 319
- Holiday General Tab on Page 321
- Object Editor Groups Tab on Page 26

Holiday Tasks

- Accessing the Holiday Editor on Page 321
- Configuring Holidays on Page 326

Accessing the Holiday Editor

You can access the Holiday Editor from the C•CURE 9000 Configuration pane.

To Access the Holiday Editor

1. Click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Holiday**.
3. Click  to open a Dynamic View showing all Holiday objects.
4. Double-click on the Holiday in the list that you want to edit, and the Holiday Editor opens.

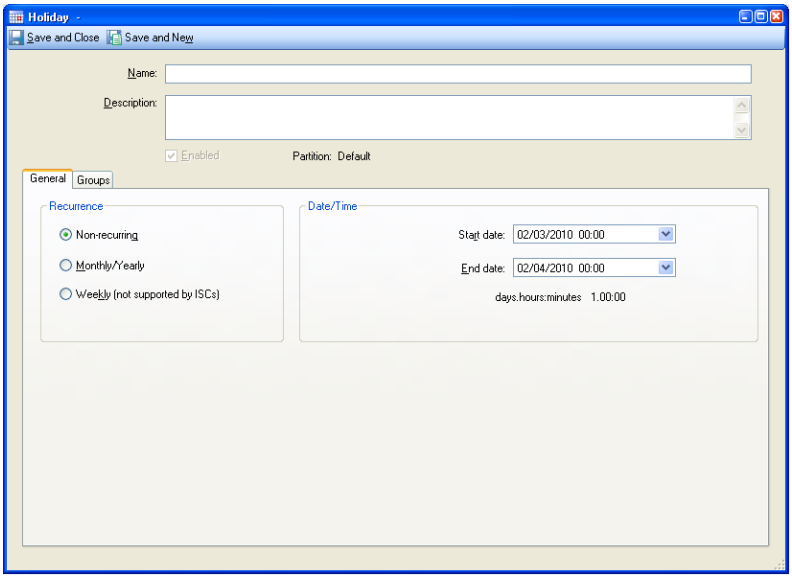
Holiday General Tab

The Holiday General tab lets you configure Recurrence, Date/Time, and Recurrence Pattern settings. Depending upon the choice you make for **Recurrence**, the Holiday General tab displays different options. These options are explained in:

- Non-recurring Holiday on Page 322
- Monthly/Yearly Holiday on Page 323
- Weekly Holiday on Page 324

The Holiday Editor General tab is shown in Figure 105 on Page 322.

Figure 105: Holiday Editor General Tab



The Holiday Editor has the common fields and buttons listed in Table 76 on Page 322.

Table 76: Holiday Editor General Tab Common Fields

Field	Description
Name	Enter a unique name, up to 100 characters long, to identify the holiday.
Description	Enter a description, up to 255 characters, to identify the holiday.
Enabled	If enabled with a check mark, the holiday becomes armed and activates when its time span is met. If the check mark is removed, the holiday is not armed and is ignored by the system.
Partition	A read-only field displaying the name of the Partition to which this holiday belongs. (This field is visible only if the C•CURE 9000 system is partitioned.)

Non-recurring Holiday

Select the **Non-recurring** option in the Recurrence box to create a holiday that occurs once. The Holiday Editor General tab displays fields to set the Start date/time and End data/time for the Holiday. Figure 105 on Page 322, shows the Non-recurring Holiday fields. The Holiday General tab Non-recurring Holiday fields are described in Table 77 on Page 323.

You can configure a Non-recurring Holiday that occurs on a specific day (full or partial) or range of days.

To Configure a Non-recurring Holiday

1. Access the Holiday Editor. See Holiday Editor on Page 321.
2. Select **Non-recurring** in the Recurrence box.
3. In the **Start date** field, use the drop-down Calendar to select the starting date for the Holiday. You can also set a starting time by typing in a time in 24-hour format (HH:MM).
4. In the **End date** field, use the drop-down Calendar to select the ending date for the Holiday. You can also set a starting time by typing in a time in 24-hour format (HH:MM).
   If you select a different date than the start date, the Holiday will extend over that number of days.

5. To configure a non-recurring partial-day Holiday, click in the **Start date** field and set the start time. Then click in the **End date** field, select the same date, and set the end time.
6. Click **Save and Close** to save the Holiday.

Table 77: Non-recurring Holiday General Tab

Field	Description
Recurrence options	Select **Non-recurring** to configure a Holiday that occurs once on a specific date or date/time range. A Non-recurring Holiday can be a partial day (less than 24 hours), or it can span multiple consecutive days.
Start Date	The start date and start time for the holiday. Use the drop-down calendar to change the start date for the holiday. Click in the hours:minutes portion of the field to change the start time for the Holiday.
End Date	The end date and end time for the holiday. Use the drop-down calendar to change the end date for the holiday. Click in the hours:minutes portion of the field to change the end time for the Holiday.
Duration	Shows the duration (day:hour:minute) of the Holiday calculated from the **Start Date** and **End Date**.

Monthly/Yearly Holiday

Select the **Monthly/Yearly** option in the Recurrence box if you want to configure a repeating holiday that recurs every month/year. The Holiday General tab displays fields to set the recurrence pattern and the months for the Holiday, as shown in Figure 106 on Page 323. The fields for configuring a Monthly/Yearly Holiday are described in Table 78 on Page 324.

You can configure a Holiday that occurs on a specific day of the month for selected months or on a specific day of the week according to a pattern of Occurrence.

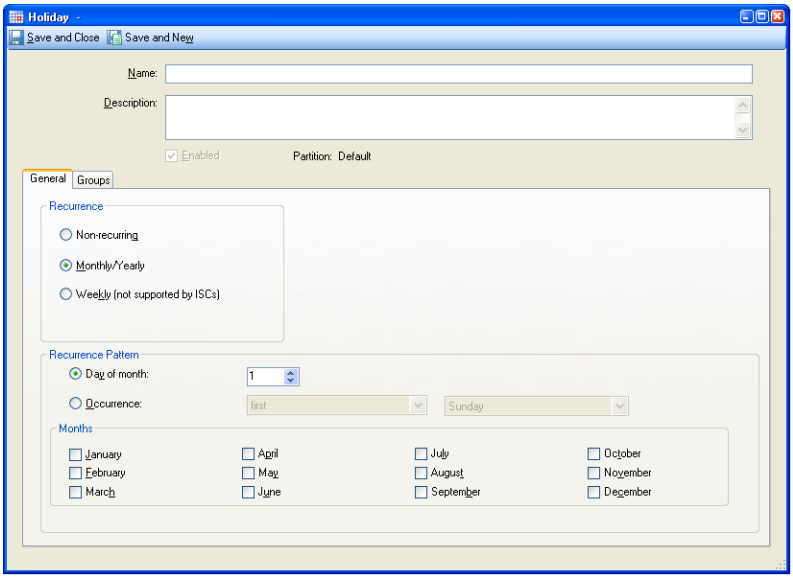
Example:

You can set an Occurrence so that a Holiday occurs on the second Thursday of every other month by selecting the following:

Occurrence fields: **second** and **Thursday**

Month fields: select **January**, **March**, **May**, **July**, **September**, **November**.

Figure 106: Holiday General Tab Monthly/Yearly Options



To Configure a Monthly/Yearly Holiday

1. Access the Holiday Editor. See Holiday Editor on Page 321.
2. Select **Monthly/Yearly** in the Recurrence box.
3. Select either **Day of month** or **Occurrence**.
4. If you selected **Day of month**, use the spinner to set the day number.
5. If you selected Occurrence, select a number from the first drop-down list and a day of the week from the second drop-down list.
6. Select or clear the check boxes for the Months during which this Holiday should occur.
7. Click **Save and Close** to save the Holiday.

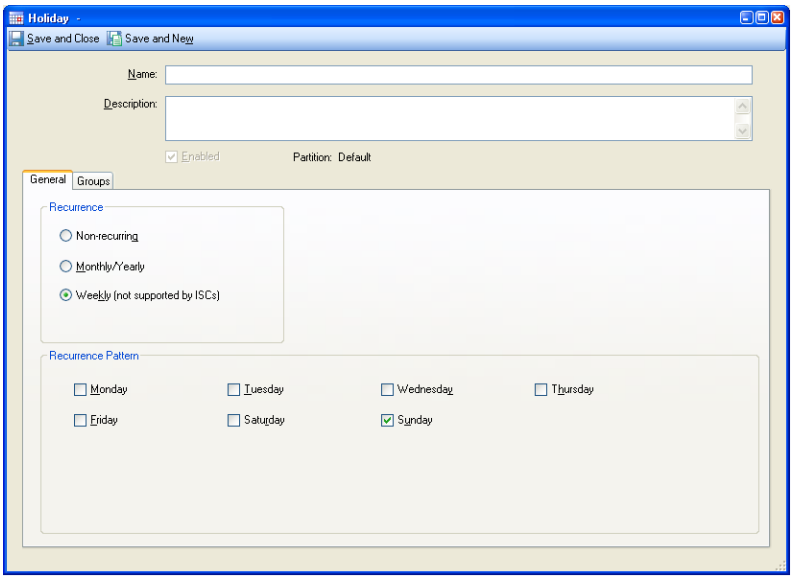
Table 78: Holiday General Tab Monthly/Yearly Fields

Field	Description
Recurrence options	Select **Monthly/Yearly** to configure a repeating holiday that occurs every month or year. This option enables day/frequency options for Recurrence Pattern and for specifying the Months in which the holiday occurs.
Day of Month	Defines the day of the month the holiday occurs (for example, the 10th day of the month). Use the drop-down list to select the day of the month. NOTE: If you select a day of the month that does not occur for a given month, that holiday is ignored. (For example February 30).
Occurrence	Defines the scheduling frequency when the holiday is active. Select the option and then select the occurrence pattern. For example, you can select **second** and **Tuesday** from the drop-down lists on the respective fields.
Months	Specifies the month(s) of the year in which the holiday occurs.

Weekly Holiday

Select **Weekly** in the Recurrence box to configure a repeating holiday that recurs every week. Specify the day(s) of the week for the holiday. The Holiday General tab displays fields to specify the days of the week for the Holiday, as shown in Figure 107 on Page 324. The fields for configuring a Weekly Holiday are described in Table 79 on Page 325.

Figure 107: Holiday General Tab Weekly Holiday Options



You can create a Holiday that occurs on one or more specific days of the week, every week. This type of Holiday is not supported on ICS controllers.

To Configure a Weekly Holiday

1. Access the Holiday Editor. See Holiday Editor on Page 321.
2. Select **Weekly** in the Recurrence box.
3. Select or clear the check boxes for the days of the week during which this Holiday should occur.
4. Click **Save and Close** to save the Holiday.

Table 79: Holiday General Tab Weekly Holiday Fields

Field	Description
Recurrence option	Select **Weekly** to configure a repeating holiday that occurs every week on the same weekday. This option enables Recurrence Pattern options for specifying the weekday(s) on which the holiday occurs.
Recurrence Pattern	Select the days of the week that the holiday occurs.

Configuring Holidays

You can perform the following tasks to configure Holidays.

Creating a Holiday

You can create a new Holiday using the Holiday Editor.

NOTE You cannot create more than 24 Holiday Groups in C•CURE 9000.

To Create a Holiday

1. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Holiday** from the Configuration pane drop-down list.
3. Click **New** to create a new Holiday. The Holiday Editor opens and you can configure the Holiday.
4. To save your new Holiday, click **Save and Close**.

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

Creating a Holiday Template

You can create a new template for a holiday. A holiday template saves you time because you can use it as a pattern for creating additional Holidays.

To Create a Holiday Template

1. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Holiday** from the Configuration pane drop-down list.
3. Click the drop-down arrow next to **New** and select **Template**. The Holiday Template opens and you can configure the holiday template.
4. To save your new Holiday Template, click **Save and Close**.

Viewing a List of Holidays

You can view a list of the Holidays you have configured.

See Viewing a List of an Object Type on Page 22 for more information.

Using the Holiday Context Menu

The context menu that opens when you right-click a Holiday in the Holiday Dynamic View includes the selections described in Using the Object List Context Menu on Page 23.

Modifying a Holiday

You can edit a Holiday that you created previously to change its configuration.

To Edit a Holiday

1. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Holiday** from the Configuration pane drop-down list.
3. Click to open a Dynamic View showing all holiday objects.
4. Right-click the holiday in the list that you want to modify and select **Edit** from the context menu.

Setting a Property for a Holiday

You can use **Set Property** to set properties for a holiday. **Set Property** enables you to set a property for a holiday without opening the holiday editor.

To Set a Property for a Holiday

1. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Holiday** from the Configuration pane drop-down list.
3. Click to open a Dynamic View showing all Holiday objects.
4. Right-click on the holiday(s) in the list that you want to set a property for, and select **Set Property** from the context menu.
5. Specify the property for the holiday by clicking the drop-down button to see a list of properties.
6. Enter the value for the property in the **Value** field and click **OK**.

Adding Holidays to a Group

You use **Add to Group** to add a Holiday to a Holiday Group.

To Add a Holiday To a Group

1. Make sure that a Holiday Group already exists to which the Holiday can be added. To create a new Group, see Creating a Group on Page 313.
2. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.
3. Select **Holiday** from the Configuration pane drop-down list.
4. Click to open a **Dynamic View** showing all Holiday objects.
5. Right-click the Holiday in the list that you want to add to a group and select **Add To Group** from the context menu.
6. When the Group list displays, select the group you want to add the holiday to, and click **OK**.

Adding Holidays to a Group

You use **Add to Group** to add a Holiday to a Holiday Group.

First, configure a group for holidays, with “Holiday” selected as the type. Then, use Add to Group to add the holiday object to a holiday-type group.

To Add a Holiday To a Group

1. Make sure that a Holiday Group already exists to which the Holiday can be added. To create a new Group, see Creating a Group on Page 313.
2. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.
3. Select **Holiday** from the Configuration pane drop-down list.
4. Click to open a **Dynamic View** showing all Holiday objects.
5. Right-click the Holiday in the list that you want to add to a group and select **Add To Group** from the context menu.
6. When the Group list displays, select the group you want to add the holiday to, and click **OK**.

11

Journal Triggers

This chapter explains how to configure Journal Triggers in C•CURE 9000.

In this chapter

Journal Triggers Editor

The Journal Triggers editor lets you define Triggers that can pulse an Event when a specified Journal Message occurs. A Journal Trigger is a Query-like object that evaluates Journal Messages and pulses an Event when the criteria specified in the trigger is logged in the Journal.

Example:

Some Journal Triggers you could configure to pulse an Event:

- A selected Message Type for a selected object(s) is logged into the Journal.
- A system error has been reported by the CrossFire service (especially in the cases when there are no other mechanisms for activating an Event like a database backup failure).
- Any access card that is rejected in a particular area.

See the following sections for information about Journal Triggers and how to use them.

- Journal Triggers General Tab on Page 332
- Pre-defined Journal Triggers and Events on Page 334
- Journal Trigger Definitions for Simple Query Mode on Page 341
- Journal Triggers Definitions for Advanced Query Mode on Page 344
- Journal Triggers in an Enterprise on Page 334
- Journal Triggers Tasks on Page 346

Maximum Number of Journal Triggers Per Server

Because Journal Triggers are evaluated for each generated Journal message, the number of Journal Triggers that can be configured for a C•CURE 9000 server is limited to 500 in order to manage memory usage.

Journal Triggers for Host and Panel Events

Journal Triggers can be configured to pulse either host Events or panel Events (Events downloaded to a controller), including panel Events and objects on different controllers. If the home controller of a panel Event is offline, pulsing that Event has no effect. If the home controller of a panel object is offline, the pulsing of an Event affecting that object is postponed until communications with the controller is restored.

Import and Export of Journal Triggers

You can export Journal Triggers from the context menu, or by creating a Data Export object with an Export Schema selector of **Journal Trigger**.

You can import a Journal Trigger by creating a Data Import object. Name, Evaluation Order, and Schedule Name are available as Match Fields.

Reporting on Journal Triggers

You can create a Report on Journal Triggers by choosing Journal Trigger as the **Report type** in the Report editor. Available Sub types are:

- Basic Configuration - create a report about Journal Trigger objects.
- Journal Trigger Audit Log - create a report about Journal Trigger entries in the Audit Log.
- Journal Trigger Journal - create a report about Journal Trigger entries in the Journal.
- Journal Trigger Group - create a report about Groups containing Journal Trigger objects.

Journal Messages about Journal Triggers

When a Journal Trigger pulses an Event, two additional separate Journal Message are logged:

- A Journal Message that identifies the Event that was pulsed and the primary object of the Journal Message that activated the Journal Trigger.

  Example:

  Event EVENT NAME is Pulsed by Card Admitted

- A Journal Message that identifies the Journal Trigger that pulsed the Event, the Event pulsed, and the Journal Message text that activated the Journal Trigger.

  Example:

  Journal trigger 'TRIGGER NAME' pulse event 'EVENT NAME' based on the journal message [MESSAGE TEXT].

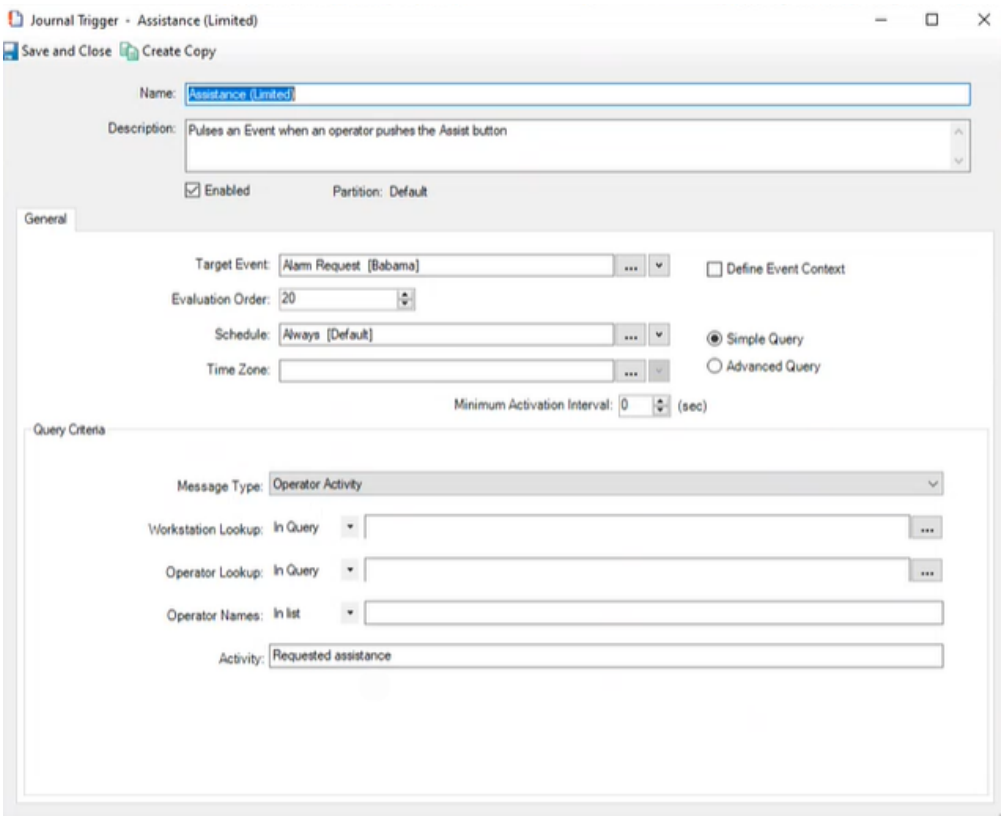
NOTE It is important to make sure that the Journal Triggers you configure are not activated again by the Journal Messages generated by the Triggers, causing a looping condition. The **Minimum Activation Interval** is provided to help guard against this, by telling Journal Triggers to ignore additional triggering within a specified time period. See Journal Trigger Definitions for Simple Query Mode on Page 341

Journal Triggers General Tab

The Journal Triggers General tab lets you configure query-like triggers that monitor Journal Messages coming into the C•CURE 9000 database for specified state changes and conditions.

Figure 108 on Page 332 shows the Journal Triggers editor General tab with Simple Query Selected.

Figure 108: Journal Triggers General Tab



You can create Triggers with simple queries to search for a single Journal Message Type in a Journal Message.

You can also create Triggers with advanced queries for handling Journal Message Types that are not supported by a simple query (like "System Error") and for providing the ability to combine several conditions to trigger the same event.

For information about the definitions of the fields and buttons on the Journal Triggers General tab:

- Journal Trigger Definitions for Simple Query Mode on Page 341
- Journal Triggers Definitions for Advanced Query Mode on Page 344

Simple Query Mode

The Simple Query mode allows selection of a single Journal Message type and lets you build a query on additional objects that are specific to that selected message type.

For example, if the Message Type "Object Changed State" is selected, the Query Criteria section on the General tab lets you choose one or more objects of any type and a combination of the possible states for those objects (like Door forced or Door held).

This control is similar to the Journal Assistant Query for Journal Replay.

Currently, the Query Criteria section supports the following message types:

- Area Activity
- Card Admitted
- Card Rejected
- Guard Tour Activity
- Visitor Management
- Manual Action
- Object Changed State
- Operator Activity
- Operator Login

If the Object field is not specified, the Event is pulsed for all messages with the selected message type.

Advanced Query Mode

The Advanced Query mode is used to allow you to query on multiple conditions, and to support message types that are not included in the simple query, so that you can build any sort of journal query supported by Journal Replay. This mode uses a standard query interface and the standard query expression builder.

This mode also allows you to combine several conditions to trigger the same event.

Example:

If you wanted a single trigger that pulsed an Event whenever a Device Error, a System Error, or an Intrusion Zone Error occurred, you could create a Journal Trigger with an advanced query using 'OR' statements to search for all three error types.

Journal Triggers in an Enterprise

While Journal Triggers are local-only objects, Journal Triggers can operate in an Enterprise environment. The Events they can trigger are local to the home server of the objects and Events named in the trigger.

The partition where a Journal Trigger is created is based on the Operator's "New object partition" selection. Journal Triggers cannot be created on the Global partition (because they are local-only objects).

However, from a SAS you can create Journal Triggers that reference Global Objects. When you create and edit a Journal Trigger on a SAS, you can select any objects (local or Global) to be used in the query expression, as allowed by Operator Privileges.

The MAS can display Journal triggers from all SAS's, but each SAS is not aware of the Journal Triggers on the MAS or other SAS's. In turn, the MAS does not evaluate any triggers created on the other SAS's, only the MAS local triggers.

Editing a SAS Journal Trigger from the MAS

Editing a SAS Journal Trigger via the Administration station connected to the MAS does not allow selection of objects from other SAS servers. Because the Trigger itself is local to a Particular SAS, it can only be configured with objects and Events that are local to that SAS, or Global.

Journal Triggers on the MAS

Editing a Journal Trigger located in a local partition of the MAS limits the trigger to selecting only events that are local to the MAS. The Selection of objects used in the query expression of the trigger is not limited to local objects.

NOTE The Journal Messages that are generated on SAS servers and replicated to MAS are not included in the Journal Trigger mechanism because these messages do not generate creation notification messages on the MAS itself - they are replicated to the MAS, not created on the MAS.

Maximum Number of Journal Message Triggers for the MAS

The MAS displays all configured Journal Triggers from all SASs, but only 500 Journal Message Triggers can be created local to the MAS, because the MAS evaluates only its local triggers.

Limitations on Local Journal Messages on the MAS

The MAS has a limited range of Journal Messages that can be used for triggers because no hardware is running on MAS, so the MAS does not create most types of Journal Messages. Therefore, some Journal Triggers can be created on the MAS, but they are never triggered (for example, a trigger on a Card Admit message) because the MAS never generates the Journal Messages for which the triggers are configured.

Pre-defined Journal Triggers and Events

C•CURE 9000 includes several pre-defined Journal Triggers that you can **Enable** and use as defined. You can use these triggers as the basis of your own Journal Triggers, using **Create Copy** to make an editable version of the trigger.

These triggers each target a pre-defined Event by default. These pre-defined Events do not include an Event action, but they are Enabled and do include **Send state changes to Monitoring Station**

- You can modify these default Events to perform actions and/or be journaled and sent to the Monitoring Station.
- You can also use the **Create Copy** button create a copy of the Event, set up actions and options, configure that new Event in the Journal Trigger, and leave the default Event unchanged.

Table 80: Pre-defined Journal Triggers and Events

Journal Trigger	Event	Message Type	Description
Device Error Journal Trigger	Device Error Journal Event (default)	Device Error	When a Device Error Journal Message is logged, this trigger pulses the Device Error Journal Event. Uses an Advanced Query.
System Error Journal Trigger	System Error Journal Trigger Event	System Error	When a System Error Journal Message is logged, this trigger pulses the System Error Journal Event. Uses an Advanced Query.
Battery Low Journal Trigger	Battery Low Journal Trigger Event	Object Changed State: Battery Low	When a Battery Low Journal Message is logged, this trigger pulses the System Error Journal Event. Uses a Simple Query.
Intrusion Zone Error Journal Trigger	Intrusion Zone Error Journal Trigger Event	Intrusion Zone Error	When an Intrusion Zone Error Journal Message is logged, this trigger pulses the System Error Journal Event. Uses an Advanced Query.
Watchlist Check-in Journal Trigger	Watchlist Check-in Journal Trigger Event	Visitor Management	When a visitor from the Watchlist has been checked in for a Visitor, this trigger pulses the Watchlist Check-in Journal Trigger Event. Uses a Simple Query. Is enabled by default and can be disabled. For more information on the Watchlist, see the Personnel chapter in the *C•CURE 9000 Personnel Guide*.
Watchlist Assistance Request Journal Trigger	Watchlist Assistance Request Trigger Event	Operator Activity	When an operator clicks the Assist button while working with a person who is on the Watchlist, this trigger pulses the Watchlist Assistance Request Trigger Event. Uses an Advance Query. Is enabled by default and can be disabled. For more information on the Watchlist and Assist button, see the Personnel chapter in the *C•CURE 9000 Personnel Guide*.
Assistance Request Journal Trigger	Assistance Request Journal Trigger Event	Operator Activity	When an operator clicks the Assist button this trigger pulses the Assistance Request Journal Trigger Event. Uses a Simple Query. Is enabled by default and can be disabled. This trigger is overrule by the Watchlist Assistance Request Trigger Event, which has a higher priority. For more information on the Assist button, see the Personnel chapter in the *C•CURE 9000 Personnel Guide*.

You can access these pre-defined triggers from the Dynamic View of Journal Triggers (see Viewing a List of an Object Type on Page 22).

Creating a Copy of Pre-defined Journal Triggers and Events

You can use the pre-defined Journal Triggers and Events as the basis for your own Journal Triggers by creating a copy of a pre-defined Journal Trigger and copy of the associated pre-configured Event, then re-configuring the Event and the Journal Trigger to meet your needs.

To Copy and Configure Pre-defined Journal Triggers and Events

1. Open the pre-defined Journal Trigger Event that you want to use by Accessing the Event Editor on Page 300.

2. Click **Create Copy** to make a copy of the pre-defined Journal Trigger Event.
3. Enter a name for the new Event in the **Name** field and click **Enabled**.
4. Configure the Event Options, Messages, Actions, and other tabs to customize the Event to meet your needs.
5. Click **Save and Close** to save the Event.
6. Open the pre-defined Journal Trigger that you want to use by Accessing the Journal Triggers Editor on Page 346.
7. Click **Create Copy** to make a copy of the pre-defined Journal Trigger.
8. Enter a name for the new Journal Trigger in the **Name** field.
9. Select the Event you just created in the Target Event field.
10. Configure the other options on the Journal Trigger General tab to meet your needs.
11. If the Query from the pre-defined Journal Trigger does not meet your needs, you can follow the steps in Configuring a Journal Trigger Simple Query on Page 347 or Configuring a Journal Trigger Advanced Query on Page 348.
12. Click **Save and Close** to save the Journal Trigger.

Monitoring Events Activated by Journal Triggers

To effectively monitor an event pulsed via a Journal Trigger, the Event has to be configured with **Send state changes to Monitoring Station** enabled (or have an Event action which changes the state of the system in some other noticeable way). To have to Event remain active in the Event Viewer long enough for an Operator to manage it, it may be helpful to:

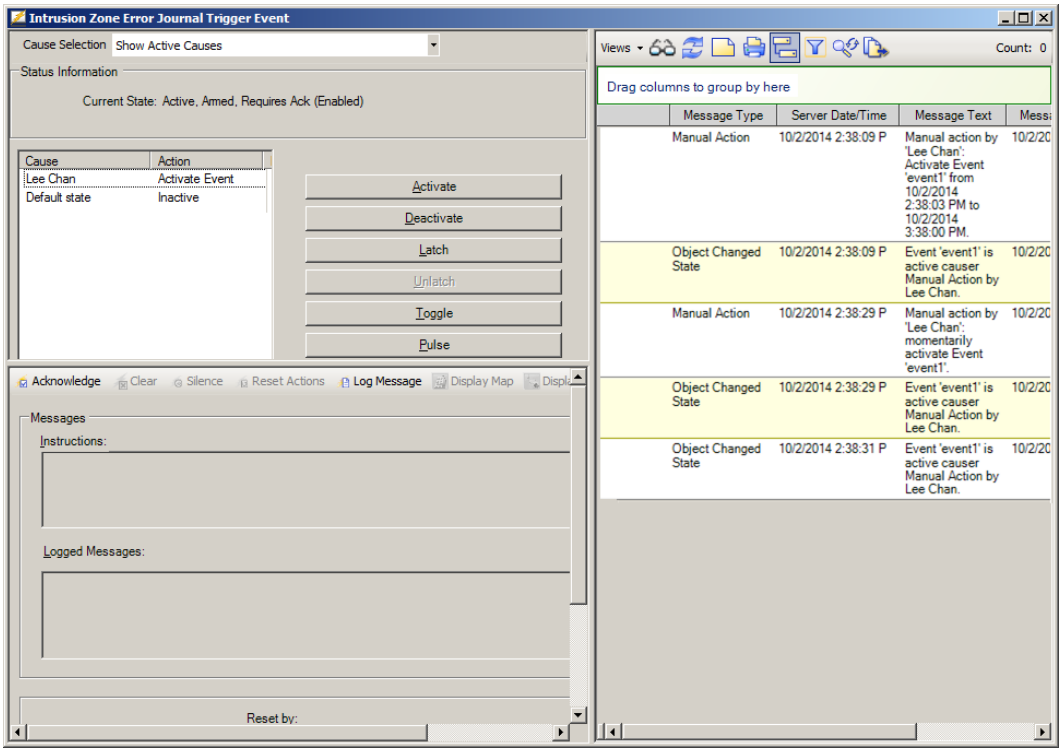
- Configure the Event with the **Min activation time** setting to keep the Event active long enough for the Operator to take note of it
- Configure the Event with the **Event requires acknowledgment** setting, so that the Event remains active in the Monitoring Station until an Operator acknowledges the Event.

Determining Why an Event Was Pulsed by a Journal Trigger

To determine why the Event was activated, right-click on the event to execute the Find in Journal… context menu selection. This shows all the Journal Messages related to the Event within last hour (or a longer time period). The list of the selected messages shall contain both type of the messages described above because the event will be primary or secondary object on those messages.

You can also right-click on the Event and execute the Event Monitoring Screen which is similar to the Event Details screen. The Event Monitoring Screen shows all the information about an Event including Cause Lists, Event details, manual action buttons, log messages, instructions and a journal log dynamic view of all activation attempts during the current lifetime (the time between active and inactive states). See Figure 109 on Page 337 for the Event Activation screen.

Figure 109: Event Activation



The Cause List Selection at the top of the screen displays a drop-down list that allows switching between Active Causes and Armed Causes and the associated manual actions.

Journal Log dynamic view displays all logged messages in which the Event acts as a Primary or Secondary object. The view is in descending order, displaying the latest activities on top.

Privileges assigned to a current operator are respected.

Journal Messages Logged for Journal Triggers

When a Journal Trigger pulses an Event, a separate Journal Message is logged for that action.

If the event is pulsed then the Journal Trigger passes the Source, a list of Cause list items and Activation Date Time as parameters to an Event Activation method. All Event Causes are then displayed in the Journal Log Dynamic View on the Event Monitoring screen. You can use Find In Journal for the same purpose.

The primary object for that Journal Message is the pulsed Event and the secondary object of the message is the primary object of the Journal Message that caused the Trigger to pulse the Event. The Journal Message also references the Message Type of the Journal Message that caused the Trigger to pulse the Event.

Example:

When a Journal Trigger pulses an Event, the Monitoring Station displays a Journal Message in to form of:

Event <EVENT NAME> is Pulsed by Card Admitted of Jim Smith

In addition to Messages generated because a Journal Trigger has pulsed an Event, another journal message is created for each Journal Trigger that was evaluated as True for the original Journal Message, as follows:

Journal trigger <TRIGGER NAME> activate event <EVENT NAME> based on the journal message [MESSAGE TEXT]

The MESSAGE TEXT portion of the message is a message created from the journal message that activated the Trigger.

If an Event that has already been activated because of another cause is pulsed by a Journal Trigger, the Event that was pulsed is logged into the journal to keep track of the triggering Event. However, the actions of the pulsed Event (which were executed when the Event was first activated) are not executed again when the Event is pulse.

Monitoring Events Activated by Journal Triggers Email

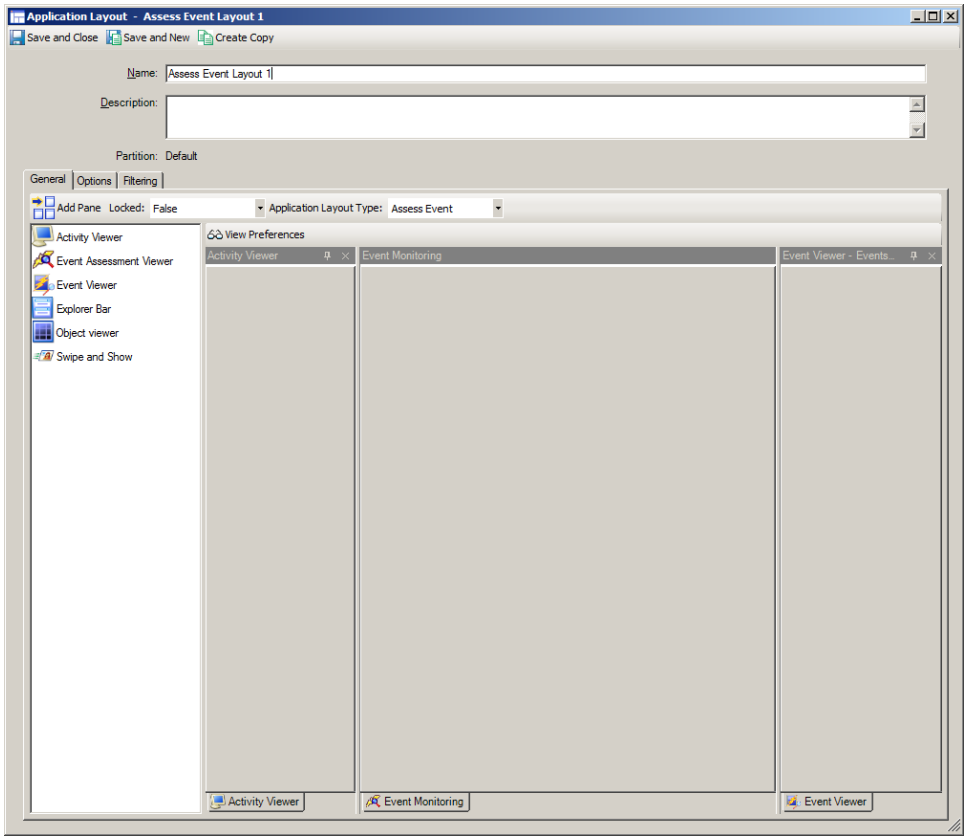
To monitor an event pulsed from a Journal Trigger, configure two Events and an application layout:

- Event 1 with **Send state changes to Monitoring Station** enabled, a valid email address.
- Event 2 with **This event requires acknowledgement** checked **Log All Causes to Journal**
- Application Layout assigned to an Operator to assess the Event cause.

To Create an Application Layout for Event Assessment

1. Create an Application Layout which contains the following Panes (see Figure 110 on Page 338):
   a. Activity Viewer
   b. Event Monitoring
   c. Event Viewer
2. Assign the **Assess event Layout 1** to an operator.

Figure 110: Assess Event Layout



To Configure Journal Triggers to Send an Email

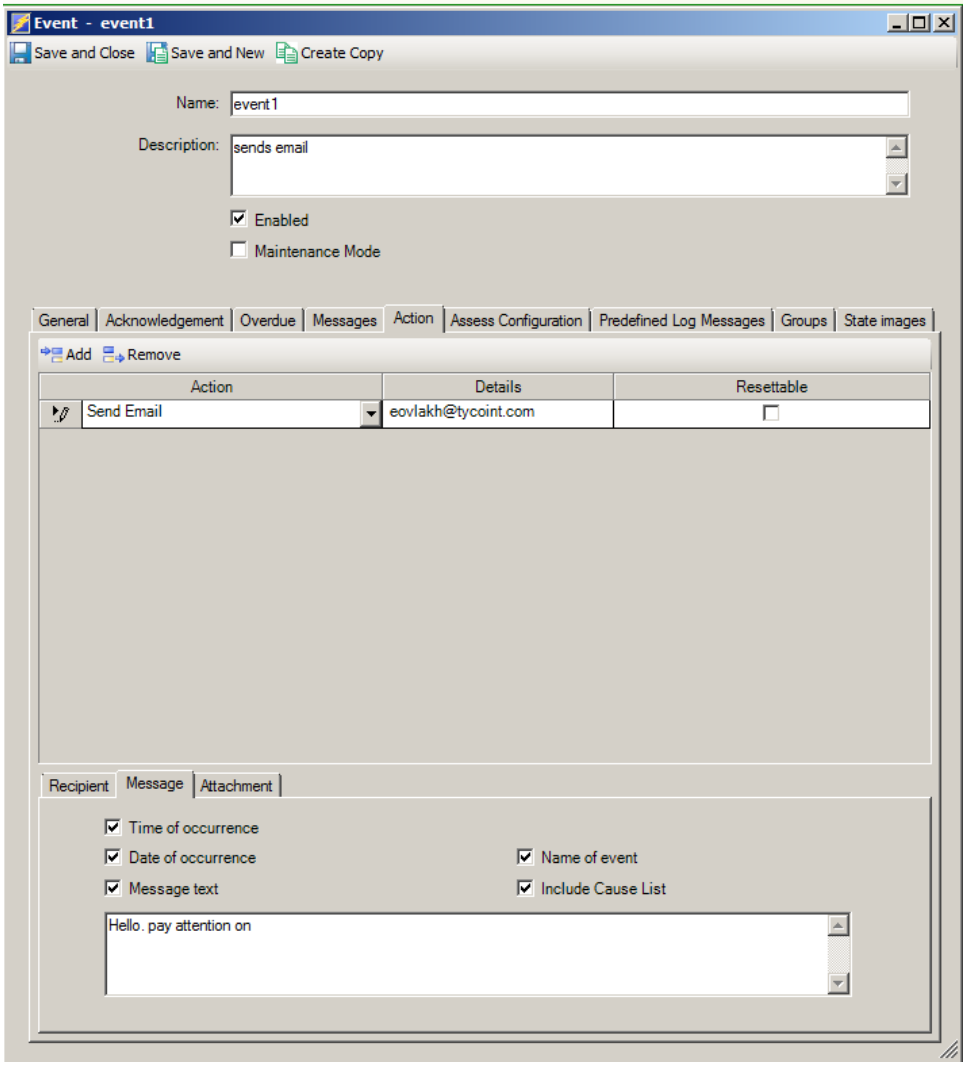
1. Configure Event 1 with the following:

a. **General Tab** - Default state armed, Priority Medium Low

b. **Acknowledgement Tab** - Send Changes to Monitoring Station, Log All causes to Journal checked

c. **Action Tab** - Send Email to person, add message text and check all check boxes. See Figure 111 on Page 339 for a display.

Figure 111: Event1 Configuration for Sending Email



2. Configure Event2 with the following:

a. **General Tab** - Check **Armed.**

b. **Acknowledgement Tab** - Check **This event requires acknowledgement.**

c. **Assess Configuration Tab** - Select **Assess Event Layout 1** from **Assess Application Layout for Assess Event.**

3. Configure the Journal Triggers to access the Event causes (see Figure 112 on Page 340):

a. Enter the name of the Journal Trigger and optionally a description.

a. Click ... in the **Target Event** field to select the Event you want triggered.

b. Click ... in the **Time Zone** field to select the Time Zone for the Event.

c. **Optional:** Leave the **Minimum Activation Interval** parameter at the default value unless you experience complications with an Audit Log entry re-triggering the Audit Trigger. If you want the event to be pulsed every time the trigger criteria is met in the Audit message, set the **Minimum Activation Interval** parameter to 0.

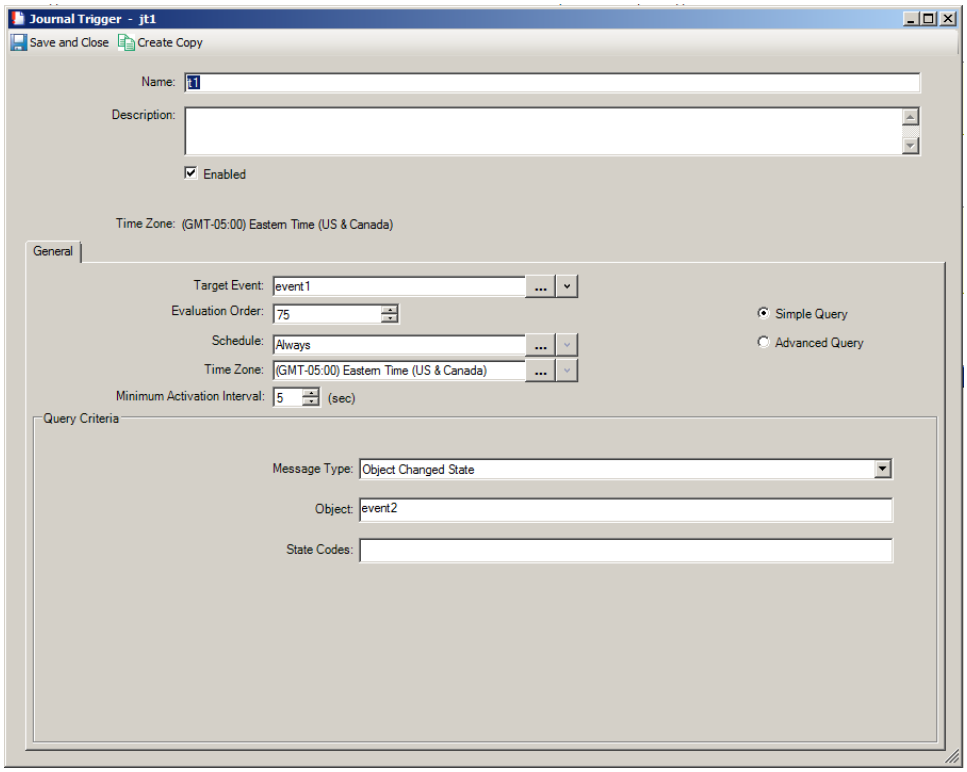
d. **Optional:** To send information about the Audit message to the activated Event, select the **Define Event Context** check box. When selected, the Event is pulsed every time the Trigger criteria is met.

e. In the Query Criteria section, select **Object Changed State** from the **Message Type** drop-down menu.

f. Enter Event2 in the **Object** field.

g. Click **Save and Close.**

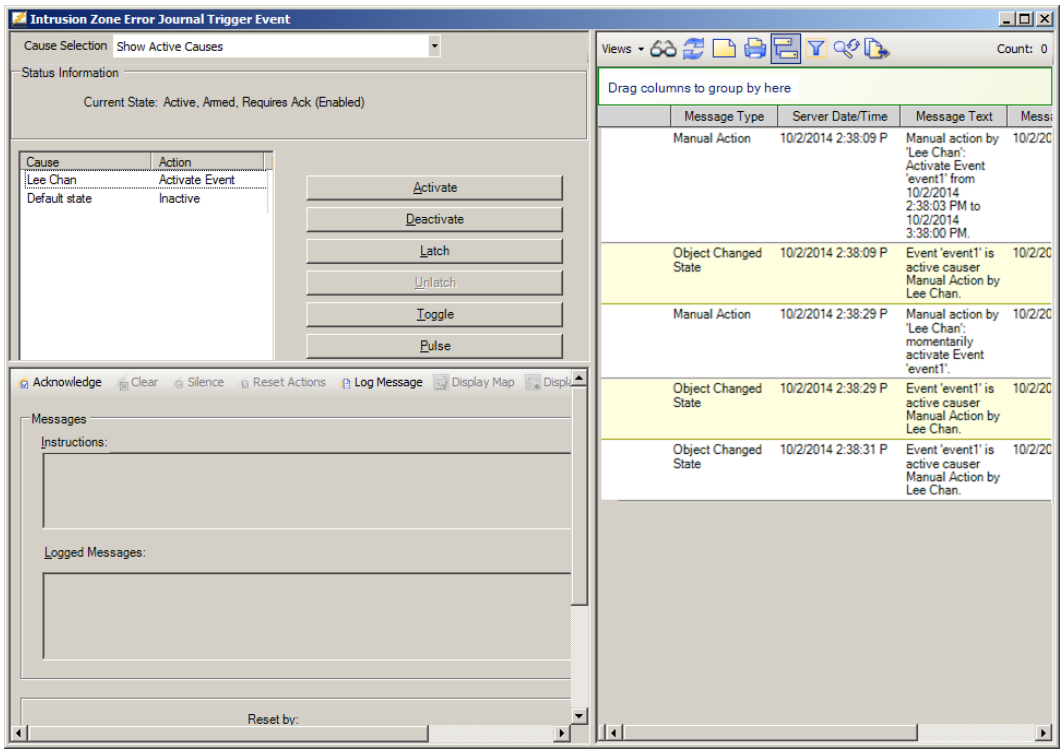
Figure 112: Create Event2



4. From the **Event** Tab, select **Event1**, right-click and select **Event Monitoring Screen**.

   The **Event1** window appears.

Figure 113: Trigger Event1 From the Even Monitoring Screen



5. Right-click on **Event1** to execute the **Find in Journal...** context menu selection.

.

Journal Trigger Definitions for Simple Query Mode

Definitions for the fields and buttons in the Journal Triggers editor Simple Query Mode are described in Table 81 on Page 342.

Simple Query mode uses the same mechanism as the Journal Query Assistant to build a query for Journal Triggers. See the C•CURE 9000 System Maintenance Guide for more information about the Journal Query Assistant.

When you choose a **Message Type** for the Query Criteria, additional fields appear in the Query Criteria area that are specific to that Message Type.

Example:

If you select **Card Rejected** as a Message Type, fields appear to allow you to select **Personnel Names**, **Door Names**, **Direction** (IN or OUT), **Rejection Reason**, **Escort Option**, and **Area Names**.

When you click in one of these fields, a selection control (or drop-down list) appears to let you pick one or more objects to query on.

See Configuring a Journal Trigger Simple Query on Page 347 for instructions on setting up a simple query.

See Journal Triggers Definitions for Advanced Query Mode on Page 344 for definitions of fields and buttons for an Advanced Query.

Table 81: Journal Triggers Editor Simple Query Definitions

Field/Button	Description
Name	Enter the name you want to assign this Journal Trigger in C•CURE 9000.
Description	Enter a textual description for this Journal Trigger.
Enabled	If selected, the Journal Trigger is enabled, and its query is evaluated upon receiving a journal message.If cleared, the Journal Trigger is disabled (its query is not evaluated upon receiving a journal message).
Partition	A read-only field displaying the name of the Partition to which this Journal Trigger belongs. (This field is visible only if the C•CURE 9000 system is Partitioned.)
Target Event	Select an event from a list of the existing events. This event is pulsed if the Query expression you define below evaluates as **True** for an incoming Journal Message. This field must be populated for a trigger to be valid. (If you create a Journal Trigger template, you can leave the target Event blank if you do not set the template as **Enabled**.
Define Event Context	Select this checkbox to instruct the Journal trigger to define the context for the event that you are pulsing. For more information, see Event Context on page 308.
Evaluation Order	This field allows you to configure the priority of a trigger. You can choose a number between 1 and 200 (the higher the value, the higher the priority). For a given Target Event, the Triggers with the highest priority are evaluated first. If at least one trigger of that priority level is evaluated as **True**, other Journal Triggers for that Target Event with lower priorities are not evaluated.
Schedule	Allows you to assign a Schedule for this Journal Trigger. When the Schedule is active, the Journal Trigger is evaluated (can be activated); when the Schedule is inactive, the Journal Trigger is not evaluated (cannot be activated). The Schedule field cannot be blank.
Time Zone	Allows you to assign a Time Zone for this Journal Trigger. If you assign a Time Zone, the Schedule that you assign is activated and deactivated according to that Time Zone. If a Time Zone is not assigned, the Journal Trigger uses the C•CURE 9000 server Time Zone for Schedule activation/deactivation.
Minimum Activation Interval	Allows you to specify the number of seconds which must elapse before the next activation of this Journal Trigger, after the trigger has been activated. This interval is used tp prevent a Journal Message from this Journal Trigger from starting a potential looping condition by re-triggering. The range of values is 0 to 99 seconds, with a default value of 5 seconds. Typically the default value of 5 seconds is long enough to suppress unintended reactivations. A value of 0 means that rapid activations are not prevented.
Simple Query	Click this button to configure a simple query. The Query Criteria portion of the screen displays the Message Type, Object, and State Codes fields.
Advanced Query	Click this button to configure an Advanced Query. The Query Criteria portion of the screen displays the Query Criteria table for an Advanced Query.

Journal Triggers Editor Simple Query Definitions (continued)

Field/Button	Description
Query Criteria (Simple)	
Message Type	The following Journal Message Types are supported: • Area Activity • Card Admitted • Card Rejected • Guard Tour Activity • Manual Action • Object Changed State • Operator Activity • Operator Login
Area Activity Message Type	
Area Names	You can choose one or more Area Names from a selection dialog box. The names you choose are used by the Journal trigger to evaluate whether a Journal message for Area Activity includes one of these Area Names.
Card Admitted Message Type	
Personnel Names	Choose one or more Personnel Names from a selection dialog box. The names you choose are used by the Journal trigger to evaluate whether a Journal message for Card Admitted includes one of these Personnel names.
Door Names	Choose one or more Door Names from a selection dialog box. The names you choose are used by the Journal trigger to evaluate whether a Journal message for Card Admitted includes one of these Door names.
Direction	Specify whether the Journal Trigger is activated by Journal Messages for Card Admits at entrance (IN) or exit (OUT) Doors.
Escort Option	Specify whether the Journal Trigger is activated by Journal Messages that have one or more Escort values, or none of them. The Escort Option selections are Escort, Escorted Visitor, and Unescorted Visitor.
Area Names	Specify whether the Journal Trigger is activated by Journal Messages that have one or more Area names. If you do not choose any Area Names, the Journal Trigger does not filter on Area Name.
Card Rejected Message Type	
Personnel Names	Choose one or more Personnel Names from a selection dialog box. The names you choose are used by the Journal trigger to evaluate whether a Journal message for Card Admitted includes one of these Personnel names.
Door Names	Choose one or more Door Names from a selection dialog box. The names you choose are used by the Journal trigger to evaluate whether a Journal message for Card Admitted includes one of these Door names.
Direction	Specify whether the Journal Trigger is activated by Journal Messages for Card Admits at entrance (IN) or exit (OUT) Doors.
Rejection Reason	Specify whether the Journal Trigger is activated by Journal Messages that include specific Rejection codes. A selection dialog appears to let you choose one or more Rejection reasons. If you do not choose any Rejection Reasons, the Journal Trigger does not filter on Rejection Reason.
Escort Option	Specify whether the Journal Trigger is activated by Journal Messages that have one or more Escort values, or none of them. The Escort Option selections are Escort, Escorted Visitor, and Unescorted Visitor.

Journal Triggers Editor Simple Query Definitions (continued)

Field/Button	Description
Area Names	Specify whether the Journal Trigger is activated by Journal Messages that have one or more Area names. If you do not choose any Area Names, the Journal Trigger does not filter on Area Name.
Guard Tour Activity	
Tour Status	Choose one or more Values from a selection dialog box.
Monitor State	Select from a list of values for the Monitor State.
Object Changed State Message Type	
Object	Specify by which objects the Journal Trigger is activated. A selection dialog appears to let you choose one or more objects. You can choose objects of multiple object types (for example, apC controllers and iSTAR controllers).
State Codes	Specify whether the Journal Trigger is activated by Journal Messages that include specific State Codes. A selection dialog appears to let you choose one or more State Codes. If you do not choose any State Codes, the Journal Trigger does not filter on State Code (i.e., the Trigger would be activated by any state change to the specified objects).
Operator Activity Message Type	
Operators	Specify one or more Operators whose actions can activate the Journal Trigger.
Activity	Specify the Operator Activities that can activate the Journal Trigger. A selection dialog box appears that lists the possible Operator activities. If you do not choose any Operator Activities, then all Operator Activity messages for the Operator's you chose will activate the Trigger.
Operator Login Message Type	
Operators	Specify one or more Operators whose login or logout can activate the Journal Trigger.
Actions	Specify the Operator Actions that can activate the Journal Trigger. A selection dialog box appears that lists the possible Operator Actions. If you do not choose any Operator Actions, then all Operator Action messages for the Operator's you chose will activate the Trigger.

Journal Triggers Definitions for Advanced Query Mode

If you click the Advanced Query radio button, the Query Criteria areas displays the fields and buttons for an Advanced Query.

Definitions for the fields and buttons in the Journal Triggers editor Advanced Query Mode are described in Table 82 on Page 344.

See Configuring a Journal Trigger Advanced Query on Page 348 for instructions on setting up an advanced query.

See Journal Trigger Definitions for Simple Query Mode on Page 341 for definitions of fields and buttons for a Simple Query.

Table 82: Journal Triggers Editor Advanced Query Definitions

Field/Button	Description
Query Criteria Buttons (Advanced Query)	
Add	Click to add a row to the Query Criteria table.

Journal Triggers Editor Advanced Query Definitions (continued)

Field/Button	Description
Remove	Click to remove the selected row(s) from the Query Criteria table.
Up	Click to move the selected row(s) up one row in the table.
Down	Click to move the selected row(s) down one row in the table.
Add Block	Click to add a block that groups rows logically. For example, if you needed to group two query terms so that the filter would evaluate correctly, you can use a block to have those terms calculated separately.
Clear Prompt Values	Click this button to clear all rows in the **Value** column.
Query Criteria Table Columns (Advanced Query)	
Operator	Select the logical operator you want the row to use: And - Creates an **And** logical relationship Or - Creates an **Or** logical relationship between this row and the preceding row.
Type	Specifies the type of messages being queried. Only Journal is available.
Field	Identifies the field in the Journal messages that is being queried. This drop-down also lets you select the Journal Query Assistant, so that you can query a Journal Message type, as in a simple query. You would use the Advanced Query with the Journal Query Assistant if you needed to filter using additional AND / OR Query terms (not possible with a simple query). See Configuring a Journal Trigger Advanced Query on Page 348 for examples of such queries.
Filter Type	Specifies the relationship between the field and value columns. The type of field you select determines the type of filters you can use. **Example:** If you pick **Partition**, the only choices available for Filter are Equals, Not equals, and In list. If you pick **Last Modified Time**, you have additional Filters such as Equals, Not equals, In range, In custom range, <, >, <=, and >=
Value	Specifies the value(s) for the field you chose in the **Field** column.

Journal Triggers Tasks

You can perform the following tasks using the Journal Triggers editor:

Accessing the Journal Triggers Editor

You access the Journal Triggers Editor from the C•CURE 9000 Configuration pane.

To Access the Journal Triggers Editor

1. Click the **Configure** pane button.
2. Click the Configure drop-down list and select **Journal Triggers**.
3. Click  to open a Dynamic View showing all Journal Triggers objects.
4. Double-click on the Journal Trigger in the list that you want to edit, and the Journal Triggers Editor opens.

Creating a New Journal Trigger or Template

You can create a new Journal Trigger that can activate an Event when a specified Journal Message occurs.

You can also create a Journal Trigger Template that you can use to create additional Journal Triggers starting with common settings pre-defined in the Template.

Creating a New Journal Trigger

To Create a Journal Trigger

1. In the Navigation Pane of the Administration Client, click the **Configuration** pane button.
2. Select **Journal Trigger** from the Configuration pane drop-down list.
3. Click **New** to create a new Journal Trigger. The Journal Triggers Editor on Page 330 opens and you can configure the Journal Trigger.

Creating a New Journal Trigger Template

You can create a new template for a Journal Trigger. A Journal Trigger template saves you time because you can reuse the same configuration repeatedly.

To Create a Journal Trigger Template

1. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Journal Trigger** from the Configuration pane drop-down list.
3. Click the drop-down arrow next to **New** and select **Template**. The Journal Trigger Template opens.
4. Configure the Journal Trigger template.
5. To save your new Journal Trigger Template, click **Save and Close**.

The new Journal Trigger template appears in the Template drop down list of the Configuration pane (select **Journal Trigger**, then click the drop-down arrow next to **New**).

Creating a Journal Trigger from a Template

You can use a Journal Trigger template that you have created as the basis of a new Journal Trigger object.

To Create a Journal Trigger from a Template

1. In the Navigation Pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Journal Trigger** from the Configuration pane drop-down list.
3. Click the drop-down arrow next to **New** and select **Template**.
4. Click the name of the template you want to use under Templates. The Journal Triggers Editor on Page 330 opens and you can configure the Journal Trigger you created from the Template.

Configuring a Journal Trigger Simple Query

You can configure a simple Query for a Journal Trigger.

To Configure a Journal Trigger with a Simple Query

1. Create a new Journal Trigger (see Creating a New Journal Trigger or Template on Page 346).
2. Enter a name and textual description for the Journal Trigger in the **Name** and **Description** fields.
3. Select a **Target Event** for the Journal Trigger. This is the Event whose Journal Messages are queried to match with other criteria in the trigger.
4. You can adjust the **Evaluation Order** (Priority of the trigger). The default value is 75; the minimum is 1; the maximum is 200.
5. You need to select the **Schedule** for when this Journal Trigger should be evaluated. When the **Schedule** you chose is Active, the Journal Trigger evaluates incoming Journal messages.
6. You should identify the **Time Zone** to which you want the Schedule to apply. This is important if you have controllers in a different time zone than the C•CURE 9000 server, and you want the triggers to use local time.
7. Select the **Simple Query** button.
8. In Query Criteria, select the Message Type you wish the trigger to evaluate. The Message Type you chose determines the additional Query criteria that are available.

9. In any of the additional Query Criteria fields you wish to use, click in the field, then click ...
10. In the Edit list of values dialog box that opens, click in a row, then click ...
11. If the Select Type field is available, click ... to select an object type. A Select type dialog box opens to let you select an object type (such as apC Door).
12. The dialog box shows available objects of the type you selected. Click the check box to select one or more objects, then click **OK**.
13. Click **OK** again to confirm your selection.
14. Repeat these steps for any additional Query Criteria you wish to add.
15. Click **Save and Close** to save your Journal Trigger.

Simple Query Message Types and Criteria

See Journal Trigger Definitions for Simple Query Mode on Page 341 for a list of the Query Criteria available for a Simple Query.

Table 83: Message Types for Simple Query

Message Type	Criteria Available
Area Activity	Area Names - you can select the Areas that you want to query for activity.
Card Admitted	Personnel Names, Door Names, Direction, Escort Options, Area Names.
Card Rejected	Personnel Names, Door Names, Direction, Rejection reason, Escort Option, Area Names.
Video Guard Tour Activity	Tour Status, Monitor State.
High Assurance Reader Activity	High assurance reader actions.
Manual Action	Operators, Target Objects, Actions.
Object Changed State	Object, State Codes.
Operator Activity	Operators, Activity.
Operator Login	Operators, Actions.
System Activity	Starting and stopping of server and stunnel.
Visitor Management	Check-in and check-out actions for visitors. Check-in and check-out action type, name of a visitor, visits, stations that completed the check-in or check-out process, operators that completed the actions.

Configuring a Journal Trigger Advanced Query

You can configure an Advanced Query for a Journal Trigger.

To Configure a Journal Trigger with an Advanced Query

1. Create a new Journal Trigger (see Creating a New Journal Trigger or Template on Page 346).
2. Enter a name and textual description for the Journal Trigger in the **Name** and **Description** fields.

3. Select a **Target Event** for the Journal Trigger. This is the Event whose Journal Messages are queried to match with other criteria in the trigger.
4. You can adjust the **Evaluation Order** (Priority of the trigger). The default value is 75; the minimum is 1; the maximum is 200.
5. You need to select the **Schedule** for when this Journal Trigger should be evaluated. When the **Schedule** you chose is Active, the Journal Trigger evaluates incoming Journal messages.
6. You should identify the **Time Zone** to which you want the Schedule to apply. This is important if you have controllers in a different time zone than the C•CURE 9000 server, and you want the triggers to use local time.
7. Select the **Advanced Query** button.
8. Click **Add** to add a row to the Query Criteria table.
9. In the **Field** column, select the type of Journal Message you want to trigger on from the drop down box. For example, pick Object if you want to trigger on Journal Messages that are related to a specific object.
10. In the **Filter Type** column, select the type of filter you wish to define. For example, for an Object field, you can choose either **Equals**, **Not equals**, **In list**, which allows you to specify a list of objects, **Not in list**, or **In Query**.
11. In the **Value** column, click  to select the values to filter on. See for an explanation of the values available with each Field type.
12. If you want to define additional Query Criteria, click **Add** again and repeat the above steps. In addition, you can change the Operator column to choose the **And** operator, the **Or** operator, or **blank**.
13. If you want to group Query Criteria rows so that they are evaluated together, click **Add Block**. Three rows are added:
    - Begin block expression
    - A Query Criteria row
    - End Block.

    If you subsequently select the Query Criteria row and Click **Add**, you can add more Query Criteria rows to the block.
14. Click **Save and Close** to save your Journal Trigger.

Query Criteria Values for Advanced Queries

Table 84 on Page 349 shows the Query Criteria values that you can select.

NOTE If you configure a Journal Trigger that is activated by System Activity Messages, that Journal Trigger will ignore System Activity Messages generated by any Journal Trigger, so that Event looping conditions are not created.

Also, if you configure a Journal Trigger for a Primary Object Type of SoftwareHouse.Common.Objects.JournalTrigger, that trigger will never be activated, to prevent Event looping conditions.

Table 84: Query Criteria Values

Field	Values			
Message Type	Application Server Activity	Double Swipe	Journal Trigger Activity	Operator Activity
	Area Activity	Event Access	Log Message	Operator Login
	Card Admitted	Message	Log Migration Activity	State Change
	Card Rejected	Intrusion Zone Activity	Manual Action	Video Alarm
	Device Activity	Intrusion Zone Error	Network Video Activity	System Activity
	Device Error	Keypad Command Activity	Object changed State	System Error

Query Criteria Values (continued)

Field	Values
Journal Query Assistant	Area Activity, Card Admitted, Card Rejected, Manual Action, Object Changed State, Operator Activity, Operator Login
Last Modified Time	A drop-down calendar to let you choose the Date, and let you type in the Time value.
Message Date/Time	A drop-down calendar to let you choose the Date, and let you type in the Time value.
Object	An Object Selection dialog opens to let you choose an Object type and one or more objects of that type.
Object Type	An Object Selection dialog opens to let you choose one or more Object types
Partition	An Object Selection dialog opens to let you choose one or more Partitions.
Primary Object Name	An Object Selection dialog opens to let you choose an Object Type, and then a specific object from a list containing object of that type. **Example:** If you choose apC Input as the Object Type, a list of apC Inputs is displayed so that you can choose a specific apC Input.
Primary Object Type	An Object Selection dialog opens to let you choose an Object Type. **Example:** You choose apC Input as the Object Type if you want the Journal Trigger to Query for Journal Message about all apC Inputs.
Primary Partition Name	An Object Selection dialog opens to let you choose a Primary Partition Name from a list of Partitions. **Example:** If you choose Primary Partition Name, a list of Partitions is displayed so that you can choose a specific Partition.
Secondary Object Name	An Object Selection dialog opens to let you choose an Object Type, and then a specific object from a list containing object of that type. **Example:** If you choose Secondary Object Name, a dialog box displays the object types you can choose, and when you choose one, a list of objects of that type appears so that you can choose a specific object.
Secondary Object Type	An Object Selection dialog opens to let you choose an Object Type, and then a specific object from a list containing object of that type. **Example:** If you choose apC Input as the Secondary Object Type, a list of apC Inputs is displayed so that you can choose a specific apC Input.
Secondary Partition name	An Object Selection dialog opens to let you choose a Secondary Partition Name from a list of Partitions. **Example:** If you choose Secondary Partition Name, a list of Partitions is displayed so that you can choose a specific Partition.
Server Name	You can type in the C•CURE 9000 Server name that you want to look for in this Journal Trigger.
Server Date/Time	An Calendar control opens to let you choose a date, and the selected Date/Time appears. You can edit the date and time by clicking in the field and changing the numbers.

Pulsing an Event on a Card Reject from an Area

You can configure a Journal Trigger to pulse an Event each time when a Card is Rejected from a designated Area.

To Pulse an Event When a Card Reject in an Area Occurs

Create a New Journal Trigger (see Creating a New Journal Trigger on Page 346).

1. Click ... in the **Target Event** field to select the Event you want triggered.
2. You can set the **Evaluation Order** (the priority for the Trigger) by adjusting the **Evaluation Order** spinner up or down, or typing a value into the **Evaluation Order** field.
3. Select **Advanced Query**.
4. Click **Add** to add a row to the Query Criteria table.
5. For the **Field** column, select **Message Type**.
6. For the **Value** column, select **Card Rejected**.
7. Click **Add** to add another row to the Query Criteria table.
8. For the Field column, select **Object**.
9. For the Value column, click ... to open the Object Selection dialog box.
10. Click ..., then select **iSTAR Area**.
11. From the list of iSTAR Areas that appears, select the Area on which you want to trigger.
12. Click **Save and Close** to save the Trigger.

Pulsing an Event on a Device Error

You can configure a Journal Trigger to pulse an Event each time that a Device Error message appears in the Journal from one or more configured devices.

To Pulse an Event When a Device Error Occurs

1. Create a New Journal Trigger (see Creating a New Journal Trigger on Page 346).
2. Click ... in the **Target Event** field to select the Event you want triggered.
3. You can set the **Evaluation Order** (the priority for the Trigger) by adjusting the **Evaluation Order** spinner up or down, or typing a value into the **Evaluation Order** field.
4. Select **Advanced Query**.
5. Click **Add** to add a row to the Query Criteria table.
6. For the Field column, select **Message Type**.
7. For the **Value** column, select **Device Error**.
8. Click **Save and Close** to save the Trigger.

Pulsing an Event on a State Change

You can configure a Journal Trigger to pulse an Event each time when the Object State is changed for one or more objects (for example when one or more doors forced open).

When configuring a Journal Trigger the user can combine objects and their states, so the Trigger will pulse an Event when one of the conditions occurs.

To Pulse an Event When a State Change Occurs

1. Create a New Journal Trigger (see Creating a New Journal Trigger on Page 346).
2. Click ... in the **Target Event** field to select the Event you want triggered.
3. You can set the **Evaluation Order** (the priority for the Trigger) by adjusting the **Evaluation Order** spinner up or down, or typing a value into the **Evaluation Order** field.
4. Select **Simple Query**.
5. Select **Object Changed State** in the **Message Type** field.
6. Click in the **Object** field, then click ....
7. In the **Edit list of values** dialog box that appears, click ....
8. In the **Select Type** field, click ....
9. Select an **Object Type** (such as apC Controller), then select (☑) one or more objects of that type from the list that appears .
10. If you wish to select additional objects of a different type, click ... in the **Select Type** field, select another type, then select (☑) one or more objects of that type from the list that appears .
11. Click **OK** when you have selected all the objects you wish to query on.
12. The Edit list of values dialog box shows the objects you selected. Click **OK** to accept the list.
13. Click ... in the **State Codes** .field, then select (☑) one or more items in the Edit list of values dialog box. For example, you could select **Door forced** and **Door held** if you wanted a Journal trigger to activate an Event when these either of these two conditions occurred.
14. Click **Save and Close** to save the Trigger.

Pulsing an Event on an Intrusion Zone Error

The user can configure a Journal Trigger which will pulse an Event each time when the Intrusion Zone Error message came from one or more Zones.

To Pulse an Event When an Intrusion Zone Error Occurs

1. Create a New Journal Trigger (see Creating a New Journal Trigger on Page 346).
2. Click ... in the **Target Event** field to select the Event you want triggered.
3. You can set the **Evaluation Order** (the priority for the Trigger) by adjusting the **Evaluation Order** spinner up or down, or typing a value into the **Evaluation Order** field.
4. Select **Advanced Query**.
5. Click **Add** to add a row to the Query Criteria table.
6. For the **Value** column, select **Intrusion Zone Error**.
7. Click **Save and Close** to save the Trigger.

Pulsing an Event on a System Error

You can configure a Journal Trigger to pulse an Event each time a System Error message gets logged.

To Pulse an Event When a System Error Occurs

1. Create a New Journal Trigger (see Creating a New Journal Trigger on Page 346).
2. Click ... in the **Target Event** field to select the Event you want triggered.
3. You can set the **Evaluation Order** (the priority for the Trigger) by adjusting the **Evaluation Order** spinner up or down, or typing a value into the **Evaluation Order** field.
4. Select **Advanced Query**.
5. Click **Add** to add a row to the Query Criteria table.
6. For the Value column, select **System Error**.
7. Click **Save and Close** to save the Trigger.

12

Operator

This chapter explains how to configure C•CURE 9000 Operators.

In this chapter

Operator Overview

An Operator is a person who has the right to use access control Objects such as Readers, Doors, Inputs, Outputs and Schedules. An Operator gains entry to the system after successful Operator authentication on the domain or workgroup of which they are a part.

Operators are configured using the Operator Editor.

For more information about creating and using Operators, see:

- Operator Editor on Page 359.
- Operator Tasks on Page 368

The following are examples of Operators:

- **System Administrator** - The Operator responsible for:
  - Configuration and maintenance of all system hardware as well as common data in the configuration database.
  - Providing system-wide services such as system backup and restore.
- **Personnel Administrator** - The Operator responsible for the configuration and maintenance of the Personnel records in the configuration database.
- **Guard** - The primary Operator of the Monitoring Station.

A Privilege is a collection of rights to use access control Objects such as Readers, Doors, Inputs, Outputs, and Schedules. In C•CURE 9000 you use the **Privilege Editor** to create Privileges. You use the **Operator Editor** to assign Privileges to an Operator.

In C•CURE 9000 the **Schedule Editor** creates Schedules. You use the **Operator Editor** to associate a Schedule with each Privilege you assign to an Operator. When the Schedule is active and the Operator is logged in, the associated Privilege is active.

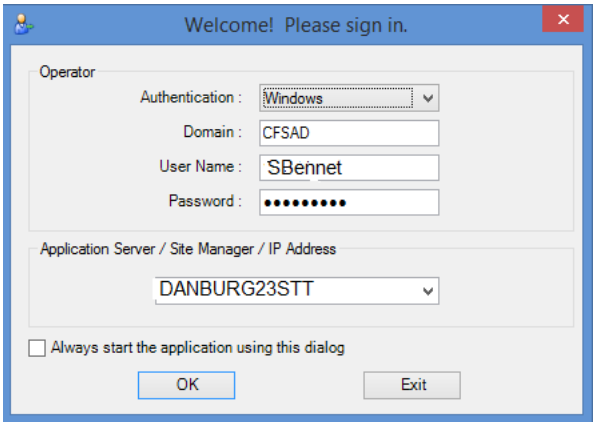
C•CURE 9000 also gives you the ability to configure and use Partitions in your system so different Operators can access only certain security Objects in their own sectors (Partitions). You assign Privileges and Schedules to Operators to allow them access to, or to limit their access to, the Objects associated with a particular Partition. For information on partitioning, see Partition Overview on Page 380.

Operator Authentication

Use the Operator Authentication section of the Operator window to configure users to log in to the C•CURE 9000 Administration Station or Monitoring Station applications with either (or both) of the following Operator authentication methods:

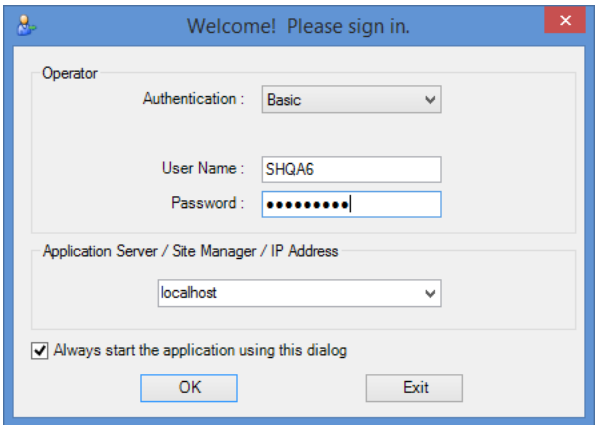
- **Windows Authentication**: Requires a username, domain name, and password to log in. You can optionally select the server or enter the server IP at Startup. If any of the fields are incorrect a warning is displayed and you can try to log in again.

Figure 114: Windows Authentication Login Screen



- **Basic Authentication**: Requires a username and password to log in. You can optionally select the server or enter the server IP at Startup. You must ensure the **Enable Enhanced Security** system variable is set to False in order to use Basic Authentication. See the Enabling and Disabling Basic Authentication on Page 356 for more information.

Figure 115: Basic Authentication Login Screen



NOTE

Operators must log in using basic authentication to print badges.

Basic Authentication can only be used if you enable it within System Variables.

Rules of Authentication

These are the rules of Operator authentication:

- If “SingleSignOn” is set to TRUE, you can log in to the Administration or Monitoring Station using the Windows Authentication method.
- If “SingleSignOn” is set to FALSE, click on either the Administration or Monitoring Station to display the Basic Authentication login window.
- If Basic Authentication is enabled and if you log out and log back in using Basic Authentication, the configuration file is updated to set “SingleSignOn” to FALSE. The next time you log in, Basic Authentication remains as the current authentication mode unless it is disabled.

Enabling and Disabling Basic Authentication

You can enable or disable Basic Authentication through the System Variables menu. You cannot log in using Basic Authentication if this System Variable has not been enabled.

Enabling and Disabling Basic Authentication

1. In the **Navigation** pane of the Administration Station, click the **Options & Tools** button.
2. Click the **System Variables** button.
3. Find the Enable Enhanced Security variable option.
4. Right-click on the Enable Enhanced Security variable option and click **Edit**.
5. You can now change the System Variable value.
   - Click **Yes** on the Verify dialog box to **disable** Basic Authentication.
   - Click **No** on the Verify dialog box to **enable** Basic Authentication.
6. Exit the System Variables window.

If you are using Basic Authentication, you can select the name of the server or the IP address of the server. You can select a previously-entered server from the drop-down box.

Check the **Always start the application using this dialog** check box if you want to display the dialog box at each log-in attempt.

The maximum length of the server name is 15 characters.

Basic Authentication Login Throttling

Operator accounts using Basic Authentication are temporarily locked if an incorrect username or password is used 5 times within a 5 minute period. You cannot attempt to login using the Basic Authentication method for 5 minutes after the fifth consecutive login failure. Each unsuccessful login attempt is logged in the Journal under the System Activity property. See Table 85: Login Throttling Scale for the throttling scale which applies to further failed login attempts.

NOTE If you successfully login after the lockout time elapses your attempt count is reset to 0.
If you are locked out from Basic Authentication you can still log in using your Windows Authentication login credentials.

Table 85: Login Throttling Scale

Login Attempts	Lockout Time
5 failed logins	You must wait 5 minutes before attempting to login.
5 subsequent failed logins	You must wait 15 minutes before attempting to login.
5 subsequent failed logins	You must wait 30 minutes before attempting to login.
5 subsequent failed logins	You must wait 60 minutes before attempting to login.

Unlocking a Locked Account

Locked Operator accounts can be unlocked by an Operator with the Unlock Operator Privilege and the View Operator Privilege, or a SYSTEM ALL privilege. See Privilege Overview on Page 416 for more information on how to assign privileges to Operators.

NOTE Operators with the Unlock Operator Privilege and View Operator Privilege can only unlock accounts in the same partition as their Unlock Operator and View Operator Privileges.

Manually Unlocking a Locked Account

1. Ensure the Operator performing the manual unlock has the correct privilege.

2. In the **Navigation** pane of the Administration Client, click **Configuration** to open the Configuration pane.
3. Select **Operator** from the Configuration pane drop down to display a Dynamic View of Operators.
4. Right-click on the column options above the Operators and click on the **Locked Out** option to display the locked/unlocked status of each Operator in the Dynamic View. The **Locked** checkbox is checked if an Operator is locked out.
5. Right-click on a locked Operator to open the Operator context menu. Click **Unlock** to unlock the Operator. The Operator account is unlocked and the Operator can attempt to log in again.

Operator Editor

The Operator editor in C•CURE 9000 lets you create and modify Operators so that they are able to access the Administration Client and Monitoring Station and perform functions according to operator privileges.

The following topics give more information about the Operator object and how to use it.

- Operator Overview on Page 355
- Operator General Tab on Page 360
- Operator Layout Tab on Page 361
- Operator victor Roles Tab on Page 363
- Object Editor Groups Tab on Page 26
- Operator User Defined Fields tab on Page 364
- Operator Web View tab on Page 364
- Operator State Images Tab on Page 365

An additional tab appears on a MAS or SAS in an Enterprise Architecture configuration.

- Application Server tab - see the Operator Applications Server Tab in the *C•CURE 9000 Enterprise Architecture Guide*

See Operator Tasks on Page 368 for a list of tasks you can perform using the Operator editor.

NOTE

To be able to run either the Administration Station or Monitoring Station application, an Operator must have at minimum a Privilege that provides Read access to their Operator record.

This can be accomplished by assigning one of the following:

- **SYSTEM ALL** Privilege.
- **Full Privilege for partition** for the Operator's home partition.
- A Privilege you create that gives Read access to the Operator class if you want the Operator to be limited (not granted Full access to all objects).

Accessing the Operator Editor

You can access the **Operator Editor** from the C•CURE 9000 Configuration pane.

To Access the Operator Editor

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

   - or -

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

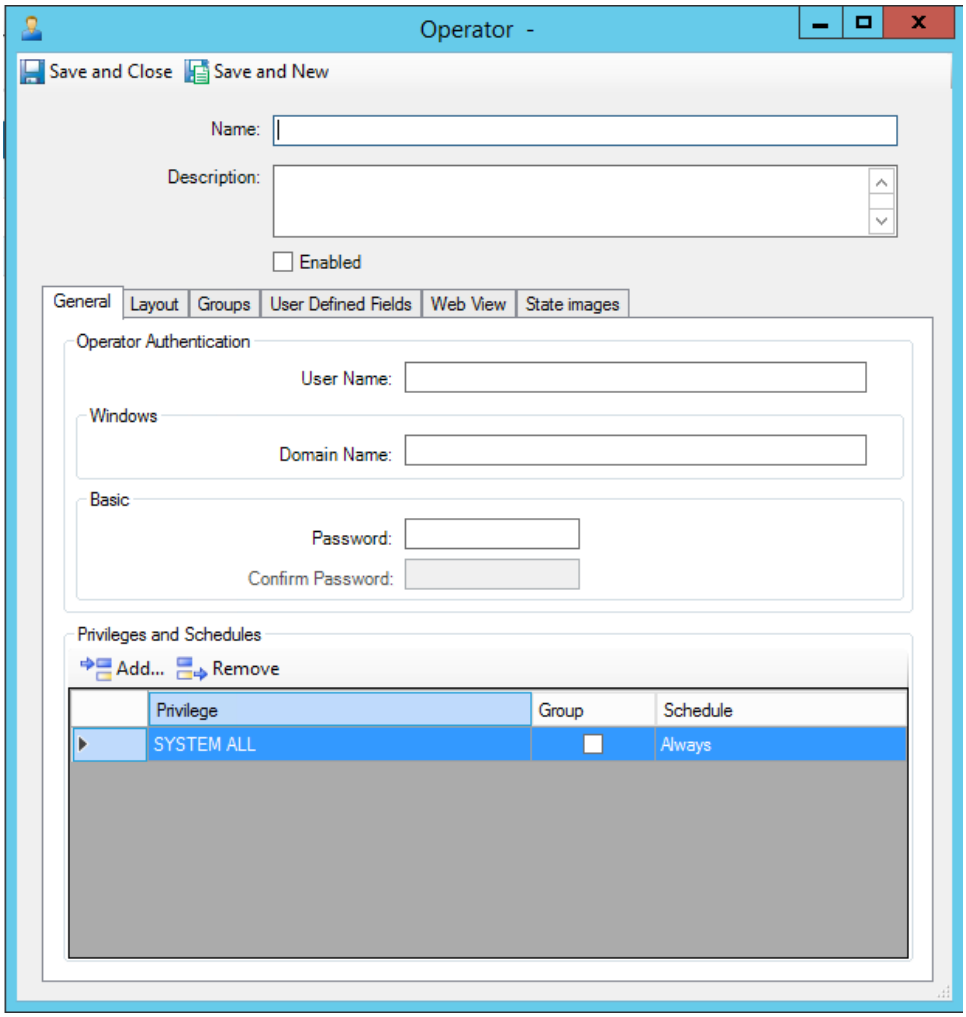
   The **Operator Editor** opens.

Operator General Tab

The Operator General tab, shown in Figure 116 on Page 360, lets you configure Operator Authentication as well as add or remove Privileges/Privilege Groups and Schedules.

If your system is Partitioned (has more than one Partition), the Operator's Partition appears on the Operator editor screen .

Figure 116: Operator Editor General Tab



Operator Editor General Tab Definitions

The Operator Editor has the buttons described in Table 86 on Page 360.

Table 86: Operator Editor Buttons

Button	Description
Save and Close	Click this button when you have completed any changes to the Operator and wish to save those changes. The Operator closes.
Save and New	Click this button when you have completed any changes to the Operator and wish to save those changes and also create a new Operator. The Operator you were editing is saved, and a new Operator opens (either blank or including template information if you were using a template to create the new Operator).

Table 86: Operator Editor Buttons (continued)

Button	Description
	Click this button when you want to close the **Operator 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.

The Operator Editor General tab has the fields and buttons shown in Table 87 on Page 361.

Table 87: Operator Editor - General Tab Fields

Fields/Buttons	Description
Name	Enter a unique name, up to 100 characters, to identify the Operator.
Description	Enter a description of the Operator, up to 255 characters.
Enabled	Select this check box to enable the Operator. Until this box is selected, the Operator cannot log into the Administration Client or Monitoring Station. NOTE: The Operator running the services cannot be disabled.
Partition	A read-only field displaying the name of the Partition to which this Operator belongs. (This field is visible only if the C•CURE 9000 system is partitioned.)
Operator Authentication	
Windows	**User Name** The Operator's Windows account user name. The maximum characters allowed is 20. You cannot use the following characters: / \ <> , : " : [] @ * + = ?. **Domain Name** The Windows domain name for the Operator's Windows user account. The maximum characters allowed is 15. You cannot use the following characters: / \ <> , : " : [] @ * + = ?.
Basic	**User Name** The Operator's Windows account user name. The maximum characters allowed is 20. You cannot use the following characters: / \ <> , : " : [] @ * + = ?. **Password** Enter a password for the Operator and confirm it. For more information, see Operator Authentication on Page 355.
Privileges and Schedules	
Add	Click to add a new row to select a Privilege and an associated Schedule for the Operator.
Remove	Click to remove a selected Privilege/Schedule row from the Operator.
Privilege	Specifies the Privilege to assign to the Operator. Click in the field to display the ... button. Then click this button to open a list of Privileges and Privilege Groups. Click an item in the list to assign that Privilege (or Privilege Group) to the Operator.
Group	This field is checked if a privilege group is added to an Operator. The check box is unchecked if an individual privilege is added to an Operator.
Schedule	Specifies the Schedule for the Privilege. Click in the field to display the ... button. Then click this button to see a list of Schedules.

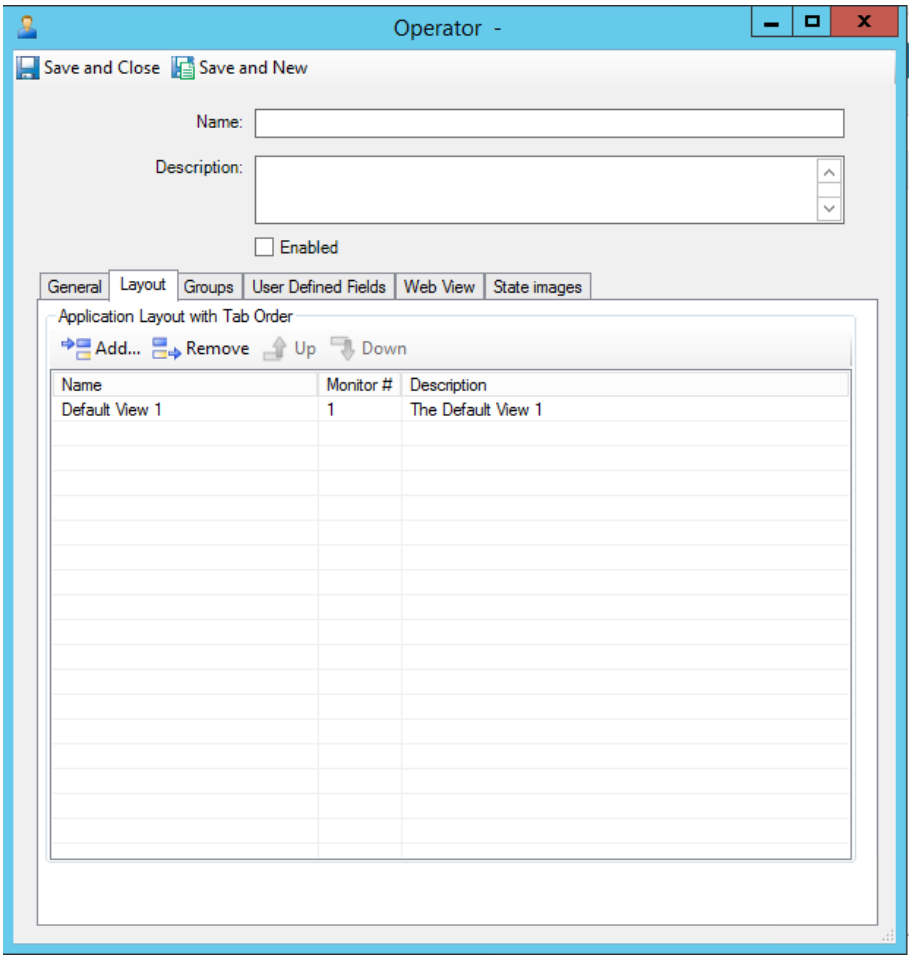
Operator Layout Tab

The Operator Layout tab, shown in Figure 117 on Page 362, lets you associate Layouts with an Operator.

An Application Layout (Layout) is a configurable C•CURE 9000 Object—an arrangement of viewers and toolbars—that defines the display of information on the Monitoring Station. You use the **Application Layout Editor** to create Layouts and this Operator Editor Layout tab to assign Layouts to an Operator. For information about assigning and removing application layouts from multiple Operators, see Assigning and removing application layouts from multiple operators on Page 377.

While an Operator can have many associated Layouts, the first Layout in the list is the primary Layout. The Monitoring Station always displays the primary Layout first.

Figure 117: Operator Editor Layout Tab



The Layout Tab has the following fields and buttons.

Table 88: Operator Editor - Layout Tab FieldsCarlos

Fields/Buttons	Description
Add	Click this button to open a list of Layouts to select for the Operator. You can select multiple Layouts at one time.
Remove	Click this button to remove a selected Layout row from the Operator.
Up	Click this button to move the selected Layout up in the list.
Down	Click this button to move the selected Layout down in the list
Name	A read-only field that specifies the name of the Layout.

Table 88: Operator Editor - Layout Tab FieldsCarlos (continued)

Fields/Buttons	Description
Monitor	To improve performance, you can assign Application Layouts to separate instances of the Monitoring Station application. The **Monitor** field lets you assign layouts to separate instances of the Monitoring Station. Click an entry in the **Monitor** column to assign a Monitor number. If all Applications Layouts are assigned to Monitor 1, one instance of the Monitoring Station opens. If there are Application Layouts assigned to additional **Monitor** numbers, additional Monitoring Station applications open when the Operator launches the Monitoring Station. If the Operator's system has multiple displays, the instances of the Monitoring Station are distributed as equally as possible to each display (for example, if there are 3 displays and 4 **Monitors** defined, the fourth **Monitor** opens on the primary display). The default value for **Monitor** is 1. The maximum value is 10. **Example:** An Operator has a system with three displays. The Operator has three Application Layouts assigned: • Default Application Layout assigned to **Monitor** 1. • Default View 1 assigned to **Monitor** 3. • Dual phase event acknowledgement layout assigned to **Monitor** 2. When the Operator launches the Monitoring Station, three instances of the Monitoring Station open. One will show the **Default Application Layout**, the second will have **Dual phase event acknowledgement Layout**, and the third will show **Default View 1**. Because the Operator's system has three displays, the first instance of the Monitoring Station opens on the primary display, the second instance of the Monitoring Station opens on the second display, and the third instance opens on the third display.
Description	A read-only field that describes the layout.

Operator victor Roles Tab

Use the operator **victor Roles** tab to assign victor roles to an operator. A victor role is a set of access rights that you can assign to an operator to control authorization and permission levels within victor. You can be customize each victor role the victor user interface, with the exception of the Administrator role. Any victor role that you create and configure in victor is available in C•CURE 9000 where you can assign the role to an operator.

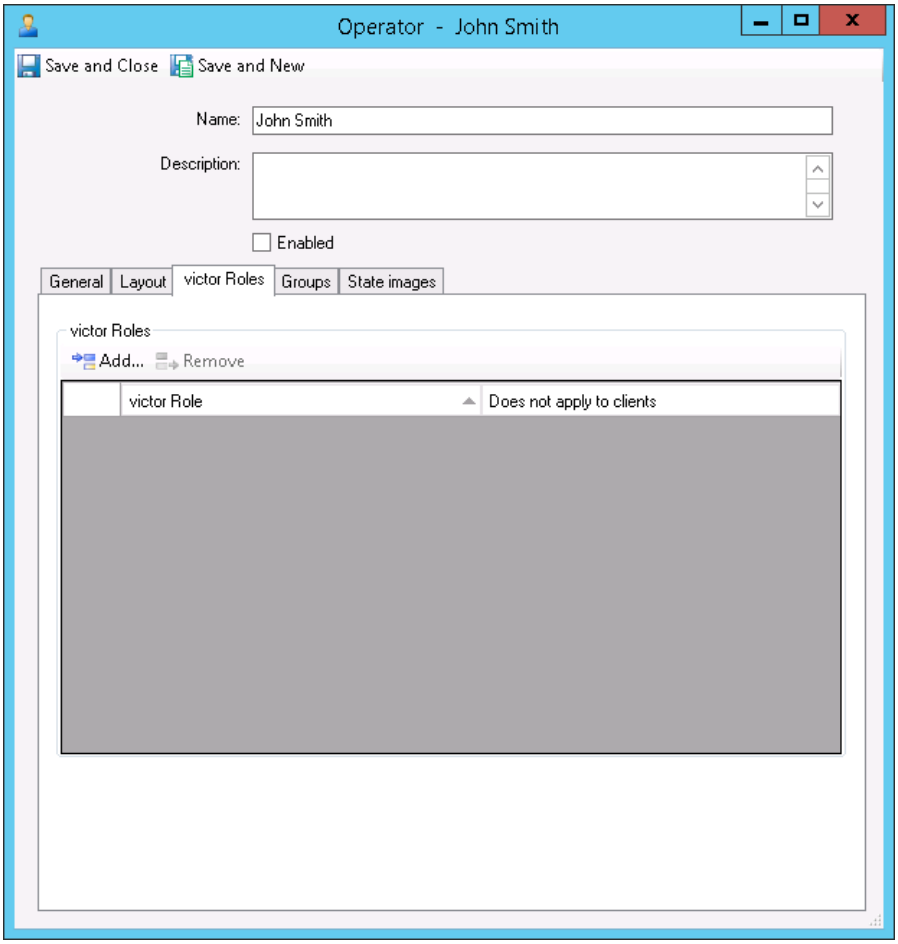
For more information about victor roles, see the *victor unified client Configuration and User Guide*.

Note The Privilege and role interaction in the unified system determines the operator's access to victor permission levels. For more information see Privilege and victor Role Interaction in a unified system on Page 420

There are 6 predefined victor roles (descending permission level):

- Administrator
- Power User
- Investigator
- Basic operator
- Guard
- Viewer

Figure 118: Operator victor roles Tab



Operator User Defined Fields tab

Use the **User Defined Fields** tab to modify user-defined fields (UDFs) that apply to the Operator. See User-defined Fields Editor on Page 502 for more information on UDFs.

Edit global operators that have existing mandatory SAS UDFs on the MAS or SAS where you originally configured them. If using more than one SAS, edit the UDF on the MAS.

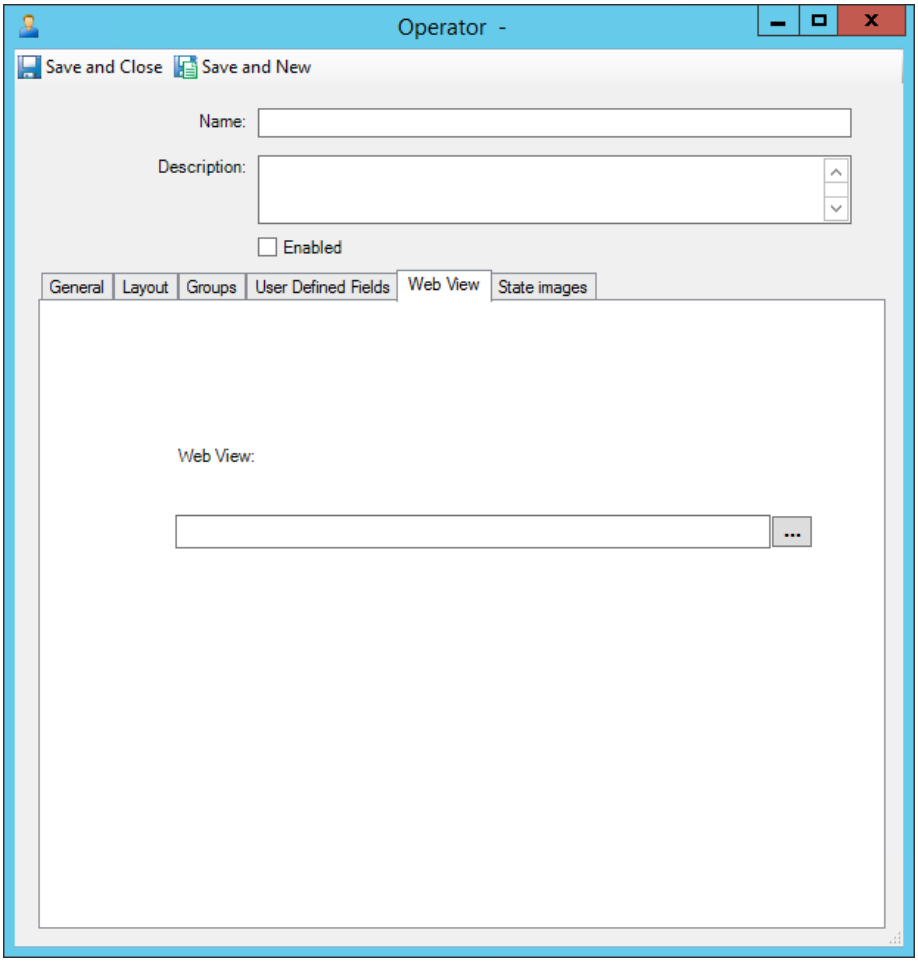
NOTE Victor does not work with UDFs. Do not create mandatory UDFs for victor, as they will not work correctly with the victor system.

Operator Web View tab

Use the **Web View** tab to associate a Web View with an operator. With the Web Views editor, you can change the appearance of the C•CURE 9000 web-based client for different operators. In the C•CURE 9000 web-based client you can visually use the interface itself to select what features should be exposed for the operator.

Click the options icon on the **Web View** tab, then select the C•CURE Web View you want to associate with this operator, and then click **Save and Close**.

Figure 119: Operator Editor Web View Tab



See the *C•CURE 9000 web-based client Guide* for more information.

Operator State Images Tab

This tab, shown in Figure 120 on Page 366, displays the current Operator state images that display in the Monitoring Station to represent activities concerning Operators. The default state images for C• CURE 9000 Operator states are defined in Table 89 on Page 366. You can select other images to display for this Operator or return to the default images, as described in the procedures below.

Figure 120: Operator Editor State Images Tab

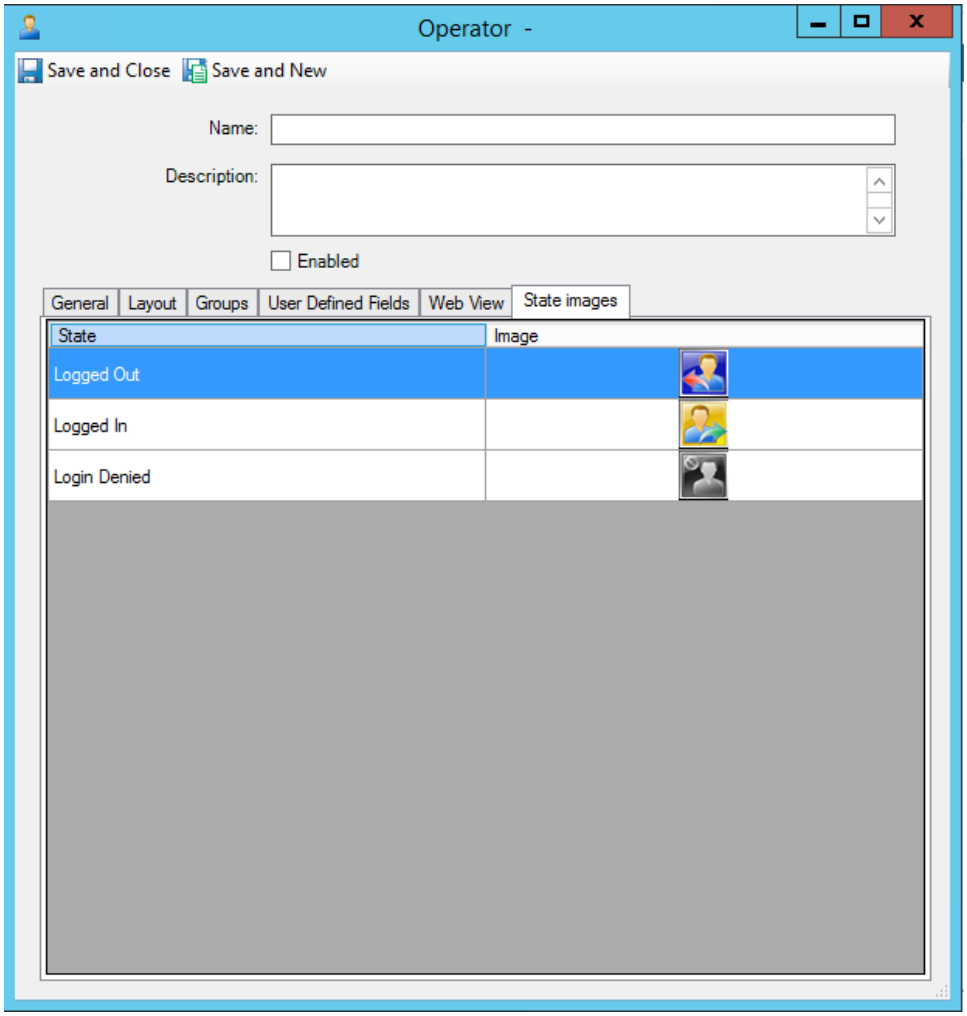


Table 89: Operator Editor State Images Tab

Image	State
	Logged Out
	Logged in
	Login Denied

To Replace an Image for a Specific Operator

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

The new image replaces the default image and displays in the **State Images** tab.

To Restore the Default Image

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

Operator Tasks

You can perform the following tasks using the Operator editor:

- Accessing the Operator Editor on Page 359
- Creating an Operator on Page 368
- Creating an Operator Template on Page 370
- Viewing a List of an Object Type on Page 22
- Modifying an Operator on Page 371
- Deleting an Object on Page 25
- Setting a Property for an Object on Page 25
- Adding Operators to a Group on Page 376
- Adding a Privilege Group to an Operator on Page 376.
- Assigning a victor role to an operator on Page 377
- Assigning and removing application layouts from multiple operators on Page 377

Creating an Operator

You can create a new Operator for your system and configure his/her information as described in the following procedure. This procedure is for configuring an Operator for a C•CURE 9000 system that is **not partitioned**.

For information on configuring an Operator for a **partitioned** C•CURE 9000 system, see:

- Creating an Administrator for a Partition on Page 398
- Creating Other Operators for a Partition on Page 398
- Giving Operators Access to Different Partitions on Page 400
- Changing Your Operator 'New Object Partition' on Page 414.

For general partitioning information, see Partition Overview on Page 380.

Creating an Operator

1. In the Navigation Pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Operator** from the **Configuration** pane drop-down list.
3. Click **New** to create a new Operator. The **Operator Editor** where you can configure the setup for this Operator opens with the **General** tab displayed.
4. On the top of the editor, enter a name and, optionally, a description to identify this Operator and select the **Enabled** check box (according to the information in Operator General Tab on Page 360).
5. Configure **Windows** or **Basic Authentication** for the Operator using the Authentication box.
   a. Configure **Windows authentication**:
      — Enter the Operator's Windows account User Name in the User Name field.
      — Enter the Domain Name for the Windows account in the Domain Name field.
   b. Configure **Basic authentication**:
      — Enter a user name in the User Name field.

— Enter a password in the Password field. The first time you log-in you must enter a password and confirm it. For subsequent log-ins you can enter the chosen password.

NOTE You can configure both Windows and Basic Authentication. If Basic Authentication is enabled in System Variables, you can choose which authentication to use when logging in.

c. In the Privileges and Schedules box,

— If you do not want this Operator to have privileges to everything in the entire system, delete the "SYSTEM ALL" Privilege by selecting the row and then clicking **Remove**. (This default privilege is given automatically to all new Operators in an unpartitioned system.)

— Click **Add** to add a new empty Privilege/Schedule row for the Operator.

— In this new row, click in the Privilege field and then click the  button to select a Privilege or Privilege Group for this Operator from the Privilege list that displays.

— In the same row, click in the Schedule field and then click the  button to select the Schedule you want to associate with the previously selected Privilege from the Schedule list that displays.

— Select a row and click **Remove** to delete any existing Privilege/Schedule that you do not want this Operator to have.

— Repeat these steps for each new operator.

6. If you want this Operator to use the C•CURE 9000 Monitoring Station, click the Layout tab to open and do the following (according to the information in Operator Layout Tab on Page 361):

• In the **Application Layout with Tab Order** box,

— Click **Add** to select an Application Layout for the Operator from the **Application Layout** list that displays.

— Click **Remove** to delete any existing Application Layout(s) that you do not want this Operator to have.

— Repeat these steps as many times as necessary.

7. You can assign a **Monitor** number to each Application Layout if you want to the Operator's Application Layouts to open in more than one instance of the Monitoring Station (can improve performance in some cases). Click in the **Monitor** column and adjust the number. See Operator Layout Tab on Page 361 for more information about the **Monitor** field.

Example:

If you assign an Operator three Application Layouts, and give each layout a different Monitor number, when the Operator launches the Monitoring Station, three separate instances of the Monitoring Station will open, each with one Application Layout.

8. If you want to change any of the default State images that display on the Monitoring Station for the Operator you are configuring, click to open the **State images** tab.

• Make any changes according to the information in Operator State Images Tab on Page 365.

9. Before saving the new Operator object, make sure you selected the **Enabled** check box in the top of the editor.

NOTE The **Enabled** option must be selected for the Operator to be able to log into the Administration Client or the Monitoring Station.

10. To save your new Operator, click **Save and Close**.

- or -

Alternatively, if you want to save the Operator and then create a new one, click **Click and New**. The current Operator is saved and closed, but the **Operator Editor** remains open to allow you to create a new Operator.

Creating an Operator Template

You can create a new template for an Operator. An Operator template saves you time because you do not have to re-enter the same operator information again. You can also create a new Active Operator Template which can be configured across multiple Operators. An existing template can also be saved as an Active Operator Template.

To Create an Operator Template

1. In the **Navigation** Pane of the Administration Client, click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Operator**.
3. Click the down-arrow on the **New** button, and click **Template**. The **Operator Editor** where you can configure the Operator template opens.
4. Configure the template to meet your requirements. Any fields for which you configure values become part of the template; then when you subsequently create a new Operator from that template, these values are already filled in.
5. In the **Name** field, enter the name you wish to use for the template

   Example:

   AdminOpTemplate1
6. To save the template, click **Save and Close**. The template will be available as an option on the pull-down menu on the **New** button in the **Configuration** pane.

To Create a new Operator Active Template

1. In the **Navigation** Pane of the Administration Client, click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Operator**.
3. Click the down-arrow on the **New** button, and click **Active Template**.The **Operator Editor** where you can configure the Operator Active Template opens.
4. Configure the template to meet your requirements. Any fields for which you configure values become part of the template; then when you subsequently create a new Operator from that template, these values are already filled in.
5. When you create a new Operator from the Active Template you can only change the following fields in the Operator Editor:
   - Name
   - Description
   - Enable
   - User Name
   - Domain Name
   - Password (if applicable).
6. In the **Name** field, enter the name you wish to use for the template.

   Example:

   AdminOpTemplate1
7. To save the template, click **Save and Close**. The template will be available as an option on the pull-down menu on the **New** button in the **Configuration** pane.

Viewing a List of Operators

You can display a list of the Operators you have created by opening a Dynamic View of Operators. See Viewing a List of an Object Type on Page 22 for more information.

Operator List Context Menu

The context menu that opens when you right-click an Operator in the Operator Import Dynamic View includes the selections described in Using the Object List Context Menu on Page 23.

Modifying an Operator

You can modify an existing Operator by editing it using the **Operator Editor**.

To Modify an Operator

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

   - or -

   Double-click the Operator you want to change.

   The **Operator Editor** opens for you to edit the Operator making changes as you wish in the fields on the top of the editor, and on the **General**, **Layout**, and **State images** tabs.
5. If you want to see which Groups the Operator is a member of or to edit any of these groups, click to open the **Groups** tab. (See the information in Object Editor Groups Tab on Page 26.)
6. To save the modified Operator, click **Save and Close**.

   - or -

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

Setting a Property for an Operator

You can use **Set Property** to set properties for Operators. Set Property enables you to quickly set a property for an Operator without opening the Operator Editor. You use Set Property for mass updates.

To Set a Property for Operators

1. In the Navigation Pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Operator** from the Configuration pane drop-down list.
3. Click  to open a Dynamic View showing all Operator objects.
4. Right-click the Operator 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 Operator. 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 operator** message box.

Add Privileges to Multiple Operators

The Operator Dynamic View has context menu items that allow you to change the privileges of multiple operators at once: **Assign Privileges** and **Remove Privileges**.

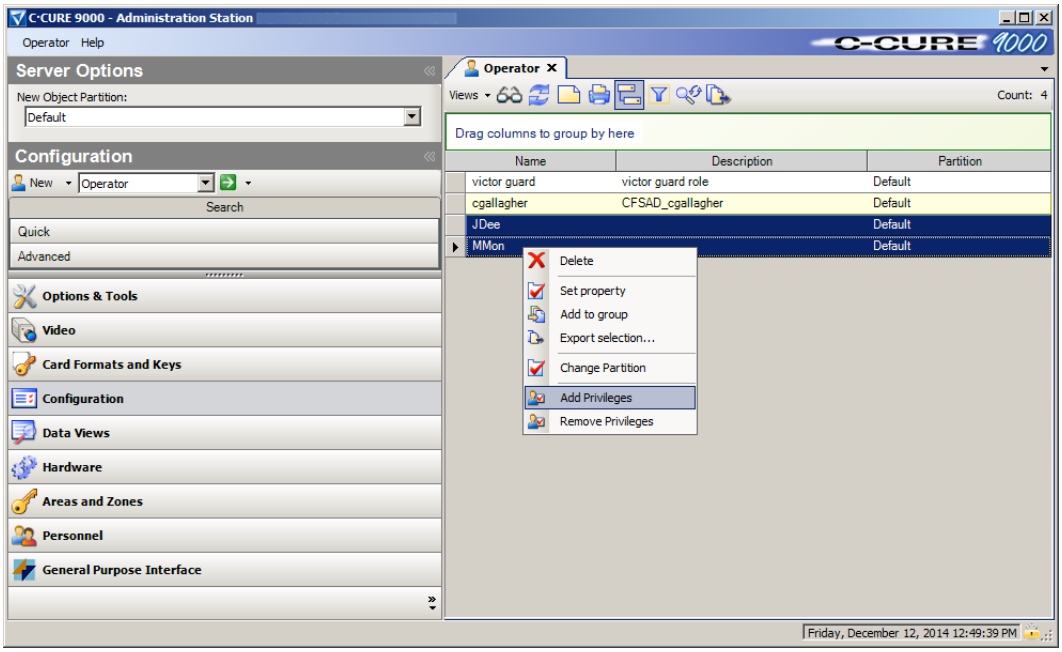
The following rules apply to assigning Operator privileges:

- Operators with duplicate privileges and schedules are rejected.
- Operators must have at least one privilege.
- If validation of a privilege fails for any reason, none of the updates of that Operator's privileges are applied.

To Add Privileges to Multiple Operators

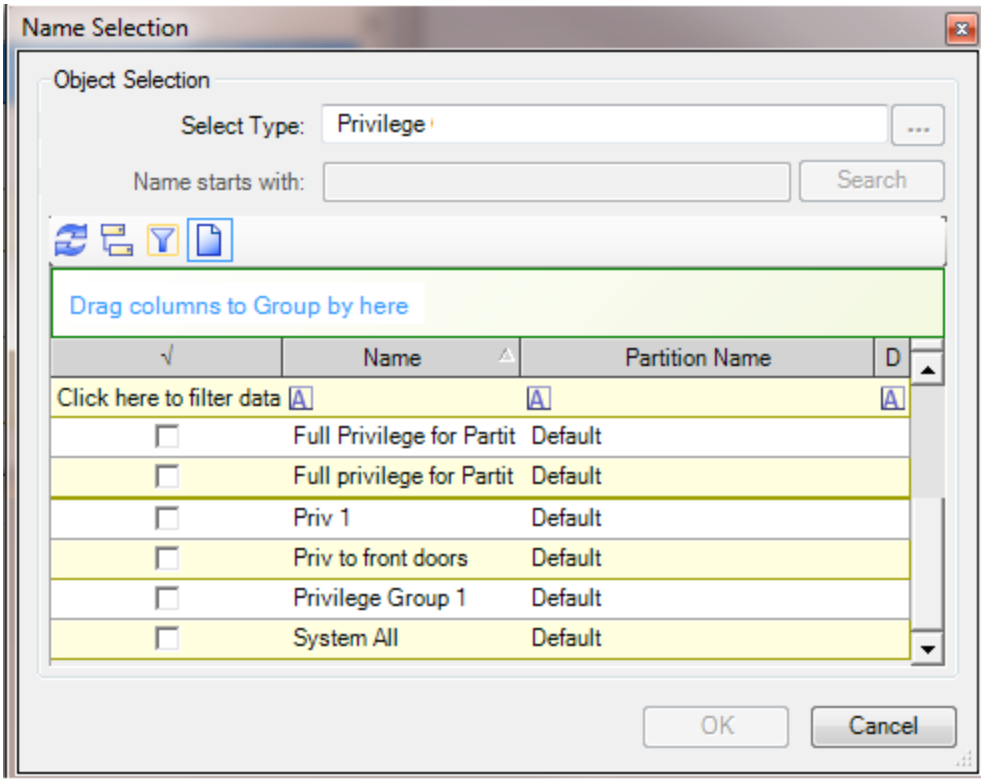
1. In the Navigation pane of the C•CURE 9000 Administration Workstation, click **Configuration.** The **Configuration** pane opens.
2. Select **Operator** from the drop-down menu and click on . The Dynamic View appears listing the Operator names. Select the names of the Operators to which you want to assign privileges.
3. Right-click on the selection and select **Add Privileges** from the context menu.

Figure 121: Add Privileges to Multiple Operator



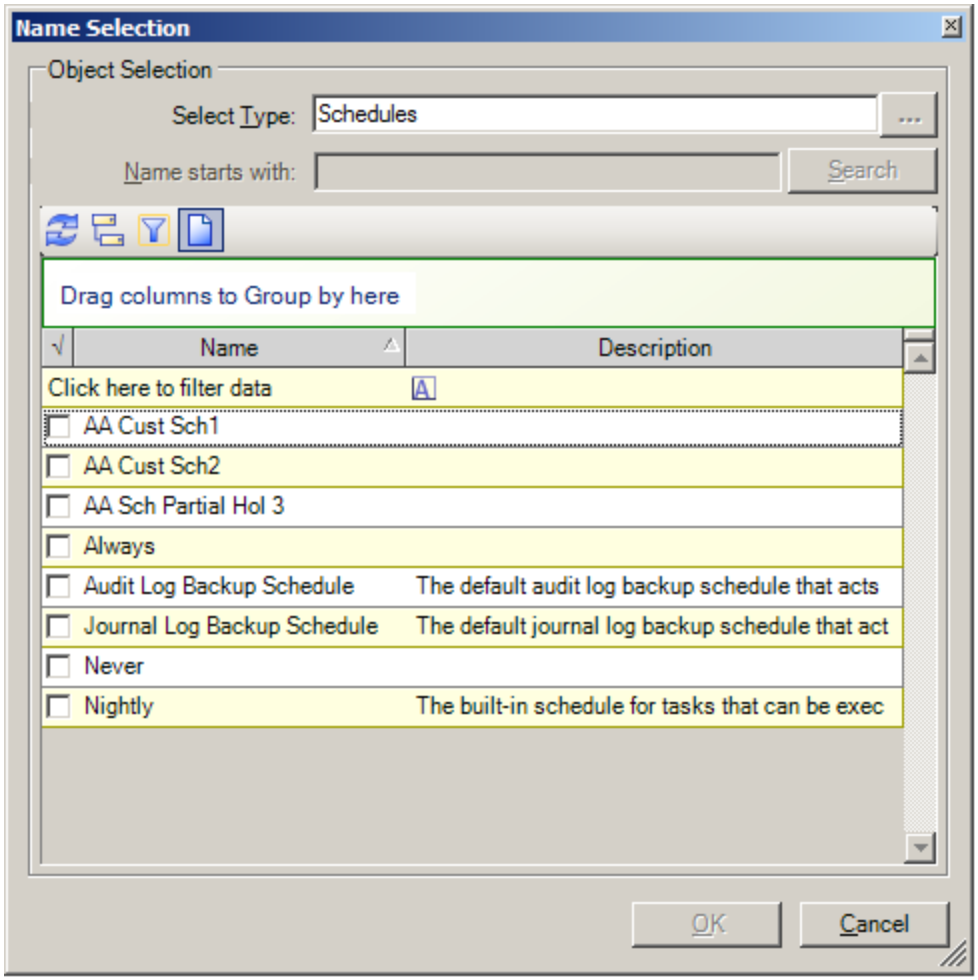
4. When you select **Add Privileges**, a selection control appears which allows you to select privileges or privilege groups and schedules. Select the privileges or privilege groups to assign them to the selected operators.

Figure 122: Selection Window for Privileges and Privilege Groups



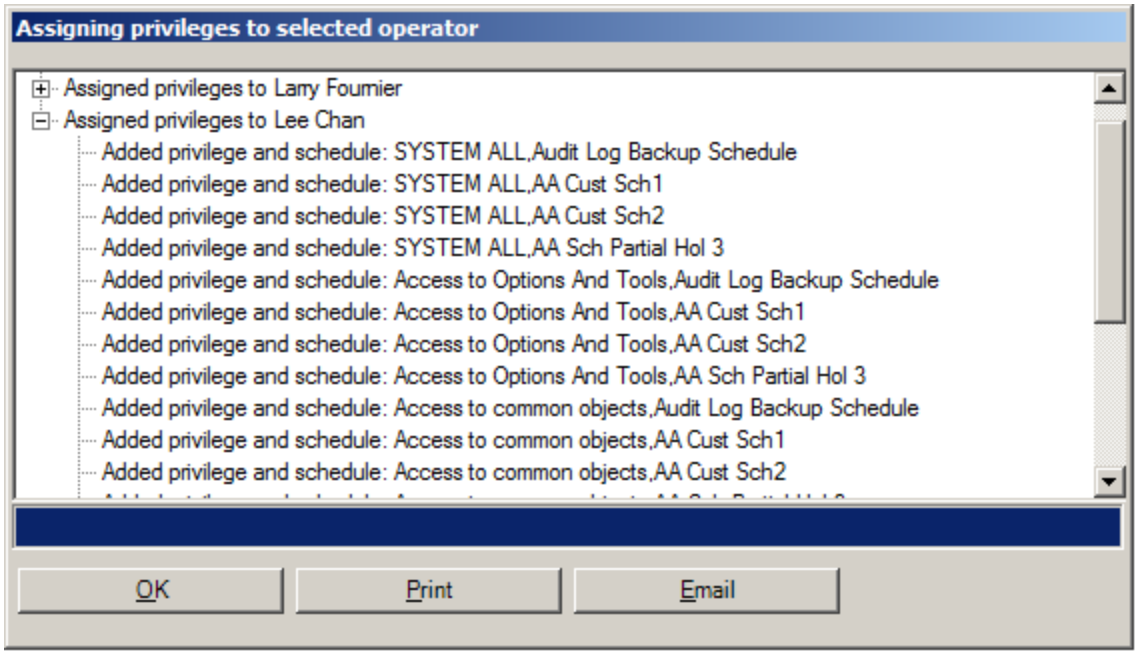
5. For selected Operators, assign a schedule. Click **OK**.

Figure 123: Select a Schedule for Operator Privilege



As C•CURE 9000 processes the adding of privileges, a progress window displays. When the assigning is complete, the **Assigning privileges to selected Operator** window appears:

Figure 124: Window for Adding Privileges



6. Click **OK**. The**Assigning privileges to selected Operator** window displays whether the Privilege was added, and if not, why it was not added.

Removing Privileges from Multiple Operators

The Operator Dynamic View has context menu items that allow you to change the Privileges of multiple Operators or groups at once.

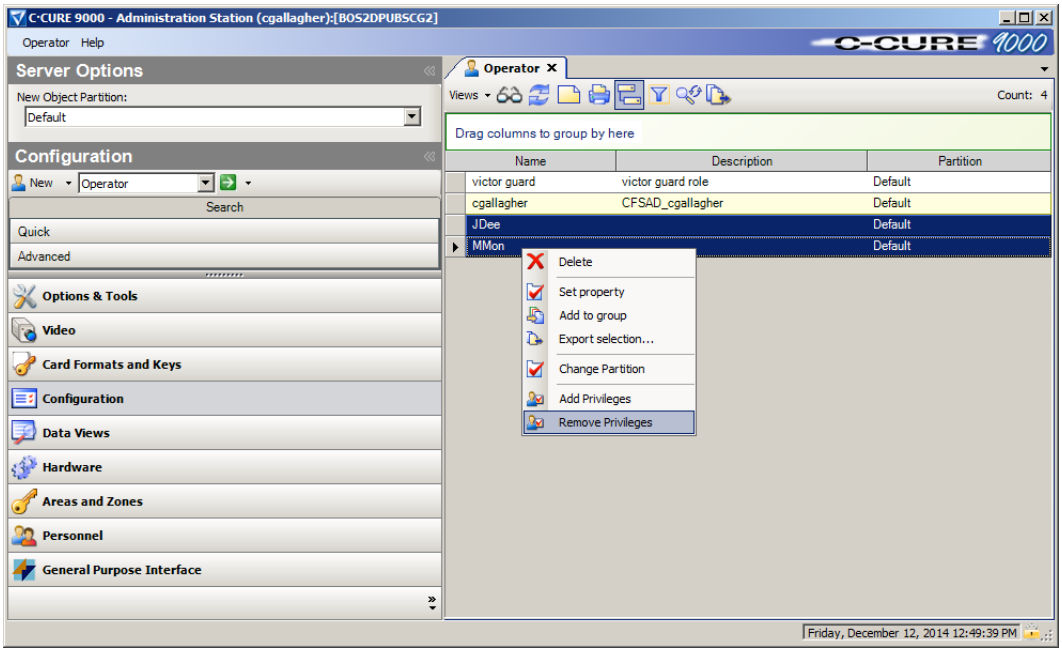
The following rules apply to removing Operator privileges:

- If you remove, for example, Priv 1, all Operator privilege pairs are removed where the privilege ID is Priv 1.
- The Remove operation does not remove privilege groups if they contain Priv1.
- The Remove Privileges menu item is unavailable if the current Operator is one of the selected Operators, in other words, you cannot remove privileges from yourself.

To Remove Privileges from Multiple Operators

1. In the Navigation Pane of the Administration Workstation, click **Configuration** to open the Configuration pane.
2. Select **Operator from the drop-down menu,** click . The Dynamic View appears listing the Operator names. Select the names of the Operators from which you want to remove privileges.
3. Right-click and select **Remove Privileges** from the context menu (see Figure 125 on Page 376).

Figure 125: Remove Operator



When you select **Remove Privileges**, a selection control appears which allows you to select the privileges or privilege groups and schedules you want to remove. Select the privileges or privilege groups to remove them from the selected Operators.

4. As C•CURE 9000 processes the removing of privileges, a progress window displays. The Progress window displays whether the privilege was removed or if there was nothing to remove.

Adding Operators to a Group

You can use **Add To Group** for an Operator. Add Operator To Group enables you to add the Operator Object to a Group.

To Add Operators To a Group

1. Make sure that the Group is already configured for the Operator to be added to it.
2. In the Navigation Pane of the Administration Client, click **Configuration** to open the Configuration pane.
3. Select **Operator** from the Configuration pane drop-down list.
4. Click to open a Dynamic View showing all Operator Objects.
5. Right-click the **Operator** in the list that you want to add to a Group and select **Add To Group** from the context menu.
6. When the **Group** list displays, select the Group to which you want to add the Operator.
7. Click **Save and Close** to save your changes.

Adding a Privilege Group to an Operator

You can create a Group of Privileges and assign the Group to an Operator.

To Add a Privilege Group to an Operator

1. In the Navigation Pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Operator** from the Configuration pane drop-down list.
3. Click  to open a Dynamic View showing all Operator Objects.
4. Double-click the **Operator** in the list that you want to edit.
5. The Operator editor opens. On the General tab, click **Add...** in the Privileges and Schedules table.
6. Click in the **Privilege** field and click  to select a Privilege.
7. Click  to display Privilege Groups.
8. Click the **Privilege Group** you wish to add.
9. Click in **Schedule** and select a schedule for the Privilege Group.
10. Click **Save and Close** to save your changes.

Assigning a victor role to an operator

Use the Operator Editor to assign a victor role's permission rights to an operator.

Note The Privilege and Role interaction in the unified system determines the Operator's access to victor permission levels. For more information see Privilege and victor Role Interaction in a unified system on Page 420

To add a victor Role to an Operator

1. In the navigation pane of the C•CURE 9000 Administration Client, click the **Configuration** button.
2. Click the **Configuration** list
3. Select **Operator** from the drop-down list.
4. Click **New**

   - or -

   Click  to open a Dynamic View that displays a list of all existing Operator Objects, right-click the Operator that you want to change, and select **Edit** from the menu.
5. Click the **victor Roles** tab.
6. Click **Add...** in the **victor Roles** table.
7. Select a victor role from the list and click **OK**.
8. Select **Save and Close** to save your changes.

Assigning and removing application layouts from multiple operators

Use the context menu options in the Operators Dynamic Views pane to add and remove application layouts from multiple Operators. You can also use the Operator editor **Layout Tab**, to assign application layouts to individual Operator records, see Operator Layout Tab on Page 361

To assign and remove application layouts from multiple operators

1. Open the **Operator Dynamic Views** pane.

2. Hold the **Ctrl** or **Shift** key, and select the Operators that you want to assign the application layouts to.
3. Right-click, and select **Add Application Layouts** or **Remove Application Layouts** from the context menu.
4. Select the application layout, or layouts, that you want to assign or remove.
5. Click **OK**.

NOTE If you use the context menu to add an application layout or layouts to an operator or operators, every application layout is added with Monitor value set 1. Therefore, it displays on Monitor 1. To change the monitor value for an added application layout, you must edit each individual Operator's record individually using the Operator editor.

13

Partitions

This chapter explains how to configure and use Partitions in C•CURE 9000 so different Operators can access only certain security Objects in their own sub-divisions (Partitions).

In this chapter

Partition Overview

Partitioning allows you to create different sub-divisions, *Partitions*, for your C•CURE 9000 system and to separate security Objects into these different Partitions for both creation and viewing. Each Partition you create will have an ID and name. Using Privileges, you can then allow an Operator access, or limit his/her access, to the Objects associated with a particular Partition or multiple partitions.

Setting Up and Using Partitions

For more information about Partitioning, see:

Operator Access to a Partition

To have any access to any Object in a Partition, an Operator must have either

- System All Privilege.
- A Privilege from a Partition that defines access to Objects in the selected Partition, or multiple Partitions if selected.

Through Privileges, Operators can have access to more than one Partition and an Operator can have a Privilege which spans multiple Partitions. But every Operator is assigned to a Partition, and this Partition is used as his/her primary **New Object Partition**. (The **New Object Partition** is the Partition to which any Objects that person creates are assigned.)

NOTE System Backup and Restore are **not** partitioned. The system administrator is responsible for backing up and restoring the entire database for C•CURE 9000. (For a list of non-partitioned system Objects, see Non-partitioned Objects on Page 383.)

When to Use Partitioning

Not all C•CURE 9000 systems will require partitioning to be used. If only one Partition is defined—the "Default Partition" set up by installation, the system is considered a **non-partitioned** system. A system will be considered **partitioned**, if it has more than the Default Partition.

Partitioning, in conjunction with privileges, can support the following customer models:

- **Multi-tenant facility** – One or more buildings controlled by a single C•CURE 9000. This facility has more than one tenant, and each tenant wants to manage the access control for their office space. The landlord administers the remainder of the system, the common data such as lobby doors and their clearances. The landlord acts as the system administrator, while each tenant assigns a person to act as administrator of the Partition.
- **Campus** – A single organization occupying one or more buildings, which are controlled by a single C•CURE 9000. The organization is divided into departments and each department wants to administer their own access control. A central security office acts as the system administrator, administering the common data in the system and providing system-wide services such as system backup and restore. The department heads administer their own Partitions.

Setting Up Partitioning

Setting your C•CURE 9000 system up to utilize partitioning requires the following steps:

1. Read the Partition overview in this chapter to acquire an understanding of how partitioning works in C•CURE 9000.
2. Create the Partitions your organization needs. For information, see Partition Editor on Page 386 and Partition Tasks on Page 391.

NOTE Only System Administrators, those with the SYSTEM ALL privilege, can create a Partition.

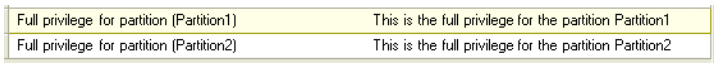
3. Create Privileges for the different Partitions with the permissions necessary to administer and monitor all the organization's Partitions. For information, see Partition Overview on Page 380.
4. Create the Operators you need for each of the Partitions and assign them the requisite Privileges for specific daily/weekly schedules. For information, see Partition-related Tasks on Page 398 and Operator Overview on Page 355.

Results of Creating a Partition

When you create a new Partition for your C•CURE 9000 system, the following occurs:

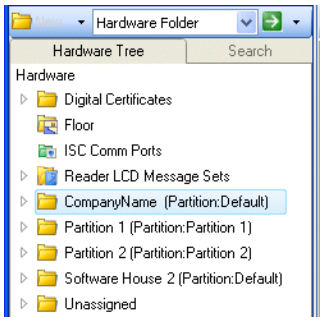
1. A new ALL Privilege for that Partition called "Full privilege for partition (partition name)" is created.

   Example:



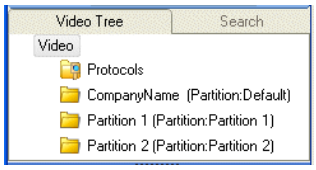
2. A new hardware folder is created for that Partition. It is given the name of the Partition, but the name can be changed.

   Example:



3. A new Video folder is created for that Partition. It is given the name of the Partition, but the name can be changed.

   Example:



Privileges Related to Partitioning

- "Full privilege for partition (Partition X)" gives an operator full access to all of the following:
  - Objects in that Partition
  - Non-partitioned objects

- 'Access to common objects' Privilege has the permissions for objects in the 'Default' Partition as detailed in Access to Common Objects on Page 418

NOTE The 'Access to common objects' Privilege or a Privilege based on its template is required for a Partition Operator to log in to the C•CURE 9000.

Objects and Partitions

In a C•CURE 9000 with more than one Partition, an Object name must be unique **only** within its Partition, not across the entire system. For such partitioned systems, the display of Object names sometimes contains the name of the Partition.

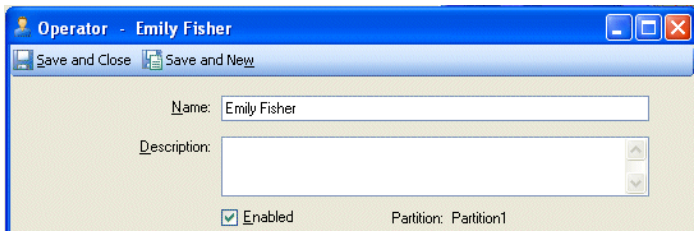
NOTE The ***unique*** fields on the **Personnel Customer** tab, **Text12** and **Int6**, must be unique within their Partition. This includes instances where you change the Partition of personnel records. The record does not save if an existing record in the new Partition has the same value in these fields.

However, the following are unique across the whole system:

- CHUIDs (Card Holder Unique Identifiers)
- IP addresses

Display of Partition and Object Names

- If an Object is partitioned, the Partition name displays in the Object's Editor as a read-only field. (This field is visible only if the C•CURE 9000 system is partitioned—has more than one Partition.)



- In Dynamic Views, if an Object from another class is named, the Partition name is included.

  Example:

  In the **Credential** list, the **Badge Layout Name** includes the Partition.

Name	Displayable CHUID	Card number	Badge Layout Name
Daly, Bill	0000000012	12	Standard1 [Partition1]
Rosenthal, Noel	0000369092	369092	Standard1 [Partition1]
Harris, Harold	0000002345	2345	Custom23 [Partition1]

- Partition is also available as a field you can select to display in the Dynamic Views.
- For Reports, if an Object from another class is named, the Partition name is included.
- For Editors with grids containing references to other objects, the Partition name is included.

  Examples:

  Clearances tab on the **Personnel Editor Triggers**
  tab on the **Door Editor**, **Event Editor Group Editor**

- For Journal and Audit replay:
  - Partition names of the Objects display in the text message.
  - You can select the Partition Name of the primary and secondary Objects to display in the Dynamic Views.

Parent and Child Objects

Child Objects always have the Partition ID of their parents. Table 90 on Page 383 lists the parent Objects with their child Objects.

Table 90: Parent/Child Objects

Parent Object	Child Object
Personnel	Credentials, Images
apC	apC Inputs, apC Outputs, apC Readers, apC Door, apC Elevators, apC Main Board, apC I32 Input Board, apC I8 Input Board, apC R48 Output Board, apC R8 Output Board
iSTAR	iSTAR Inputs, iSTAR Outputs, iSTAR Readers, iSTAR Doors, iSTAR Elevators, iSTAR ACM Boards, iSTAR Input Boards, iSTAR Output Boards
Badge Layout	Images
Cluster	Comm Methods, iSTARs
Video Servers	Video Cameras
CCTV Switches	CCTV Cameras

Non-partitioned Objects

The following C•CURE 9000 security Objects are not partitioned:

- Time Zones
- Logical Elevator Floors*
- Digital Certificates
- System Variables
- Log Format Objects
- CCTV Protocols

*The Inputs/Outputs controlling the Elevator Buttons can be partitioned; hence access to physical elevator floors can be managed through Partitions

Renaming a Partition

An Operator with the appropriate Privilege can rename a Partition. When this is done, the associated Privilege is changed accordingly with the correct new name. The Hardware/Video folder names, however, are **not** corrected. The Operator must manually change their names.

Changing an Object's Partition

You can change the Partition of an Object as follows:

- For Objects **not** in a Hardware or Video tree – right-click the Object in a Dynamic View list and then click **Change Partition** from the Context menu that appears.
- For Objects in a Hardware or Video tree – drag an iSTAR Cluster, apC, or Comm Port or a Video Server, Camera, or CCTV Switch to a folder in another Partition.

NOTE You **cannot** drag an **iSTAR Controller** to another Partition folder, **only** the **Cluster**, of which it is a member. However, if you delete a Cluster in a Partition, but not the Controller(s) in it, the Controller(s) are put in an 'Unassigned' folder in the Hardware tree. The Controller(s) still remain in the same Partition, which you can change as follows: right-click one or more of them and then click **Change Partition** from the Context menu that appears.

When the Partition of an Object is changed, the following occurs:

- All its **child** Objects **change** their Partition.
- Objects that are **referenced** do **not** change their Partition since they are separate high-level Objects.

Example:

If the Partition of some **Personnel** changes from **P1** to **P2**, all of their **Credentials** and **Images** would also change from **P1** to **P2**. However, the assigned Badges would stay in their original **P1** Partition.

Operators can only change the Partition of an Object if they have the Privileges that give them the following Permissions:

- To 'Change Partition' for that Object class. (This Permission is Partition-based.) If the Object's Partition is **P1**, the Operator must have the Permission to 'Change Partition' for that Object class in the **P1** Privilege.)
- To 'New' for that object class in the target Partition. If the target Partition is **P2**, the Operator must have the Permission to create a new Object of that class in Partition **P2**, to be able to change the Object's Partition to **P2**.
- To access any children associated with the Object both in the source Partition and the target Partition.

  Example:

  To change the Partition of a **Personnel** record from **P1** to **P2**, an Operator must have edit access in both Partitions to its child Objects, **Credentials** and **Images**.)

Deleting a Partition

Partitions can be deleted, but only if they are empty. Therefore, if the Partition is populated with system Objects, before you can delete the Partition itself you need to do one or the other, or both, of the following:

- Move the Objects to another Partition.
- Delete the Objects

NOTE You cannot delete the Default Partition.

To see what Objects are in the Partition you want to delete, open the Partition on the **Partition Editor** and review the **Details** and **Template Details** tabs' listings—see the example in Figure 127 on Page 387.

Since the system automatically creates one Hardware and one Video folder when it creates a new Partition, remember to move these folders to another Partition (if you want to keep the Objects in them) or to delete them. If the Hardware/Video folder is populated, the Objects in it are deleted when you delete the Partition.

NOTE To delete a Partition, it is not necessary to delete its "Full privilege for partition (partition name)." The system automatically deletes this Privilege when it deletes the Partition.

For detailed procedures, see Deleting a Partition on Page 392.

Groups of Objects

The system allows Objects belonging to different Partitions to be members of the same Group, or Objects from one Partition to be members of a Group in another Partition.

NOTE Operators cannot execute a manual action on a Group if any of its member Objects is one for which the Operator does not have Permission to execute the Action.

Operators and Partitions

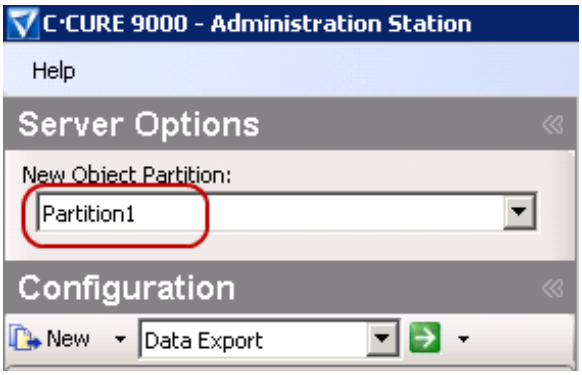
The following guidelines apply to Operators in a partitioned system:

- An Operator cannot see Objects from a particular Partition unless the Operator has a Privilege to view Objects in that Partition.
- If Operators have Privileges to create new Objects in more than one Partition, their 'New Object Partition,' shown in the upper-left of the Administration Client screen, is the Partition used when they create new Objects.

  The **New Object Partition** drop-down list includes all Partitions for which the current Operator has Privileges to create new Objects and allows Operators to switch their New Object Partition. This list is refreshed as Partitions and Privileges for Partitions are added, updated, and deleted. If the current Operator has rights only to a single Partition, only that Partition displays in the list.

  In the following example, the Operator has selected **Partition1** as her 'New Object Partition.' When the Operator adds a new Event, it will be in **Partition1**.

  Example:



NOTE If the Operator did not have the Privilege to add an Event to **Partition1**, the **New** button would not be available for this Object while 'New Object Partition' was set to **Partition1**.

- Since **Clusters** and **apCs** have the same Partition as their hardware folder, Operators cannot add these objects unless their **New Object Partition** matches the folder's Partition.

NOTE Operators **can** add Inputs, Outputs, Reader, and Boards to a **Controller/Panel** even if their **New Object Partition** does **not** match the Controller's/Panel's Partition. The system appropriately sets the Partition of the Objects to be the same as that of the **Controller/Panel**.

- When an Operator clicks  to open a Dynamic View list for a particular Object, the view displays **all** the Objects the Operator has Privileges to see. It does **not** use the Operator's **New Object Partition** to filter the Objects. If the Operator wants to see only the Objects from a particular Partition, she or he will have to create and run a Query.

Partition Editor

The Partition Editor lets you create and administer Partitions in the C•CURE 9000 system. Partitions let you divide security objects into sectors, and give Operators access to only certain security objects in their own Partitions.

The following topics give more information about Partitions and how to use them.

- Partition Overview on Page 380
- Partition Details Tab on Page 386
- Partition Template Details Tab on Page 387
- Partition Application Server Tab on Page 388

Partition Tasks

- Accessing the Partition Editor on Page 391
- Creating a Partition on Page 391
- Viewing a List of Partitions on Page 392
- Deleting a Partition on Page 392
- Modifying a Partition on Page 392
- Setting a Property for a Partition on Page 397

Partition-related Tasks

- Creating an Administrator for a Partition on Page 398
- Giving Operators Access to Different Partitions on Page 400
- Changing Your Operator 'New Object Partition' on Page 414
- Changing the Partition of an Object on Page 395

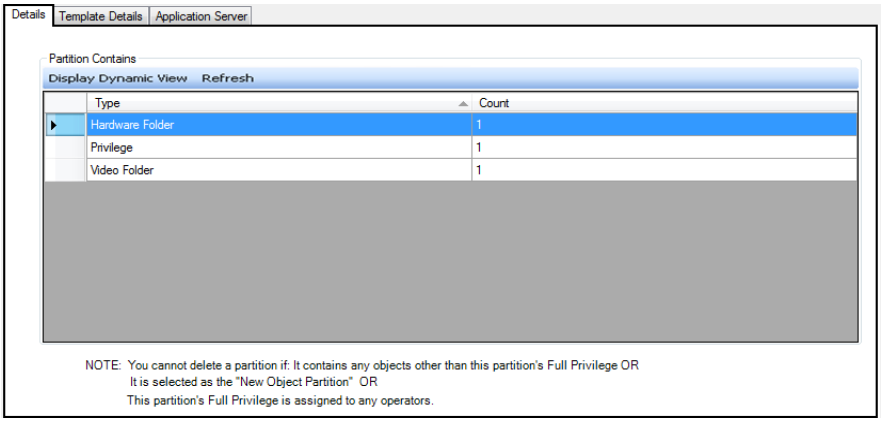
Partition Details Tab

The **Partition Editor** lets you create Partitions for the C•CURE 9000 system and is empty when it first opens.

The Details tab on the Partition Editor lets you view which top-level Object types have Objects assigned to this Partition.

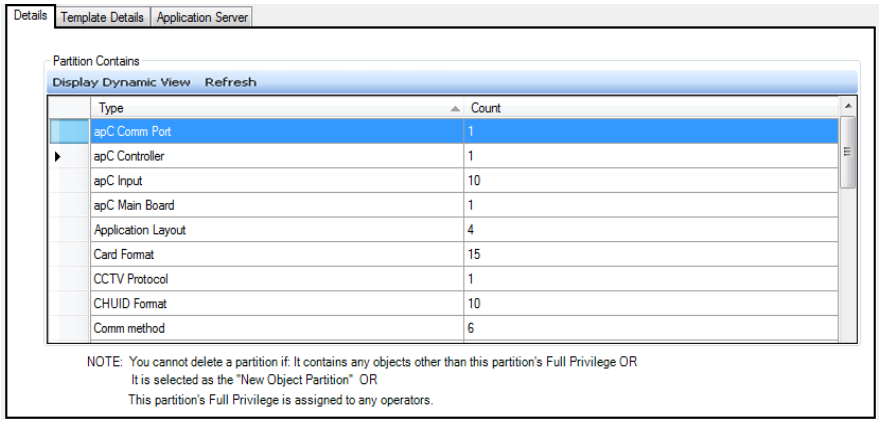
Once you create the Partition with a name (and optionally a description) and save it, the system automatically creates a new ALL Privilege, a new Hardware Folder, and a new Video Folder for the Partition. (See Results of Creating a Partition on Page 381.) If you reopen any newly created Partition, the Details tab appears as shown in Figure 126 on Page 387.

Figure 126: Partition Editor Details Tab for Saved New Partition



After you have created other Objects in the Partition, or moved them to it, the **Details** tab lets you view the number of C•CURE 9000 Object types and Connected Program Object types (if partitionable) with Objects assigned to the Partition, as shown in the example in Figure 127 on Page 387.

Figure 127: Partition Editor Details Tab for Populated Partition

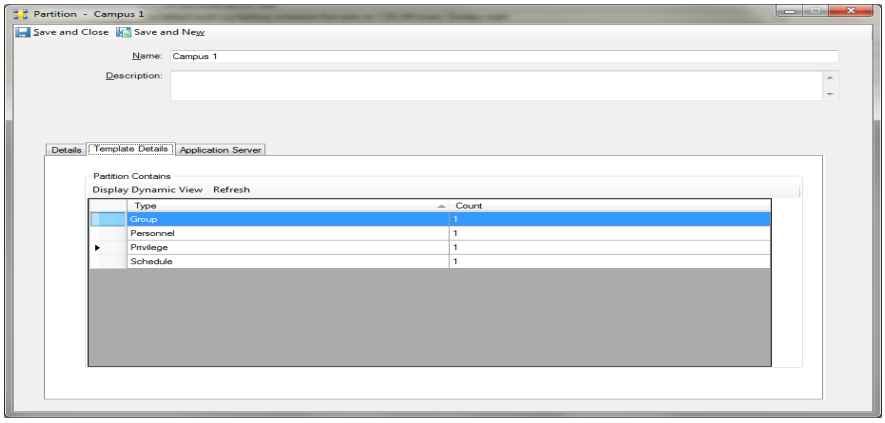


You can sort the Object types on the **Details** tab by Type or by Count.

Partition Template Details Tab

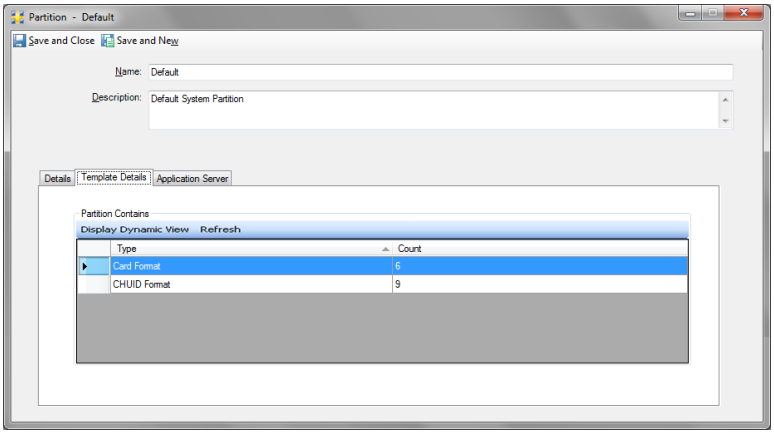
The **Template Details** tab lets you view the C•CURE 9000 Object types and Connected Program Object types (if partitionable) with Templates assigned to this Partition. This tab is also empty when you first open it while creating a new Partition, as shown in Figure 128 on Page 388. It remains empty until you create templates for Objects in this Partition.

Figure 128: Partition Editor Empty Template Details Tab for New Partition



The System 'Default' Partition, which you can view in read-only mode, includes the system default templates, shown in Figure 129 on Page 388.

Figure 129: Partition Editor Template Details Tab for Default Partition



You can sort the Object types on the **Template Details** tab by Type or by Count by clicking on a column heading.

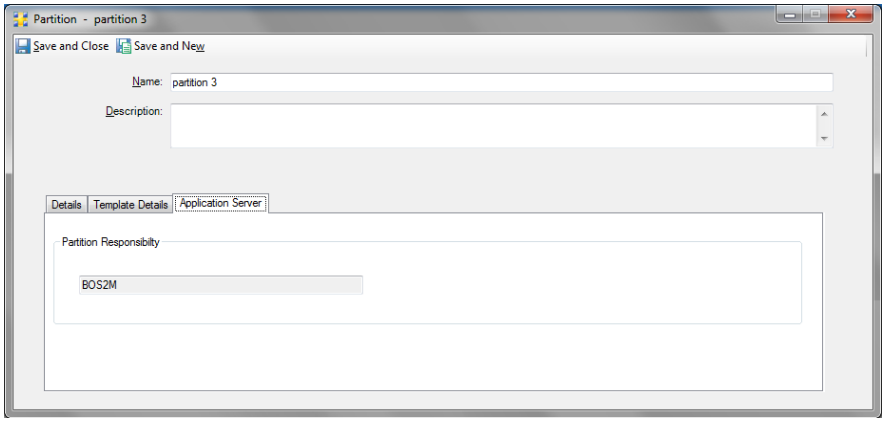
NOTE You cannot create a Partition Template.

Partition Application Server Tab

The Partition Application Server tab , as shown in Figure 130 on Page 389 identifies the C•CURE 9000 server that is responsible for administering the Partition. On a standalone C•CURE 90000 server, this tab shows the system on which C•CURE 9000 is installed.

In an Enterprise Architecture, the tab lists the C•CURE 9000 system that is responsible for the Partition and its objects. If the Partition is Global, it is owned by the MAS (Master Application Server). If the Partition is not Global, it is owned by a SAS (Satellite Application Server), or if it is a local Partition on the MAS, it is owned by the MAS).

Figure 130: Partition Application Server Tabn



Partition Editor Definitions

The **Partition Editor** has the buttons described in Table 91 on Page 389.

Table 91: Partition Editor Buttons

Button	Description
Save and Close	Click this button when you have completed any changes to the Partition and wish to save those changes. The Partition closes.
	Click this button when you want to close the **Partition 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.

The **Partition Editor** and the **Details** and **Template Details** tabs have the fields and buttons shown in Table 92 on Page 389.

Table 92: Partition Editor Details and Template Details Tab Fields

Field	Description
Name	Enter a unique name, up to 100 characters, to identify the Partition.
Description	Enter a description, up to 500 characters, to describe the Partition.
Details Tab (View this list to see which Objects need to be deleted or moved before trying to delete the Partition.)	
Type	This column lists the Object types in the system assigned to the Partition. You can sort the items by Type. NOTE: To delete the Partition, it is not necessary to delete its "Full privilege for partition (partition name)." The system automatically deletes this Privilege when it deletes the Partition.
Display Dynamic View	Select an Object type (row) in the list and click this button to display a floating dynamic view of the selected object in the list. For example, if you have selected Card Format, a Dynamic View of Card Formats appears, so that you can tell which Card Format objects are associated with the Partition. This is helpful if you have to delete the Partition, because you need to remove objects from the Partition before you can delete the Partition.
Count	This column shows how many Objects of the Object type are currently assigned to this Partition. You can sort the items by Count. NOTE: For Hardware and Video, the list shows only the number of Hardware and Video **folders** assigned to the Partition, not the specific Hardware or Video **Objects** within the folders.

Table 92: Partition Editor Details and Template Details Tab Fields (continued)

Field	Description
Refresh	Click this button to refresh the Details tab so that you can see an updated count of each object type in the Partition.
Template Details Tab (View this list to see which Objects need to be deleted or moved before trying to delete the Partition.)	
Type	This column lists the Templates in the system assigned to the Partition. You can sort the items by Type.
Count	The field shows how many Templates for this Object type are currently assigned to this Partition. You can sort the items by Count.
Display Dynamic View	Select an Object type (row) in the list and click this button to display a floating dynamic view of the selected object in the list. For example, if you have selected Card Format, a Dynamic View of Card Formats appears, so that you can tell which Card Format objects are associated with the Partition. This is helpful if you have to delete the Partition, because you need to remove objects from the Partition before you can delete the Partition.
Refresh	Click this button to refresh the Template Details tab so that you can see an updated count of each object type in the Partition.
Application Server Tab	
Partition Responsibility	This read-only field identifies the Application Server that owns this Partition. On a standalone C•CURE 90000 server, this field shows the system on which C•CURE 9000 is installed. In an Enterprise Architecture, the field lists the C•CURE 9000 system that is responsible for the Partition and its objects. If the Partition is Global, it is owned by the MAS (Master Application Server). If the Partition is not Global, it is owned by a SAS (Satellite Application Server), or if it is a local Partition on the MAS, it is owned by the MAS).

Partition Tasks

You can perform the following tasks with the Partition editor.

Accessing the Partition Editor

You access the Partition Editor from the C•CURE 9000 Configuration pane.

To Access the Partition Editor

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

   - or -

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

   The **Partition Editor** opens, as shown in the examples for a new Partition and for an existing Partition in Partition Details Tab on Page 386.

Creating a Partition

Only System Administrators, or those with the SYSTEM ALL privilege, can create a Partition. When you create a new partition in C•CURE 9000, a new ALL Privilege called “Full privilege for partition_name” is created. Also created are a Hardware folder and a Video folder (with the same name as the Partition). The names of these folders can be changed. on Page 391 shows the new Hardware and Video folders displayed in their respective navigation panes.

You can create a new Partition if you are the System Administrator and have the ‘SYSTEM ALL’ default access privilege.

To Create a Partition

1. In the Navigation Pane of the Administration Workstation, click the **Configuration** pane button.
2. Select **Partition** from the Configuration pane drop-down list.
3. Click **New** to create a new Partition. The Partition Editor opens (see on Page 386).
4. Configure a new Partition by entering a name for it and optionally, a description.
5. If your C•CURE 9000 system has multiple Application Servers, click the Application Server tab to open and select the Application Server you want to have responsibility for this Partition.
6. To save your new Partition, click **Save and Close**.

Viewing a List of Partitions

You can display a list of the Partitions you have created by opening a Dynamic View of Partitions. See Viewing a List of an Object Type on Page 22 for more information.

Partition List Context Menu

The context menu that opens when you right-click a Partition in the Partition Dynamic View includes the selections described in Using the Object List Context Menu on Page 23. The Context menu option specific to Partitions is described in Table 93 on Page 392.

Table 93: Partition List Right-Click Context Menu Options

Menu Selection	Description
Grace All for this Partition	Click this menu selection to grace all Personnel in the selected Partition(s)–reset their cards' antipassback and timed antipassback information so on their next access, they are not checked for antipassback violation. If the system was not partitioned, only the Default Partition would display in the list. In that case, the command would grace all system Personnel.

Modifying a Partition

You can modify an existing Partition by editing it using the Partition Editor.

To Modify a Partition

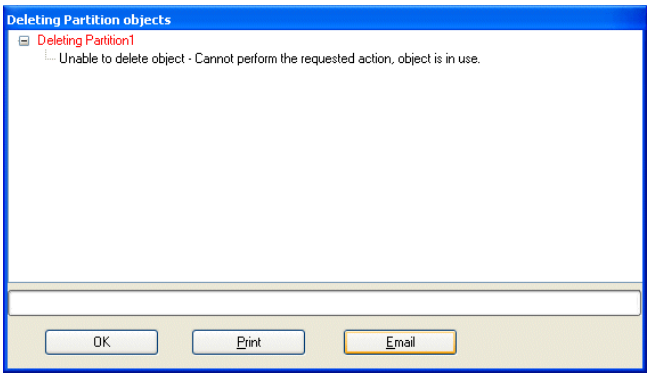
1. In the Navigation Pane of the Administration Workstation, click **Configuration** to open the Configuration pane.
2. Select **Partition** from the Configuration pane drop-down list.
3. Click  to open a Dynamic View showing all Partition Objects.
4. Right-click the Partition in the list that you want to edit and select **Edit** from the context menu.
5. Edit the Partition as needed and click **Save and Close**.

Deleting a Partition

You can delete a Partition only if there is nothing in it. Consequently, you must either delete any Objects belonging to the Partition you want to delete or move them to another Partition. The system will then permit you to remove the empty Partition. Since both a Partition Hardware folder and a Video folder are automatically created when the Partition is created, before you can delete the Partition you must take the following actions:

- If the Hardware and/or Video folders are **populated**, you must either:
  - Move the contained Hardware/Video Objects to another Partition in the tree (using drag-and-drop) to retain the Objects.
  - Delete the entire folder, which automatically deletes the Objects in it.
- If the Hardware and/or Video folders are **empty**, just delete the folder.

If you fail to move or delete the Objects in the Partition, the following message displays when you confirm your deletion of the Partition:



When the Partition is deleted, the system automatically deletes the Partition ALL Privilege for the deleted Partition.

To make Partition deletion easier, the Partition editor now includes a toolbar button to allow you to display a Dynamic View of each object type in the Partition. From this view you can use the context menu **Delete** option to delete one or more of the objects, or the **Change Partition** option (if applicable) to move objects to a different Partition. Being able to delete these objects from within the Partition editor means that you can quickly clear out a Partition and then delete it without needing to close the Partition editor.

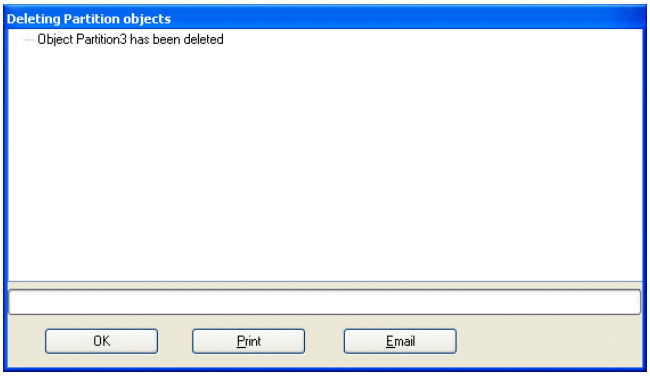
To Delete a Partition

1. Access the Partition you wish to delete in the Partition editor (see Accessing the Partition Editor on Page 391).
2. Review the information on the **Details** and **Template Details** tabs to see how many Objects of different types and how many Templates the Partition contains.
3. Delete objects that are no longer needed or cannot be moved - see Deleting Objects from a Partition on Page 394.
4. Change the Partition of any objects that you wish to keep (not all objects can be moved to another Partition - those that can be moved have a Change Partition context menu selection when viewed in a Dynamic View) - see Changing the Partition of an Object on Page 395.

   When you have removed all objects in the Partition, you can then delete the Partition itself

   NOTE You do not need to delete the Partition's **Full privilege for partition (partition name)** because the system automatically deletes it when it deletes the Partition.

5. Click **Save and Close** to close the Partition editor.
6. From the Configuration Pane, select **Partition** and click  to display a Dynamic View of Partition objects.
7. Select the Partition you wish to delete and right-click.
8. Choose **Delete** from the context menu. A Deleting progress dialog box appears to confirm the deletion.



9. Click one of the following:
   - **OK** to close this dialog box.
   - **Print** to print messages in the dialog box.
   - **Email** to email the messages in the dialog box to the recipient specified in the Customer Support System Variables (see the *C•CURE 9000 System Maintenance Guide*for more information.

Deleting Objects from a Partition

You can delete the objects in a Partition from the Partition editor Details tab and Template Details tab.

For each type of object in the Partition, you can display a Dynamic View that lists the objects of that type, and allows you to use the context menu to move the object to a different Partition (if possible) or delete the object.

NOTE You do **not** have to move the Objects from a populated Hardware folder in order to delete it. When you delete the folder, the system automatically deletes any Objects it contains—**except** for **iSTAR Controllers**. They move to the **Unassigned** folder.

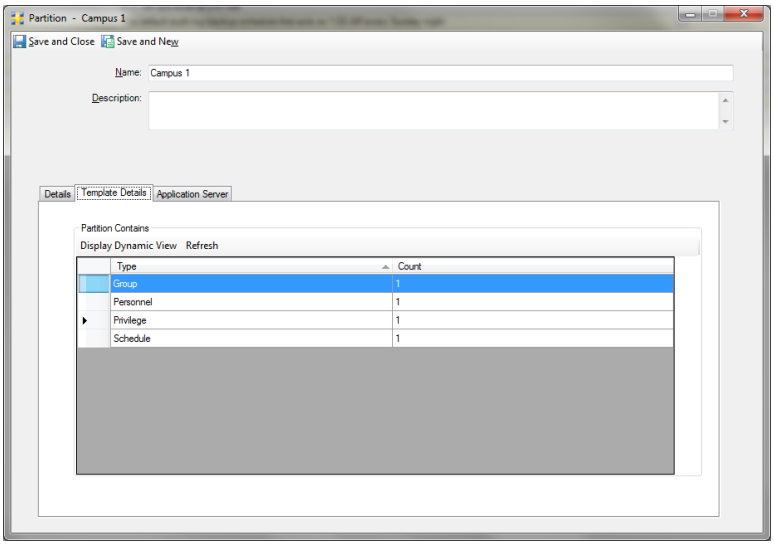
To Delete Objects from a Partition

1. From the Partition editor Details tab or Template Details tab, select an object type from the **Partition Contains** list, then click **Display Dynamic View**. A Dynamic View showing all the Group objects in the Partition appears (see Figure 131 on Page 394).

   Example:

   Select **Group**, then click **Display Dynamic View**.

   Figure 131: Partition Object Dynamic View



2. Select the objects you wish to delete (you can use multi-selection key combinations like **SHIFT+Left-click** and **CTRL+Left-click** to select multiple objects).
3. Right-click to display the context menu.
4. Select **Delete** and left-click.
5. Click **Yes** on the delete confirmation message that opens.
6. A Deleting progress dialog box appears to confirm the deletion. Click:

- **OK** to close this dialog box.
- **Print** to print messages in the dialog box.
- **Email** to email the messages in the dialog box to the recipient specified in the Customer Support System Variables (see the *C•CURE 9000 System Maintenance Guide*for more information.

Changing the Partition of an Object

If you have Privileges with the necessary Permissions, as described in Changing an Object's Partition on Page 383, you can change the Partition of an Object. This is done differently for non-hardware objects than it is Hardware Tree and Video Tree objects.

Example:

From a Dynamic View of Events, you can right-click on one or more Events and use **Change Partition** to move the Events to another Partition.

You can change the Partition of an Object in several ways:

To Change an Object's Partition from the Partition Editor

1. From the Partition editor Details tab or Template Details tab, select an object type from the **Partition Contains** list, then click **Display Dynamic View**.

Example:

Select **Group**, then click **Display Dynamic View**. A Dynamic View showing all the Group objects in the Partition appears.

2. Select the objects you wish to delete (you can use multi-selection key combinations like **SHIFT+Left-click** and **CTRL+Left-click** to select multiple objects).
3. Right-click to display the context menu.
4. Select **Change Partition** and left-click.

NOTE If the **Change Partition** choice does not appear, you cannot change the object's Partition, and you will need to delete the object in order to delete the Partition.

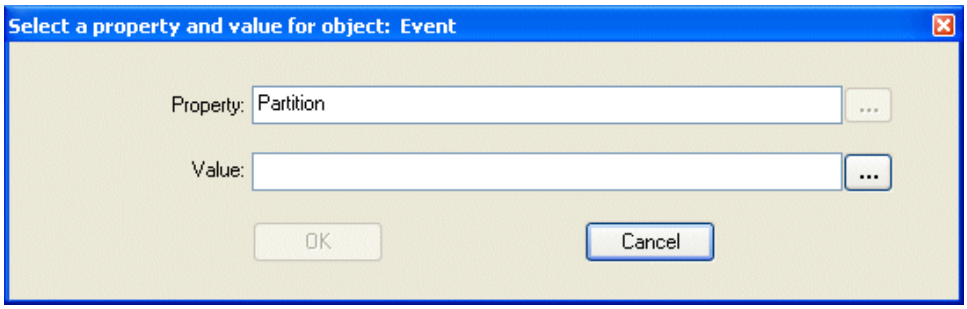
5. A dialog box appears to let you choose the Partition to which you want to move the objects. Click ... for the **Value** field and select the target Partition.
6. Click **OK**.
7. A Setting Properties progress dialog box appears to confirm the change. Click:
   - **OK** to close this dialog box.
   - **Print** to print messages in the dialog box.
   - **Email** to email the messages in the dialog box to the recipient specified in the Customer Support System Variables (see the *C•CURE 9000 System Maintenance Guide* for more information.

To Change the Partition of a Non-hardware Object

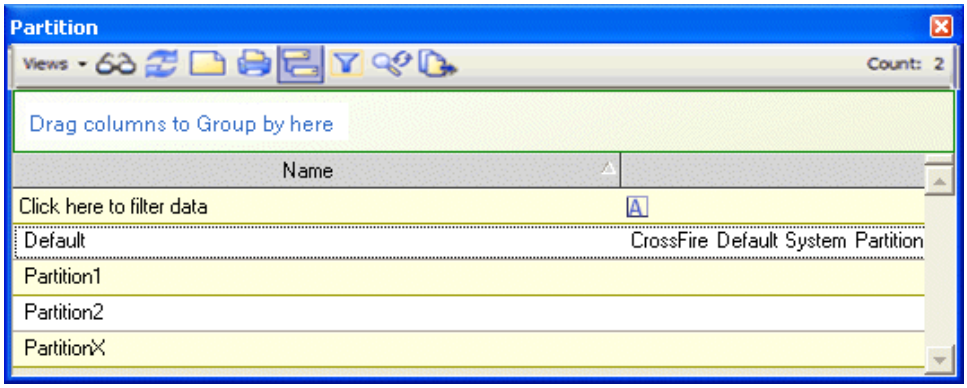
1. In the Navigation Pane of the Administration Client, click the pane for the object whose Partition you want to change.
2. Select the Object from the pane drop-down list.
3. Click  to open a Dynamic View showing all the Objects. (To see the **Partition** column if it is not shown, right-click any column heading and click **Partition** in the context menu that appears.)

4. Right-click the Object in the list whose Partition you want to change and select **Change Partition** from the context menu.

   A dialog box similar to the following opens.



5. In the **Value** field, click ..., and select the Partition to which you want to move the object from the list that appears.



   The Partition name is entered in the **Value** field.

6. Click **OK**. The Partition is changed as indicated by the entry for the object in the Partition column.

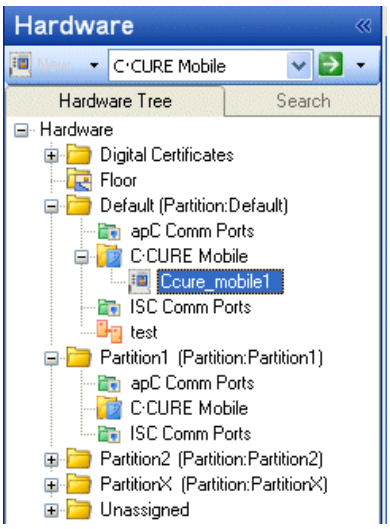
To Change the Partition of a Hardware/Video Tree Object

1. In the Navigation Pane of the Administration Client, click **Hardware**/**Video** to open that pane.
2. From the Hardware/Video Tree, click to select the Object whose Partition you want to change and drag it to the folder of another Partition.

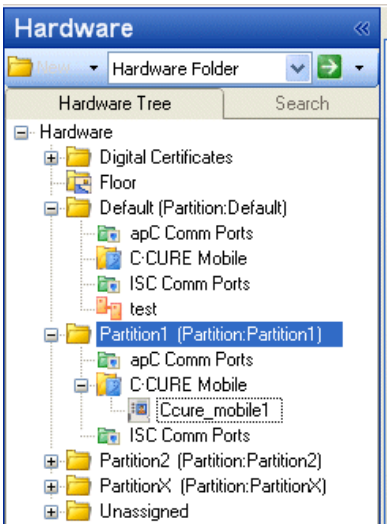
   Example:

   Ccure_mobile 1 is part of the **Default** Partition folder. After dragging and dropping, it belongs to the **Partition1** Partition.

In Default Partition



Dragged and dropped to Partition1



Setting a Property for a Partition

You can use Set Property to set properties for a Partition. Set Property enables you to quickly set an Partition property without opening a Partition. You use Set Property for mass updates.

To Set a Property for Partitions

1. In the Navigation Pane of the Administration Workstation, click **Configuration** to open the Configuration pane.
2. Select **Partition** from the Configuration pane drop-down list.
3. Click to open a Dynamic View showing all Partition objects.
4. Right-click the Partition 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 Partition. Click the drop-down button to see a list of properties.
6. Enter the value for the property and click **OK**.

Partition-related Tasks

The following tasks are related to Partitions but are not performed using the Partition editor.

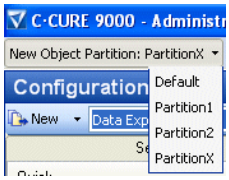
- Creating an Administrator for a Partition on Page 398
- Creating Other Operators for a Partition on Page 398
- Giving Operators Access to Different Partitions on Page 400
- Changing Your Operator 'New Object Partition' on Page 414

Creating an Administrator for a Partition

The System Administrator can create an administrator for a new Partition. In a partitioned C•CURE 9000 system, such an Administrator is the Operator in charge of access control for the Partition—creating Partition Operators and administering the Partition's Objects.

To Create an Administrator for a New Partition

1. Create the new Partition, **PartitionX**, as described in Creating a Partition on Page 391.
2. Set **New Object Partition** to the new Partition (**Partitionx**) by clicking the down-arrow next to the **New Object Partition** item and selecting a different partition from the drop-down list.



3. Create a new Operator, as described in Creating an Operator on Page 368.

   By default, the system automatically assigns the following two Privileges to the new Operator:

   - "Full privilege for partition (Partitionx)" that gives the operator full access to all Objects in that Partition and to all Non-partitioned Objects.
   - "Access to common objects" privilege that gives the operator Read access to certain Objects in the Default Partition required to get started.

     Example:

     Dynamic views, Queries, Schedules, etc.

     For details of the Object Permissions given by the 'Access to common objects' privilege, see Privileges Related to Partitioning on Page 381.

NOTE	You can create a Privilege based on the "Access to common objects" Privilege Template to give Operators the access they need to log in and to get started on the system. In addition, creating the Privilege in this way allows you to view the Permissions included in this Privilege and to change or add to them.

Creating Other Operators for a Partition

The System Administrator or the Administrator of the Partition can create Operators for a Partition who perform particular tasks within the Partition, and who therefore require different Privileges.

Example:

- An Administrative Operator in **Parition1** responsible only for **Personnel**.
- An Administrative Operator in **Partition2** responsible only for running **Reports**.

To Create Operators of Different Types for a Partition

1. Set your New Object Partition to the Partition for which you want to create the Operators by clicking the down-arrow next to the **New Object Partition** item and selecting the Partition from the drop-down list.
2. Create a new Operator, as described in Creating an Operator on Page 368.

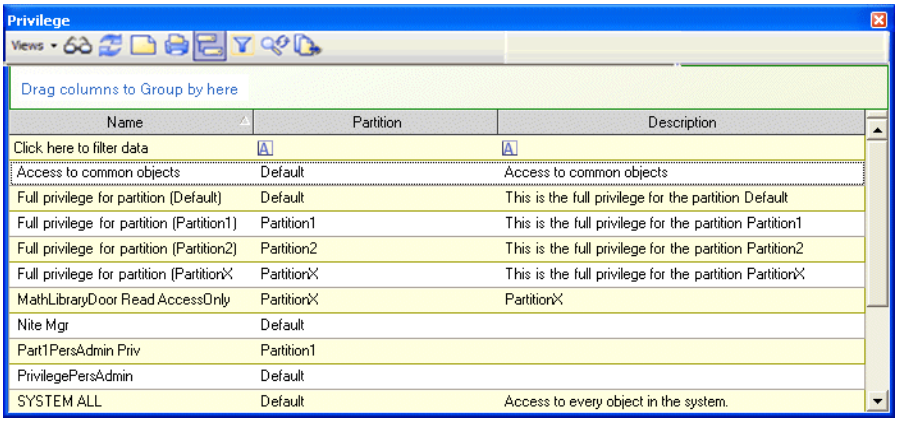
   By default, the system automatically assigns the following two Privileges to the new Operator, as shown in the example in Figure 116 on Page 360:

   - "Full privilege for partition (Partitionx)" that gives the Operator full access to all of the following:
     - Objects in that Partition
     - Non-partitioned Objects
   - "Access to common objects" Privilege that gives the Operator Read access to certain Objects in the Default Partition required to get started.
3. Delete the "Full privilege for partition (Partitionx)" by selecting the row and then clicking **Remove**.
4. Click **Add** to add a new Privilege/Schedule row for the Operator.
5. Click in the Privilege field and then click the ... button that appears.

   From the **Privilege** list that displays, select the Privilege you want to give this Operator that will enable him to do his job.

   Example:

   'Part1PersAdmin Priv (Partition1)' – a Privilege allowing the Operator to administer Personnel records for this Partition.

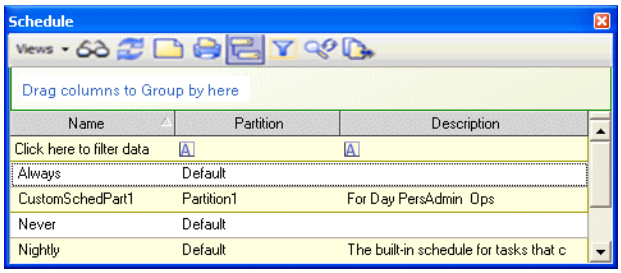


6. Click in the **Schedule** field and then click the ... button that appears.

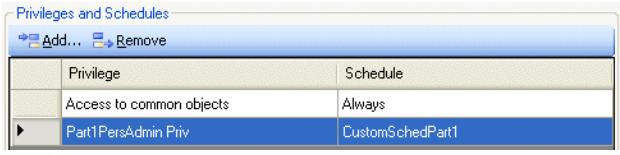
   From the **Schedule** list that displays select the Schedule you want to associate with the Privilege you selected for this Operator.

   Example:

   'CustomSchedPart1 (Partition1)'



The **Privileges and Schedules** box now appears as follows:



7. You could repeat Steps 4 through 6 to give the Operator Privileges in other Partitions.
8. If you wanted this Operator to use the Monitoring Station, you would use the **Layout** tab to customize views for him or her.
9. Repeat Steps 1 through 8 to create as many Operators as you need for the Partition.

Giving Operators Access to Different Partitions

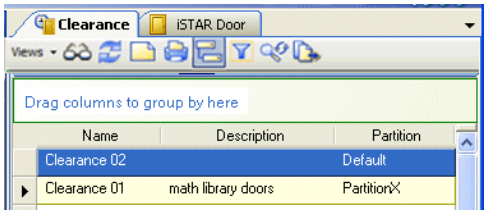
Your C•CURE 9000 partitioned system can be configured so Operators assigned to one Partition can have Privileges that allow them to access Objects within another totally different Partition. You can also configure the system so Operators can be assigned a Privilege which spans across multiple Partitions.

Example:

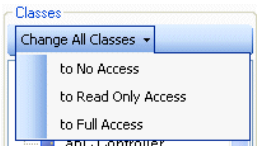
The Administrators for **Partition1** (the physics department) and **Partition2** (the chemistry department) are configured with Privileges that let them access the doors to the mathematics library in **PartitionX** (the mathematics department). These Administrators of **Partition1** and **2** can then give the Personnel in their respective Partitions—the physics majors and the chemistry majors—**clearances** for the math library doors, giving them the right to use this library in another Partition.

To Give Operators Access to Objects in a Different Partition

1. Acting as the System Administrator, create a **clearance** to the math library doors in **PartitionX**.



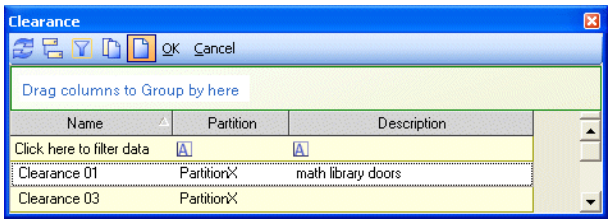
2. Using the **Privilege Editor** (see Privilege Overview on Page 416 for information), create a Privilege in **PartitionX** that only gives Read access to the math library clearance you created in Step 1, as follows:
   a. On the **Defaults** tab, click the **Change All Classes** down-arrow and from the drop-down list, click to select the **to No Access** option.



b. When the Warning message appears, click **Yes**.

c. On the **Exceptions** tab

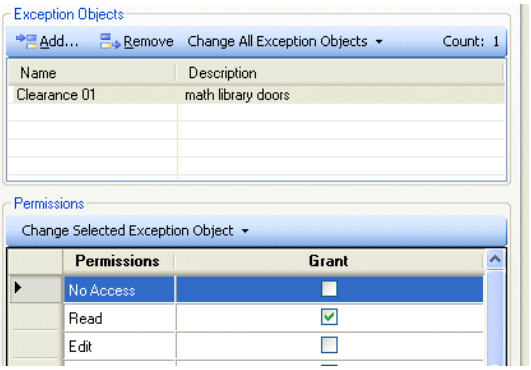
— Select **Clearance** in the **Classes** list on the left and click **Add** in the **Exceptions Objects** box on the right. A **Clearance** list for **PartitionX** opens.



— Select the **Clearance 01** for the math library doors and click **OK**. That Clearance is now entered in the **Exceptions Objects** box.

— In the **Permissions** box, click to grant only **Read** access for this Clearance exception.

The boxes now appear as follows:



d. Be sure to select the **Enabled** check box on the top of the **Privilege Editor** to make this Privilege active and then save the Privilege.

3. From the **Operator** Dynamic View, select the Operators who are the Administrators of the physics and chemistry department partitions (**Partition1** and **Partition2** respectively) and in turn double-click their names to edit their information on the **Operator Editor** as follows:

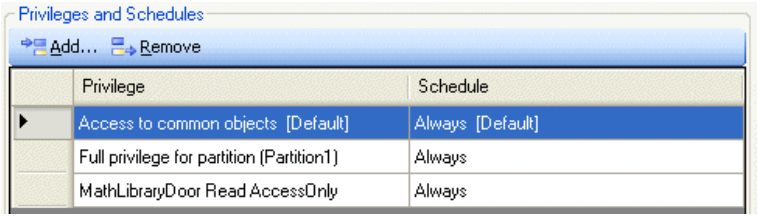
a. Click **Add** to add a new Privilege/Schedule row.

b. Click in the **Privilege** field of the new row to display  and then click this button to display the **Privilege** list.

c. Click the 'MathLibraryDoor ReadAccessOnly' Privilege for **PartitionX** to give this Privilege to these two Operators.

d. Associate a Schedule with this Privilege as detailed in Step 6 on Page 399.

The **Privileges and** Schedules box appears as follows for these Administrators:



These two Operators, the Administrators of the physics and chemistry department Partitions, can now give students in their Partitions the **Clearance** to access the mathematics library in **PartitionX**.

To Give Operators Access to Objects in multiple Partitions using one Privilege

1. Create a new Privilege, as described in Creating a Privilege on Page 442
2. Configure your Privilege.
3. Click on the **Partitions** tab.
4. Click the **Add** button in the Partitions tab.
5. From the Name Selection window, select the Partition, or Partitions, you want to assign to this Privilege.
6. Click **Save and Close**.

14

Predefined Log Messages

This chapter explains how to configure Predefined Log Messages.

In this chapter

Predefined Log Message Overview

Predefined Log Message allows you to create log messages containing instructions and assign them to events, so that they are available to Operators who are responding to the Events. You can group multiple log messages and then assign them to specific events.

Operators using the Monitoring Station can choose from a list of assigned event log messages based on the Predefined Log Message instructions to determine the action required for the event. See the *C•CURE 9000 Monitoring Station Guide* for more information.

Predefined Log Messages can also be used with Guard Tours to log messages to the Monitoring Station and Journal. For information, see the *C•CURE 9000 Guard Tours Guide*.

Operator privileges are required to add, modify, or delete messages or message groups. See Operator Tasks on Page 368 for information about assigning operator privileges.

For information about Privileges that Operators need to create, assign, and edit Predefined Log Messages, see Privileges for Predefined Log Messages on Page 405.

NOTE No predefined log messages are supplied with the system. You must create them.

For more information about Predefined Log Messages, see:

- Predefined Log Message Editor on Page 408
- Predefined Log Message Tasks on Page 410

Accessing the Predefined Log Message Editor

To Access the Predefined Log Message Editor

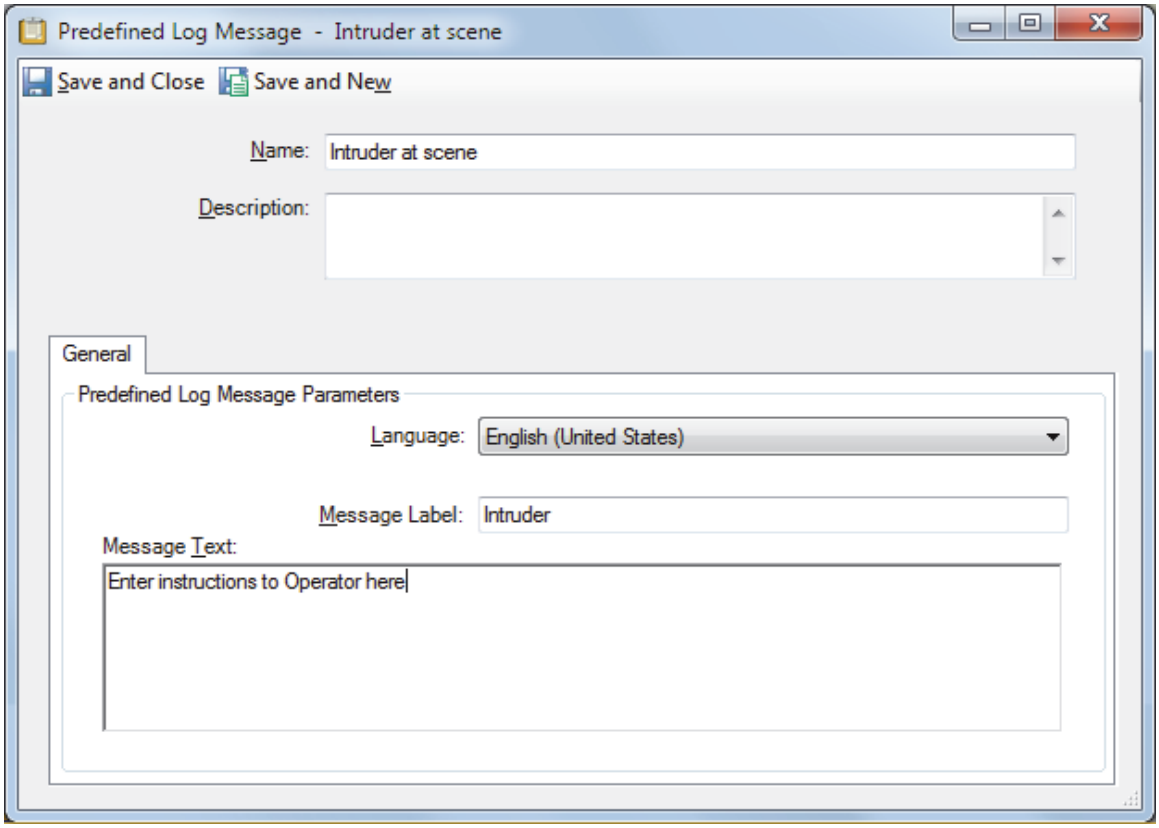
1. In the Admin station, click the **Configuration** pane button
2. Click the **Configuration** drop-down list and select **Predefined Log Message**.
3. Click **New** to create a new Predefined Log Message.

   - or -

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

   The Predefined Log Message Editor on Page 408 opens.

Figure 132: Predefined Log Message Editor



4. Enter a name for the Predefined Log Message in the Name field.
5. Enter a description for the Predefined Log Message in the Description field.

TIP Entering a description makes it easier for the Operator to select Predefined Log Messages to add to an event or a group. Predefined Log Message descriptions are displayed in the Name Selection dialog box.

6. Select a language from the Language drop-down menu.
7. Enter a description for the message label.
8. Enter the log message in the Message Text box.
9. Click Save and Close to save your changes.

To save the Predefined Log Message and then create a new one, click **Save and New**.

Privileges for Predefined Log Messages

For Operators with limited Privileges, specific Privileges must be assigned to allow the creation, editing, and assignment of Predefined Log Messages to Events.

Table 94 on Page 406 shows the Operator action, the object class in the Privilege to modify, and the Permission setting required.

Table 94: Privilege Settings for Predefined Log Message Operator Actions

Operator Action	Object Class	Permissions
Administrator Operator Actions		
Edit a Predefined Log Message	Predefined Log Message	Edit
Assign a Predefined Log Message to an Event	Predefined Log Message	Read
	Event	Edit
Create a new Predefined Log Message	Predefined Log Message	New
Delete a Predefined Log Message	Predefined Log Message	Delete
Monitoring Station Operator Actions		
Select a Predefined Log Message as a Log Message	Predefined Log Message	Read
	Event	Read
Select a Predefined Log Message as a Log Message and edit the message (an optional capability for Monitoring Station Operators).	Predefined Log Message	Read
	Event	Read
	Event	Allow Edit of Predefined Log Messages

Limiting Operator Access to Predefined Log Messages

An administrator can use the Privilege Exception tab to limit access for an Operator to specific Predefined Log Messages.

Example:

The Predefined Log Message Group assigned to an Event contains Pre-defined Log Messages named Message1, Message2, Message3 and Message4.

If a limited Privilege Operator only should have access to Message1 and Message2, the Administrator can edit the Privilege for that Operator to restrict access to

The Administrator uses the Privilege Exceptions tab to add Message3 and Message4, and assign them the No Access permission.

When the Operator processes an Event that includes this Group, only the messages in the Group that the Operator has permissions for are available for selection.

To Limit Operator Access to Predefined Log Messages

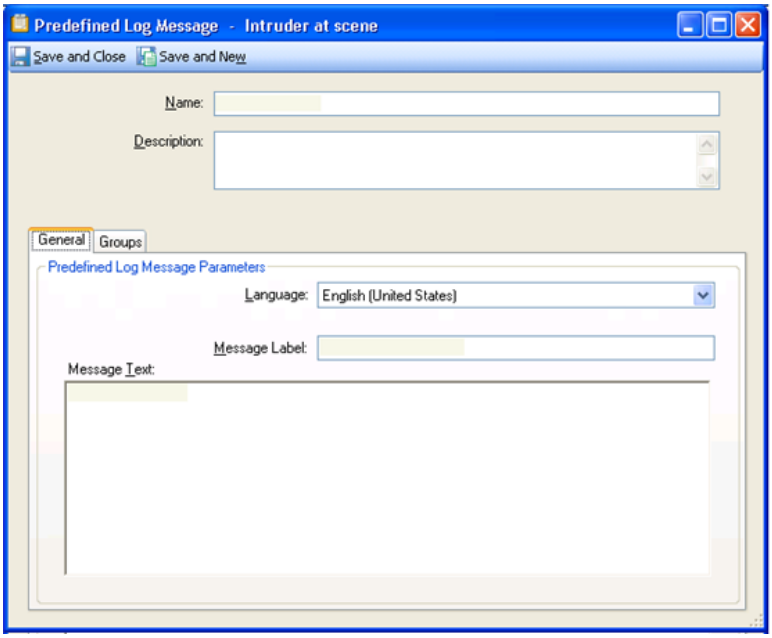
From the Configuration pane, select Privilege.

1. Click  to open a Dynamic View of Privileges.
2. Select the Privilege you wish to edit from the list.
3. Click the Exceptions tab.
4. Click Predefined Log Messages in the Classes list.
5. Click **Add** to add an exception to the Privilege.
6. Select the Predefined Log Message you want to add as an exception and click OK.
7. Select **No Access** from the available Permissions.
8. Click **Save and Close** to save your changes to the Privilege settings.

Predefined Log Message Editor

The Predefined Log Message editor, shown in Figure 133 on Page 408, is used to create and edit log messages.

Figure 133: Predefined Log Message Editor



NOTE The text fields in a Predefined Log Message cannot contain non-printable characters. If you add non-printable characters to a Predefined Log Message, an error message appears when you attempt to save the Predefined Log Message.

See the following:

- Predefined Log Message editor field descriptions in Table 95 on Page 408
- Predefined Log Message Tasks on Page 410

Table 95: Predefined Log Message Editor Fields and Buttons

Fields/Buttons	Name
General Tab	
Name	Enter a unique name, up to 500 characters, to identify the The Preset Log Message.
Description	Enter a description, up to 500 characters, to identify the Predefined Log Message.
Language	The language used for the Predefined Log Message.
Message Label	Enter a message label, up to 100 characters, to identify the Predefined Log Message. This field cannot contain non-printable characters.

Table 95: Predefined Log Message Editor Fields and Buttons (continued)

Fields/Buttons	Name
Message Text	The message to display, or log, when this Preset Log Message is used to log information about an event. In addition to regular text, you can enter a: • Website address • UNC address • Local file path. These appear as blue underscored hyperlinks in the Monitoring Station, and if they point to a valid location, a Monitoring Station Operator can click the link and open a webpage, a file location, or a specified file. If the link contains any blank spaces, enclose the link in angle brackets ('<' and '>' as in the examples below). **Examples:** www.swhouse.com \\servername\Tyco\CrossFire file:///c:\Windows\notepad.exe <file:///c:\Program Files (x86)\Tyco\CCURE Client\Help\MainHelp.chm> The maximum number of characters for Event Message Text is 3000. This field cannot contain non-printable characters.
Groups Tab This tab is not visible when you create a new Predefined Log Message. See Object Editor Groups Tab on Page 26 for more information.	

Predefined Log Message Tasks

See the following tasks:

- Creating a Predefined Log Message on Page 410
- Creating a Predefined Log Message Template on Page 411
- Assigning Predefined Log Messages to a Group on Page 411
- Assigning Predefined Log Messages to Events on Page 413
- Using the Predefined Log Message View Context Menu on Page 413
- Viewing a List of Predefined Log Messages on Page 413
- Editing Predefined Log Messages on Page 414
- Deleting an Object on Page 25

NOTE If you delete a Predefined Log Message, all references to that log message in a group or an event are also removed.

Accessing the Predefined Log Message Editor

You access the Predefined Log Message editor from the C•CURE 9000 Configuration pane.

To Access the Predefined Log Message Editor

1. Click the **Configure** pane button .
2. Click the **Configuration** drop-down list and select **Predefined Log Message**.
3. Click **New** to create a new log message. The Predefined Log Message Editor on Page 408 opens.

   or

   To edit a Predefined Log Message, click  to view a list of Predefined Log Messages. Click the Predefined Log Message that you want to edit to open the editor.

Creating a Predefined Log Message

To Create a Predefined Log Message

1. In the Navigation Pane of the Administration Workstation, click the **Configuration** pane button.
2. Select **Predefined Log Message** from the Configuration pane drop-down list.
3. Click **New** on the **Configuration** Pane. The Predefined Log Message Editor on Page 408 opens.
4. Enter a name for the Predefined Log Message in the **Name** field.
5. Enter a description for the Predefined Log Message in the **Description** field.

TIP Entering a description makes it easier for the operator to select Predefined Log Messages to add to an event or a group. Predefined Log Message descriptions are displayed in the Name Selection dialog box.

6. Select a language from the **Language** drop-down menu.
7. Enter a description for the message label.
8. Enter the log message in the **Message Text** box.

9. Click **Save and Close** to save your changes.

   To save the Predefined Log Message and then create a new one, click **Save and New**.

NOTE The **Message Label** and **Message Text** fields cannot contain non-printable characters.

Creating a Predefined Log Message Template

You can create a new template for a Predefined Log Message. A Predefined Log Message template saves you time because you can reuse the same configuration repeatedly.

To Create a Predefined Log Message Template

1. In the Navigation pane of the Administration Workstation, click **Configuration** to open the Configuration pane.
2. Select **Predefined Log Message** from the Configuration pane drop-down list.
3. Click the drop-down arrow next to **New** and select **Template**. The Predefined Log Message Template opens.
4. Configure the Predefined Log Message template.
5. To save your new Predefined Log Message Template, click **Save and Close**.

The new Predefined Log Message template appears under Templates in the Template drop down list.

To Select a Predefined Log Message Template

1. In the Navigation Pane of the Administration Workstation, click **Configuration** to open the Configuration pane.
2. Select **Predefined Log Message** from the Configuration pane drop-down list.
3. Click the drop-down arrow next to **New** and select **Template**.
4. Select the template you want to use under Templates.

Assigning Predefined Log Messages to a Group

For more information on Groups, see , Group Editor Overview.

To Assign Predefined Log Messages to a Group

1. In the **Navigation** Pane of the Administration Workstation, click the **Configuration** pane button.
2. Select **Group** from the Configuration pane drop-down list.
3. Click **New** to create a new Group. The Group Editor General Tab on Page 312 opens.
4. Enter a Name and Description for the group.
5. Click  to open the **Select Type** dialog box.
6. Scroll down and select **Predefined Log Message** as the object class.

   Predefined Log Message now appears in the Group Type field of the Group Editor.
7. Click **Add** to open the Name Selection dialog box.

   A list of Predefined Log Messages is displayed.
8. Select the Predefined Log Messages to add to the Group, and click **OK**.

NOTE You can only assign a maximum of 100 Predefined Log Messages to a group.

9. To save the Group, click **Save and Close**.

   To save the Group and then create a new one, click **Save and New**.

Assigning Predefined Log Messages to Events

Use the **Predefined Messages** tab in the Event editor to assign a predefined log message to an event. You can also assign a predefined log message to an event, or multiple events, in the Event Dynamic Views pane.

For more information about events, see Understanding Events on Page 237.

NOTE You can only assign a maximum of 100 Predefined Log Messages to an event. This includes the number of Predefined Log Messages in a group assigned to the event. If the same Predefined Log message is assigned to different groups, then that log message counts as one in each group.

If you assign more than 100 Predefined Log Messages to an event, the second time you open the event for editing, you will not be able to save it.

To Assign Predefined Log Messages to Existing Events

1. In the navigation Pane of the Administration Station, click **Configuration**.
2. Select **Event** from the Configuration pane drop-down list.
3. Click  to display a list of pre-configured events.
4. Double-click an event. The Event Editor opens.
5. Click the **Predefined Messages** tab.
6. Click  . The Name Selection dialog box opens.
7. Select the Predefined Log Messages, or the Predefined Log Message groups, in the list that you want to add to the event, and click **OK**. This list only displays log messages and groups that have not been assigned to the event.
8. Select **Enabled** to activate the event.
9. To save the Event, click **Save and Close**.

   To save the Event and then create a new one, click **Save and New**.

To Assign Predefined Log Messages to multiple events

1. Open the Event Dynamic Views list.
2. Hold the **Ctrl** or **Shift** key, and select the Events that you want to assign the application layouts to.
3. Right-click and select **Assign Predefined Log Message**.
4. Select the predefined log message or messages from the list and click **OK**.

Viewing a List of Predefined Log Messages

You can display a list of the Predefined Log Messages you have created by opening a Dynamic View of Predefined Log Messages. See Viewing a List of an Object Type on Page 22 for more information.

Using the Predefined Log Message View Context Menu

The Predefined Log Message View context menu opens when you right-click a Predefined Log Message in the Dynamic View.

See Using the Object List Context Menu on Page 23 for information about using the context menu.

Editing Predefined Log Messages

You can edit Predefined Log Messages in the editor or delete a Predefined Log Message from the Dynamic View.

To Access the Predefined Log Message Editor

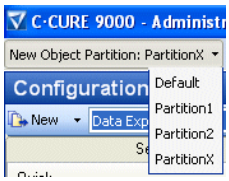
1. Click the **Configure** pane button.
2. Click the **Configure** drop-down list and select **Predefined Log Message**.
3. Double-click the Predefined Log Message in the list that you want to edit, and the Predefined Log Message editor opens.
4. Click **Save and Close** when done.

Changing Your Operator 'New Object Partition'

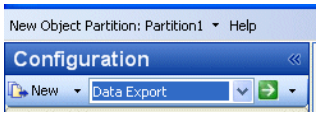
The ability of Operators to change their **New Object Partition** allows them to create new security Objects for their C•CURE 900 system and control the Partitions to which the Objects belong. (This only applies if you have Privileges to create new Objects in several Partitions.)

To Change Your New Object Partition

1. Click the down-arrow next to the **New Object Partition** to open the drop-down list as follows:



2. Click the desired Partition to select it, **Partition1**, for example. Your New **Object Partition** will be changed and the name of the New Partition will appear on the window. Now, any Objects you create for the system—from Personnel to Operators to Events—will belong to **Paritition1** instead of **PartitionX**.



15

Privilege

This chapter explains how to configure Privileges in C•CURE 9000.

In this chapter

Privilege Overview

A Privilege Object is a collection of rights you configure to allow Operators access to security Objects such as Readers, Doors, Inputs, Outputs and Privileges. These individual rights are called Permissions.

- Each access control Object has a number of Permissions associated with it such as No Access, Read, Edit, View, Delete and New.
- **Read** and **Edit** are mutually exclusive. If you choose Read, you **cannot** select Edit. If you choose Edit, you **cannot** select Read.
- You have the ability to grant a Permission or deny a Permission.
- When you create a new Privilege, all Permissions are set to No Access. You can modify the settings to grant Permissions to only the objects your Operators require.

An Operator is a person who has the right to use access control Objects such as Readers, Doors, Inputs, Outputs and Privileges.

- In C•CURE 9000 you use the Operator Editor to assign Privileges to an Operator.
- When the Schedule configured for the Privilege is Active and the Operator is logged in, the associated Privilege is active.

For more information about Privileges, see:

- Privilege Editor on Page 423
- Privileges and a Partitioned System on Page 419
- Privilege Tasks on Page 442
- How Privileges are Evaluated on Page 416
- Limited Operators on Page 417
- Access to Common Objects on Page 418

How Privileges are Evaluated

An Operator's overall Privileges in the system are actually a combination of all Privileges assigned to that Operator (with Schedules assigned to the Privileges taken into account). The Operator's Privileges are compared using an OR relationship. The access grants given by a Privilege apply only to objects in the same Partition as the Privilege, or they can apply across multiple Partitions if selected. For a given object, the **least** restrictive Privilege assigned to the Operator is granted.

Example:

The Operator has three user-defined Privileges which are compared as follows:

No Personnel – this Privilege gives the Operator no access to Personnel objects

OR

Read Personnel – this Privilege gives the Operator only Read access to Personnel objects

OR

Edit Personnel – this Privilege gives the Operator Edit and Read access to Personnel objects

Because the OR comparison allows all three Privileges, the Operator is granted both Edit and Read access to Personnel objects.

In this instance, assigning the two more restrictive Privileges to the Operator has no effect.

The preceding evaluation of Privileges is also true for the System Tools and Viewable Message Types, neither of which are partitioned Objects.

Limited Operators

Because of the way Privileges are evaluated, if you need to have limited Operators (who can only view/edit specific objects), you should create Privileges that only grant access to the specific objects your Operators need.

When you create a new Privilege, all object classes are set to **No Access** by default, so that you can enable only those object classes your Operators need.

At minimum, a Limited Operator should have:

- Access to common objects (a pre-defined Privilege included with C•CURE 9000)
- A user-defined Privilege that grants Read access to the Operator class (to enable the Operator to run C•CURE 9000 applications.)
- A user-defined Privilege that grants appropriate access to the objects that the Operator needs to use.

Example:

An Operator has four Privileges which are compared as follows:

Operator Login – a user-defined Privilege that grants Read access to the Operator class, so that an Operator assigned this Privilege can run C•CURE 9000 Applications.

OR

Access to Common Objects – this Privilege is very restrictive, allowing mostly read access to common objects user interface objects like Dynamic Views and Application Layouts, but no access to Personnel, Hardware, Credential, or Video objects.

OR

View Personnel – a user-defined Privilege that grants Read access to Personnel, Image, Clearance, Credential, and related objects.

OR

View Video - a user-defined Privilege that grants Read access to Video servers, Cameras, Views, and Tours.

Because the OR comparison allows the least restrictive Privileges, the Operator is granted the ability to:

- Run the Administration Station application
- View but not edit both Personnel and Video objects
- View Dynamic Views, Monitoring Station Application Layouts

Using Multiple Privileges for Specialized Operators

You can make maintaining Privileges for your Operators easier by creating a basic Privilege for tools and functions that all Operators need, then creating specialized Privileges for tools and functions needed by only a few Operators. This is easier than trying to maintain all-encompassing specialized Privileges for each Operator. If a change needs to occur, you change the Basic Privilege rather than every single specialized Privilege.

Example:

You need to have a set of Privileges for Operators that allow them to monitor activities, but restrict them from editing Personnel or Hardware. However, one of your Operators needs to design and create Badges, while another needs to

perform system backups and volume management.

You can create a basic Operator privilege that provides only the access that all of your Operators need, then you can create a Privilege for your badging Operator that enables only the Tools and object permissions needed for badging, and another Privilege for the Operator who does backups that only enables the Tools and object permissions needed to perform system backups and volume management.

- Basic Operators: Basic Operator Privilege.
- Badging Operator: Basic Operator Privilege + Badging Privilege.
- Backup Operator: Basic Operator Privilege + Backup Privilege.

Access to Common Objects

Access to common objects is a pre-defined Privilege that comes with C•CURE 9000. It provides basic access to the objects that provide the basis of the C•CURE 9000 applications, as shown in Table 96 on Page 418, as well as read access to all of the System Tools tab components (except when a new tool is added on an upgrade).

Table 96: Access to Common Objects Privilege

Classes	Read Access	No Access
Privilege Defaults tab		
Application Layout - Read plus View, Popup View, View in current Tab	✓	
Application Server	✓	
Audit Log	✓	
Card Format	✓	
CHUID Format	✓	
Customer Field Labels	✓	
Dynamic Views - Read plus View, Popup View, View in Tab	✓	
Images - Exception object for Default Image (Read)		✓
Journal	✓	
Operator	✓	
Partition	✓	
Personnel Type	✓	
Personnel Views	✓	
Privilege	✓	

Table 96: Access to Common Objects Privilege (continued)

Classes	Read Access	No Access
Query, plus View, Popup View, View in Tab	✓	
Report Form	✓	
Schedule	✓	
Schedule/Time Zone pairs	✓	
System Variables	✓	
Floors	✓	
CCTV Protocols	✓	
Time Zones	✓	
User-defined Fields	✓	
All other Objects		✓

You can view the settings of **Access to common objects** in the Privilege editor, but you cannot change them. However, you can use **Create Copy** to make a copy of this Privilege, give it a new name, and use it as the basis of user-defined Privileges.

Example:

You can use **Create Copy** to make a new Privilege, and then remove access to License, Backup System, System Variables, Encryption Options, etc. if you do not want your Operators to access these tools.

Privileges and a Partitioned System

Your C•CURE 9000 system can be partitioned into different sectors for both creating and viewing system security Objects. Using Privileges, you can allow or limit an Operator's access to Objects associated with a specific Partition.

- When C•CURE 9000 is installed, the system is unpartitioned and has:
  - The pre-defined SYSTEM ALL Privilege – which gives total Privileges to everything in the C•CURE 9000 system, including the system Default Partition, any Partitions created in the future, and the right to create new Partitions.
  - The pre-defined **Access to common objects** Privilege – which gives Read access to certain basic Objects required for most Operators to get started. (For details, see Table 96 on Page 418.)

    Example:

    Dynamic Views, Queries, Schedules, System Tools, etc.

NOTE SYSTEM ALL actually includes access to the Objects in the 'Access to common Objects' Privileges. The latter Privilege, or a Privilege based on its Template, is needed when you don't want to grant an Operator the blanket SYSTEM ALL Privilege, but lesser Privileges.

- Once you add another Partition, each newly created Partition in your system has its own ALL Privilege:
  - Full Privilege for partition (partition name).

To have access to Objects in a Partition, an Operator must have one of the following Privileges:

- SYSTEM ALL Privilege
- Full privilege for that Partition: “Full Privilege for partition (partition name)”. Full Privilege for Partition causes all system tools to display in the Options and Tools pane.
- A lesser Privilege for that Partition that defines access to one or more Objects in that Partition

  And

  - A user-defined Privilege that includes Read Access to the Operator class in order for the Operator to run C•CURE 9000 applications (can be included in another Privilege).

  And

  - Access to common objects [default]

For information about partitioning, see Partition Overview on Page 380.

Example:

To set up an Operator as a Partition Administrator, with full access Privileges only to objects within the Partition, assign:

- Full Privilege for partition (partition name)
- Access to common objects [default]

Example:

To set up a limited Operator with no access to Personnel objects in the Partition, assign:

- A user-defined Privilege that resides in the partition and specifies No Access to Personnel and related objects.
- Access to common objects [default]
- A user-defined Privilege that includes Read Access to the Operator class in order for the Operator to run C•CURE 9000 applications (can be included in another Privilege).

Privilege and victor Role Interaction in a unified system

Within the unified system, you can customize victor role and C•CURE 9000 privileges to control access levels and to interact with objects in both systems.

There are two levels that determine access to permission classes:

- The client level: the privilege and role interaction rule applies only when you select a common application Client .
- The object level: action and object specific rules are applied to the privilege and role interaction.

Use the Privilege Clients Tab to separate which privilege and which role applies to an operator based on the client.

Note A victor role is a set of access rights that you can assign to an operator to control authorization and permission levels within victor.

Client level evaluation of the privilege and role interaction

The privilege and role interaction rule applies only when the privilege and role have a common application client.

When you select a common application client, permission is evaluated as a combination of both privilege and role and is applied to the Client. When you do not have a common application client, the privilege and role evaluate separately and apply the permission to the client.

For information about assigning application clients to a privilege, see Assigning Application Clients to a Privilege on Page 446.

Example:

If you select the **C•CURE Administration Station** check-box in a privilege, and if you select **victor Unified Client** in the check-box in a role, then the privilege and role interaction does not apply to either client because there is no common client selected. Privilege and role evaluate separately and apply to the client.

Example:

If you select the **C•CURE Administration Station** and **victor Unified Client** check-box in a privilege, and if you select the **victor Unified Client** check-box in a role, then the privilege and role interaction is applied to the **victor Unified Client** because it is the common client. It is not applied to the **C•CURE Administration Station** client.

Example:

If you select the **C•CURE Adminsitration Station Client** and **victor Unified Client** check-box in a privilege, and if you select the **C•CURE Administration Station Client** in a role, then the privilege and role interaction is applied to the **C•CURE Administration Station Client** because it is the common client. It is not applied to the **victor Unified Client**.

Object level evaluation of the privilege and role interaction

There are four rules for privilege and role interaction when you access C•CURE 9000 and victor Unified Client actions. These consist of two types of actions, CRUD and non-CRUD, that consist of their own two rules, as shown in Table 97 on Page 421and Table 98 on Page 421

- CRUD - refers to actions related to creating, viewing, editing, and deleting objects in victor and C•CURE 9000.
- non-CRUD - refers to any action that is an object specific action. For example, Door Lock, Door Unlock, Arm and Disarm.

Table 97: Rules for the privilege and role combination for CRUD operations

CRUD Operation Rule	C•CURE Client Outcome	victor Client Outcome
• C•CURE denies permission • victor grants permission	Access Denied	Access Denied
• C•CURE grants permission • victor denies permission	Access Denied	Access Denied

Table 98: Rules for the privilege and role combination for non-CRUD operations

non-CRUD Operation Rule	C•CURE Client Outcome	victor Client Outcome
• C•CURE denies permission • victor grants permission	Access Denied	Access Granted
• C•CURE grants permission • victor denies permission	Access Granted	Access Denied

An additional rule applies to CRUD and non-CRUD actions in the privilege and role interaction, as shown in Table 99 on Page 422

Table 99: Application of CRUD and non-CRUD rules in a privilege and role interaction

Action	Rule
CRUD	Both privilege and roles evaluate the permission classes.
Non-CRUD	The combined client is ignored and each system evaluates independently.

Privilege Editor

The **Privilege Editor** in C•CURE 9000 lets you create Privilege Objects so that you can assign a Privilege to an Operator and give that Operator rights to use access control Objects.

The **Privilege Editor** displays the following tabs for configuring Permissions:

- Privilege Defaults Tab on Page 427
- Privilege Exceptions Tab on Page 430
- Privilege Partition Tab on Page 434
- Privilege System Tools Tab on Page 435
- Privilege Viewable Message Types Tab on Page 436
- Privilege Manual Actions Tab on Page 437
- Privilege Operators Tab on Page 438
- Object Editor Groups Tab on Page 26

NOTE You **cannot** edit the 'SYSTEM ALL' Privilege, the 'Access to common Objects' Privilege, or any 'Full Privilege for Partition' Privilege.

Accessing the Privilege Editor

You can access the **Privilege Editor** from the C•CURE 9000 **Configuration** pane.

To Access the Privilege Editor

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

   - or -

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

   The **Privilege Editor** opens.

The **Privilege Editor** has the buttons described in Table 100 on Page 423.

Table 100: Privilege Editor Buttons

Button	Description
Save and Close	Click this button when you have completed any changes to the Privilege and wish to save those changes. The **Privilege Editor** closes.
Save and New	Click this button when you have completed any changes to the Privilege and wish to save those changes and also create a new Privilege. The Privilege you were editing is saved, and a new Privilege opens (either blank or including template information if you were using a template to create the new Privilege).
Create Copy	Click this button to make a new Privilege, and then remove access to License, Backup System, System Variables, Encryption Options, etc. if you do not want your Operators to access these tools. Exceptions are not copied if the new Partition is different from the Partition of the Privilege.

Table 100: Privilege Editor Buttons (continued)

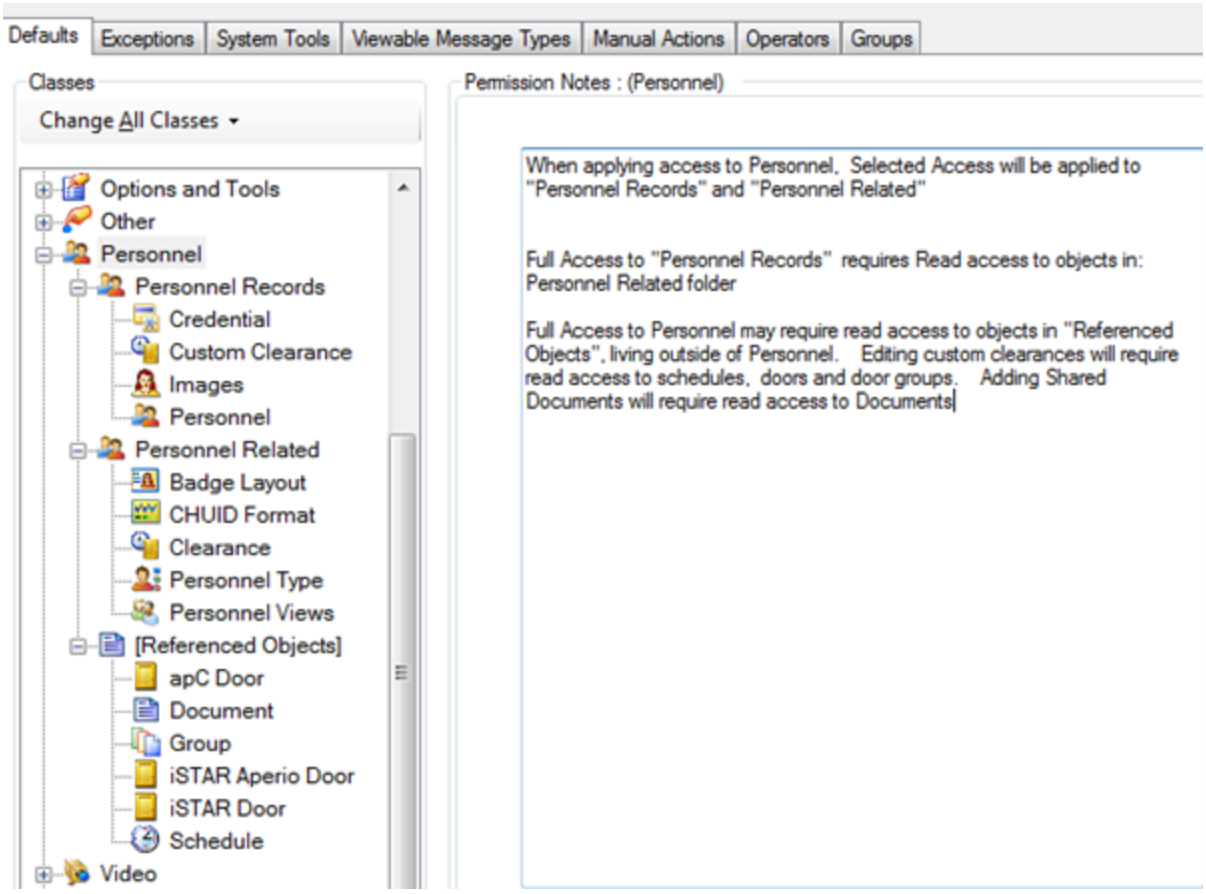
Button	Description
	Click this button when you want to close the **Privilege Editor** without saving your changes. A warning appears asking whether or not you want to save your changes before closing the editor. Click **Yes** to exit and save and **No** to exit and cancel your changes.

Privilege Screen

The Privilege screen uses a tree view with items organized in the same order of categories as on the Administration Configuration Panes. The categories are as follows:

- Areas and Zones
- Configuration
- Data Views
- Card Formats and Keys
- General Purpose Interface
- Guard Tour
- Hardware
- Other (Manual Actions?)
- Personnel
- Options and Tools
- Video
- Visitor Management

Figure 134: Privilege Screen



Every privileged Object Type falls under one of these main categories. Categories may have sub-categories. Some object types, for example, documents, can occur in more than one category. Documents appear under Configuration and also in a “Referenced Objects” folder under other categories.

Permission Notes vary according to Object Types.

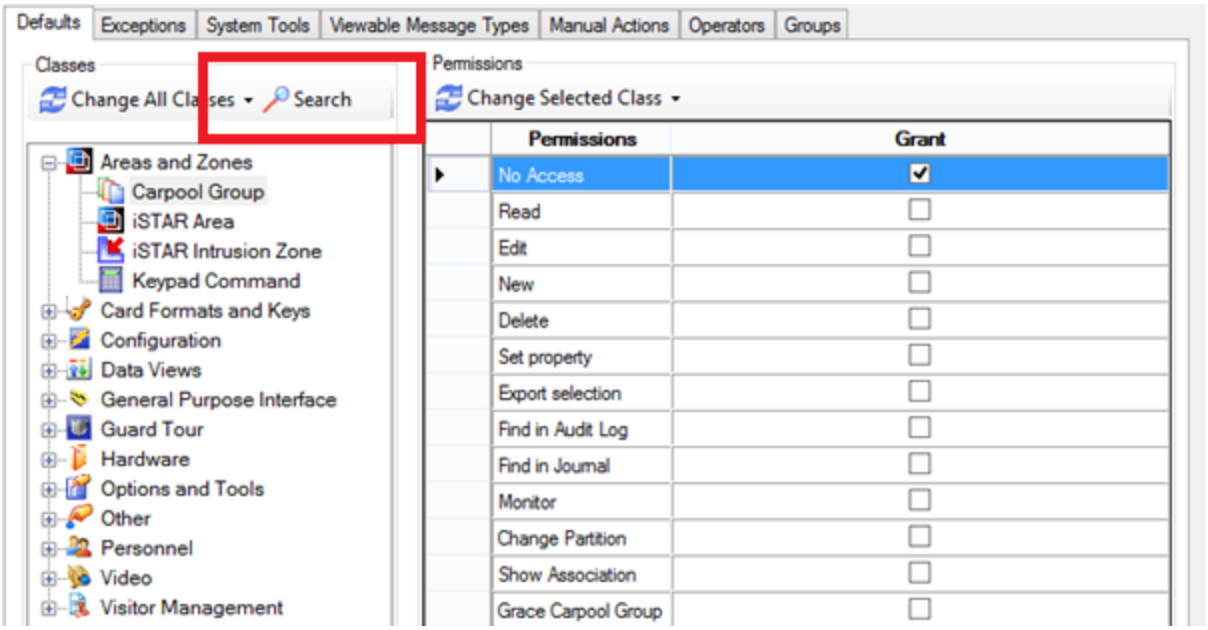
Searching for Types

The **Privilege** Tree is designed to group objects. In order to find a specific type of object, the Defaults tab provides a menu option that allows you to search for a object type in the tree.

To Search for a Type of Object

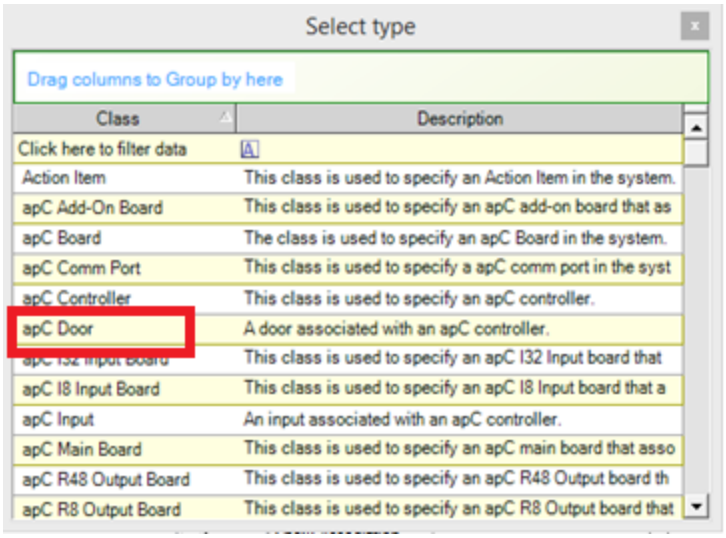
1. From the Defaults tab, select Search for a typeof object, in this case, and apC door:

Figure 135: Search from Defaults tab View

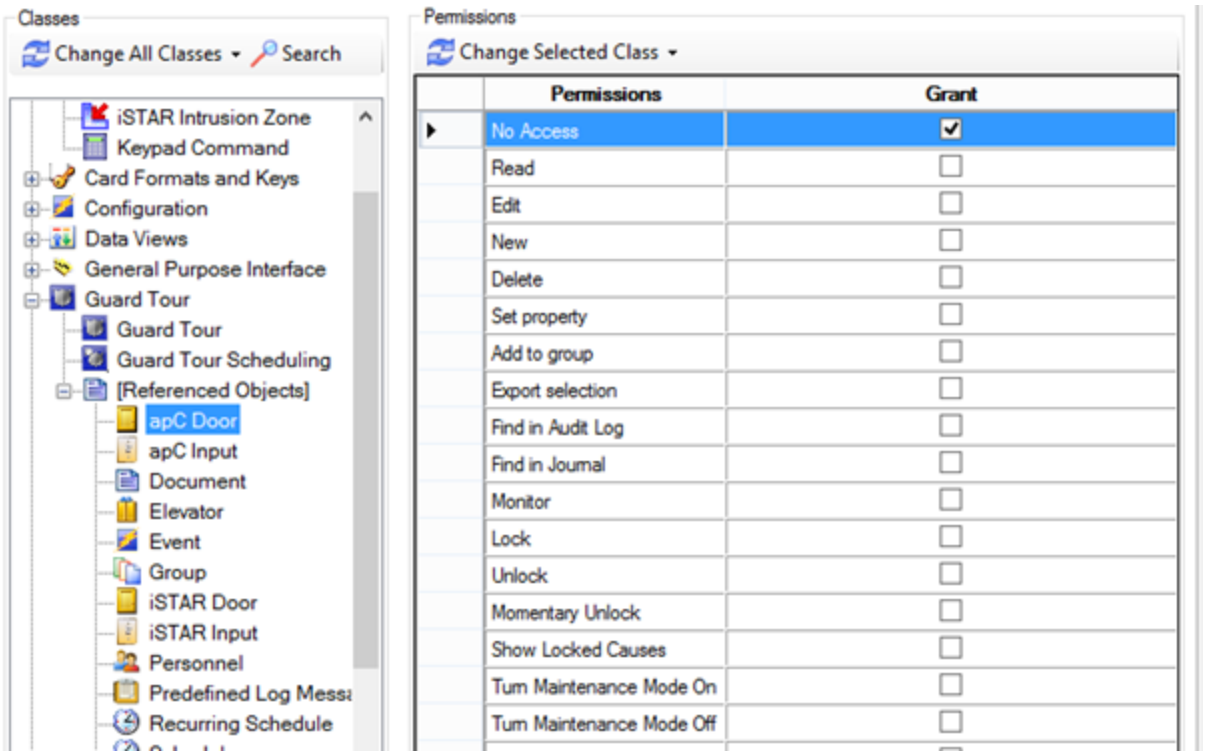


2. A type selection dialog box appears:

Figure 136: Search Selection Type Dialog Box



The apC Door Node appears under References Objects:



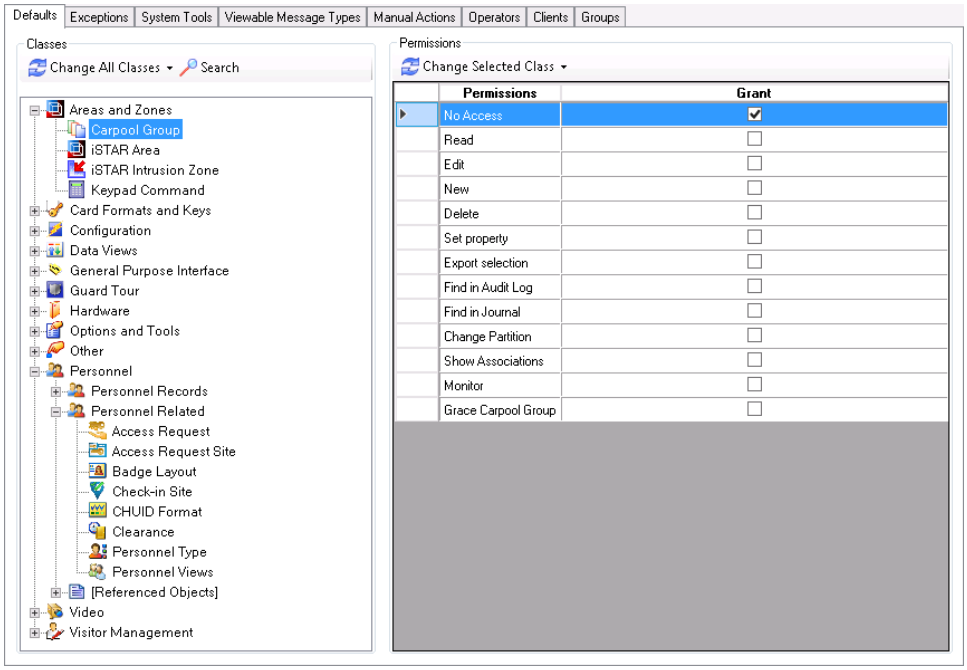
3. Select the Permissions you want to assign for that Door.

If you select Search again, the Search begins from the selected node. If the Search finds nothing, it starts at the top of the tree until the item is found. If nothing is found, a dialog box displays a message that the Search cannot find the type.

Privilege Defaults Tab

The **Defaults** tab lets you give or deny Permissions for security Objects. See Figure 137 on Page 428.

Figure 137: Privilege Editor - Defaults Tab



Example:

The Personnel Category has three subcategories, as shown in Figure 137.

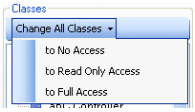
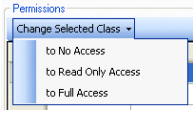
- **Personal Records** includes tables that are modified when you edit a Personnel record.
  - Credential, Custom Clearance, Images, and Personnel
- **Personnel Related** includes tables that are accessed but not modified when you edit a Personnel record.
  - Badge Layout, CHUIDFormat, Clearance, Personnel Type, and Personnel Views
- **Referenced Objects** includes tables that belong to other categories, but may be referenced when you edit a Personnel record.
  - Documents: needed if the user wants to add shared documents
  - Group, Door, Schedule. Elevators, Floors: needed if the user is configuring custom clearances

The **Privilege Editor** and **Defaults** tab have the fields and buttons described in Table 101 on Page 428.

Table 101: Privilege Editor Defaults Tab Fields

Fields/Buttons	Description
Name	Enter a unique name, up to 100 characters, to identify the Privilege.
Description	Enter a description, up to 255 characters, to describe the Privilege.
Enabled	Select this check box to enable this Privilege for Operators assigned this Privilege. If this check box is **not** selected, this Privilege is disabled and ignored by the system.
Partition	A read-only field displaying the Partition to which this Privilege belongs. (This field is visible **only** if the C•CURE 9000 system is partitioned.)
Classes	
Classes	A list of all access control Objects.

Table 101: Privilege Editor Defaults Tab Fields (continued)

Fields/Buttons	Description
Change All Classes	Click the down-arrow to open the following drop-down list:  Selecting one of these options changes all the Permissions for all the Object classes in the system to that Permission level.
Search	Provides a menu option that allows you to search for an object type in the tree.
Permissions	
Change Selected Class	Click the down-arrow to open the following drop-down list:  Selecting one of these options changes all the Permissions for the Object class selected in the **Classes** list to that Permission level.
Permissions	A list of Permissions for the selected Object. Select the Permission that you wish to **grant** or **not grant**. NOTE: In addition to the standard set of Permissions described below, different Classes may have other Permissions particular to that Class, such as New, Delete, Add to group, Export selection, Find in Journal, Change Partition, etc. **No Access** No access to this Object. Object is hidden from the view of the Operator who holds this Privilege. **No Access** is mutually exclusive. If you select No Access, you **cannot** select other Permissions. **Read-Only Access** Allows only Read access **Full Access** All access for all objects
Permission Notes	**Grant** is used to **give** or **deny** Permissions. • Select the check box to **grant** the Permission. - or - • Clear the check box to **deny** the Permission.

Node Context Menu

The Defaults tab contains nodes that support right-click menu items (see Privilege Overview on Page 416

Each node may have different menus (see Figure 138 on Page 430). For example, the Personnel Node has the following menu:

- **No Access**

  Allows no access to the selected Object. The Object is hidden from the view of the Operator who holds this Privilege.

  No Access is mutually exclusive. If you select No Access, you **cannot** select other Permissions.
- **Read-Only Access**

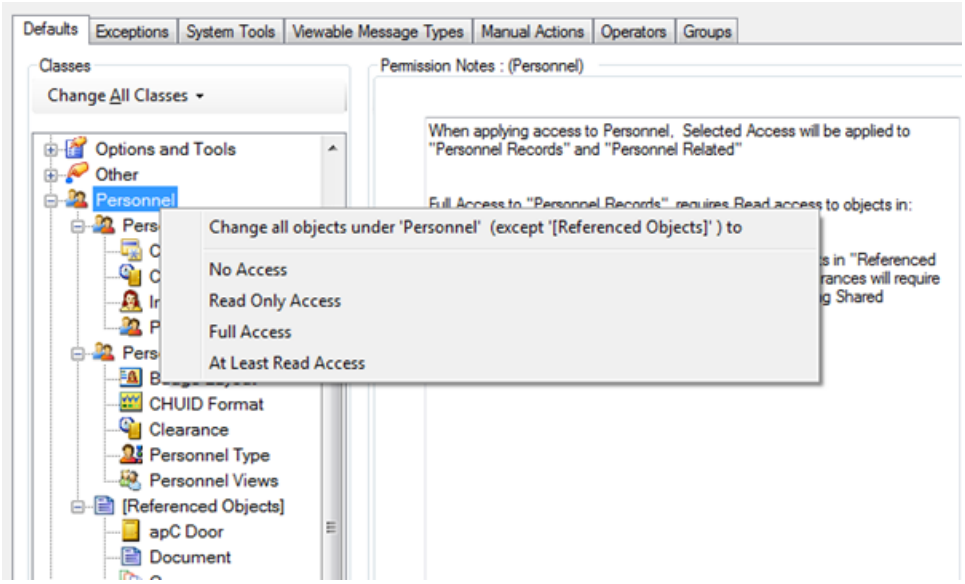
  Allows only Read access.
- **Full Access**

  Allows all access for all objects in the node.

- **At Least ReadAccess**

  Sets the access to Read-Only Access but only if the previous access was not Edit.

Figure 138: Context Menu for Nodes

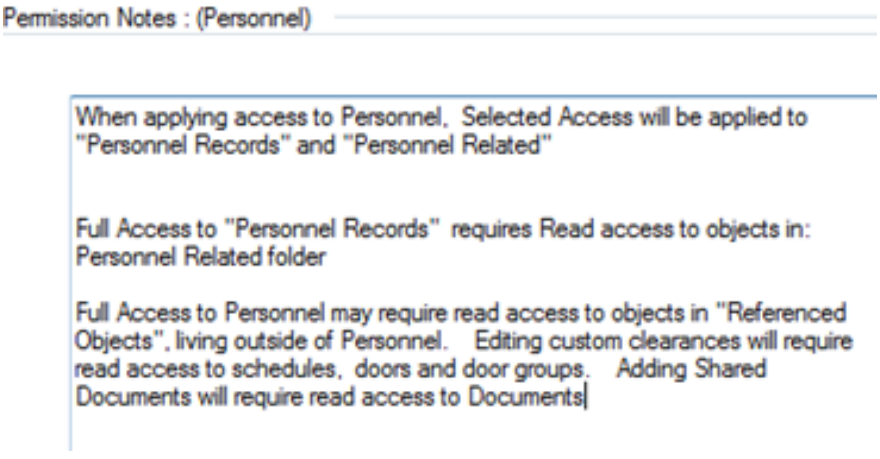


When you select one of these menus, that access applies to all of the objects under the Personnel node. Access applies to all items in the sub-folders EXCEPT for the “Referenced Objects” Folder.

For example, if you select Personnel and “Full Access”, Full Access applies to all entries under **Personnel Records** and under **Personnel Related**. Full Access is not applied to the **Referenced Objects** unless you select the **Referenced Objects** Folder.

Explanation of Permissions

When you click a parent node, for example, **Personnel**, a window displaying **Explanation of Permissions** gives more information about the permissions. For example, Personnel Node provides the following text:



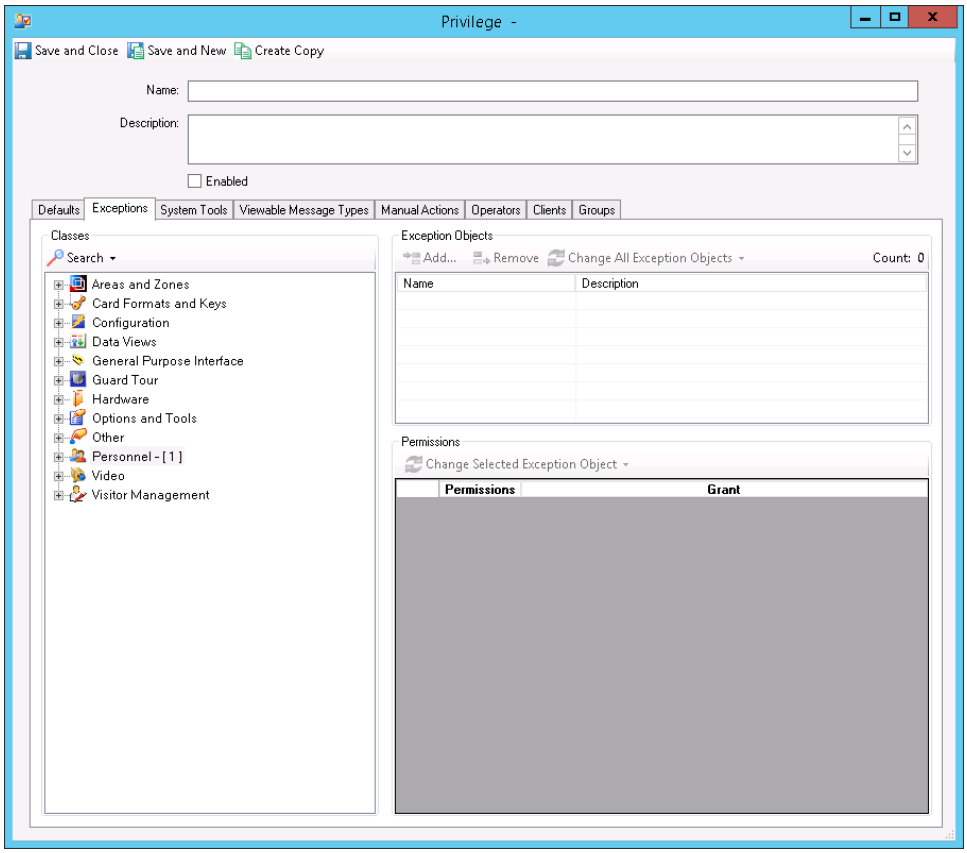
Privilege Exceptions Tab

The **Exceptions** tab, shown in Figure 139 on Page 431, lets you set individual item Permissions. You use this tab to set Exceptions for access control Objects.

Example:

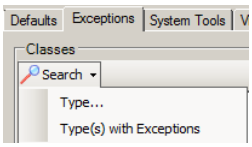
If you have several Holiday Objects and you don't want to give Permission for a particular Holiday Object, you would include that particular Holiday Object in the **Exception Objects** box.

Figure 139: Privilege Editor Exceptions Tab

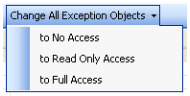
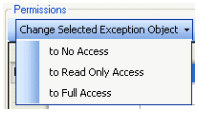


The Exceptions tab has the fields and buttons described in on Page 430.

Privilege Editor - Exceptions Tab Fields

Fields/Buttons	Description
Classes	
Search	Click the down-arrow to open the following drop-down list:  Selecting **Type...** opens a window that lets you select a class type. Selecting **Type(s) with Exceptions**, causes a search for a list of permissions.
Classes	A list of all access control Objects.
Exception Objects	
Add	Click this button to add an Exception to the Privilege by selecting it from the list of Objects that opens for the selected Class.
Remove	Click to remove the selected Exception from the Privilege.

Privilege Editor - Exceptions Tab Fields (continued)

Fields/Buttons	Description
Count	Displays the number of
Change All Exception Objects	Click the down-arrow to open the following drop-down list:  Selecting one of these options changes all the Permissions for all the Exception Objects listed in this box to that Permission level.
Permissions	
Change Selected Exception Object	Click the down-arrow to open the following drop-down list:  Selecting one of these options changes all the Permissions for the Exception Object selected in the **Exceptions Objects** box to that Permission level.
Permissions	A list of Permissions for the selected Object. Select the Permission that you wish to **grant** or **not grant**. You can bulk assign permission exceptions to all objects in the exception list for that object. NOTE: In addition to the standard set of Permissions described below, different Objects may have other Permissions particular to that Object, such as New, Delete, Add to group, Export selection, Find in Journal, Change Partition, etc. **No Access** No access to this Object. Object is hidden from the view of the Operator who holds this Privilege. **No Access** is mutually exclusive. If you select No Access you **cannot** select other Permissions. **Read** Object can be viewed and **not** edited. If you select **Read**, you can select any other Permission except **Edit** and **No Access**. **Edit** Edit the Object. If you select **Edit**, you can select other Permissions except **Read** and **No Access**.
Grant	**Grant** is used to **give** or **deny** Permissions. • Select the check box to **grant** the Permission. - or - • Clear the check box to **deny** the Permission.

Group Exceptions

Group Exceptions are defined as group objects that you can select on the Exceptions tab. If you set a group exception, all the permissions you selected for the group are applied to every member of the group even if the group members are in a different Partition from the Privilege.

Examples:

- With Group Exceptions, you can permit a guard to unlock doors in a specified door group.
- You could also control the list of doors that display at the Monitor Station for a particular Guard.

Rules for Group Privilege Exceptions

- The Groups you select for group exceptions must have a group type that matches the Class type of the client component. For example, if you select iSTAR Doors in the Exceptions tab, all the selected groups must have the iSTAR Doors type.
- When a group (used by an Operator who is currently logged in) is changed, The operator's privileges will be updated.
- The maximum number of group exceptions is 100. The maximum number of group members in a group exception is 1000.
- You **cannot** group the following objects:

Synchronization Conflicts	Audit Log	Customer Labels	Documents
Export Result	Group	Import Results	Journal Log Base
Manual Action	Report Result	Schedule Time Zone Pair	System Variables
UDF Field Definition	Card Format	CHUID Format	Comm Method
Controller	Credential	Images	Journal
Personnel View	RM Reader LCD Message Set	Smart Card Key	

How Group Exceptions are Evaluated

The Group Exceptions are evaluated on each object as follows:

- Each Privilege is evaluated separately:
  - If an object has **no** exceptions, the permissions on the Default tab apply.
  - If the object has any exceptions, the permissions of the Exceptions tab apply.
  - If the object has an exception and is part of a group that has an exception, the permissions of the exceptions are applied in this order:
    1. If an object is part of group exception the permissions on the group apply.
    2. If the object has an exception, the permissions of the Exceptions tab apply.
    3. If an object has no exceptions, the permissions on the default tab will apply.
- The results of the evaluations of each privilege are then OR'd together, so that the Operator permission for each object is the permission of the highest value.

Example:

Scenario 1

Privilege X: No Access to Readers.

Privilege Y: No Access to Readers, with Exception of Read Access to “Reader 1”.

Result: The Operator with privileges X and Y will have Read access to “Reader 1”.

Scenario 2

Privilege X: No Access to Readers.

Privilege Y: No Access to Reader, with the exception of Read Access to “Reader Group A”, where “Reader Group A” contains “Reader 1” and “Reader 4".

Result: The Operator with privileges X and Y will have Read access to “Reader 1” and “Reader 4”.

Scenario 3

Privilege X: Full Access to Readers.

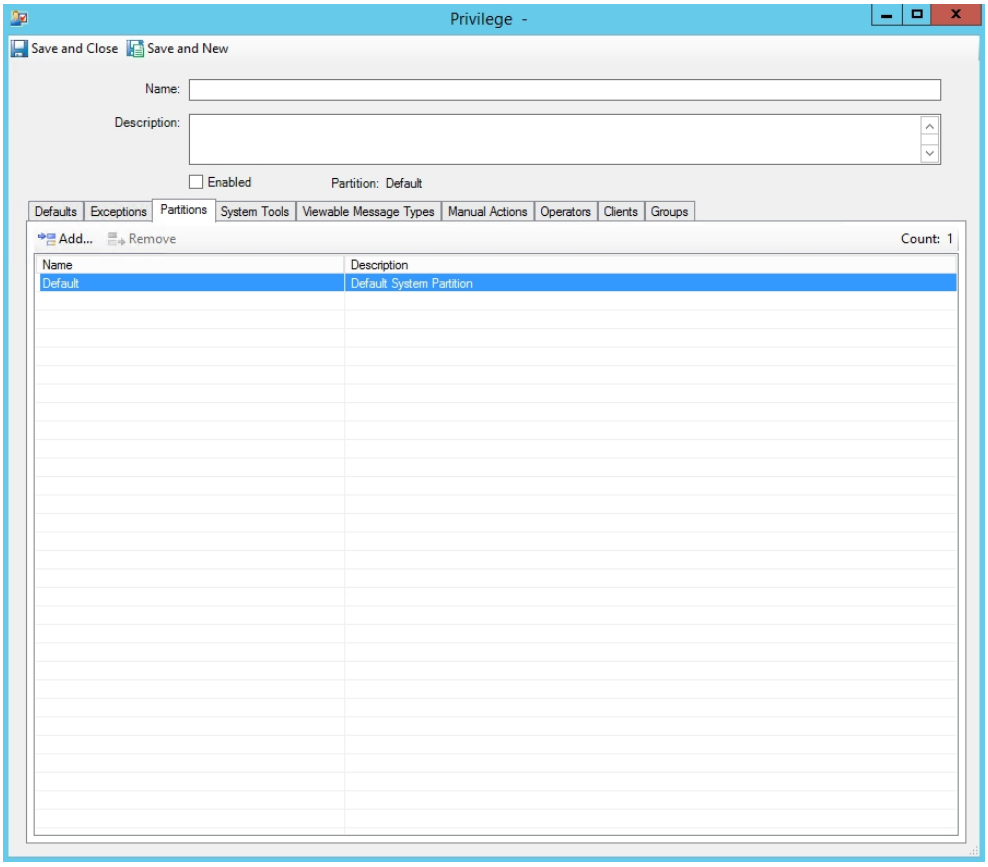
Privilege Y: Read Access to Readers, with exception of No Access to “Reader 1”.

Result: The Operator with privileges X and Y will have Full access to “Reader 1”.

Privilege Partition Tab

The Privilege Partition Tab, shown in Figure 140 on Page 434 , is used to add individual Partitions to a Privilege.

Figure 140: Privilege Partition Tab



Example:

If you have many Partitions and want to give Operators the ability to edit some Partition Objects, but not all Partition Objects, you would add Partitions to the Privilege using **Add** in the Partitions tab and selecting the desired Partitions within the **Object Selection** box.

The Partitions tab has the fields and buttons described in Table 102 on Page 434.

Table 102: Privilege Editor - Partitions Tab Fields

Fields/Buttons	Description
Name	Enter a unique name, up to 100 characters, to identify the Privilege.
Description	Enter a description, up to 255 characters, to describe the Privilege.

Table 102: Privilege Editor - Partitions Tab Fields (continued)

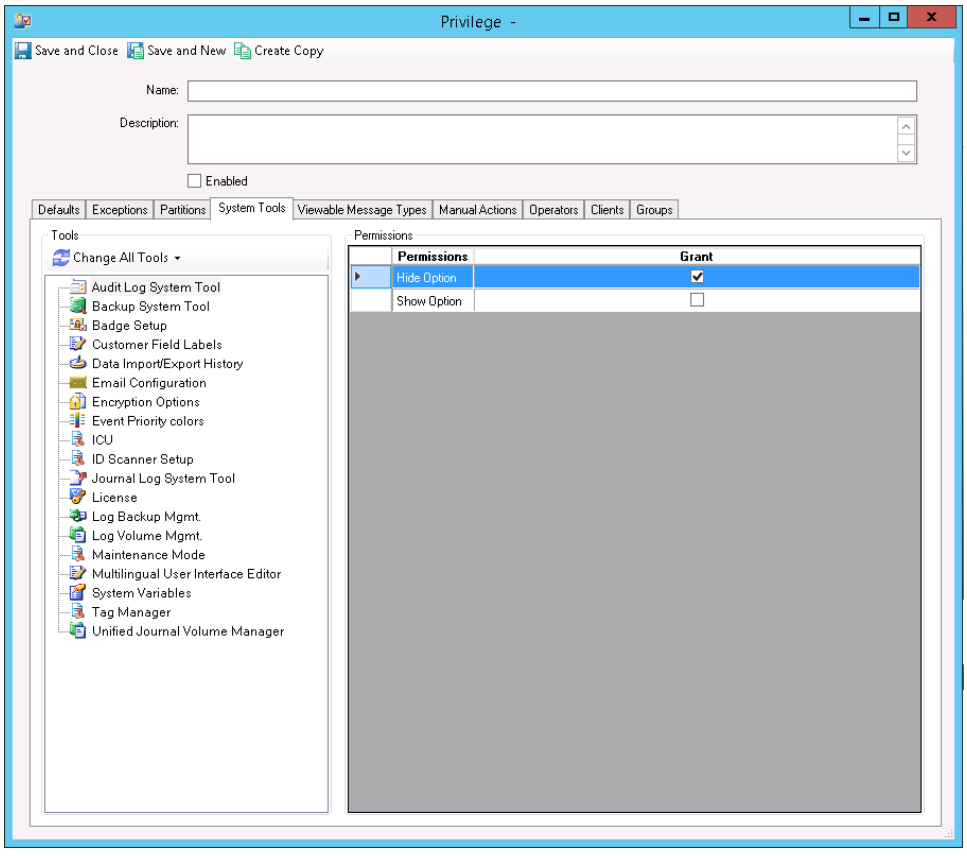
Fields/Buttons	Description
Enabled	Select this check box to enable this Privilege for Operators assigned this Privilege. If this check box is **not** selected, this Privilege is disabled and ignored by the system.
Partition	A read-only field displaying the Partition to which this Privilege belongs. (This field is visible **only** if the C•CURE 9000 system is partitioned.)
Add	Click this button to add a Partition, or Partitions, by selecting it from the list of Objects that opens for the selected class.
Remove	Click to remove the selected Partition, or Partitions, from the Privilege.
Count	Displays the number of Partitions added to the Privilege.

Privilege System Tools Tab

The **System Tools** tab lets you grant or deny Permissions for non-security Objects. See Figure 141 on Page 435.

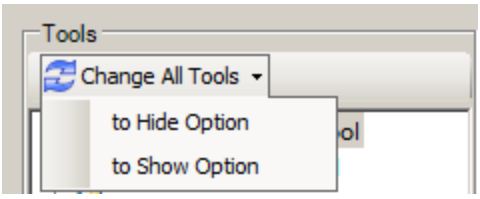
NOTE The Privileges for System Tools are **not** restricted by Partition.

Figure 141: Privilege Editor System Tools Tab



The **System Tools** tab has the fields and buttons described in Table 103 on Page 436.

Table 103: Privilege Editor System Tools Tab Fields

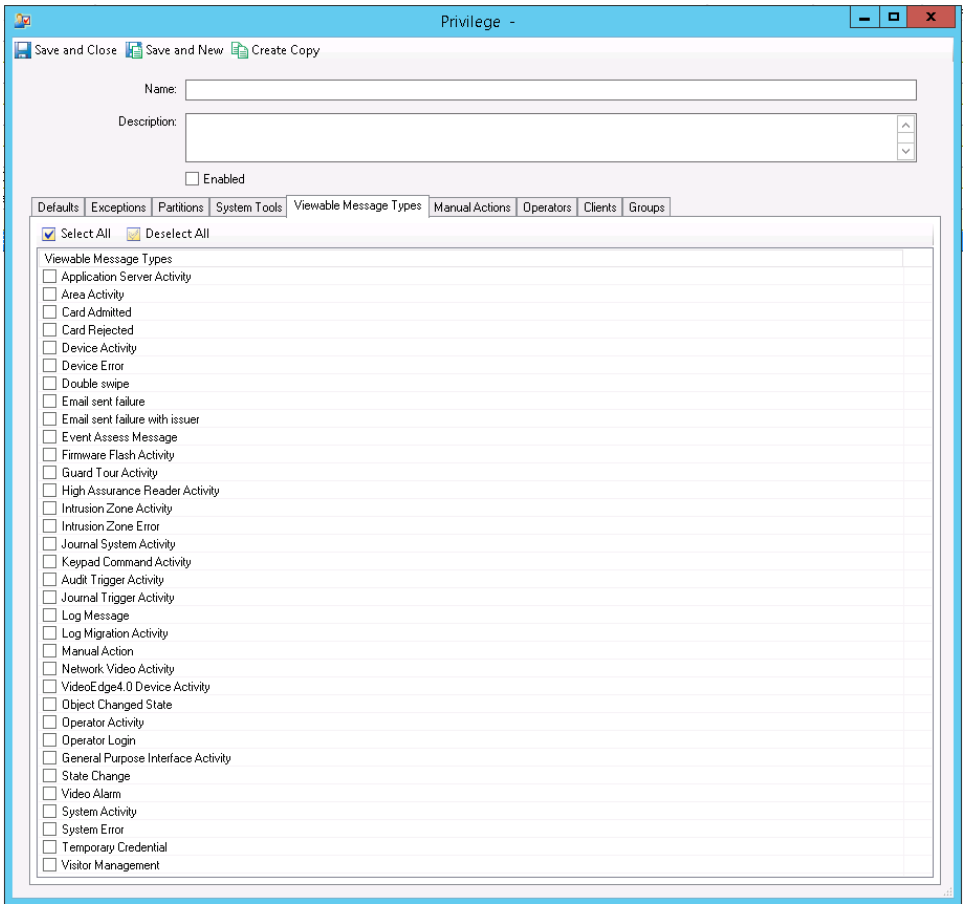
Fields/Buttons	Description
Tools	
Change All Tools	Click the down-arrow to open the following drop-down list:  Selecting one of these options changes all the Permissions for all the System tools in the **Tools** list to that Permission level.
Tools	A list of the non-security Objects.
Permissions	A list of Permissions for the selected Object. Select the Permission that you wish to **grant** or **not grant**. NOTE: In addition to the standard set of Permissions described below, different Objects may have other Permissions particular to that Object, such as Popup view, Delete, Export Selection, etc. **to Hide Option** To hide this Object. Object is hidden from the view of the Operator who holds this Privilege. **to Show Option** To Show the Object. The Object is shown in the View of the Operator who holds this Privilege.
Grant	**Grant** is used to **give** or **deny** Permissions. • Select the check box to **grant** the Permission. - or - • Clear the check box to **deny** the Permission.

Privilege Viewable Message Types Tab

The **Viewable Message Types** tab, shown in Figure 142 on Page 437, lets you select which Message Types this Privilege allows to be viewed on the Monitoring Station. Once you make your selection(s), any Operators assigned this Privilege can view Messages of these types on the Monitoring Station (assuming they have the relevant Privileges for the Monitoring Station).

NOTE The Privileges for Message Types are **not** restricted by Partition.

Figure 142: Privilege Editor Viewable Message Types Tab



The **Viewable Message Types** Tab has the fields and buttons described in Table 104 on Page 437.

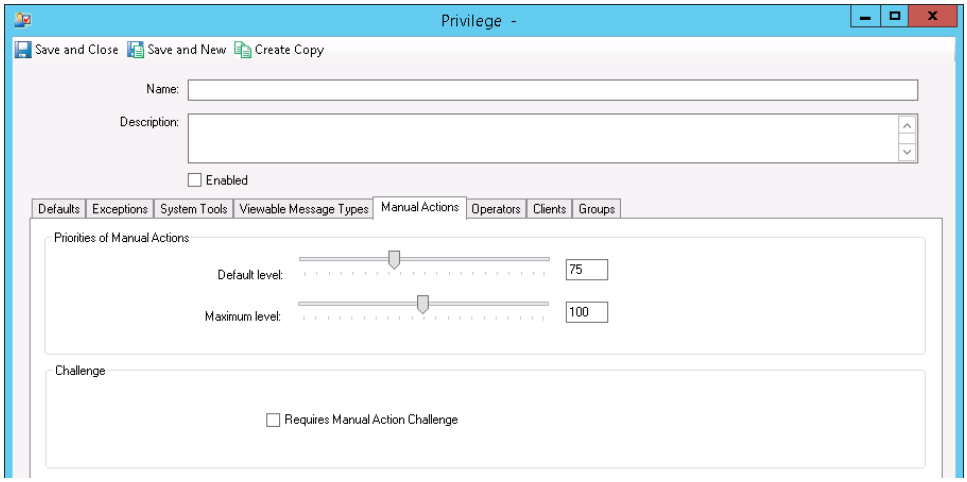
Table 104: Privilege Editor - Viewable Message Types Tab Fields

Fields/Buttons	Description
Select All	Selects **all** the Viewable Message Types.
Deselect All	**Clears all** the Viewable Message Types.
Viewable Message Types	A list of Viewable Message Types for the Privilege. If Message Types are **selected**, Operators assigned this Privilege can view Messages of the selected type on the Monitoring Station and/or the Journal. If Message Types are **not** selected, Operators cannot view messages of the type.

Privilege Manual Actions Tab

The **Manual Actions** tab lets you set the priorities, default and maximum, for this Privilege and whether or not the Manual Action Challenge is enabled. See Figure 143 on Page 438.

Figure 143: Privilege Editor Manual Actions Tab



The **Manual Actions** tab has the fields and buttons described in Table 105 on Page 438.

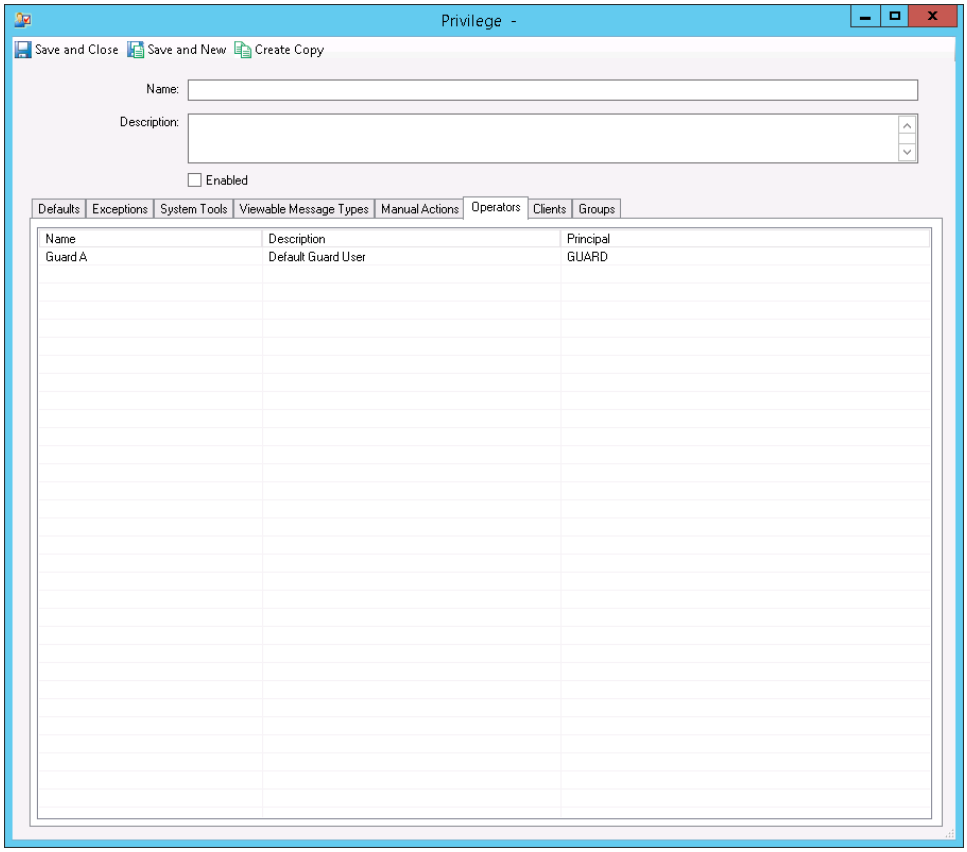
Table 105: Privilege Editor - Manual Actions Tab Fields

Fields/Buttons	Description
Priorities of Manual Actions	
Default Level	Specify the default priority that Operators with this Privilege can assign to Manual Actions. The **Default Level** value must be a value less than the **Maximum Level** value. The default is 75. The range is 1 to 200.
Maximum Level	Specify the maximum priority that Operators with this Privilege can assign to Manual Actions. The **Maximum Level** determines the priority for Manual Actions allowed with this Privilege. Operators **cannot** manually execute an Action that has a higher priority. **Example:** An Operator with a maximum priority level of 100 **cannot** activate an Event with a priority of 115. The default is 200. The range is 0 to 200.
Challenge	
Requires Manual Action Challenge	Select this option to require the Manual Action Challenge for Operators with this Privilege. An enabled Manual Action Challenge requires the Operator attempting to execute a manual action to authenticate with the system to successfully perform the manual action. (Authentication includes entry of Domain/Workgroup Name, User Name, and Password.) The default is unselected.

Privilege Operators Tab

Use the **Operators** tab to view a read-only list of Operators who hold this Privilege. See Figure 144 on Page 439.

Figure 144: Privilege Editor Operators Tab



The **Operators** tab has the fields and buttons described in Table 106 on Page 439.

Table 106: Privilege Editor Operators Tab Fields

Fields/Buttons	Description
Name	Name of the Operator who holds this Privilege.
Description	Description of the Operator who holds this Privilege.
Principal	The username and password assigned to the Operator in either of the following: • **Basic Authentication:** Operators can use Basic Authentication to define user names and passwords for each Operator, without using Windows authentication. NOTE: Basic Authentication can only be used if you enable it within System Variables. • **Windows User Account Authentication:**Windows User Account Authentication: Windows Authentication (Domain Name/User Name) for the Operator who holds this Privilege is identified at login, for example, AMERICAS/FKRAFT.

Privilege Clients Tab

Use the privilege **Clients** tab to assign C•CURE 9000 and victor client applications to a privilege. When an Application Client is assigned to a privilege, operators with that privilege will have access to permissions associated with that client application.

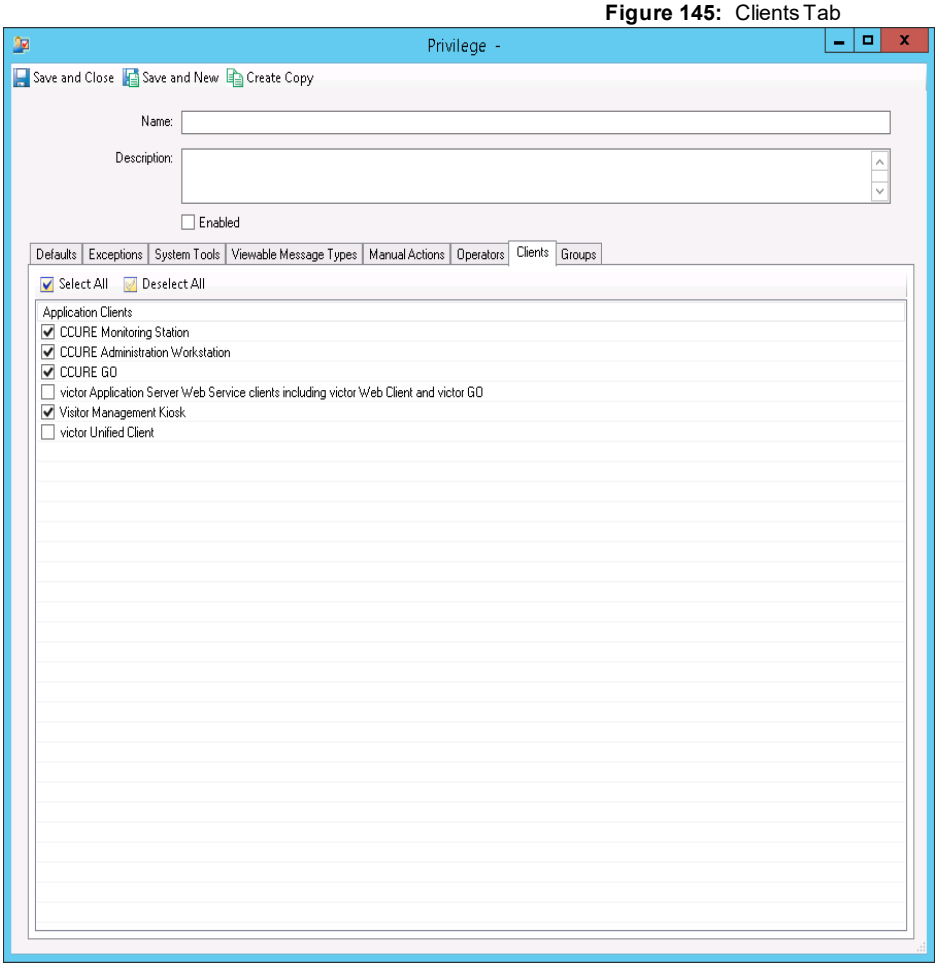
For more information about the use of Application Clients in a Unified system, see Privilege and victor Role Interaction in a unified system on Page 420.

You can assign the following application clients to a privilege:

- C•CURE Monitoring Station

- C•CURE Administration Workstation
- C•CURE GO
- victor Application Server Web Service clients victor Web Client and victor Go
- Visitor Management Kiosk
- victor Unified Client privilege

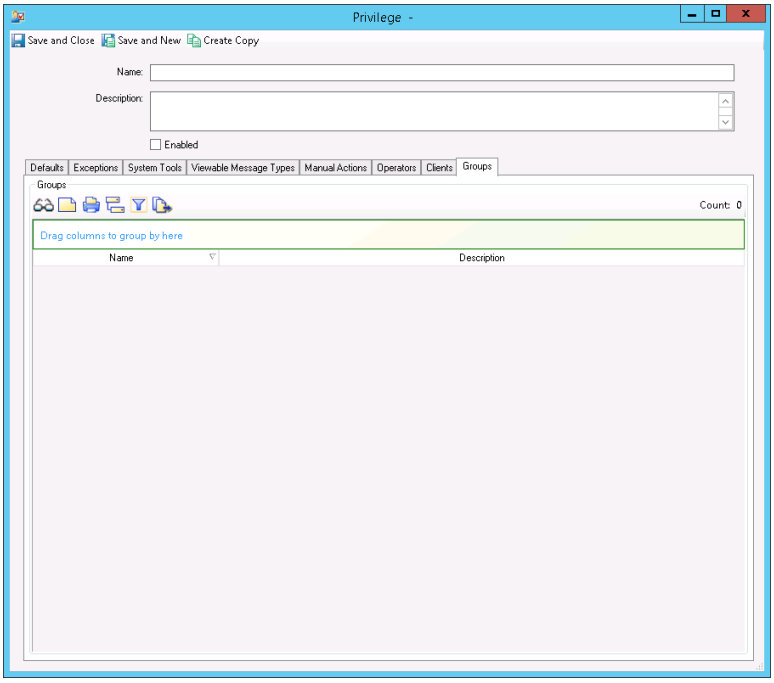
Figure 145: Clients Tab



Privilege Group Tab

The **Groups** tab enables you to view a read-only list of Groups to which this Privilege belongs. See Figure 146 on Page 441.

Figure 146: Privilege Editor Groups Tab



The **Groups** tab has the fields and buttons described in Table 107 on Page 441.

Table 107: Privilege Editor Groups Tab Fields

Fields/Buttons	Description
Name	Name of the Group of which this Privilege is a member.
Description	Description of the Group of which this Privilege is a member.
Groups Toolbar	A Dynamic View toolbar that has the following icons: • Card View - Click to toggle viewing the tab contents as a card view. • Print - Click to open a Windows Printer dialog box to preview and print the tab contents. • Group - Click to toggle the data grouping bar. When the data grouping bar is displayed, you can drag a column onto the bar to cause the data to be grouped by that property. • Filter - Click to toggle the data filtering bar. When the data filtering bar is displayed, you can click the bar to set filtering criteria. • Export view contents to Excel® - Click this button to save the contents of this Dynamic View as an .XLSX (Microsoft Office Open XML Format Spreadsheet) workbook file.

Privilege Tasks

You can perform the following tasks with the Privilege editor.

- Creating a Privilege on Page 442
- Creating a Privilege Template on Page 442
- Configuring Event Permissions for Dual Phase Acknowledgement on Page 443
- Viewing a List of Privileges on Page 445
- Modifying a Privilege on Page 445
- Setting a Property for a Privilege on Page 445
- Creating Privilege Groups on Page 446
- Assigning Application Clients to a Privilege on Page 446
- Deleting an Object on Page 25

NOTE If a Privilege is assigned to any Operators, you must edit the Operators and remove the Privilege before you can delete it.

If you do **not** do this and the Privilege is in use when you try to delete it, an error message displays and the Privilege is **not** deleted.

Creating a Privilege

You can create a new Privilege. For procedures for creating Privileges for setting up and using partitioned systems, see Creating Other Operators for a Partition on Page 398 and Giving Operators Access to Different Partitions on Page 400.

To Create a Privilege

1. In the Navigation Pane of the Administration Workstation, click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Privilege**.
3. Click **New** to create a new Privilege. The **Privilege Editor** opens, and you can configure a Privilege.
4. To save your new Privilege, click **Save and Close**.

   - or -

   Alternatively, if you want to save the Privilege and then create a new one, click **Save and New**. The current Privilege is saved and closed, but the **Privilege Editor** remains open ready for a new Privilege (either blank or including template information if you were using a template to create the saved Privilege).

Creating a Privilege Template

You can create a new Privilege template. A Privilege template saves you time because you do not have to re-enter the same Privilege information again. You can also create an Active Privilege Template so that a Privilege can be configured across multiple Partitions.

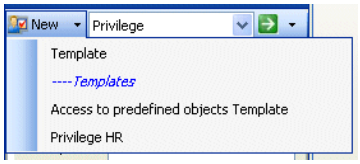
To Create a Privilege Template

1. In the Navigation Pane of the Administration Workstation, click the **Configuration** pane button.
2. Select **Privilege** from the Configuration pane drop-down list.
3. Click the down-arrow next to **New** and select **Template**.

The **Privilege Editor** where you can configure the import template opens.

4. Configure the template to meet your requirements. Any fields for which you configure values become part of the template; then when you subsequently create a new Privilege from that template, these field values are already filled in.
5. In the **Name** field, enter the name you wish to use for the template, such as **Privilege HR**.
6. To save the template, click **Save and Close**.

   The template will be available as an option on the pull-down menu on the **New** button in the **Configuration** pane, underneath the system-supplied template.



To Create a Privilege Active Template

1. In the Navigation Pane of the Administration Workstation, click the **Configuration** pane button.
2. Select **Privilege** from the Configuration pane drop-down list.
3. Click the down-arrow next to **New** and select **Active Template**.

   The **Privilege Editor** where you can configure the template opens.
4. Configure the template to meet your requirements. Any fields for which you configure values become part of the template; then when you subsequently create a new Privilege from that template, these field values are already filled in.
5. When you create a new Privilege from the Active Template you can only change the following fields in the Operator Editor:
   - Name
   - Description
   - Enable
   - Exception Objects
   - Partitions
6. In the **Name** field, enter the name you wish to use for the template, such as **Privilege HR**.
7. To save the template, click **Save and Close**.

   The Active Template will be available as an option on the pull-down menu on the **New** button in the **Configuration** pane.

Configuring Event Permissions for Dual Phase Acknowledgement

This procedure only describes the Event permissions that need to be configured to use Dual Phase Acknowledgement. See Creating a Privilege on Page 442 for detailed procedures and field descriptions.

Table 108: Dual Phase Acknowledgement Permissions

Permission	Grant Meaning
Acknowledge	Selecting the **Acknowledge** check box, and not the Clear check box, allows the Operator to only acknowledge Events.
Clear	Selecting the **Clear** check box, and not the Acknowledge check box, allows the Operator to only clear Events.

Acknowledge Clear	Selecting the **Acknowledge** check box and the **Clear** check box allows the Operator to Acknowledge Events, and if required, Clear the Event.
Acknowledge and Clear	Selecting the **Acknowledge and Clear** check box allows the Operator to acknowledge and clear Events individually, or in one step. NOTE: The **Acknowledge** check box and the **Clear** check box must also be selected.

To Configure the Event Permissions for Dual Phase Acknowledgement

1. In the Navigation Pane of the Administration Workstation, click the **Configuration** pane button.
2. Click the **Configuration** drop-down list and select **Privilege**.
3. Click  to display a list of privileges in the Dynamic View, or click **New** to create a new privilege. The **Privilege Editor** opens.
4. Click on the **Defaults** tab.
5. Click on **Event** located in the **Classes** list.
6. In the **Permission** list, select the Permissions for the privilege. Ensure that the correct permission for Dual Phase Acknowledgement is selected, see Table 108 on Page 443
7. Click **Save and Close**.

Configuring Privileges for the Security View

You need to configure privileges for Security View so you can interact fully or restrict access to this feature. When enabling the Security View privilege the user should have read access to the Application Layout object.

NOTE For a C•CURE 9000 System that is upgraded from a previous version to v2.80, existing Operator Privileges are set with these Privileges **not** enabled, so that Operators do not gain unintended access to a new feature.

This means that an Operator who does not have System All Privilege needs to have these Privileges enabled for Security Association.

The Operator must have the following minimum privileges:

- Read access to the Security View Application Layout object.
- Read and View permissions for Documents and other associated objects if included in assessments.
- Security View if you want the operator to view the Security View for objects.
- Save Security View if you want the Operator to save camera associations.

NOTE Each object type (for example, door, event, area) has its own set of Security View and Save Security View privileges. The object type privileges are enabled and disabled by an administrator.

Assigning Security Association privileges

1. In the **Configuration** pane, select **Privilege** from the drop-down menu.

   If you are editing privileges for an existing record, click the green arrow. If you are creating a new privilege for the Security View, click **New**.
2. In the **Privilege** editor **Defaults** tab, expand the section you want to add as a privilege.
3. Select the object.
4. In the **Permissions** window, select the **Security View** check box to grant permission to view the Security View for objects.

5. Select the **Save Security View** check box if you need the user to save changes to the video camera associations.

   You can also select the **Change Selected Class** drop-down to assign: no access, read only access, or full access.

Viewing a List of Privileges

You can display a list of Privileges by opening a Dynamic View of Privileges. See Viewing a List of an Object Type on Page 22 for more information.

Privilege List Context Menu

The context menu that opens when you right-click a Privilege in the Privilege Dynamic View includes the selections described in Using the Object List Context Menu on Page 23.

Modifying a Privilege

You can modify an existing Privilege by editing it using the **Privilege Editor**.

To Modify a Privilege

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

   - or -

   Double-click the Privilege you want to change.
5. The **Privilege Editor** opens for you to edit the Privilege making changes as you wish.
6. To save your modified Privilege, click **Save and Close**.

   - or -

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

Setting a Property for a Privilege

You can use **Set Property** to set properties for a Privilege. Set Property enables you to quickly set a Privilege property without opening a Privilege. You use Set Property for mass updates.

To Set a Property for Privileges

1. In the Navigation Pane of the Administration Workstation, click **Configuration** to open the Configuration pane.
2. Select **Privilege** from the Configuration pane drop-down list.
3. Click  to open a Dynamic View showing all Privilege Objects.
4. Right-click the Privilege 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 Privilege. Click the drop-down button to see a list of properties.
6. Enter the value for the property and click **OK**.

Assigning Application Clients to a Privilege

Use the **Clients** tab in the Privilege Editor to assign an application client to a privilege.

For more information about the use of Application Clients in a unified system, see Privilege and victor Role Interaction in a unified system on Page 420.

NOTE

- By default, all clients are applied to the **Access to common objects** and **Access to Options and Tools.**
- By default, victor clients are not applied to New or Copied Privileges.

To Assign Client Applications

1. In the navigation pane of the Administration Workstation, click **Configuration** .
2. From the **Configuration** list, select **Privilege**.
3. Click **New**.

   - or -

   Click  to open a **Dynamic View** that shows a list of all existing privilege objects, right-click the privilege that you want to change, and select **Edit** from the menu.
4. Click the **Clients** tab.
5. Select the **Application Client** that you want to assign to the Privilege.
6. Click **Save and Close** to save your changes.

Creating Privilege Groups

You can create a Privilege Group to associate related Privileges, and then assign that group to Operators.

Example:

You create several Privileges that are intended to be used by security officers. Three of the Privileges are designed for Video Monitoring, while three others are designed for Door monitoring. You can create two Privilege Groups - Video Monitoring and Door Monitoring that include the appropriate Privileges, and assign these Privileges to the security officers who need them.

Adding a Privilege to a Group

You can use **Add To Group** to add the Privilege to a Group of Privileges.

To Add a Privilege To a Group

1. Make sure that a Privilege Group is already configured to which the Privilege can be added.
2. In the Navigation Pane of the Administration Workstation, click **Configuration** to open the Configuration pane.
3. Select **Privilege** from the Configuration pane drop-down list.
4. Click  to open a Dynamic View showing all Privilege Objects.
5. Right-click the Privilege in the list that you want to add to a group and select **Add To Group** from the context menu.
6. When the **Group** list displays, select the group you want to add the Privilege to, and click **OK**.

16

Recurring Schedule

This chapter explains how to configure Recurring Schedules in C•CURE 9000.

In this chapter

Recurring Schedule Overview

The Recurring Schedule object in C•CURE 9000 is used to define hourly, weekly, bi-weekly, monthly, quarterly, semi-annual, and annual time schedules that can be used with Guard Tours and other objects.

These schedules can be used to control access to doors, schedule imports and system tasks, and trigger events. The C•CURE 9000 server uses schedules for access control and to perform certain activities, such as time based events, at specified times.

Recurring Schedules can be used to:

- Activate and arm host events.
- Schedule Guard Tours.

Example:

You can use a Recurring Schedule to specify at which times a guard can conduct a Guard Tour

Recurring Schedules cannot be used to:

- Activate and arm panel events - recurring schedules cannot be downloaded for panel events - the iSTAR and apC controllers do not support these schedule types.

NOTE If a host event that is configured to activate or arm by a Recurring Schedule is changed to be a panel event (downloaded to an iSTAR controller), the Event will require a valid Schedule to be selected before the Event can be saved.

You can include one or more Holiday Groups on a recurring schedule. Holiday Groups specify the Holidays that apply to the recurring Schedule (days on which normal activation of the Schedule does not occur).

For more information about Recurring Schedules, see Recurring Schedule Editor on Page 449.

Recurring Schedule Editor

The Recurring Schedule Editor in C•CURE 9000 lets you create a Recurring Schedule object, which is a Schedule type for configuring schedules that recur hourly, daily, weekly, monthly, and yearly. These Schedules are used primarily for Guard Tours, but they also can be used for host Events (see Host Only Event Actions on Page 242).

The following topics give more information about the Recurring Schedule object and how to use it.

NOTE The fields on the General tab change when you change the selection for Recurrence.

Accessing the Recurring Schedule Editor

You can access the Recurring Schedule Editor from the C•CURE 9000 Administration application, Configuration pane.

To Access the Recurring Schedule Editor

1. Click the **Configuration** pane button.
2. Select **Recurring Schedule** from the **Configuration** drop-down list.
3. Click **New** to create a new Recurring Schedule.

   —or—

4. Click  to open a Dynamic View showing all Schedule objects, then double-click the **Recurring Schedule** in the list that you want to edit, and the **Recurring Schedule Editor** opens (see Recurring Schedule Editor on Page 449).
5. Edit the schedule as needed, and click **Save and Close**.

Configuring an Hourly Schedule

Select the **Hourly** option in the Recurrence box to create a Recurring Schedule that first occurs at a specific time and follows a recurrence pattern based on hours thereafter. You can configure the Schedule to activate a single time, or Hourly over a defined period, or repeat in a defined pattern, such as every three hours.

The Recurring Schedule Editor General tab displays fields to set the Start date/time and End data/time for the Recurring Schedule. Figure 147 on Page 451 shows the Hourly Recurring Schedule fields. The Recurring Schedule General tab Hourly Recurring Schedule fields are described in Table 109 on Page 451.

To Configure an Hourly Recurring Schedule

1. Access the Recurring Schedule Editor. See Accessing the Recurring Schedule Editor on Page 449.
2. Select **Hourly** in the Recurrence box.
3. In the **Date/Time** field, select the minutes past the hour and the activation duration for the Recurring Schedule in Minutes. You can use the , or you can type number of minutes you want.
4. In the **Start date**field,
5. Choose one of the settings for **End By**. You can specify an exact number of occurrences, or set an End by date and time (last date/time on which the Schedule can be activated), or set the Schedule to recur repeatedly until the setting is changed.
6. In the Recurrence Pattern section, set how often the Schedule activates by adjusting the **Recur every __ hours** field. You can use the , or you can type number of hours you want between Schedule activations.
7. Click **Save and Close** to save the Recurring Schedule.

Figure 147: Hourly Recurring Schedule

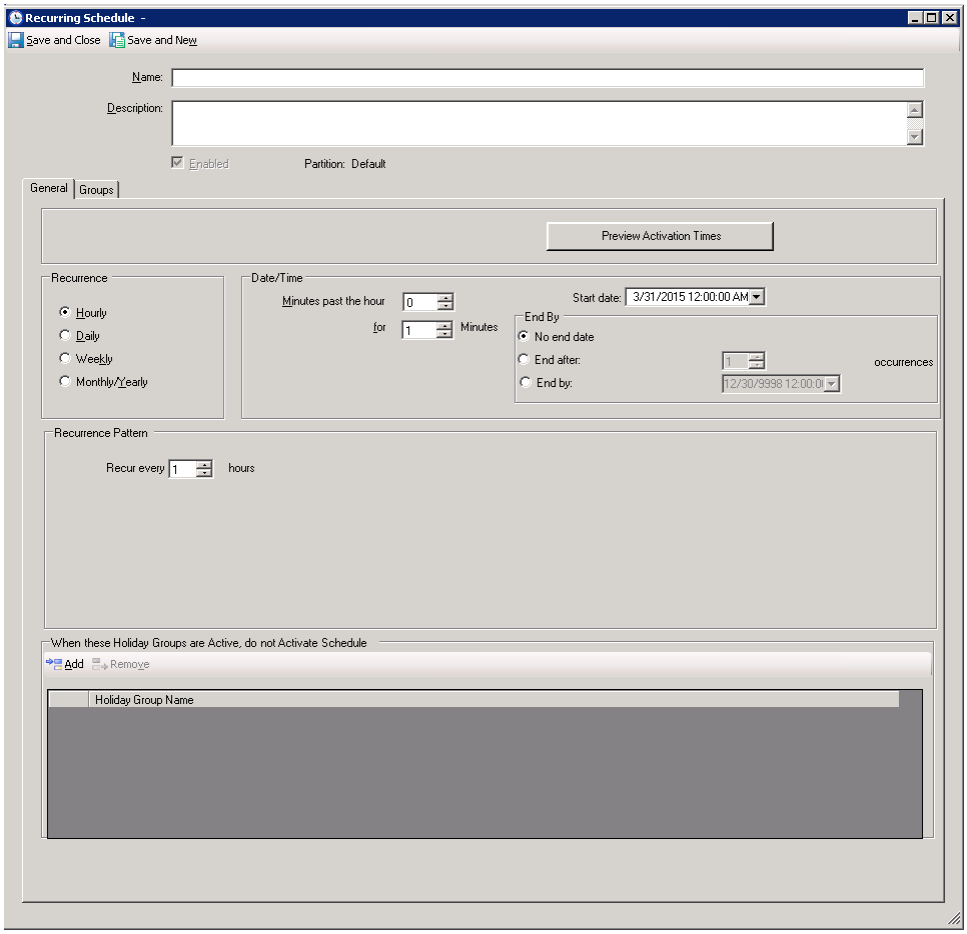


Table 109: Hourly Recurring Schedule Definitions

Field/Button	Description
Preview Activation Times	You can click the **Preview Activation Times** button on the Recurring Schedule General tab to see a graphical representation of a schedule's effect - when the Schedule will be active. See Preview Activation Times on Page 462 for more information.
Recurrence	You can select the type of recurrence for the Schedule. Select **Hourly** for a Schedule that will recur on an hourly Recurrence Pattern.
Date/Time	
Minutes past the hour	You can select the minute after the hour mark for the Schedule to become active. **Example:** Set Minutes past the hour to 15 to activate the Schedule at 12:15, 1:15 ... 11:15). The combination of **Minutes past the hour** and **for __ Minutes** cannot exceed 60.
for __ Minutes	Sets the activation duration for the Recurring Schedule in minutes. **for __ Minutes** accepts a range from 0 to 60. The combination of **Minutes past the hour** and **for __ Minutes** cannot exceed 60.
Start Date	The date and time that the Recurring Schedule is first active. Use the drop-down arrow to choose the date from a calendar, or type a date/time in the field.

Table 109: Hourly Recurring Schedule Definitions (continued)

Field/Button	Description
End By	You must select one of the **End By** values for the Recurring Schedule: **No end date** – the Schedule recurs according to pattern until this value is changed to another End By setting. **End after __ occurrences** – sets a number of times the Schedule can recur. You can use the  to change the value, or type a number. The minimum value is 0 and maximum value is 100. If you change the value to a number greater than 100, the control automatically reverts the value to 100. **End by <date>** – the Schedule recurs until the date you specify. Use the drop-down arrow to choose the date from a calendar, or type a date in the field.
Recurrence Pattern Recur every __ hours	You must specify the pattern for the Schedule's recurrence (every hour,every two hours, etc). The minimum value is 1 and the maximum is 24 hours.
When these Holiday Groups are Active, do not Activate Schedule	You can specify the Holiday Groups that affect this Recurring Schedule. When a Holiday group in this list is active, the Recurring Schedule will not be activated.

Configuring a Daily Schedule

Select the **Daily** option in the Recurrence box to create a Recurring Schedule that occurs on a Day and follows a recurrence pattern thereafter. You can configure the Schedule to activate a single time, or daily over a defined period, or repeat in a defined pattern, such as every three days.

The Recurring Schedule Editor General tab displays fields to set the Start date/time and End data/time for the Recurring Schedule. Figure 148 on Page 454 shows the Daily Recurring Schedule fields. The Recurring Schedule General tab Daily Recurring Schedule fields are described in Table 110 on Page 454.

You can configure a Daily Recurring Schedule that occurs on a specific day (full or partial) or range of days.

To Configure a Daily Recurring Schedule

1. Access the Recurring Schedule Editor. See Accessing the Recurring Schedule Editor on Page 449.
2. Select **Daily** in the Recurrence box.
3. In the **Start Time**field, select the starting time for the Recurring Schedule (HH:MM:AM/PM). You can use the , or you can put the cursor in hours, minutes, or AM/PM and type in the time you want.
4. In the **End Time**field, select the ending time for the Recurring Schedule HH:MM). You can use the , or you can put the cursor in hours, minutes, or AM/PM and type in the time you want.
5. In the **Start Date** field, select the starting date for the Recurring Schedule. Use the drop-down arrow to choose the date from a calendar, or type a date in the field.
6. Choose one of the settings for **End By**. You can specify an exact number of occurrences, or set an End by date (last date on which the Schedule can be activated), or set the Schedule to recur repeatedly until the setting is changed.
7. Set the **Recurrence Pattern** for the Schedule. You can set the Schedule to recur every day, every two days, etc.
8. Click **Save and Close** to save the Recurring Schedule.

Figure 148: Daily Recurring Schedule

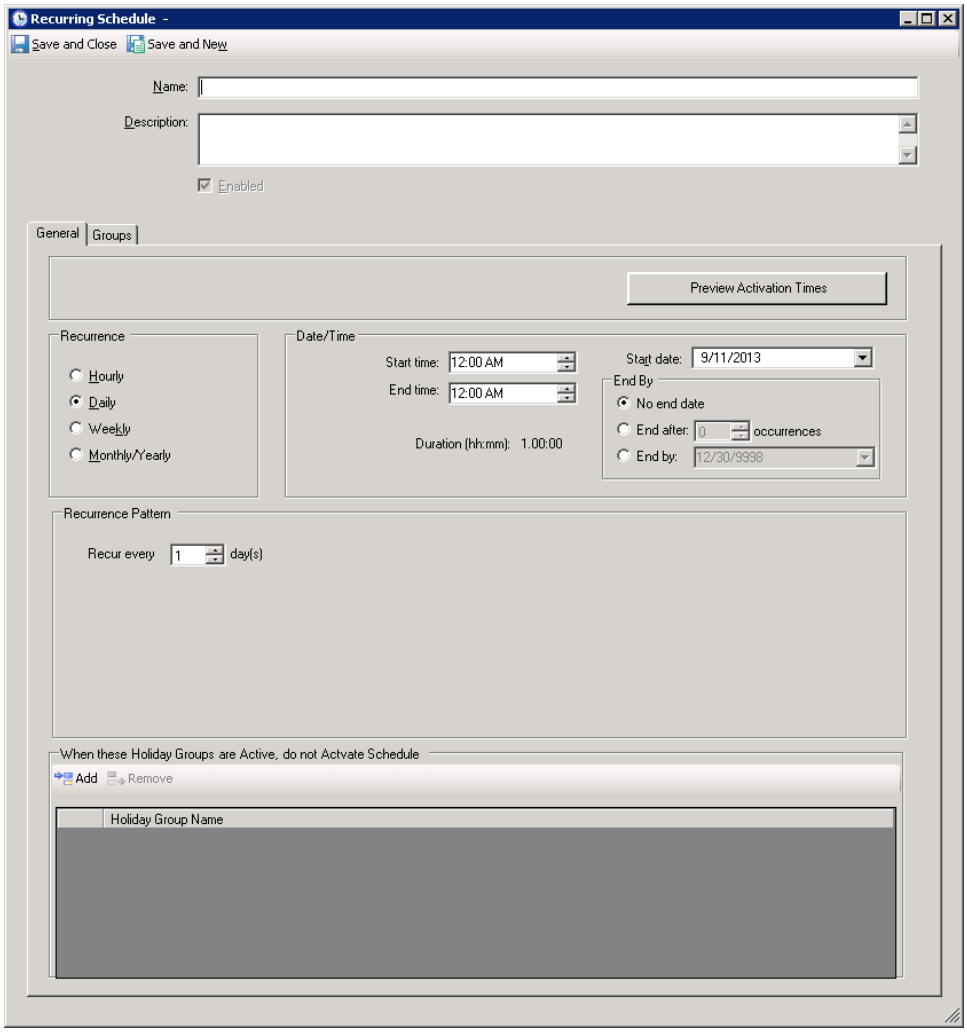


Table 110: Daily Recurring Schedule Definitions

Field/Button	Description
Preview Activation Times	You can click the **Preview Activation Times** button on the Recurring Schedule General tab to see a graphical representation of a schedule's effect - when the Schedule will be active. See Preview Activation Times on Page 462 for more information.
Recurrence	You can select the type of recurrence for the Schedule. Select **Daily** for a Schedule that will recur on a daily Recurrence Pattern.
Date/Time	
Start Time	Choose the time that you want the Recurring Schedule to become active. The field is divided into hours, minutes, and AM/PM. You can use the to change each of these units, or you can put the cursor in hours, minutes, or AM/PM and type in the time you want.
End Time	Choose the time that you want the Recurring Schedule to become inactive. The field is divided into hours, minutes, and AM/PM. You can use the to change each of these units, or you can put the cursor in hours, minutes, or AM/PM and type in the time you want.

Table 110: Daily Recurring Schedule Definitions (continued)

Field/Button	Description
Duration	The calculated amount of time that the recurring schedule will be active.
Start Date	The date that the Recurring Schedule is first active. Use the drop-down arrow to choose the date from a calendar, or type a date in the field.
End By	You must select one of the **End By** values for the Recurring Schedule: **No end date** – the Schedule recurs according to pattern until this value is changed to another End By setting. **End after __ occurrences** – sets a number of times the Schedule can recur. You can use the  to change the value, or type a number. The minimum value is 0 and maximum value is 100. If you change the value to a number greater than 100, the control automatically reverts the value to 100. **End by <date>** – the Schedule recurs until the date you specify. Use the drop-down arrow to choose the date from a calendar, or type a date in the field.
Recurrence Pattern	You must specify the pattern for the Schedule's recurrence (every day, every two days, etc). The minimum value is 1 and the maximum is 366 days. The default value is 1 day.
When these Holiday Groups are Active, do not Activate Schedule	You can specify the Holiday Groups that affect this Recurring Schedule. When a Holiday group in this list is active, the Recurring Schedule will not be activated.

Configuring a Weekly Schedule

Select the **Weekly** option in the Recurrence box to create a Recurring Schedule that occurs on one or more days on a weekly basis and follows a recurrence pattern thereafter. You can configure the Schedule to activate a single time, or Weekly over a defined period, or repeat in a defined pattern, such as every Monday, Wednesday, and Friday.

The Recurring Schedule Editor General tab displays fields to set the Start date/time and End data/time for the Recurring Schedule. Figure 149 on Page 457 shows the Weekly Recurring Schedule fields. The Recurring Schedule General tab Weekly Recurring Schedule fields are described in Table 111 on Page 457.

You can configure a Weekly Recurring Schedule that occurs on a specific day (full or partial) or range of days.

To Configure a Weekly Recurring Schedule

1. Access the Recurring Schedule Editor. See Accessing the Recurring Schedule Editor on Page 449.
2. Select **Weekly** in the Recurrence box.
3. In the **Start Time**field, select the starting time for the Recurring Schedule (HH:MM:AM/PM). You can use the , or you can put the cursor in hours, minutes, or AM/PM and type in the time you want.
4. In the **End Time**field, select the ending time for the Recurring Schedule (HH:MM). You can use the , or you can put the cursor in hours, minutes, or AM/PM and type in the time you want.
5. In the **Start Date** field, select the starting date for the Recurring Schedule. Use the drop-down arrow to choose the date from a calendar, or type a date in the field.
6. Choose one of the settings for **End By**. You can specify an exact number of occurrences, or set an End by date (last date on which the Schedule can be activated), or set the Schedule to recur repeatedly until the setting is changed.
7. Set the **Recurrence Pattern** for the Schedule. You can set the Schedule to recur every week, every two weeks, etc.
8. Select the day(s) of the week on which the Schedule should be activated.
9. Click **Save and Close** to save the Recurring Schedule.

Figure 149: Weekly Recurring Schedule

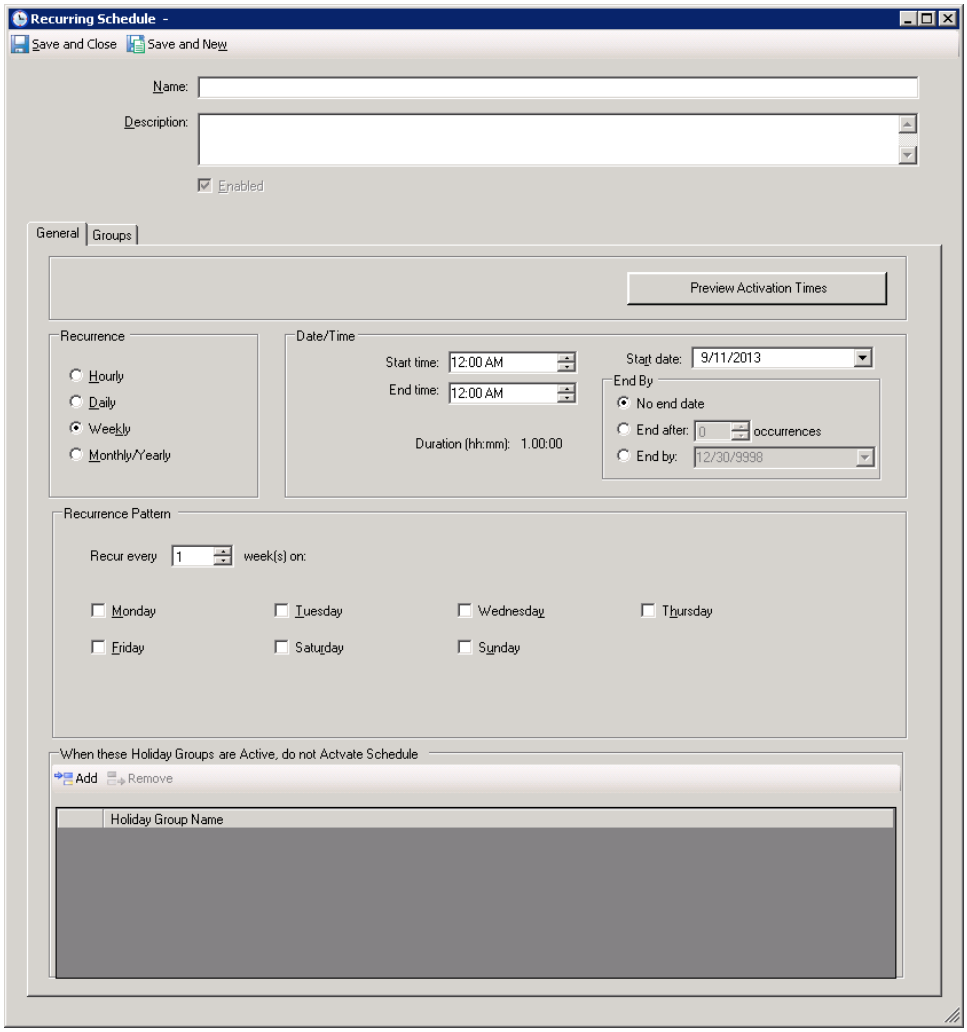


Table 111: Weekly Recurring Schedule Definitions

Field/Button	Description
Preview Activation Times	You can click the **Preview Activation Times** button on the Recurring Schedule General tab to see a graphical representation of a schedule's effect - when the Schedule will be active. See Preview Activation Times on Page 462 for more information.
Recurrence	You can select the type of recurrence for the Schedule. Select **Weekly** for a Schedule that will recur on a weekly Recurrence Pattern.
Date/Time	
Start Time	Choose the time that you want the Recurring Schedule to become active. The field is divided into hours, minutes, and AM/PM. You can use the to change each of these units, or you can put the cursor in hours, minutes, or AM/PM and type in the time you want.
End Time	Choose the time that you want the Recurring Schedule to become inactive. The field is divided into hours, minutes, and AM/PM. You can use the to change each of these units, or you can put the cursor in hours, minutes, or AM/PM and type in the time you want.

Table 111: Weekly Recurring Schedule Definitions (continued)

Field/Button	Description
Duration	The calculated amount of time that the recurring schedule will be active.
Start Date	The date that the Recurring Schedule is first active. Use the drop-down arrow to choose the date from a calendar, or type a date in the field.
End By	You must select one of the **End By** values for the Recurring Schedule: **No end date** – the Schedule recurs according to pattern until this value is changed to another End By setting. **End after __ occurrences** – sets a number of times the Schedule can recur. You can use the  to change the value, or type a number. The minimum value is 0 and maximum value is 100. If you change the value to a number greater than 100, the control automatically reverts the value to 100. **End by <date>** – the Schedule recurs until the date you specify. Use the drop-down arrow to choose the date from a calendar, or type a date in the field.
Recurrence Pattern	You must specify the pattern for the Schedule's recurrence (every day, every two days, etc). The minimum value is 1 and the maximum is 366 days. The default value is 1 day.
Recur every x week(s) on:	You can specify the weekly pattern for the Schedule's recurrence. You can choose a value between 1 and 52. You can also choose the day(s) of the week on which the Schedule should be activated.
When these Holiday Groups are Active, do not Activate Schedule	You can specify the Holiday Groups that affect this Recurring Schedule. When a Holiday group in this list is active, the Recurring Schedule will not be activated.

Configuring a Monthly or Yearly Schedule

Select the **Monthly/Yearly** option in the Recurrence box to create a Recurring Schedule that occurs on a Day in one or more months, or on a yearly basis, and follows a recurrence pattern thereafter. You can configure the Schedule to activate a single time, or monthly over a defined period, or repeat in a defined pattern, such as on the 15th of the month, every three months.

The Recurring Schedule Editor General tab displays fields to set the Start date/time and End data/time for the Recurring Schedule. Figure 150 on Page 460 shows the Yearly/Monthly Recurring Schedule fields. The Recurring Schedule General tab Monthly/Yearly Recurring Schedule fields are described in Table 112 on Page 460.

To Configure a Monthly/Yearly Recurring Schedule

1. Access the Recurring Schedule Editor. See Accessing the Recurring Schedule Editor on Page 449.
2. Select **Monthly/Yearly** in the Recurrence box.
3. In the **Start Time**field, select the starting time for the Recurring Schedule (HH:MM:AM/PM). You can use the , or you can put the cursor in hours, minutes, or AM/PM and type in the time you want.
4. In the **End Time**field, select the ending time for the Recurring Schedule (HH:MM). You can use the , or you can put the cursor in hours, minutes, or AM/PM and type in the time you want.
5. In the **Start Date** field, select the starting date for the Recurring Schedule. Use the drop-down arrow to choose the date from a calendar, or type a date in the field.
6. Choose one of the settings for **End By**. You can specify an exact number of occurrences, or set an End by date (last date on which the Schedule can be activated), or set the Schedule to recur repeatedly until the setting is changed.
7. Set the **Recurrence Pattern** for the Schedule. You can set the Schedule to recur every day, every two days, etc.
8. Click **Save and Close** to save the Recurring Schedule.

Figure 150: Monthly or Yearly Recurring Schedule

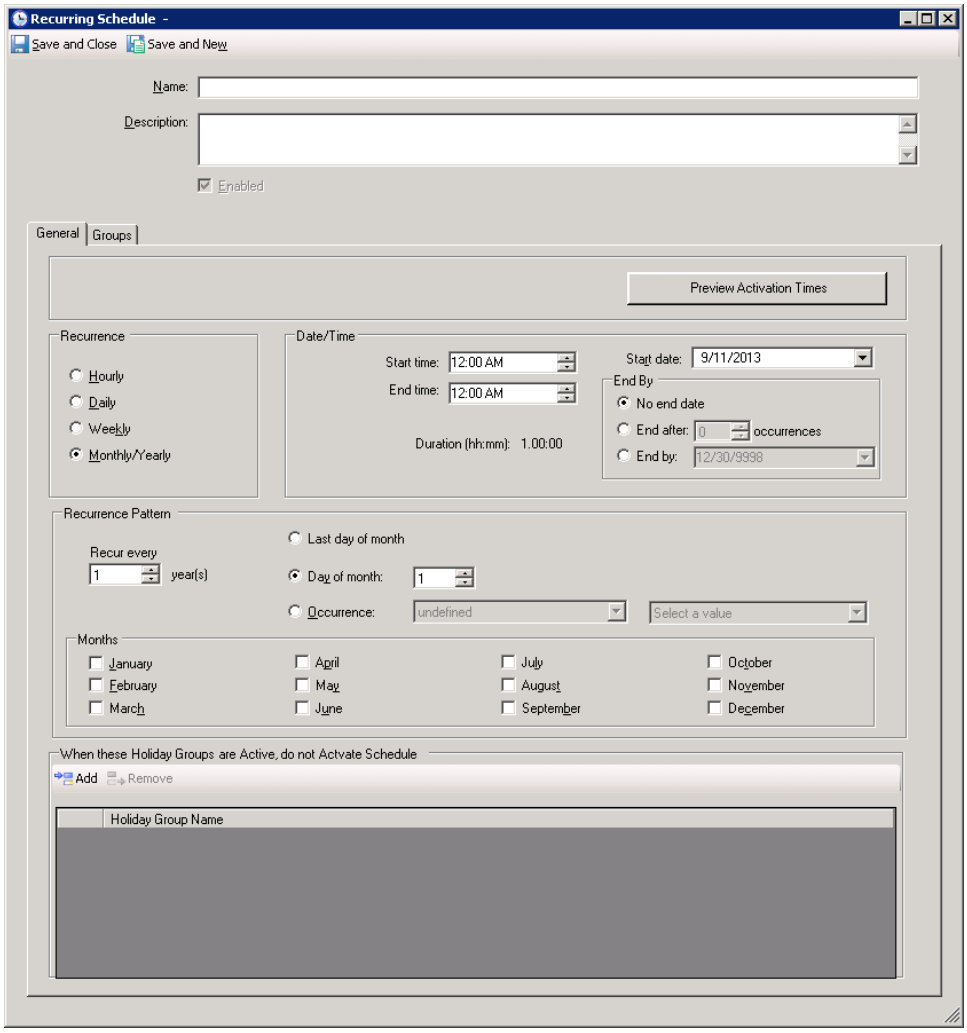


Table 112: Monthly or Yearly Recurring Schedule Definitions

Field/Button	Description
Preview Activation Times	You can click the **Preview Activation Times** button on the Recurring Schedule General tab to see a graphical representation of a schedule's effect - when the Schedule will be active. See Preview Activation Times on Page 462 for more information.
Recurrence	You can select the type of recurrence for the Schedule. Select **Monthly/Yearly** for a Schedule that will recur on a Monthly or Yearly Recurrence Pattern.
Date/Time	
Start Time	Choose the time that you want the Recurring Schedule to become active. The field is divided into hours, minutes, and AM/PM. You can use the to change each of these units, or you can put the cursor in hours, minutes, or AM/PM and type in the time you want.
End Time	Choose the time that you want the Recurring Schedule to become inactive. The field is divided into hours, minutes, and AM/PM. You can use the to change each of these units, or you can put the cursor in hours, minutes, or AM/PM and type in the time you want.

Table 112: Monthly or Yearly Recurring Schedule Definitions (continued)

Field/Button	Description
Duration	The calculated amount of time that the recurring schedule will be active.
Start Date	The date that the Recurring Schedule is first active. Use the drop-down arrow to choose the date from a calendar, or type a date in the field.
End By	You must select one of the **End By** values for the Recurring Schedule: **No end date** – the Schedule recurs according to pattern until this value is changed to another End By setting. **End after __ occurrences** – sets a number of times the Schedule can recur. You can use the  to change the value, or type a number. The minimum value is 0 and maximum value is 100. If you change the value to a number greater than 100, the control automatically reverts the value to 100. **End by <date>** – the Schedule recurs until the date you specify. Use the drop-down arrow to choose the date from a calendar, or type a date in the field.
Recurrence Pattern	
Recur every __ Year(s)	You can specify the yearly pattern for the Schedule's recurrence. You can choose a value between 1 and 7.
Last Day of month	You can select to have this Schedule activate on the last day of each Month selected in the **Months** section.
Day of Month	You can select the day of the month on which this Schedule is activated.
Occurrence	You can use the drop-down lists to specify what day of the week during a month the Schedule is activated. You can choose the first, second, third, fourth, or last weekday (Sunday, Monday, Tuesday, etc.).
Months	You can select one or more Months in which this Schedule will be activated.
When these Holiday Groups are Active, do not Activate Schedule	You can specify the Holiday Groups that affect this Recurring Schedule. When a Holiday group in this list is active, the Recurring Schedule will not be activated.

Preview Activation Times

You can click the **Preview Activation Times** button on the Recurring Schedule General tab to see a graphical representation of a schedule's effect. The active times for the Schedule are shown with a color-coded bar. These active time previews show the effect of any Holiday Groups that are active on the dates being previewed.

You can also use the **Preview Activation Times** context menu selection from a Dynamic View of Recurring Schedules to preview a Recurring Schedule. See Recurring Schedule List Context Menu on Page 464.

For more information about **Preview Activation Times**, see:

- Previewing Schedule Activation Times on Page 481
- Previewing Schedule Activation Times for a Recurring Schedule on Page 463

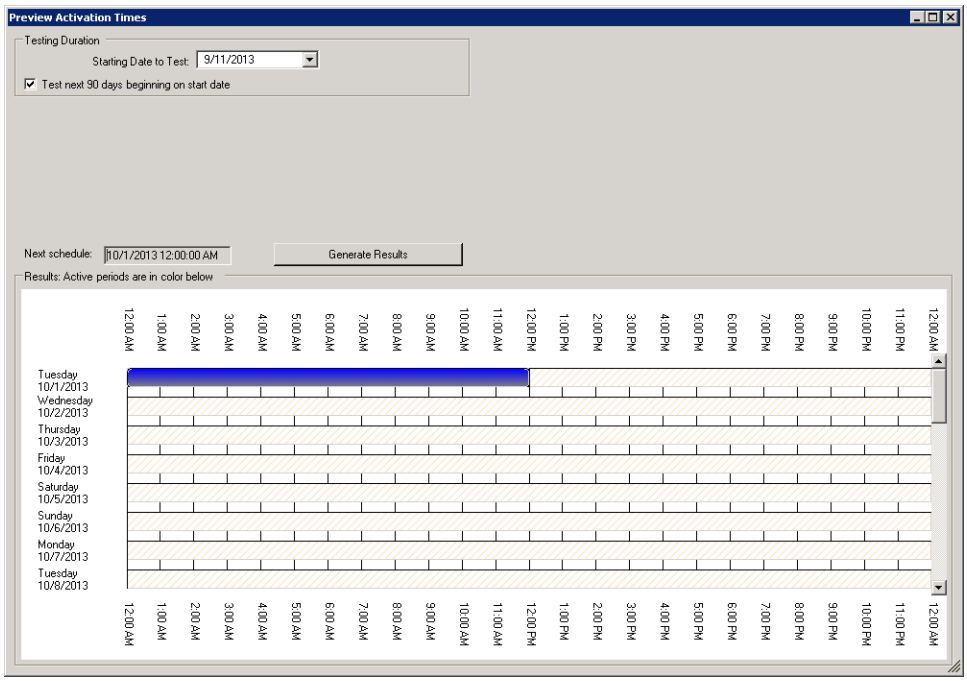
Privilege for Preview Activation Times

You can control the access Operators have to the Preview Activation Times function through the Privilege editor by granting or denying permission to the Recurring Schedule Privilege called **Preview Activations Times**. See Privilege Overview on Page 416 for more information about configuring Privileges.

Preview Activation Times Example

Figure 151 on Page 462 shows an example of the Preview Activation Times screen displaying the activation times for the Recurring schedule for the week of 10/1/2013.

Figure 151: Preview Activation Times Example



The Schedule being tested is active from Monday through Friday from 9:00 AM to 5:00 PM, and 9:00 AM to 12:00 PM on Saturdays and Sundays.

Note that on Saturday 1/1/11 and Monday 1/3/2011:

- A Holiday called New Year's Day is active on 1/1/2011.
- A company Holiday is active on 1/3/2011.

Previewing Schedule Activation Times for a Recurring Schedule

You can use the Preview Activation Times screen to learn how the settings you have configured for a Recurring Schedule will work on a specific date or week, on multiple controller types and on the C•CURE 9000 server.

You can preview the activation times for a single day by selecting a date from the **Starting Date to Test** calendar control drop-down, and for a seven-day period by additionally selecting the **Test entire week beginning on start date** check box.

To Preview a Schedule

1. Edit a Recurring Schedule (see Accessing the Recurring Schedule Editor on Page 449).
2. Click **Preview Activation Times**. The Preview Activations Times screen appears.
3. Select a date from the **Starting Date to Test** calendar control drop-down.
4. Optionally, if you want to preview an entire week starting on the **Starting Date to Test**, select the **Test entire week beginning on start date** check box.
5. Click **Generate Results** to display a graphic representation of your Schedule's activation times. The day and date is listed on the vertical axis of the chart, while the activation times for the Recurring Schedule are displayed on the horizontal axis of the chart as a colored bar.

NOTE If you hover the mouse pointer over a graphical bar showing when a Recurring Schedule is active, a tooltip appears showing the exact time the Recurring Schedule is active for that range.

Preview Activation Times Definitions

Table 113 on Page 463 provides definitions for the fields and buttons on the Preview Activation Times screen.

Table 113: Preview Activation Times Definitions

Field/Button	Description
Testing Duration	
Starting Date to Test	Pick a start date from the drop-down Calendar.
Test next 90 days beginning on start date	Select this check box to display the Schedule preview for 90 days following the starting date you selected.
Results: Active periods are in color below	
Dates and Times	Dates are represented by rows in the preview. The time periods during the day are shown in hourly columns.
Active Periods	Active periods are shown as colored bars in the preview. Each bar represents a time span when the Schedule is active on a device.
Inactive Periods	Inactive periods are shown as blank in the preview.

Viewing a List of Recurring Schedules

You can display a list of Recurring Schedules by opening a Dynamic View of Recurring Schedules. See Viewing a List of an Object Type on Page 22 for more information.

NOTE The **Active on Server** column is a status indicator that is read only. If the schedule is active, a check mark appears in the **Active** column. If the schedule is not active, the check box is blank. In addition, you can right-click the column header to add columns such as **Partition**, **Schedule** and **Template**.

Recurring Schedule List Context Menu

The context menu that opens when you right-click a Schedule in the Recurring Schedule Dynamic View includes the selections described in Table 114 on Page 464.

Table 114: Schedule Context Menu

Selection	Description
Change Partition	Click to open a dialog box that allows you to change the Partition to which the Schedule(s) belong. This menu selection does not display if your system is non-partitioned.
Preview Activation Times	Click to open the Preview Activation Times window for this Recurring Schedule. You can see a graphical representation of the active and inactive times for a day or a week on the server and each controller type for this Schedule. See Preview Activation Times on Page 462.

17

Schedule

This chapter explains how to configure Schedules in C•CURE 9000.

In this chapter

Schedule Overview

The Schedule object in C•CURE 9000 is used to define weekly time schedules that can be used throughout the system. These schedules can be used to control access to doors, schedule imports and system tasks, and trigger events. The C•CURE 9000 server uses schedules for access control and to perform certain activities, such as time based events, at specified times.

Example:

You can use a Schedule to specify at which times a person has access to a door (access control) or at which times alarms will be automatically armed (time-based event). Schedule time is local to the client or controller/panel.

These topics provide information about configuring Schedules:

- Schedule Editor on Page 473.
- How Schedules and Holidays Work Together on Page 467 .
- System Variable That Affects Schedules on Page 470.
- Schedule and Holiday Examples on Page 483.

Each schedule is composed of one or more Day Time Intervals that make up a week. A Schedule is designed to provide the same active and inactive time periods every week of the year. The Day Time Intervals define the days of the week and periods of time in hours, minutes, and seconds when the schedule is active.

You can include one or more Holiday Groups on a schedule. Holiday Groups specify the Holidays that apply to the Schedule, on which days normal activation of the Schedule does not occur.

Example:

If you have a Holiday Group that identifies several days as holidays, on those days a Schedule that normally allows employees to use a Clearance to gain access is instead inactive. Consequently, the employees are not be able to use a Clearance to gain access to the building.

You can specify Holiday Time Intervals on a Schedule that 'override' the normal effect of the Holidays. These Intervals specify a Holiday Group and optionally the Start and End Time for the Holiday Group. See Holiday Override on Page 467 for more information.

Schedules and Holidays operate according to the capabilities of the controller they are downloaded to, or the capabilities of the C•CURE 9000 Server, for server-based Events and Actions (such as running a Report or performing a backup).

How Schedules and Holidays Work Together

A Schedule is either active or inactive. When you configure a Schedule, you select the days of the week that the Schedule is Active, and you select the **Start Time** (when the Schedule becomes Active on a day) and the **End Time** (when the Schedule becomes inactive on a day).

When a Schedule is active, objects that reference that Schedule perform any behaviors that are configured to occur.

Example:

If you configure an Event to Arm an Intrusion Zone and you configure a Schedule called "All Weekend" in the **Activate on Schedule** field, the Event arms the Intrusion Zone when the Schedule becomes Active, and the Intrusion Zone remains Armed while the Schedule is active.

Similarly, Holidays are either active or inactive. Holidays can affect Schedules if the Holidays are members of a Holiday Group that applies to the Schedule.

You can add Holiday Groups to a Schedule so that the Schedule's Activation and Inactivation can be adjusted to meet your needs.

The following rules describe the behavior of Schedules relative to Holidays in general:

- A Holiday is active during the period(s) specified on the Holiday General tab.
- Likewise, a Holiday Group is active if any Holiday that is a member of the group is active.
- Only Holiday Groups may be referenced in a Schedule, so Holidays can only be referenced in a Schedule if they are part of a Holiday Group.
- A Holiday Group can be referenced in a Schedule by adding it to the **When These Holiday Groups Are Active, do not Activate Schedule** section of the Schedule General tab. When any Holiday in the Holiday Group is active, the Schedule is treated as inactive.
- You can create a "Holiday override" that changes the behavior of a Holiday Group that would normally apply to the Schedule. A Holiday override is created by adding a Holiday Group to the **When These Holiday Groups Are Active, Activate Schedule Only During Times Specified Below** section of the Schedule General tab and specifying a **Schedule Start Time** and **Schedule End Time**. During the time duration specified, the Schedule is active. Outside the override interval, the Schedule is inactive. See Holiday Override on Page 467 for more information.
- The pre-configured "Always", "Never", and "Nightly" Schedules are never overridden by Holidays. The 'Always" Schedule is always active. The "Never" Schedule is never active. The "Nightly" Schedule is active every night between 2:17 AM and 2:41 AM.
- All Controllers and the C•CURE 9000 Server can process partial-day holidays provided the holiday is a non-recurring type. You cannot configure partial-days for recurring holidays. (A partial-day holiday is defined as any holiday that does not cover a full 24-hour period, from midnight to midnight.)

Holiday Override

A "Holiday override" provides a way to make an exception to the effect of a Holiday Group on a Schedule. You can specify a time period during which the Schedule is active. While the Holiday Group is active but the time period is outside of the Holiday override interval, the Schedule is inactive.

A "Holiday override" is created by adding a Holiday Group to the **When These Holiday Groups Are Active, Activate Schedule Only During Times Specified Below** section of the Schedule General tab, and specifying a **Schedule Start Time** and **Schedule End Time**. During the time duration specified, the active Holiday causes the Schedule to be active. Outside the override interval, the active Holiday behaves normally and causes the Schedule to be inactive.

Example:

Your Schedule is usually Active for 12 hours on Mondays, and inactive on most Holidays. On a particular 24-hour Holiday that occurs on a Monday, you want the Schedule to be active in the morning only, and inactive the rest of the day.

You can add a Holiday Group containing only the Monday Holiday to the **When These Holiday Groups Are Active, Activate Schedule Only During Times Specified Below** section of the Schedule General tab, and specify a **Schedule Start Time** and **Schedule End Time** from 6:00 AM to Noon. On that Holiday, the Schedule is active from 6:00 AM to Noon. During the rest of the time the Holiday is active (midnight to 6:00 AM and Noon to midnight), the Schedule is inactive.

Example:

You have set up a Schedule for your site's normal work week. This Schedule is used to allow Clearances to be used at specific doors between 7:00 AM and 7:00 PM. On specific Holidays, you do not want the Clearances to be used. However, you have two half-days during which you want the Clearances to be usable from 7:00 AM until 2:00 PM. One way to accomplish this is to define two Holidays, put them in a Holiday Group, and add a Holiday override to the Schedule for 7:00 AM until 2:00 PM. The Schedule is active during this time interval. For the rest of the Holiday, the Schedule is inactive.

You cannot configure a Holiday override with 0 duration; when you try to save the Schedule, the Schedule editor remains open, an error message is displayed, and the Schedule is not saved.

Schedules and Holidays on the C•CURE 9000 Server and the iSTAR Controller

NOTE Beginning with Version 2.0 of C•CURE 9000, the server and iSTAR controllers treat Schedules and Holidays the same.

The following rules summarize how Schedules and Holidays interact on the C•CURE 9000 Server and the iSTAR Controller.

- Schedules that run on the C•CURE 9000 Server control such things as when Reports are run, backups are started, and numerous other functions. They also handle cross-Controller operations that cannot be performed at the Controller level (for example, input on one Controller triggers an output on another. However, if both objects are in the same iSTAR cluster, the Scheduling occurs on the iSTAR controllers). Additionally, they control all time-based Door mode actions, Input arm/disarm actions, Output control actions, and PIN Enable actions for apC Controllers while the apC is not in comm. fail, as well as any other time-based control of apC objects.
- When the C•CURE 9000 Server and the iSTAR Controller process a Schedule, if the Schedule does not explicitly include a Holiday Group, the Schedule ignores the existence of that Holiday Group and processes the Schedule as if that Holiday Group did not exist.
- If a Holiday Group is added to the **When These Holiday Groups Are Active, do not Activate Schedule** section of the Schedule General tab, when a Holiday that is a member of that Holiday Group is Active, the C•CURE 9000 server treats the Schedule as inactive.
- You can add a Holiday Group to the **When These Holiday Groups Are Active, Activate Schedule Only During Times Specified Below** section of the Schedule General tab, and specify a Holiday Override (a **Schedule Start Time** and **Schedule End Time**). When a Holiday that is a member of that Holiday Group is active, the Schedule is active during the Holiday override interval. Outside of the Holiday override interval, the Schedule is inactive.
- If there are multiple Holiday override intervals on a Schedule, they are each dealt with independently; if several Holiday overrides are Active on the same day, the Schedule is active during any time interval specified in a Holiday override.

Schedules and Holidays on the apC Controller

The following rules summarize how Schedules and Holidays interact on an apC Controller.

- All Schedules, and Holidays that are included in at least one Holiday Group that has been configured on the apC controller Editor Holiday Group tab, are downloaded to that apC controller. Holidays that are not a member of any Holiday Group or are not part of a Holiday Group selected for the specific apC are not downloaded to the apC.

- apC controllers use downloaded Schedules and Holidays to do controller processing of activity, such as determining when and how Clearance rules are enforced.
- While in comm. fail, the apC controllers use downloaded Schedules and Holidays to do processing of Door unlock and secure actions, Input arm actions, and Output activate actions that have been configured through host-based Events, as well as to Enable PIN at readers via the reader PIN Enable Schedule. If so configured, the apC in comm. fail changes the Door mode, Input arm/disarm state, PIN Enable state and Output state each time the relevant Schedule changes.
- In the period between being in good communication and going into comm. fail the apC does not affect any hardware state, but if a Schedule happens to change during this period, then the required actions are executed when the apC does decide it is in comm. fail. The apC does not record activity messages when it executes these offline timed actions. **The timed actions are not reported, but the object state changes are.**
- The apC ignores the **When These Holiday Groups Are Active, do not Activate Schedule** section of the Schedule General tab.
- You can configure a Holiday override for an apC Schedule by adding a Holiday Group to the **When These Holiday Groups Are Active, Activate Schedule Only During Times Specified Below** section of the Schedule General tab, and specifying a **Schedule Start Time** and **Schedule End Time**. The override works the same as described for the C•CURE 9000 Server.
- When an apC processes a Schedule that does not include a Holiday override, the Schedule will be inactive when a Holiday Group is active. In other words, because no behavior is specified in the Schedule configuration for that particular Holiday Group, the Schedule remains inactive.
- An individual apC can have up to eight Holiday Groups downloaded to it. These Holiday Groups are configured on the apC Editor Holiday Groups tab.

System Variable That Affects Schedules

There is a System Variable that has an impact on how Schedules and Holidays are used in C•CURE 9000. The System Variable is briefly described in Table 115 on Page 470. The way this System Variable works is described in more detail in Schedules Respect All Holiday Groups in Partition on Page 470.

Table 115: System Variables that Affect Schedules

Category/ System Variable	Description	Default Setting
System Operations Schedules Respect all Holiday Groups in Partition	Determines how Holiday Groups affect Schedules relative to Partitions. • True: All Schedules are automatically influenced by all Holiday Groups located in the default partition, the Global Partition (if Application Server is enabled), and the Schedule's own partition. • False: You must choose which Holiday Groups to add to each Schedule in the **When These Holiday Groups Are Active, do not Activate Schedule** section of the Schedule General tab.	**True** if C•CURE 9000 was installed on a new system. **False** if the C•CURE 9000 system was upgraded from a previous version (so that the way Schedules function remains unchanged).

NOTE In C•CURE 9000 Version 2.0, the **Force iSTAR Schedules to Respect all Holiday Groups** system variable was removed. Schedules on both iSTAR and the C•CURE 9000 Server respect only the holiday Groups that are explicitly added to the schedule.

Schedules Respect All Holiday Groups in Partition

This system variable determines whether or not all Schedules are affected by all Holiday Groups accessible to the Schedule (contained in the same Partition as the Schedule, or in the Default Partition of the C•CURE 9000 System).

You could use this setting if you have a single set of Holidays, or a separate set for each Partition, and you want all your Schedules to respect all of the Holidays you have defined.

When the System Variable is **True**, each accessible Holiday Group is automatically added to the **When These Holiday Groups Are Active, do not Activate Schedule** section of the Schedule General tab.

When the System Variable is **False**, Holiday Groups are not automatically added to the **When These Holiday Groups Are Active, do not Activate Schedule** section of the Schedule General tab. You need to manually add any Holiday Groups that you want the Schedule to respect.

The default value of this System Variable depends on whether the C•CURE 9000 system is a new installation or has been upgraded from a prior version.

- This System Variable is set to **True** for a new installation.
- This System Variable is set to **False** for an upgrade installation, so that the behavior of existing Schedules is not changed during upgrade.

To change the value of the **Schedules Respect all Holiday Groups in Partition** System Variable, you must have the SYSTEM ALL Privilege.

Including All Holiday Groups in Schedules

If you want to have all Holiday Groups affect all Schedules in a Partition, you can change the system variable **Schedules Respect all Holiday Groups in Partition** from **False** to **True**. When this change is made, the following message pops up:

WARNING: You are forcing all schedules to respect Holiday Groups. This means that all schedules will be influenced by all Holiday Groups subject to Partitioning rules. Make sure you do a database backup before continuing, because, once the change is done, it cannot be undone. Do you want to continue (Yes/No)?

The message notes that the change "cannot be undone" because changing this setting causes C•CURE 9000 to modify every Schedule in the system to include every accessible Holiday Group, and changing the System Variable back to **False** does **not** undo this action. To restore the system to its prior state, you would either have to restore a backup database, or manually modify every Schedule in the system to remove the Holiday Groups that were not previously included in the Schedule.

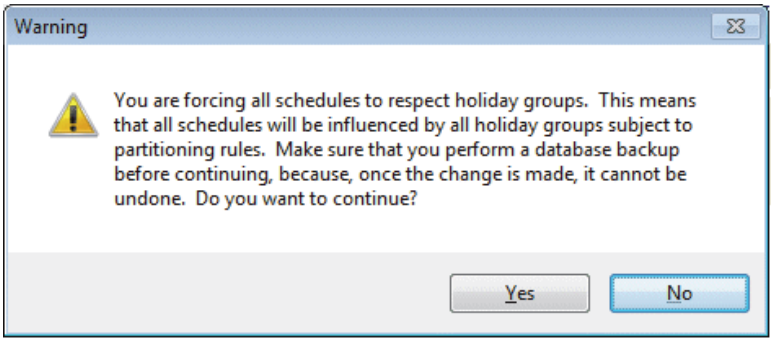
When this change is made, the schedules are changed so that they reference all accessible Holiday Groups, and all schedules are re-downloaded to all iSTAR controllers.

The Audit log records the changes to Schedules caused when this System Variable changes from **False** to **True**, as well as the changes to schedules caused when Holiday Groups are added to or deleted from the Schedule. This means that the resulting changes to the schedules are audited as well as the changes to the system variable itself.

You can still create overrides by adding Holiday Groups to the **When These Holiday Groups Are Active, Activate Schedule Only During Times Specified Below** section of the Schedule General tab. See Holiday Override on Page 467 for more information.

To Have Schedules Respect All Holiday Groups

1. From the Options & Tools pane of the Administration Station, select **System Variables**.
2. Click **System Operations** to open this section of the System Variables.
3. In the **Value** column for **Schedules Respect all Holiday Groups in Partition**, double-click to change the setting from **False** to **True**.
4. The following warning appears:



5. Click **Yes** to confirm the setting change and add all accessible Holiday Groups to all Schedules, or **No** to cancel it.
6. Click to close the System Variables.

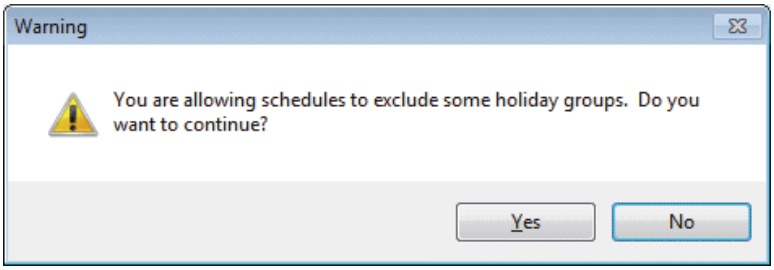
Choosing Holiday Groups for Schedules Manually

You can change this System Variable from **True** to **False** if you no longer want to force all Schedules to respect all Holidays. When this System Variable change is made, the Schedules are **not** changed; they still contain references to all Holiday Groups available to their Partition. However, from now on, the **Remove** button is available, allowing you to modify a Schedule so that it does not reference some Holiday Groups.

To Choose Holiday Groups for Schedules

1. From the Options & Tools pane of the Administration Station, select **System Variables**.

2. Click **System Operations** to open this section of the System Variables.
3. In the **Value** column for **Schedules Respect all Holiday Groups in Partition**, double-click to change the setting from **True** to **False**.
4. The following warning appears:



5. Click **Yes** to confirm the setting change, or **No** to cancel it.
6. Click to close the System Variables.

Schedule Editor

The Schedule Editor in C•CURE 9000 lets you create Schedule objects so that you can trigger events that perform access control and event monitoring.

The following topics give more information about the Schedule object and how to use it.

- Schedule Overview on Page 466
- How Schedules and Holidays Work Together on Page 467
- System Variable That Affects Schedules on Page 470
- Accessing the Schedule Editor on Page 473
- Schedule General Tab on Page 474
- Object Editor Groups Tab on Page 26
- Preview Activation Times on Page 480
- Scheduling Tasks on Page 477
- Schedule and Holiday Examples on Page 483

Accessing the Schedule Editor

You can access the Schedule Editor from the C•CURE 9000 Administration application, Configuration pane.

To Access the Schedule Editor

1. Click the **Configuration** pane button.
2. Select **Schedule** from the **Configuration** drop-down list.
3. Click **New** to create a new Schedule.

   —or—

4. Click  to open a Dynamic View showing all Schedule objects, then double-click the **Schedule** in the list that you want to edit, and the **Schedule Editor** opens (see Schedule Editor on Page 473).
5. Edit the schedule as needed, and click **Save and Close**.

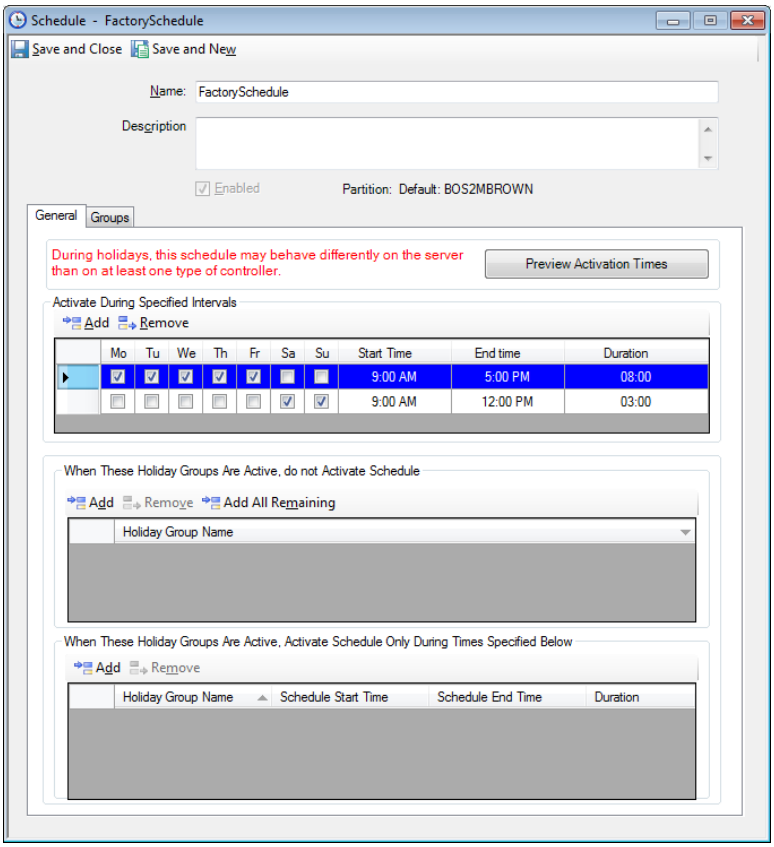
Schedule General Tab

The **Schedule General** tab lets you configure Day Time Intervals, the Holiday Groups that affect the Schedule, and Holiday Overrides that you can use to make the Schedule active on Holidays at specific times. See Figure 152 on Page 474.

NOTE C•CURE 9000 only supports one Schedule per downloadable event. Host events do not have this limitation; this only applies to downloadable events.

See Table 116 on Page 474 for definitions of the fields and buttons on the Schedule General tab.

Figure 152: Schedule Editor General Tab



Schedule Editor General Tab Definitions

The Schedule Editor General tab has the following fields and buttons.

Table 116: Schedule Editor - General Tab

Field/Button	Description
Name	Enter a unique name, up to 100 characters, to identify the schedule.
Description	Enter a description of the schedule, up to 255 characters long.
Enabled	A read-only field that signifies that the Schedule is always enabled.
Partition	A read-only field displaying the name of the Partition to which this schedule belongs. (This field is visible only if the C•CURE 9000 system is partitioned.)

Table 116: Schedule Editor - General Tab (continued)

Field/Button	Description
Activate During Specified Intervals	
Add	Add Day Time Interval to schedule.
Remove	Remove Day Time Interval from schedule.
Days of the Week	Place a check mark next to the day or days of the week that you want the schedule active.
Start Time	The time of day the Day Time the Interval becomes active.
End Time	The time of day the Day Time the Interval becomes deactivated. If you enter a Duration, the End Time is calculated as the Start Time plus the Duration.
Duration	The length of time from the Start Time that the Day Time Interval is active. The schedule is deactivated when the Start Time plus Duration are reached. If you enter an End Time, the Duration is calculated as the End Time minus the Start Time. Duration is read only.
When These Holiday Groups Are Active, do not Activate Schedule	
Add	Add a Holiday Group to the Schedule. Unavailable if the System Variable **Schedules Respect all Holiday Groups in Partition** is **True.** When you add a Holiday Group to this column, that Holiday Group is removed from the **When These Holiday Groups are Active, Activate Schedule Only During Times Specified Below** section, if it was present.
Remove	Remove the selected Holiday Group from the Schedule. Unavailable if the System Variable **Schedules Respect all Holiday Groups in Partition** is **True.**
Add All Remaining	Click this button to add all Holiday Groups to this section, so that all Holidays Groups apply to this Schedule. Unavailable if the System Variable **Schedules Respect all Holiday Groups in Partition** is **True.**
Holiday Group Name	This column lists the Holiday Groups that are respected by the Schedule. On the Holidays in these groups, the Schedule is inactive, unless an override has been added to the **When These Holiday Groups are Active, Activate Schedule Only During Times Specified Below** section. If the System Variable **Schedules Respect all Holiday Groups in Partition** is **True**, all Holiday Groups (accessible by this Schedule's Partition) are listed in this column.
When These Holiday Groups are Active, Activate Schedule Only During Times Specified Below	
Add	Add a Holiday Group override to the Schedule. When you add a Holiday Group to this column, that Holiday Group is removed from the **When These Holiday Groups Are Active, do not Activate Schedule** section, if it was present.
Remove	Remove a Holiday Group row from the **When These Holiday Groups Are Active, do not Activate Schedule** section.
Holiday Group Name	The Holiday Group for which you are defining an override. During the times you enter in this row, the Schedule will be active. When you add a Holiday Group to this column, that Holiday Group is removed from the **When These Holiday Groups Are Active, do not Activate Schedule** section, if it was present.
Schedule Start Time	The time of day the Schedule becomes active during a Holiday belonging to this Holiday Group.
Schedule End Time	The time of day the Schedule becomes deactivated during a Holiday belonging to this Holiday Group.

Table 116: Schedule Editor - General Tab (continued)

Field/Button	Description
Duration	The length of time from the Start Time to the End Time that the Schedule is active. The Schedule is deactivated when the End Time is reached. The Duration is a read-only field calculated from the Start Time and End Time.

Configuring Schedule Time Intervals

To configure a Schedule, you add Schedule intervals to the **Activate During Specified Intervals** section of the General tab. Each Schedule interval is added as a row in this section. In each row you can specify different days of the week, and times during those days, that you want the Schedule to be active. During any times of the week that are not included in this section, the Schedule is inactive.

To Configure Schedule Active Intervals

1. On the Schedule General tab, click **Add**. A row is added to the section.
2. Select the check box for each day that you want the Schedule to be active.
3. Enter a **Start Time** to specify when you want the Schedule to become active.
4. Enter an **End Time** for when you want the Schedule to become inactive.
5. Repeat these steps if you need to add another row with different active days and times.

Example:

Your site has different hours of operation on several days during each week.

- You add a row for Monday, Wednesday, and Friday, with 8:00 AM to 5:00 PM.
- You add a row for Tuesday and Thursday, with 8:00 AM to 7:00 PM.
- You add a row for Saturday and Sunday, with 9:00 AM to 1:00 PM.

Adding Holiday Groups to the Schedule

You can specify the Holiday Groups that you want this Schedule to respect by adding them to the **When These Holiday Groups Are Active, do not Activate Schedule** section. During any Holiday Groups that you add to this section, the Schedule is inactive.

NOTE If the System Variable **Schedules Respect all Holiday Groups in Partition** is **True**, all Holiday Groups that are accessible to the Schedule's Partition are automatically added to this sections, and the **Add**, **Remove**, and **Add All Remaining** buttons are unavailable.

To Add Holiday Groups to the Schedule

1. From the Schedule General tab, click **Add** in the **When These Holiday Groups Are Active, do not Activate Schedule** section. A new row is added to the section.
2. Alternatively, you can click **Add All Remaining** to add all Holiday Groups that are not currently included in the Schedule in either this grid or the **When These Holiday Groups are Active, Activate Schedule Only During Times Specified Below** grid.
3. To add a Holiday Group, click in the new row, then click [...]. Pick a Holiday Group from the selection box that appears.

4. If the Holiday Group you selected is in the **When These Holiday Groups are Active, Activate Schedule Only During Times Specified Below** section, a prompt appears asking if you want to remove that Holiday Group from that section. Click **Yes** to remove the group and add it to this section, or **No** to cancel the action.

Configuring Holiday Overrides

If you want this Schedule to be active at specific times during Holidays that are respected by the Schedule, you can add the Holiday Groups to this section along with the time intervals during which you want this Schedule to be active. You can add a Holiday Group to this section more than once to activate the Schedule during multiple time intervals.

If you add a Holiday Group to this section the Schedule is inactive during the Holidays in the group, outside of override interval you specify.

If you add a Holiday Group to this section that is in the **When These Holiday Groups Are Active, do not Activate Schedule** section, the Holiday Group is removed from that section.

To Configure Holiday Overrides

1. From the Schedule General tab, click **Add** in the **When These Holiday Groups are Active, Activate Schedule Only During Times Specified Below** section. A new row is added to the section.
2. To add a Holiday Group, click in the new row, then click ... . Pick a Holiday Group from the selection box that appears.
3. If the Holiday Group you selected is in the **When These Holiday Groups Are Active, do not Activate Schedule** section, a prompt appears asking if you want to remove that Holiday Group from that section. Click **Yes** to remove the group and add it to this section, or **No** to cancel the action.
4. Enter a **Schedule Start Time** to specify when you want the Schedule to be active during the Holidays.
5. Enter a **Schedule End Time** for when you want the Schedule to become inactive during the Holidays.
6. Repeat these steps if you need to add another row with different active days and times.

Scheduling Tasks

You can perform the following tasks to create and manage Schedules:

- Creating Configuration Pane Objects and Templates on Page 21
- Viewing a List of Schedules on Page 478
- Modifying a Schedule on Page 479
- Exporting an Object on Page 24
- Setting a Property for a Schedule on Page 479
- Adding a Schedule to a Group on Page 479
- Deleting an Object on Page 25

NOTE

You can not delete a schedule that is in use by other objects in the system.

If the Schedule is being used by another object, you need to edit the other object to remove the Schedule. For example, if your Schedule is attached to a Door object, you need to remove the Schedule from the Door before you can delete the Schedule.

Creating a Schedule

You can create a new Schedule that can be attached to other objects to provide time scheduling.

To Create a Schedule

1. In the Navigation pane of the Administration Workstation, click **Configuration** to open the Configuration pane.
2. Select **Schedule** from the Configuration pane drop-down list.
3. Click **New** to create a new Schedule. The Schedule Editor opens, and you can configure the schedule.
4. Configure the Schedule intervals during which you want the Schedule to be active (see Configuring Schedule Time Intervals on Page 476).
5. Configure the Holiday Groups which affect the Schedule (see Adding Holiday Groups to the Schedule on Page 476).
6. Configure any Holiday overrides you want to apply to the Schedule (see Configuring Holiday Overrides on Page 477).
7. Use the Preview Activation Times button to verify that your Schedule is configured to activate and de-activate at the times and dates you planned. See Previewing Schedule Activation Times on Page 481.
8. To save your new Schedule, click **Save and Close**.

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

Creating a Schedule Template

You can create a new Schedule Template. A Schedule Template saves you time because you do not have to reenter the same schedule information again.

To Create a Schedule Template

1. In the Navigation pane of the Administration Workstation, click **Configuration** to open the Configuration pane.
2. Select **Schedule** from the Configuration pane drop-down list.
3. Click the down arrow next to **New** and select **Template**. The Schedule Template opens and you can configure the Schedule Template.
4. To save your new Schedule Template, click **Save and Close**

Viewing a List of Schedules

You can display a list of Schedules by opening a Dynamic View of Schedules. See Viewing a List of an Object Type on Page 22 for more information.

NOTE The **Active on Server** column is a status indicator that is read only. If the schedule is active, a check mark appears in the **Active** column. If the schedule is not active, the check box is blank. In addition, you can right-click the column header to add columns such as **Partition**, **Schedule** and **Template**.

Schedule List Context Menu

The context menu that opens when you right-click a Schedule in the Schedule Dynamic View includes the selections described in Table 117 on Page 479.

Table 117: Schedule Context Menu

Selection	Description
Change Partition	Click to open a dialog box that allows you to change the Partition to which the Schedule(s) belong. This menu selection does not display if your system is non-partitioned. If you change the Partition of a Schedule and the System Variable **Schedules Respect all Holiday Groups in Partition** is True, then the Holiday Groups in the **When These Holiday Groups Are Active, do not Activate Schedule** will be changed to reflect the new Partition of the Schedule.
Preview Activation Times	Click to open the Preview Activation Times window for this Schedule. You can see a graphical representation of the active and inactive times for a day or a week on the server and each controller type for this Schedule. See Preview Activation Times on Page 480.
Show Association	Click this menu selection to view a list of Security Objects associated with this Schedule. For more information, see "Showing Associations for an Object" in the *C•CURE 9000 Getting Started Guide*.

Modifying a Schedule

You can edit an existing Schedule to change any of the Schedule settings.

To Modify a Schedule

1. View the list of Schedules (see Viewing a List of an Object Type on Page 22).
2. Right-click the Schedule in the list that you want to edit and select **Edit** from the context menu. The Schedule Editor on Page 473 opens.
3. Edit the schedule as needed and click **Save and Close**

Setting a Property for a Schedule

You can use **Set Property** to set properties for a Schedule. **Set Property** enables you to quickly set a Schedule property without opening a Schedule.

To Set a Property for Schedules

1. View the list of Schedules (see Viewing a List of an Object Type on Page 22).
2. Right-click the schedule in the list for which you want to set a property and select **Set Property** from the context menu.
3. Click  to specify the property for the schedule.
4. Type the value for the property and click **OK**

Adding a Schedule to a Group

You can use **Add To Group** from the context menu for a Schedule. **Add To Group** enables you to add the schedule object to a group.

To Add a Group To a Schedule

1. View the list of Schedules (see Viewing a List of an Object Type on Page 22). Right-click the Schedule in the list to which you want to add to a group and select **Add To Group** from the context menu.
2. When the Group list displays, select the group you want to add the schedule to, and click **OK**.

Preview Activation Times

You can click the **Preview Activation Times** button on the Schedule General tab to see a graphical representation of a schedule's effect on your server and controllers. The active times for the Schedule are shown with a color-coded bar for each type of controller you choose to preview. These active time previews show the effect of any Holiday Groups that are active on the dates being previewed.

You can also use the **Preview Activation Times** context menu selection from a Dynamic View of Schedules to preview a Schedule. See Schedule List Context Menu on Page 478.

For more information about **Preview Activation Times**, see:

- Previewing Schedule Activation Times on Page 481
- Previewing Schedule Activation Times on Page 481

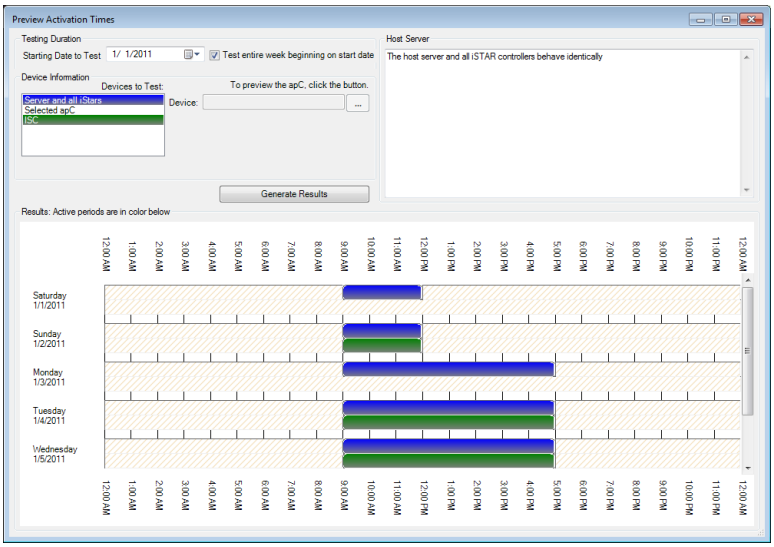
Privilege for Preview Activation Times

You can control the access Operators have to the Preview Activation Times function through the Privilege editor by granting or denying permission to the Schedule Privilege called **Preview Activations Times**. See Privilege Overview on Page 416 for more information about configuring Privileges.

Preview Activation Times Example

Figure 153 on Page 480 shows an example of the Preview Activation Times screen displaying the activation times for the schedule on iSTAR controllers for the week of 1/1/2011.

Figure 153: Preview Activation Times Example



This example was created with the following System Variable setting:

- **Schedules Respect all Holiday Groups in Partition** is set to **False**.

The Schedule being tested is active from Monday through Friday from 9:00 AM to 5:00 PM, and 9:00 AM to 12:00 PM on Saturdays and Sundays.

Note that on Saturday 1/1/11 and Monday 1/3/2011:

- A Holiday called New Year's Day is active on 1/1/2011.
- A company Holiday is active on 1/3/2011.

- The Schedule includes a Holiday override that activates the Schedule between 9:00 AM and 12:00 PM on the server and all iSTARs controllers.

Preview Activation Times Definitions

Table 118 on Page 481 provides definitions for the fields and buttons on the Preview Activation Times screen for Recurring Schedule.

Table 118: Preview Activation Times Definitions

Field/Button	Description
Testing Duration	
Starting Date to Test	Pick a start date from the drop-down Calendar.
Test entire week beginning on start date	Select this check box to display the Schedule preview for seven days following the starting date you selected.
Device Information	
Devices to Test	You can select the type of device(s) for the Schedule preview. Use **CTRL+Left-click** to select multiple items. The Selections available on this screen vary depending upon the System Variable setting for your system.
	If the System variable **Schedules respect all holiday groups** is **True**, and if all Holiday Groups in the system are in the Default partition, the following choices are available: • Server and all iSTARs • Selected apC
Device	You can click and choose a specific apC controller to preview. Because apC controllers can respect different Holiday Groups, you can only preview one apC at a time.
How Schedules Behave	The title of this box changes depending upon the choices you make for **Devices to test**. This area shows a textual summary of the reasons the Schedule behaves differently on the selected device compared to the C•CURE 9000 host server. When you click on a device type in Devices to test, the textual summary changes to describe the rules for that device type without regenerating the results, so that you can view the text for each device type while viewing the graphical depiction.
Generate Results	Click to display a preview of this Schedule on the devices you selected for the specified time period.
Results: Active periods are in color below	
Dates and Times	Dates are represented by multiple rows in the preview. Each day can display the status of four device types. The time periods during the day are shown in hourly columns.
Active Periods	Active periods are shown as colored bars in the preview. Each bar represents a time span when the Schedule is active on a device.
Inactive Periods	Inactive periods are shown as blank in the preview.

Previewing Schedule Activation Times

You can use the Preview Activation Times screen to learn how the settings you have configured for a Schedule will work on a specific date or week, on multiple controller types and on the C•CURE 9000 server.

You can preview the activation times for a single day by selecting a date from the **Starting Date to Test** calendar control drop-down, and for a seven-day period by additionally selecting the **Test entire week beginning on start date** check box.

To Preview a Schedule

1. Edit a Schedule (see Accessing the Schedule Editor on Page 473).
2. Click **Preview Activation Times**. The Preview Activations Times screen appears.
3. Select a date from the **Starting Date to Test** calendar control drop-down.
4. Optionally, if you want to preview an entire week starting on the **Starting Date to Test**, select the **Test entire week beginning on start date** check box.
5. Select the controller(s) types you wish to preview in the **Devices to Test** box. Use **CtrL+Left-Click** to select multiple controller types.
6. Click **Generate Results** to display a graphic representation of your Schedule's activation times. The day and date is listed on the vertical axis of the chart, while the activation times for each controller type are displayed on the horizontal axis of the chart as a colored bar (with a distinct color for each controller type).

NOTE If you hover the mouse pointer over a graphical bar showing when a Schedule is active, a tooltip appears showing the exact time the Schedule is active for that range.

Schedule and Holiday Examples

The following examples illustrate how System Variable and Schedule settings affect Schedules on the server and controllers.

Schedule Without Overrides

This example defines a Holiday Group containing two Holidays and a typical work schedule. This example was created with the following System Variable setting:

- **Schedules Respect all Holiday Groups in Partition** is set to **False**.

CompanyHolidays is a Holiday Group that contains two Holidays as described in Table 119 on Page 483.

Table 119: CompanyHolidays

Holiday Group	Holidays	Duration
CompanyHolidays	New Years Day	Saturday, 1/1/2011 (24 hours).
	Off-site Conference Day	Monday 1/3/2011 (24 hours).

CompanySchedule (see Table 120 on Page 483) defines the times when employees can use Clearances. There are no overrides in the Schedule.

Table 120: CompanySchedule

Days	Times	When These Holiday Groups Are Active, Activate Schedule Only During Times Specified Below
Monday - Friday	9:00 AM to 5:00 PM	None.
Saturday - Sunday	9:00 AM to 12:00 PM	

Schedule with Overrides

This example uses the same two Holidays but places them in separate Holiday Groups to show the effect of a Holiday Override on a Schedule, and also how ISC controllers handle Holidays differently. This example was created with the following System Variable setting:

- **Schedules Respect all Holiday Groups in Partition** is set to **False**.

CompanyHolidays and National Holidays are Holiday Groups that contain several Holidays as described in Table 121 on Page 484.

Table 121: CompanyHolidays

Holiday Group	Holidays	Duration
NationalHolidays	New Years Day Election Day	Saturday, 1/1/2011 (24 hours). Tuesday, 11/8/2011 (24 hours)
CompanyHolidays	Off-site Conference Day CEO's Birthday	Monday, 1/3/2011 (24 hours) Friday, 2/4/2011 (24 hours)

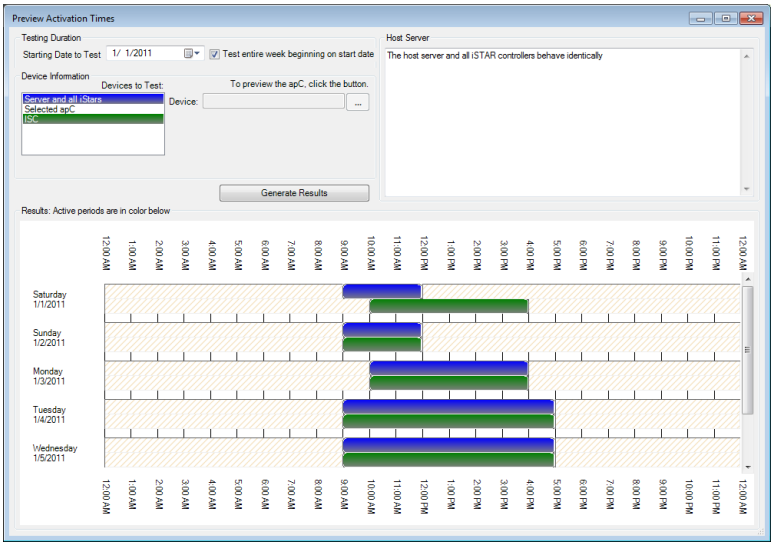
This Schedule has a Holiday override that specifies a six-hour override for the Holiday in the CompanyHoliday Group (see Table 122 on Page 484).

Table 122: FactorySchedule

Days	Times	When These Holiday Groups Are Active, Activate Schedule Only During Times Specified Below
Monday - Friday	9:00 AM to 5:00 PM	CompanyHoliday 10:00 AM - 4:00 PM
Saturday - Sunday	9:00 AM to 12:00 PM	

Figure 154 on Page 484 shows the Preview Activation Times for FactorySchedule on a C•CURE 9000 Server and iSTAR controllers, and ISC controllers.

Figure 154: Schedule with Overrides



In this example, the Schedule does not specify the NationalHolidays group, so the server and the iSTARs (blue bars) do not respect the NewYearsDay holiday, and the normal Saturday Schedule activation is used.

The ISC controllers (green bars) also recognize all Holidays, but the Holiday override defined for CompanyHoliday Group is applied to all Holidays, so on the ISC controllers, the Schedule is active for the six-hour Holiday override.

On Monday 1/3/11, CompanyHoliday is respected by all controllers and each applies the six-hour Holiday override.

Schedules with Separate Holiday Groups

This example shows the use of separate Holiday Groups for locations that observe different Holidays. In this example, separate Holiday Groups are used to represent Holidays for Canada and the USA.

This example was created with the following System Variable setting:

- **Schedules Respect all Holiday Groups in Partition** is set to **False**.

CanadaHolidays and USAHolidays are Holiday Groups that contain several Holidays as described in on Page 485.

Table 123: Canada and USA Holidays

Holiday Group	Holidays	Duration
CanadaHolidays	New Years Day Canada Day Thanksgiving Day	1/1/20110 (24 hours) July 1 (24 hours) Second Monday of October (24 hours)
USAHolidays	New Years Day Independence Day Thanksgiving	1/1/2010 (24 hours) July 4 (24 hours) Fourth Thursday of November (24 hours)

A separate schedule is used for locations in each country.

- Work Schedule (Canada) includes CanadaHolidays in the **When These Holiday Groups Are Active, do not Activate Schedule** grid.
- Work Schedule (USA) includes USAHolidays instead (see Figure 155 on Page 485.)

Both Schedules use the same active days and times (see on Page 485).

Figure 155: Work Schedules (Canada and USA)

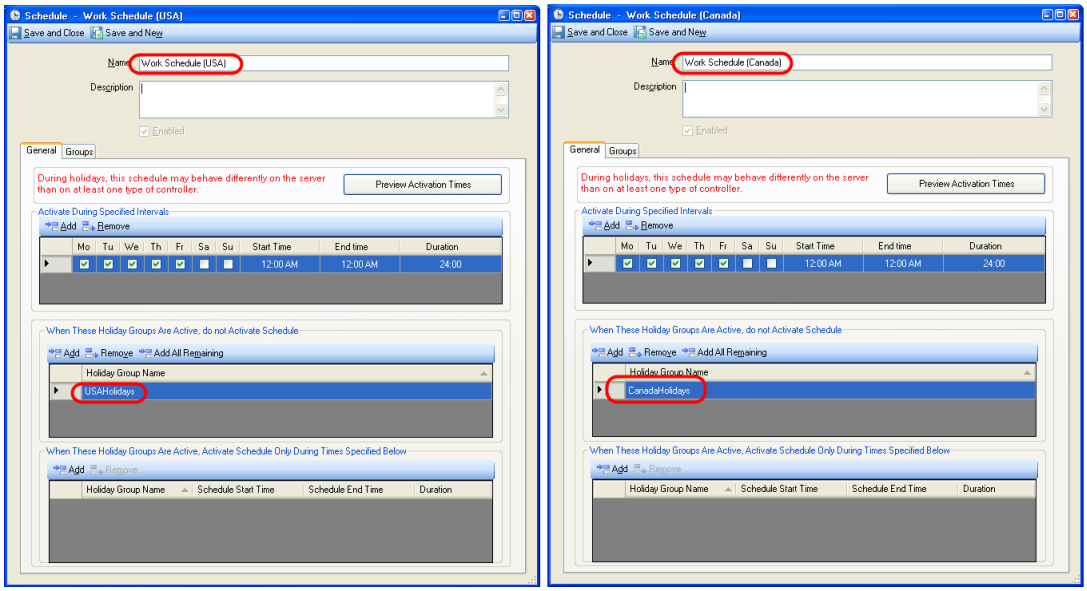


Table 124: Work Schedules

Schedule	Days/Times	When These Holiday Groups Are Active, do not Activate Schedule
Work Schedule (Canada)	Monday - Friday 7:00 AM to 7:00 PM	CanadaHolidays
Work Schedule (USA)	Monday - Friday 7:00 AM to 7:00 PM	USAHolidays

Figure 156 on Page 486 shows the Preview Activation Times for Work Schedule (Canada) on a C•CURE 9000 Server and iSTAR controllers, and ISC controllers.

Observe that on the Canada Day Holiday (7/1/11), the server, iSTAR controllers and ISC controllers (green bars) all observe the Holiday. The server and iSTAR controllers recognize that Monday 7/4/11 is a normal work day for Canadian locations.

Figure 156: Work Schedule (Canada)

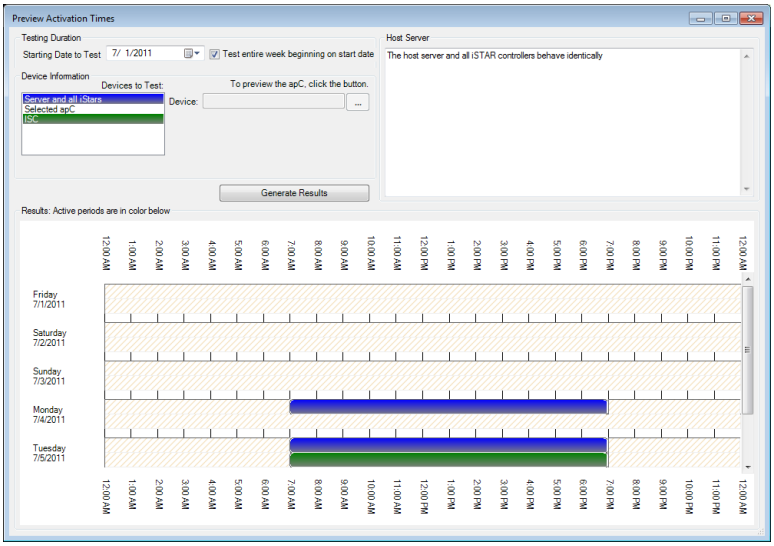
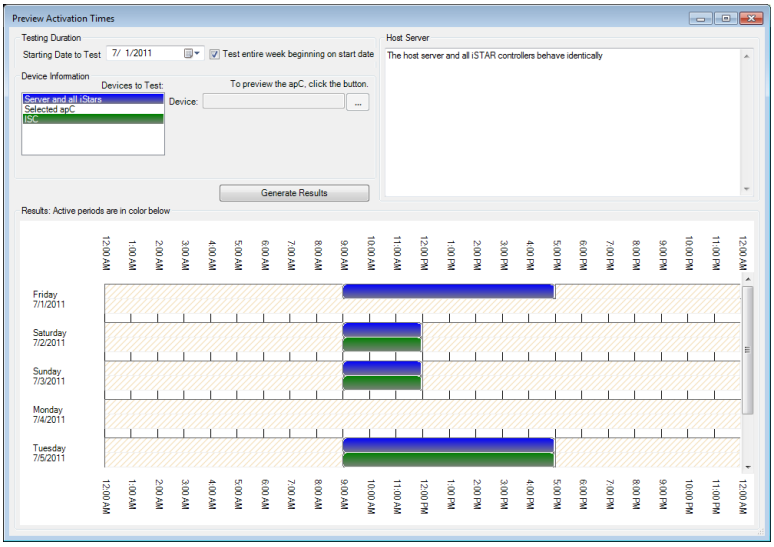


Figure 157 on Page 487 shows the Preview Activation Times for Work Schedule (USA) on a C•CURE 9000 Server and iSTAR controllers (blue bars), and ISC controllers (green bars).

Observe that on the Independence Day Holiday (7/4/11), the server, iSTAR controllers , and ISC controllers all observe the Holiday. The server and iSTAR controllers recognize that Friday 7/1/11 is a normal work day for USA locations.

Figure 157: Work Schedule (USA)



Schedules Respect All Holiday Groups

This example shows the use of Holiday Groups when the System variable **Schedules Respect all Holiday Groups in Partition** is set to true.

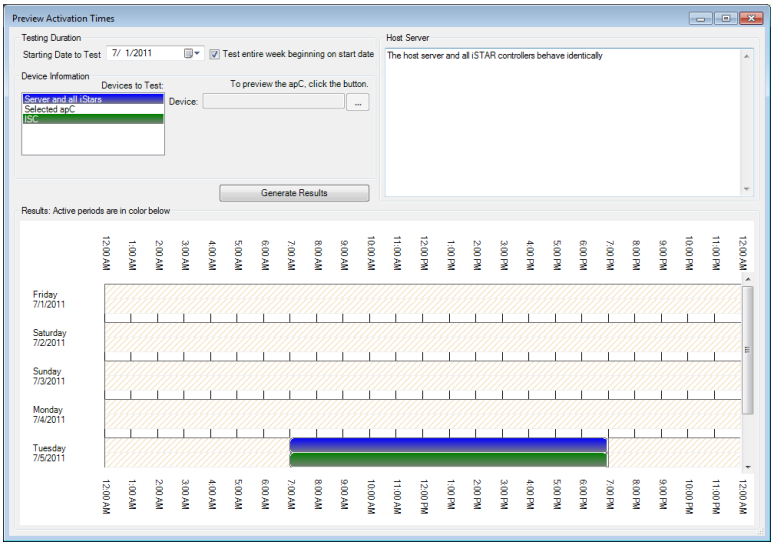
This example was created with the following System Variable setting:

- **Schedules Respect all Holiday Groups in Partition** is set to **True**.

Figure 158 on Page 487 shows the Preview Activation Times for Holiday Groups on a C•CURE 9000 Server, an iSTAR controllers, and an ISC controller.

If you need to have Schedules that should not be affected by all Holidays, consider moving the Holiday Groups to a Partition other than the Default Partition, and moving the Schedules that should not observe these Holidays to another Partition.

Figure 158: When Schedules Respect All Holidays

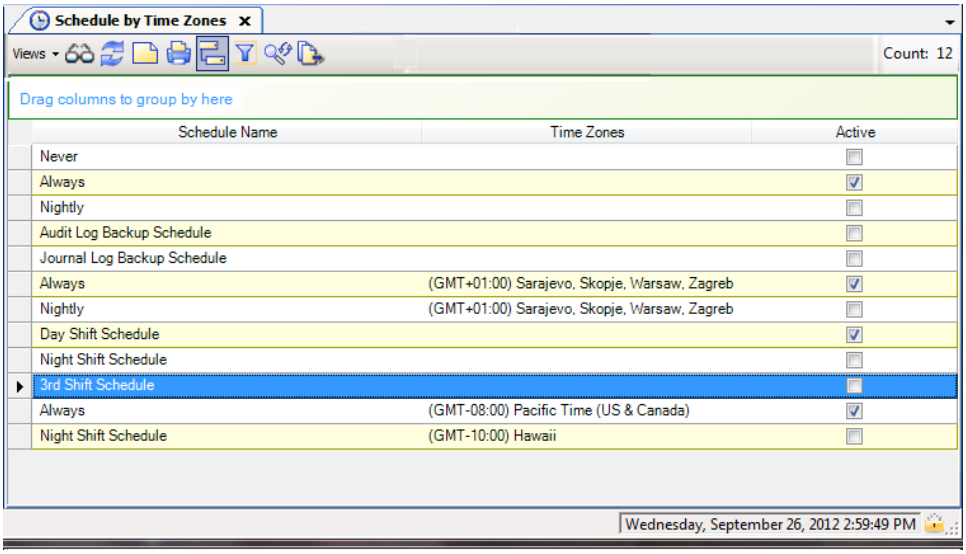


Schedule by Time Zones

The Schedule by Time Zones selection in the Configuration pane lets you display a Dynamic View that lists the Schedules (and Holidays) in the C•CURE 9000 database, and whether that Schedule/Holiday is active in each Time Zone in which it is used.

This Dynamic View displays the Schedule name, the Time Zone for the Schedule, and whether the Schedule is currently active in that Time Zone.

Figure 159: Schedule by Time Zones Dynamic View



This list of Schedules displays the state of a Schedule in a particular Time Zone only if that Schedule has been used by an object in that time zone.

Example:

If an Event in Central Time Zone gets activated by schedule "9 to 5 schedule", a row in this Dynamic View displays whether the "9 to 5 schedule" is currently active in Central Time Zone.

There is always a row in this view for each Schedule in the C•CURE 9000 server (host) Time Zone.

If a Schedule is used in more than one Time Zone, the Schedule appears on this Dynamic View more than once.

Example:

The C•CURE 9000 Server resides in the Eastern US Time Zone. One of the iSTAR controllers configured on this server resides in the Hawaii Time Zone. A Schedule that resides on the server but is associated with an Event on the iSTAR in the Hawaii Time Zone appears on this Dynamic View twice: once for the Eastern Time Zone, and once for the Hawaii Time Zone.

For iSTAR controllers, the Active status displayed for a Schedule agrees with the active status on the panels because all Holidays are downloaded to the panels.

However, for apC panels, Holidays are assigned on each panel. This means that the apC might or might not have the Holidays that are a part of the Holiday group used by the Schedules on the C•CURE 9000 server. To get an accurate view of the state of a Schedule for apC, use the **Preview Activation Times** button in the Schedule editor (see Preview Activation Times on Page 480).

ISC panels handle Holidays differently, so the Active status in the Dynamic View won't necessarily match the state of the Schedule on the ISC panel . To get an accurate view of the state of the schedule for apC, use the **Preview Activation Times** button in the Schedule editor (see Preview Activation Times on Page 480).

Privilege for Schedule By Time Zones

The Schedule by Time Zones Privilege allows you to restrict or allow access to Schedule by Time Zones. Typically you would set this Privilege for an Operator to the same access level (for No Access, Read, Edit, Delete, Export Selection, and Find in Audit Log) that the Operator has for Schedules.

When you upgrade C•CURE 9000, an existing Operator will have no access to Schedule by Time Zones by default. You need to edit a Privilege assigned to the Operator and set access to Schedule by Time Zones to at least Read access.

18

Sound

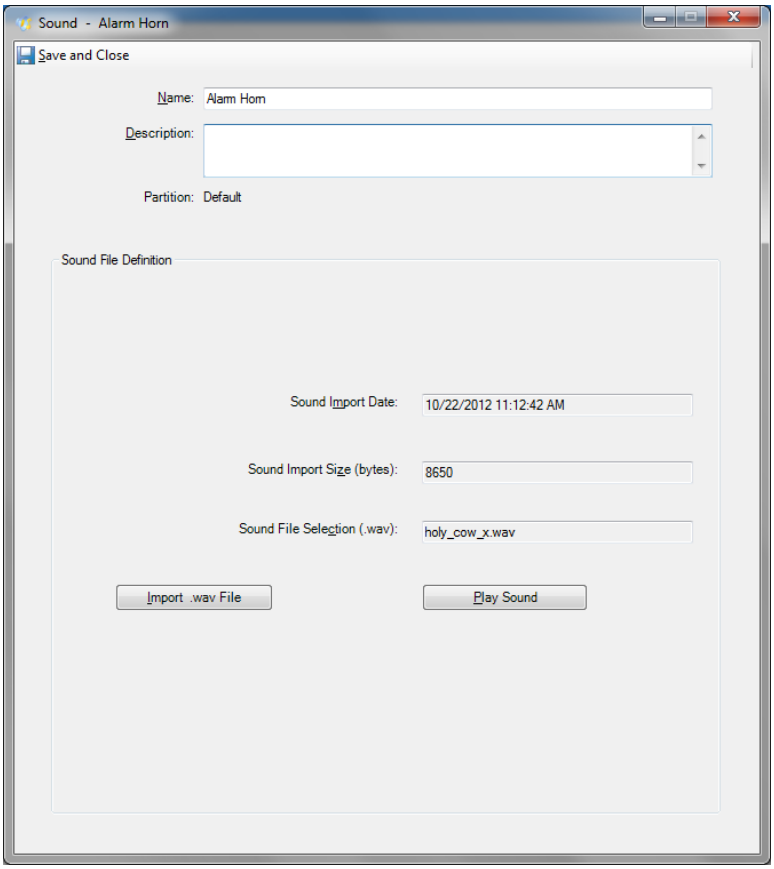
This chapter explains how to configure Sound objects in C•CURE 9000.

In this chapter

Sound Editor

The Sound editor allows you to create Sound objects that reside in the C•CURE 9000 database. You can then use the Event editor to configure Sound actions using these Sound objects.

Figure 160: Sound Editor



A Sound object is a named database object that represents a sound file that you imported into the C•CURE 9000 database. The imported Sound file must be a .WAV file that is less than 500kb in size.

By saving Sound objects to the database, you can assign the same Sound object to multiple Events. Previously, each Event saved a unique copy of the Sound file, taking up a greater amount of space: the same Sound file used in 10 Events would be saved 10 separate times as distinct Sound actions.

Existing Sound Actions Converted to a Single Sound Object During Upgrade

If you have previously added Sound files to Events on the Actions tab, these sounds will be saved to the C•CURE 9000 database when you upgrade to the latest version of C•CURE 9000.

If the same Sound file has been configured in more than one Event, the upgrade will re-map these instances to a single Sound object, rather than create multiple Sound objects from the original Sound file.

Example:

You have 10 Events that play the same Sound when activated, each using its own copy of the original sound file you attached to each Event. When you upgrade C•CURE 9000 to the latest version, a single Sound object is added to the C•CURE 9000 database and is mapped to each of the Sound actions you previously configured.

Using the Sound Editor

You can perform the following tasks with the Sound editor.

- Accessing the Sound Editor on Page 492
- Importing a Sound File on Page 492
- Configuring an Event with a Sound on Page 493

For definitions of the Fields and Buttons in the Sound Editor, see:

- Sound Editor Definitions on Page 492

Sound Editor Definitions

Definitions for the fields and buttons in the Sound editor are described in Table 125 on Page 492.

Table 125: Sound Editor Definitions

Field/Button	Description
Name	Enter the name you want to assign this Sound in C•CURE 9000.
Description	Enter a textual description for this Sound.
Sound Import Date	A read-only field that displays the date when this sound file was imported
Sound Import Size (bytes)	A read-only field that displays the size of the Sound file in bytes. Files larger than 500 Kb cannot be imported.
Sound File Selection (.wav)	Displays the name of the sound file you imported.
Import .wav File	Click this button to import a .WAV Sound file. A Windows dialog box opens to let you navigate and choose a Sound file to import.
Play Sound	Click this button to play the Sound you imported.

Accessing the Sound Editor

You access the Sound Editor from the C•CURE 9000 Configuration pane.

To Access the Sound Editor

1. Click the **Configure** pane button .
2. Click the Configure drop-down list and select **Sound**.
3. Click  to open a Dynamic View showing all Sound objects.
4. Double-click on the Sound in the list that you want to edit, and the Sound Editor opens.

Importing a Sound File

You can use the Sound editor to import a Sound file into the C•CURE 9000 database. You can then add the Sound to an Event so the Sound is played when the Event is activated.

You can only import Sounds that are .WAV files smaller than 500Kb. If you try to import a larger Sound file, you will not be able to save the Sound to the C•CURE 9000 database.

To Import a Sound File

1. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Sound** from the Configuration pane drop-down list.
3. Click **New** to create a new Sound object. The Sound Editor opens and you can configure the Sound.
4. Type a Name for the Sound in the **Name** field.
5. Type a textual description for the Sound in the **Description** field.
6. Click **Import Sound**. A Windows dialog box opens to let you navigate to the folder where your Sound file is stored.
7. Select the Sound you want to import from the sound files listed in the dialog box.
8. Click **Open**. The Sound file is imported into the C•CURE 9000 database.
9. You can click **Play Sound** to verify that you imported the sound file you intended.

Configuring an Event with a Sound

You can configure an Event to play a Sound (that was previously imported) when the event is activated.

To Configure an Event with a Play Sound Action

1. In the Navigation pane of the Administration Client, click **Configuration** to open the Configuration pane.
2. Select **Event** from the Configuration pane drop-down list.
3. Click  to open a Dynamic View showing the Events in your C•CURE 9000 database.
4. Select an Event from the list and choose **Edit** from the right-click context menu. The Event editor opens.
5. Click the Action tab in the Event editor.
6. Click **Add** to add a new Event action.
7. Select **Play Sound** from the **Action** column drop-down list.
8. Click  to select a Sound object. Only .WAV sound files under 500kb size are supported.
9. Select a **Play mode** for the Event Sound.
    - **Play sound once**.
    - **Play sound instead of beep** - the sound you configured is played at the Monitoring Station rather than the default 'beep' sound.
    - **Play sound Interval** - if you select this mode, you can configure the interval at which the Sound is repeated until the Event is resolved. The minutes value (mins) can be 0 to 9999999. The seconds value (secs) can be 0 to 59.
10. You can click **Play** to verify that you selected the correct sound file.
11. Click **Save and Close** to save the Event.

19

Time Zones

C•CURE 9000 lets you manage sites that span time zones by specifying different time zones for C•CURE 9000 computers and panels.

In this chapter

Time Zones Overview

In C•CURE 9000, Time Zones are predefined. You cannot modify a Time Zone. It is recommended that you use this feature only when your organization relies on controllers that are actually located in different time zones.

C•CURE 9000 lets you manage sites that span time zones by specifying different time zones for C•CURE 9000 clients, servers and controllers. The C•CURE 9000 server and clients are associated with a time zone that is configured on each computer. To set a computer's time zone, double click the Date/Time icon in the computer's Control Panel and specify a time zone in the Time Zone tab. See your Windows Operating System documentation for more information.

See the following topics for more information about Time Zones.

- Time Zone Tasks on Page 496.
- Time Zone Definitions on Page 500.

You can use the following administration workstation dialog boxes to set up time zones for other C•CURE 9000 components:

- The controller editor lets you specify a time zone for each iSTAR, apC, and ISC controller.
- The CCTV Switch dialog box let you specify a time zone for each CCTV switch.
- Manual actions can be set to execute in a time zone.

You can also link these objects to time zones:

- Inputs, outputs and readers on a controller are associated with the controller's time zone.
- Doors with inputs, outputs, and readers on a controller are associated with the controller's time zone.
- Elevators with inputs, outputs, or readers on a controller are associated with the controller's time zone.
- Activation date and times and the host received date and times displayed at the Monitoring Station are associated with the time zone of the computer that is running the Monitoring Station.

Time Zone Tasks

You can perform the following tasks with Time Zones.

- Enabling or Disabling a Time Zone on Page 496.
- Viewing a List of Time Zones on Page 497.
- Setting a Property for a Time Zone on Page 497
- Displaying Time Zones in Dynamic Views on Page 498

Enabling or Disabling a Time Zone

You can enable or disable a Time Zone.

- If a time zone is enabled, it appears in the Time Zone lists and can be selected for use in C•CURE 9000. If a time zone is disabled, it does not appear in the Time Zone lists and cannot be assigned to a controller, CCTV Switch, or manual action in C•CURE 9000.

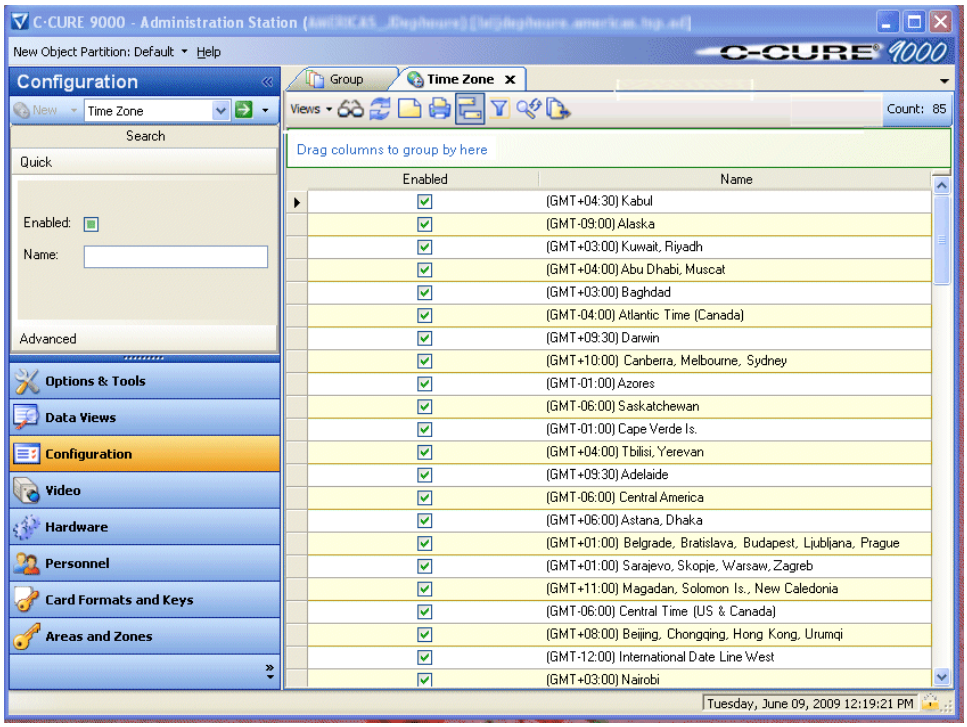
To Enable a Time Zone

1. In the Navigation Pane of the Administration Workstation, click **Configuration** to open the Configuration pane. See Figure 161 on Page 497.
2. Select **Time Zone** from the Configuration pane drop-down list.
3. Click to open a Dynamic View showing all time zones.
4. Click in the **Enabled** check box of the time zone you wish to enable.

To Disable a Time Zone

1. In the Navigation Pane of the Administration Workstation, click **Configuration** to open the Configuration pane.
2. Select **Time Zone** from the Configuration pane drop-down list.
3. Click to open a Dynamic View showing all time zones.
4. Click in the **Enabled** check box of the time zone you wish to disable to remove the check mark.

Figure 161: Time Zone Selection



Viewing a List of Time Zones

You can view a list of Time Zone objects in C•CURE 9000.

To View a List of Time Zones

1. In the Navigation Pane of the Administration Workstation, click **Configuration** to open the Configuration pane.
2. Select **Time Zone** from the Configuration pane drop-down list.
3. Click to open a Dynamic View showing all time zones.

NOTE You can right-click on the column header to add the columns Daylight Name and Standard Name. You can also Filter and Group the Time Zones in the list using the Dynamic View Toolbar.

Setting a Property for a Time Zone

You can use Set Property to set properties for time zones. Set Property enables you to quickly set a Time Zone property.

To Set a Property for Time Zones

1. In the Navigation Pane of the Administration Workstation, click **Configuration** to open the Configuration pane.
2. Select **Time Zone** from the Configuration pane drop-down list.
3. Click to open a Dynamic View showing all time zones.
4. Right-click the time zone that you want to set the property and select **Set Property** from the context menu
5. Click the drop-down button to see a list of properties and select a property for the time zone.
6. Enter the value for the property and click **OK**.

Displaying Time Zones in Dynamic Views

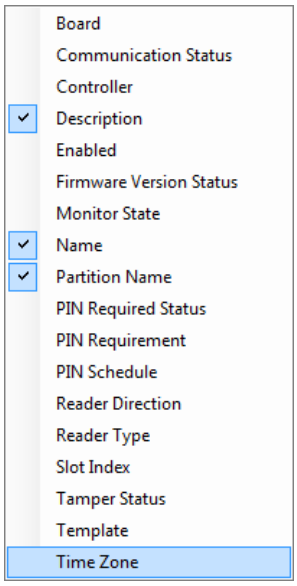
For object types that have assigned Time Zones, you can display the Time Zones for those objects in a Dynamic View.

To Show a Time Zone Column in a Dynamic View

While you are displaying a Dynamic View of an object, you can show a Time Zone column to list the Time Zone of every object in the view.

NOTE This change is not saved. The next time you open this Dynamic View, the Time Zone Column is not displayed. If you want to permanently add the Time Zone column to the default Dynamic View for an object, see To Create a Default Dynamic View to Show a Time Zone Column on Page 499.

1. Open a Dynamic View of the object type (see Viewing a List of an Object Type on Page 22).
2. Right-click on a column heading (such as **Name**) in the view to display a context menu that lets you change the columns displayed by the Dynamic View.



3. Click **Time Zone** to add the Time Zone column to the Dynamic View.
4. To resize the Time Zone column, if needed, hover over the left edge of the Column Heading of Time Zone until the pointer changes to ⇿, then drag the mouse to resize the column.

To Create a Dynamic View that Includes a Time Zone Column

You can create a Dynamic View that includes the Time Zone column (for an object type that includes a Time Zone).

1. Create a new Dynamic View for the object type. See the chapter on Dynamic Views in the *C•CURE 9000 Data Views Guide*.
2. Click **Add** to add a column to the view and choose **Time Zone**.
3. Click **Save and Close** to save your changes.

Whenever you display this Dynamic View it will include the Time Zone column.

To Create a Default Dynamic View to Show a Time Zone Column

You can create a Dynamic View for an object type so that it contains the Time Zone column, and make it the default Dynamic View for that object type.

1. Create a new Dynamic View for the object type. See the chapter on Dynamic Views in the *C•CURE 9000 Data Views Guide*.
2. Click **Add** to add a column to the view and choose **Time Zone**.
3. Select the **Make default view** check box
4. Click **Save and Close** to save your changes.

Whenever you click  to display a default Dynamic View for that object type, it will include the Time Zone column.

Time Zone Definitions

Table 126 on Page 500 defines the fields available on the Time Zone Dynamic View list.

Table 126: Time Zone Fields

Field	Description
Enabled	If Enabled is selected ,this Time Zone appears in any list of Time Zones that can be assigned to a controller, CCTV Switch, or manual action. If this field is not selected, this Time Zone is unavailable (it cannot be assigned to a controller, CCTV Switch, or manual action).
Name	The name assigned to the Time Zone. The Time Zone names are the same as the Time Zone names in the Windows operating system. This name cannot be changed.
Daylight Name	The name used to signify this Time Zone when Daylight Savings Time is in effect. This name can be changed.
Standard Name	The name used to signify this Time Zone when Standard Time is in effect. This name can be changed.

20

User-defined Fields

The C•CURE 9000 User-defined Field Editor is used to create user-defined fields for Personnel, Credentials, apC Controllers, iSTAR Controllers, Inputs, Outputs, Readers, Doors, Elevators, Video Cameras, Video Servers, Axis IP Cameras, and CCTV Cameras.

In this chapter

User-defined Fields Editor

User-defined fields are new fields that can be added to Personnel, hardware, and video objects in C•CURE 9000. You can define additional fields that are linked to every object of a specific type in your C•CURE 9000 system. You can specify the type of field, its characteristics, and its translatable labels. You can set up basic validation for field values. (The User-defined fields are integrated with the supported object types, but internally these fields are stored in separate database tables.)

User-defined Fields are available in Dynamic Views, Reports, Queries, Exports, and Imports for their object type, just as if they were fields stored in the object's record. Personnel and Credential User-defined fields are also available for use in badging with C•CURE ID badge layouts and smart card programming, enrollment, and printing.

Personnel and Credential User-defined Fields

When you add Personnel and Credential User-defined fields to C•CURE 9000, those fields are not initially placed on existing Personnel Views - you can add them manually using the Personnel Views editor.

If you create new Personnel Views after adding the User-defined fields to C•CURE 9000, the User-defined fields are placed on the Personnel User-defined Fields tab or the Credential tab User-defined Fields tab .

Hardware and Video User-defined Fields

When you add hardware or video User-defined fields to C•CURE 9000, those fields are placed on the User-defined fields tab of their object type.

Example:

A User-defined field or the iSTAR Controller object type is automatically placed on the User-defined Fields tab of the iSTAR Controller editor.

You can create User-defined fields for the following Hardware and Video object types.

Table 127: Hardware and Video User-defined Fields

Hardware	Video
apC Controller	Video Camera
iSTAR Controller	Video Server
Input (iSTAR and apC)	Axis IP Camera
Output (iSTAR and apC)	CCTV Camera
Reader (iSTAR and apC)	
Door (iSTAR and apC)	
Elevator (iSTAR and apC)	

Hardware and Video User-defined fields support Import and Export, and can be used in Reports and configured as columns in Dynamic Views, just like other fields of that object type.

C•CURE 9000 supports a maximum of 20 User-defined fields (total, not per object type) for Hardware and Video objects.

Clearance User-defined Field

When you create a Clearance user-defined field (UDF), it displays in the Clearance editor, dynamic views, queries reports and exported data in C•CURE 9000.

Visitor Management User-defined Field

When you create a Visit user-defined field (UDF), it displays in the Visit editor, dynamic views, queries, reports and exported data in C•CURE 9000. The Visit UDF displays in the Visitor Management web application and in the self check-in kiosk application used by visitors, after it is assigned to aVisit Site.

For more information about Visitor Management, see the *C•CURE 9000 Visitor and Access Management Guide.*

Access Management User-defined Field

When you create a new Access Request Custom user-defined field, it displays in dynamic views, queries, reports and exported data in C•CURE 9000. The Access Request UDF displays in the Access Management web application after it has been assigned to an Access Request Site.

For more information about Access Management, see the *C•CURE 9000 Visitor and Access Management Guide.*

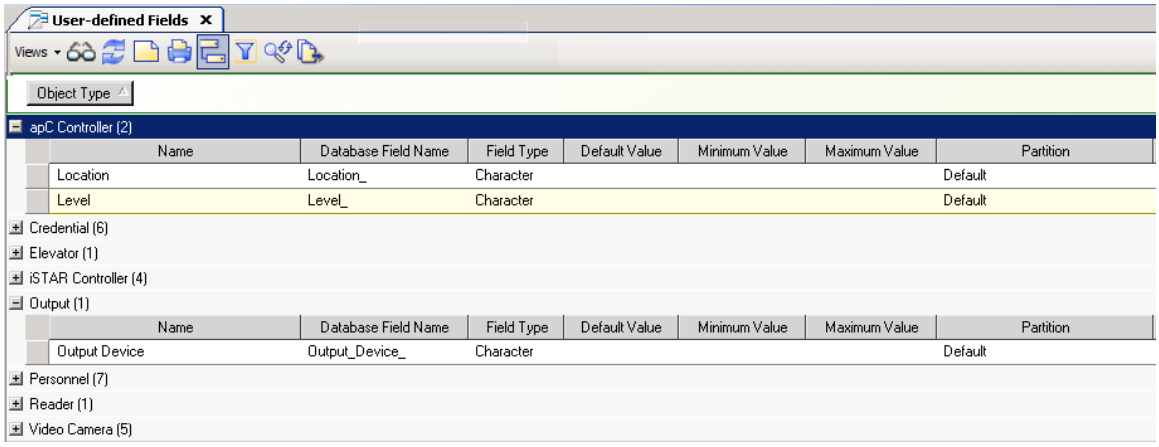
Operator Privileges for User-defined Fields

For an Operator to use User-defined Fields, the Operator must have appropriate Permission settings in Privileges for the class type UdfFieldDef. Available settings are: Edit, Delete, ReadOnly, or No Access. An operator must have at least readOnly access to the User-defined Field definition to see a User-defined Field on the object's editor, or in a Dynamic View.

Viewing a List of User-defined Fields

You can view a list of the User-defined fields you have configured. The Dynamic View shows all User-defined fields grouped by Object Type.

Figure 162: User-defined Fields Dynamic View



See Viewing a List of an Object Type on Page 22 for more information about how to display this Dynamic View.

More Information

The following sections provide more information about the User-defined fields editor and tasks you can perform to create, configure, and employ User-defined fields.

- User-defined Fields Types on Page 504
- User-defined Fields Validation on Page 504
- User-Defined Fields Editor Tabs on Page 505
- User-defined Fields Tasks on Page 505

User-defined Fields Types

You can create user-defined fields of the following types in C•CURE 9000:

- Character
- Multi-line character
- Integer
- Logical
- Date
- Date Time (stored in UTC)
- Time (Hours: Minutes)
- Decimal
- Enumerated (see Enumerated Field Type on Page 504)
- Identity (see Identity Field Type on Page 504)
- Custom (see Custom Field Type on Page 504)

User-defined fields cannot be configured as indexed fields. For this reason, if you are creating an Import definition and want to use a Matched field, you should use an indexed Customer field (such as Int1, Int2, Int6, Text1, Text12 and Text13), or a User-defined field that is defined as Unique.

Enumerated Field Type

An Enumerated field provides the user with a drop-down list of valid values that you define when you configure the User-defined field.

When the enumerated User-defined field appears on an object editor tab, the user can select a value from a long list for an 'Enumerated' field by typing successive letters. For example, typing 'A' selects all items that begin with 'A': Allen/Albright/Aldrich/Arthur. If the user then types 'All', it would select only 'Allen'. However if the user back-spaced to delete the second 'l', 'Al' would select Allen/Albright/Aldrich.

Identity Field Type

The Identity field type is provided as a counter for objects of a type. You can use it if you need an ID for objects that never changes and is never re-used when an object is deleted.

When you create an Identity User-defined field for an object type, the Identity field each object of the type is assigned a value equal to the ObjectID of that object. Every time an additional object of the type is created, its Identity type field is assigned a value 1 greater than the highest existing value. The Identity type field never re-uses a value. Typically, there is no need for more than one Identity field per object type. Because the field is always assigned a value, there is no need for a Field Attributes tab or Restrictions tab for this User-defined field type.

Custom Field Type

The Custom field type can be created for Personnel or Credential objects using a Custom Control developed using the Connected Program Kit for development partners. If you have installed a Connected Program Integration that includes a Custom User-defined field type, you will be able to create a Custom User-defined field with a Custom Control Type. For more information see the *Connected Program Kit Programmers Guide*.

User-defined Fields Validation

You can configure the following types of validation for User-defined fields:

- Minimum/Maximum value (for all field types except Logical, Time, and Enumerated fields).
- Mandatory within a C•CURE 9000 system (including a default value if an Operator editing the record does not have access to the field). See Field Attributes Tab Definitions on Page 510 for more information about Mandatory fields.
- Mandatory within a C•CURE 9000 partition.
- Uniqueness within a C•CURE 9000 system. See Field Attributes Tab Definitions on Page 510 for more information about Unique fields.
- Uniqueness within a C•CURE 9000 partition.
- Masks (Character fields only) – used to define the format of the characters in the field by specifying the character types and literal values that make up valid data. For example, you can choose a pre-defined mask that formats a telephone number field as (000)-000-0000, where the characters **( ) -** are part of the field that cannot be changed by the Operator, and the “000” characters indicate the data that can be changed, but only integer characters are valid.

User-Defined Fields Editor Tabs

The User-defined Fields Editor stores personnel information on several tabbed views. The following sections give more information about each User-defined Fields tab and how to use them.

- User-defined Fields Editor Field Information Section on Page 508
- User-defined Fields Editor Field Attributes Tab on Page 510
- User-defined Fields Editor Restrictions Tab on Page 512
- User-defined Fields Editor Enumeration Values Tab on Page 524

User-defined Fields Tasks

You can perform the following tasks with the User-defined Fields editor to configure User-defined Fields.

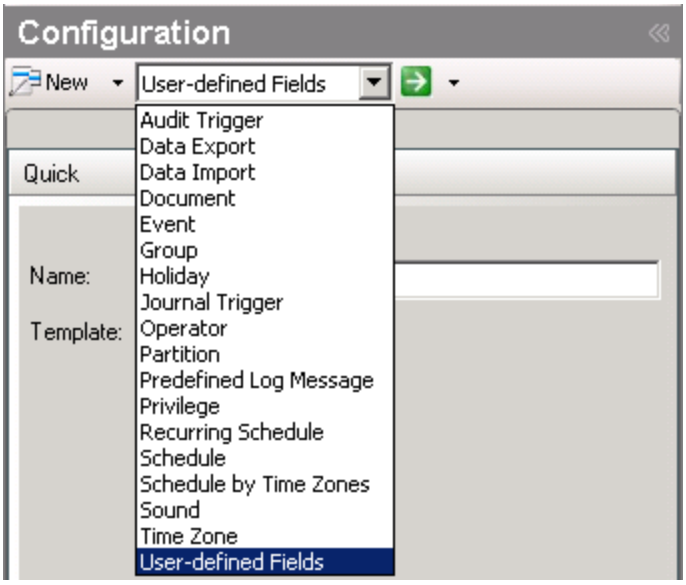
- Using the Object List Context Menu on Page 23.
- Accessing the User-Defined Fields Editor on Page 505.
- Creating a User-defined Field Template on Page 507.
- Deleting a User-defined Field on Page 507.
- Specifying User-defined Field Information on Page 508.
- Selecting a Language on Page 509.

Accessing the User-Defined Fields Editor

You can access the User-defined Fields editor from the C•CURE 9000 Configuration pane.

To Access the User-defined Fields Editor

1. Click the **Configuration** pane button.
2. Select **User Defined Fields** from the drop-down list in the Configuration pane toolbar.



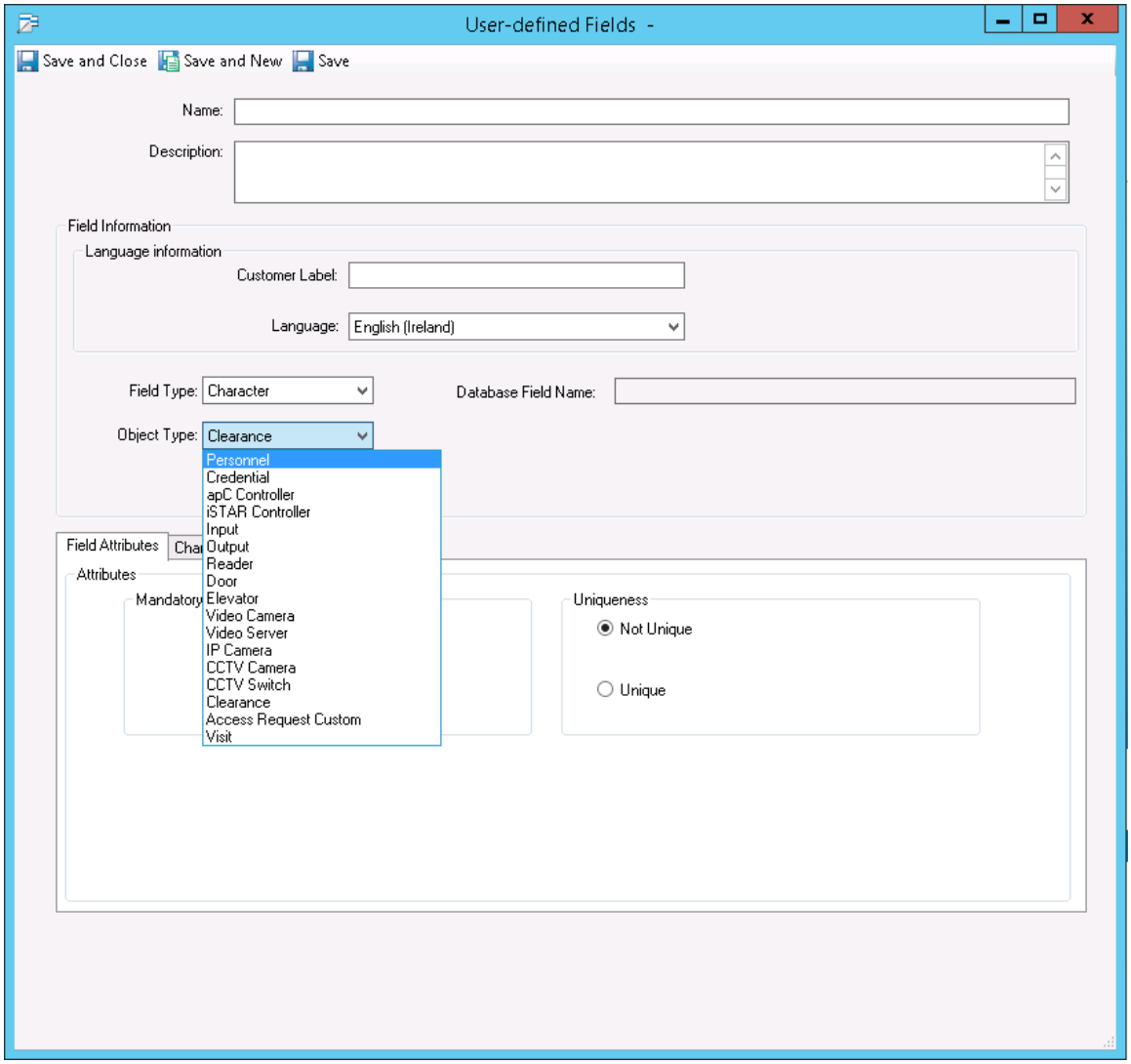
3. To create a new User-defined field, click **New**.

   or

   To edit an existing User-defined field, click . A Dynamic View that lists all existing User-defined fields opens. From this view you can double-click the name of the User-defined field in the list that you want to edit.

   The User-defined Field Editor opens (see Figure 163 on Page 507). On a non-Partitioned system, the **Mandatory System Wide** and **Unique System Wide** selections are invisible because they do not apply to a non-Partitioned system.

Figure 163: User-defined Field Editor



Creating a User-defined Field Template

You can create a User-defined Field template, which you can then use as the basis of new User-defined Fields. In a template, you can fill in field values , and then use the template to create a new User-defined Field with these values already filled-in.

Example:

You could create a template for a character type User-defined Field, and specify the validation that you want to perform on the field. You can then use this template when you are creating a new character type User-defined Field, and your validation will already be defined consistently with other character type fields you create, saving you time.

Deleting a User-defined Field

You can delete a User-defined Field from C•CURE 9000 if it is no longer needed.

If you delete a User-defined field that is used in a saved Dynamic View, Report, Query, Export, or Import, a warning occurs when you try to display or use that object, and your action may not complete. You will need to edit the object to remove the reference to the User-defined field that was deleted.

The steps for deleting a User-defined field are covered in Deleting an Object on Page 25.

User-defined Fields Editor Field Information Section

The Field Information section of the User-defined Fields editor defines the database name of the User-defined field, as well as the Customer Label (the name for the field that appears in an object editor), the Language for the field, and the field type.

Specifying User-defined Field Information

You can specify the general settings for User-defined Field from the User-defined Field editor.

NOTE You can change the Field Type and Related Table of a User-defined field when you create the field, but once you save the field, the Field Type and Related Table become read-only.

If a user-defined field is saved while the Mandatory setting is cleared (i.e. the field is saved as not Mandatory), you cannot subsequently change the setting to Mandatory.

To Specify User-defined Field Information

1. Open the **User-defined Fields** editor. See Accessing the User-Defined Fields Editor on Page 505.
2. In the **Name** field, type the name that you want the field to have in the C•CURE 9000 database for the User-defined field. This is not the name that is displayed in the object editor and in other views. The name must be unique and cannot contain spaces.

NOTE You should not use a SQL Server reserved keyword to name your User-defined Field; doing so will cause a failure if you subsequently attempt to perform Imports. Microsoft lists the SQL Server reserved keywords at http://msdn.microsoft.com/en-us/library/ms189822.aspx.

3. Type a textual description for the field in the **Description** field.
4. To specify the name for the field that appears in the object editor, Report, Queries, and elsewhere in C•CURE 9000, type a label in the **Customer Label** field.
5. To specify the language with which this Customer Label is used, select a language from the **Language** field drop-down list. (Selecting a language allows you to create a different label for the selected language. See Selecting a Language on Page 509 for more information.)
6. To specify the Field Type for this User-defined field, select a field type from the **Field Type** field drop-down list. See User-defined Fields Types on Page 504 for more information.
7. Select from the **Object Type** drop-down list the object type with which the User-defined field is associated.

   Example:

   If you are creating a User-defined Field for use with video cameras, choose **Video Camera** from the **Object Type** list.
8. For most field types you can specify **Mandatory Settings** and **Uniqueness** on the Field Attributes tab.
9. For some field types, you can specify a **Default Value** for the User-defined Field by clicking on the Restrictions tab. The value you choose must valid for the field type (for example, you cannot specify a character string if the User-defined field is a Logical).

NOTE If you are using a mask for a character field, you cannot enter text directly into **Default Value**. Instead you enter text into the **Test Mask on Sample Value** field, and if the test mask is valid, click **Use Test as Default** to copy the text to the **Default Value** field.

10. To save the field click **Save**. To close the editor, you can click **Save and Close**.

    Alternatively, you can continue to edit the field on the remaining editor tabs.

Selecting a Language

When you are editing a User-defined field, you can make changes to the way the field appears in one or more languages.

NOTE When you use the User-defined Field editor to make changes in any language, you are changing **only the label** of the field that is used in the object editor only, not the meaning of the field, or how it is used by C•CURE 9000 for other purposes such as Dynamic Views, Reports, or Queries.

You can only make language changes for language versions currently residing on your system. When you choose a language from the **Language** field drop-down list, the list only contains the languages for which language resources already exist on your system.

There are two ways for language resources to be added to a C•CURE 9000 system.

- Install a C•CURE 9000 Language Pack. See the *C•CURE 9000 Installation and Upgrade Guide* for more information.
- Create a language translation using the Multilingual User Interface Editor, a purchasable option. See the *C•CURE 9000 System Maintenance Guide* for more information.

In addition, language resources created via any of these three methods can be installed on a remote C•CURE 9000 client.

To Select a Language

1. Open the User-defined Fields editor. See Accessing the User-Defined Fields Editor on Page 505.
2. Click the down-arrow in the **Language** field to view a list of the languages for which resources exist on your system.
3. Select a language from the **Language** drop-down list. The resources for that language are applied to the settings for your User-defined Field.
4. To save the field click **Save**. To close the editor, you can click **Save and Close**.

   Alternatively, you can continue to edit the field on the remaining editor tabs.

User-defined Fields Editor Field Attributes Tab

The **User-defined Field Field Attributes** tab lets you specify the display attributes of the field, the field type, and information about how the field is displayed and used within C•CURE 9000.

Figure 163 on Page 507 shows the Field Attributes tab.

See Field Attributes Tab Definitions on Page 510 for definitions of all fields and buttons on the Field Attributes Tab.

Setting User-defined Field Attributes

You can set attributes for a User-defined Field on the Field Attributes tab.

To Set User-defined Field Attributes

1. Open the User-defined Fields editor. See Accessing the User-Defined Fields Editor on Page 505.
2. To define this field as mandatory, select the **Mandatory** button. The default setting is **Not Mandatory**.

NOTE On a partitioned system, you can choose either **Mandatory in Partition** or **Mandatory System Wide**.
If you save a User-defined field as **Not Mandatory**, you cannot subsequently change it to **Mandatory**. However, if you save a User-defined field as **Mandatory**, you can subsequently change it to **Not Mandatory** or **Mandatory in Partition**.
See Field Attributes Tab Definitions on Page 510 for more information about Mandatory fields.

3. To define the degree of Uniqueness for this field, choose one of the options in the Uniqueness box. The default setting is **Not Unique**.

NOTE On a partitioned system, you can choose either **Unique in Partition** or **Unique System Wide**. If you save a User-defined field as **Not Unique**, you cannot subsequently change it to any form of **Unique**. However, if you save a User-defined field as any form of **Unique**, you can subsequently change it to **Not Unique**.

See Field Attributes Tab Definitions on Page 510 for more information about Unique fields.

4. To save these settings click **Save**. To close the editor, you can click **Save and Close**.

   Alternatively, you can continue to edit the field on the remaining editor tabs.

Field Attributes Tab Definitions

The fields and buttons on the User-defined Fields Field Attributes tab are shown in Table 128 on Page 511.

Table 128: User-defined Fields Field Attributes Tab Definitions

Field/Button	Description
Mandatory	A Mandatory field is a field that must have a value. If the field does not have a value, the record cannot be saved. Every field must be specified as either **Not Mandatory**, or some degree of Mandatory. The following field types can be designated as Mandatory: • Character • Integer • Decimal • Date • Date Time • Enumerated The default value is **Not Mandatory**. On a non-partitioned system, every field must be either **Mandatory** or **Not Mandatory**. On a partitioned system, a field can be: • **Not Mandatory** • **Mandatory in Partition** • **Mandatory System Wide** You can define a default value for a Mandatory field. If you define Mandatory fields, any Operator creating a record must have access to the Mandatory fields in a Personnel View in order to enter a non-blank value and save the record. If a user-defined field is **Mandatory in Partition**, all new Personnel belonging to that Partition must have a non-null value in that User-defined field. When new a Mandatory User-defined Field is created, it is added to every existing Personnel record, and all newly created Personnel records, with a null value. When a new Personnel record is edited, it cannot be saved until a valid value is entered in that Mandatory User-defined field. For Personnel records that existed prior to the Mandatory User-defined Field's addition to the record, the User-defined field is given the **Initial Value**, and validation is not enforced unless the field is changed by an Operator edit.
Uniqueness	On a non-partitioned system, every field must be either **Unique** or **Not Unique**. On a partitioned system, a field can be: • **Not Unique** • **Unique Within System** – a value entered by an Operator is validated so that the value is unique for all Personnel records. • **Unique Within Partition –** a value entered by an Operator is validated so that the value is unique within the partition of the Personnel record, even if the partition where the User-defined Field was defined is different from that of the Personnel record. The following field types can be designated as Unique: • Integer • Decimal • Character

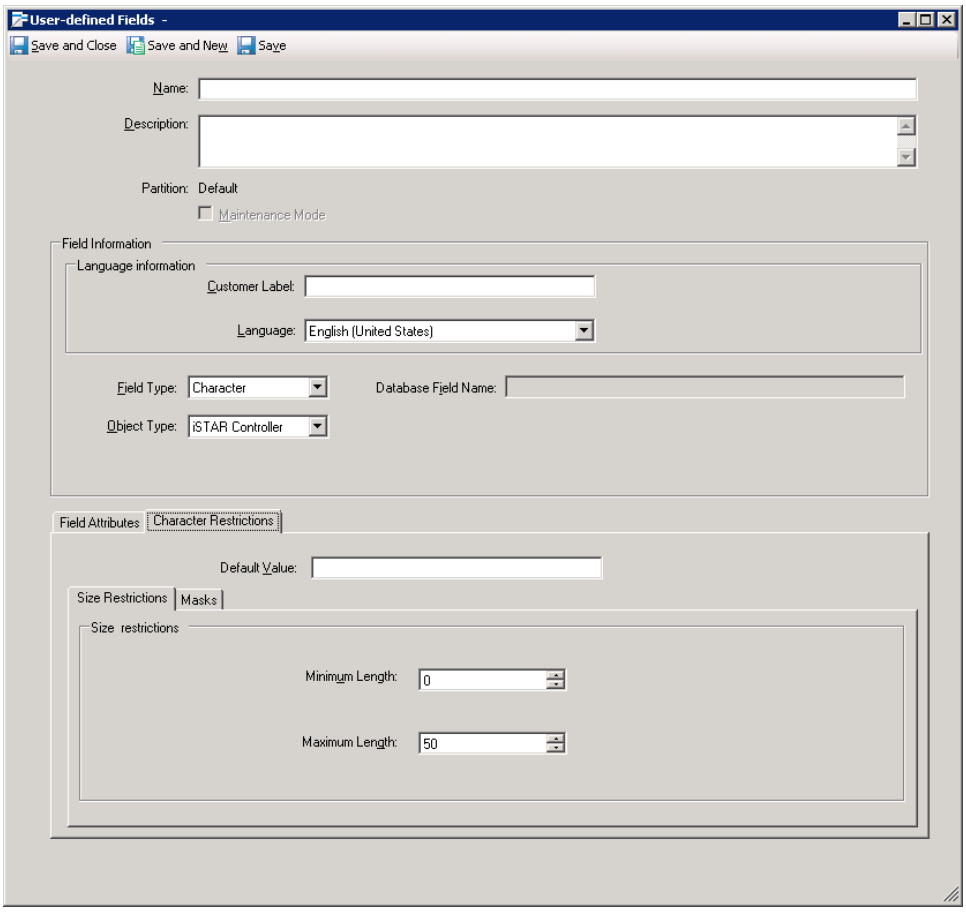
User-defined Fields Editor Restrictions Tab

The **User-defined Fields Restrictions** tab lets you set restrictions for the field that are appropriate to the field type. The Restrictions tab differs for the various field types you can define.

The definitions of fields on the Restrictions tab for each type of field are listed in User-defined Fields Editor Enumeration Values Tab on Page 524.

Figure 164 on Page 512 shows the User-defined Fields Restrictions tab for a character field.

Figure 164: User-defined Fields Restrictions Tab



The Restrictions tab can itself have two tabs:

- Size Restrictions tab
- Masks tab (for Character type User-defined Fields).

Restrictions Tab Tasks

You can perform the following tasks from the Restrictions tab:

NOTE The Identity and Custom User-defined Field types do not have a Restrictions tab.

- Setting Restrictions for a Character Field on Page 513.
- Mask Symbol Definitions for Character Fields on Page 516.

- Setting Restrictions for a Date Field on Page 518.
- Setting Restrictions for a Date Time Field on Page 519.
- Setting Restrictions for a Decimal Field on Page 519.
- Setting Restrictions for an Integer Field on Page 520.
- Setting the Initial Value for a Logical Field on Page 521.
- Setting Restrictions for a Multi-Line Field on Page 522.
- Setting Restrictions for a Time Field on Page 522.

Setting Restrictions for a Character Field

The Restrictions tab for Character fields itself has two tabs:

- **Size Restrictions** tab - for setting the minimum and maximum lengths for a Character field. See Table 129 on Page 514 for definitions of the fields on the Size Restrictions tab.
- **Masks** tab - for defining a Mask for the Character field that restricts and formats the data an Operator can enter into the field. See Table 129 on Page 514 for definitions of the fields on the **Masks** tab.

  See Defining a Mask for a Character Field on Page 515 for more information about defining Masks for Character fields.

To Set Size Restrictions for a Character Field

1. Open the User-defined Fields editor. See Accessing the User-Defined Fields Editor on Page 505.
2. Select **Character** in Field Type if you are creating a new User-defined field (if you are editing an existing field, **Character** is already set).
3. Click the Character Restrictions tab.
4. Enter the **Minimum Length** for the Character field.

   Example:

   If you enter '5' for the **Minimum Length**, the Operator has to enter at least five characters when they edit the field or an error message appears.
5. Enter the **Maximum Length** for the Character field.

   Example:

   If you enter '25' for the **Maximum Length**, the Operator can enter no more than 25 characters when they edit the field or an error message appears.
6. Click **Save** to save your changes. Click **Save and Close** if you want to close the editor.

Character Fields Restrictions Tab Definitions

Table 129 on Page 514 defines the fields on the Restrictions tab for Character fields.

Table 129: Character Fields Restrictions Tab Definitions

Field/Button	Description
Default Value	You can set a default value for your User-defined Field. If you selected **Mandatory** (**Mandatory System Wide** or **Mandatory in Partition** for a partitioned system) on the Field Attributes tab, this field is labeled **Initial Value** rather than **Default Value**.
Initial Value	If you selected **Unique** (**Unique System Wide** or **Unique in Partition** for a partitioned system), this field becomes read-only. If you define a Mask for the User-defined Field, this field becomes read-only, but you can enter a test mask in **Test Mask on Sample Value** and click **Use Test as Default** to add the sample mask to this field.
Size Restrictions tab	
Minimum Length	The minimum number of characters that an Operator must enter when editing this field. The value can range from 0 to 1000. The default value is 0. The Minimum Length is only validated when the field is non-blank. **Example:** If you enter a minimum length of '10' then the Operator must type at least 10 characters in this field when editing the objector an error occurs. If you save the User-defined Character field and subsequently edit this value, you cannot increase the **Minimum Length**, but you can decrease the **Minimum Length**.
Maximum Length	The maximum number of characters that an Operator can enter when editing this field. The value can range from 0 to 1000, but it can not be less than the **Minimum Length**. The default value is 50. If you save the User-defined Character field and subsequently edit this value, you cannot decrease the **Maximum Length**, but you can increase the **Maximum Length**.
Masks tab	
Mask	This field contains the mask that is applied to the field to limit the characters that a user can type in, and also to provide formatting, including placeholder characters, so that entries to this field in all Personnel are consistently formatted. **Example:** If you create a phone number field, you can define a mask for the field that forces the Operator to enter the phone number in a specific format, such as 1+ 234.567.8900 (i.e., country code, area code, 3 digits, then four digits, separated by periods).
Use Predefined Mask	Click this button to select from a list of predefined masks to use as a pattern for your mask. You can choose masks of the following types. • Alphabetic • Numeric • Phone Number (United States format) • Social Security number (United States format – 000-000-0000) • Zip Code (United States format – 00000) • Zip Code + 4 (United States format – 00000-0000) • Alphabetic – All Caps • Alphabetic – All lower case After you choose a mask, you can customize it to meet your needs. **Example:** If you choose a Phone Number mask, but the predefined mask does not conform to your telephone number format, you can change the mask to fit your format, adding an international calling code, for example.
Test Mask on Sample Value	You can test the mask you defined by typing a sample value into the text box field and clicking the **Test Mask on Sample Value** button.
View Sample Masks	Click to open a Help topic that displays the mask symbols and definitions, along with examples of mask usage.
Use Test as Default	You can set the **Test Mask** as the Default Value for the field by clicking this button.

Masks for Character User-defined Fields

Masks provide a way of formatting data that is entered by Operators so that the data is stored and displayed in a standardized format. The Mask for a User-defined field specifies the type of characters an Operator can enter in the field, or portions of the field. The Mask can include characters that are mandatory and are non-editable elements of the field.

Example:

You can define a mask for a telephone number that restricts the type and number of characters an Operator can enter, and can include conventions like parentheses characters enclosing the Area Code – as in (123) 456-7890 – the characters **( ) -** are displayed by default in the User-defined field. The Operator can enter no more than three numbers inside the parentheses. This mask could be defined (using the mask symbols in Mask Symbol Definitions for Character Fields on Page 516, as:

(999) 000-0000

Because '0' is the symbol for a required digit; thus the mask specifies that noSymbol more than 10 digits must be entered in the format shown.

When an Operator edits a field that has a mask, the mask prevents the Operator from entering or saving invalid data. If the mask was added to the User-defined field after data was entered, the data remains in the field, but a message warning that the data conflicts with the mask is displayed. The Operator can choose to click **OK** to erase the data and apply the mask, or **Cancel** to leave the current value in place.

Several pre-defined masks are included in the User-defined Fields editor, or you can create new masks.

Masks are applied in to the User-defined field in the obejct editor, and also appear when the field is shown in Dynamic Views.

Defining a Mask for a Character Field

When you define a mask, you can use a combination of standard characters and symbols to specify the format of Operator-entered data.

Mask Symbol Definitions for Character Fields on Page 516 provides definitions of the symbols you can use to define a Mask for a User-defined field.

To Define a Mask for a Character Field

1. Create a new Character field or edit an existing Character field. See Accessing the User-Defined Fields Editor on Page 505.
2. Click the Character Restrictions tab.
3. Use the Size Restrictions tab to set the size for the Character field. See To Set Size Restrictions for a Character Field on Page 513.
4. Click the Masks tab.
5. You can click **Allow spaces** to enable the space bar when the cursor is in the field. If **Allow spaces** is not enabled, the space bar is disabled when the cursor is in the field. (An Operator can paste spaces into the field, however.)
6. If you want to use (or start with) a standard mask, click **Use Predefined Mask**. A dialog box opens with a drop-down list of Predefined Masks.
7. Click on a mask in the list to choose it and click **OK**. The new mask is shown in the Mask field.
8. You can click **View Sample Masks** to open the Help topic that provides definitions of the symbols you can use to define a mask for a User-defined field.

9. You can use **Test Mask on Sample Value** to type data into the mask to determine if the mask is working as you intended. If the characters you type do not conform to the mask restrictions (or the **Size Restrictions** for the field) an error message is displayed.
10. If the sample value you type in is valid and you wish to use it as a **Default Value** for the field, you can click **Use Test as Default**.
11. To save the changed mask settings for your User-defined field, click **Save**. To close the editor click **Save and Close**.

Mask Symbol Definitions for Character Fields

Table 130 on Page 516 provides definitions of the symbols you can use to define a Mask for a User-defined field, and examples of usage.

Table 130: Mask Symbols Definitions

Symbol	Description
0	Represents a digit, required. This Mask element accepts any single digit between 0 and 9. **Example:** 000 in a mask means the Operator must enter three digits, such as 617.
9	Represents an optional digit. This Mask element accepts any single digit between 0 and 9. **Example:** 999 in a mask means the Operator can enter from zero to three digits, such as 6, 35, or 777.
#	Represents an optional digit or space. If this position is blank in the mask, it is rendered as a space. Plus (+) and minus (-) signs are allowed. **Example:** ### in a mask means the Operator can enter from zero to three digits or spaces, including a + or - sign, such as +6, 3 5, or -77.
L	Represents a required letter. Restricts input to the ASCII letters a-z and A-Z. **Example:** LLL in a mask means the Operator must enter three letters, such as AaA, CAT, or cat.
?	Represents an optional letter, optional. Restricts input to the ASCII letters a-z and A-Z. **Example:** ??? in a mask means the Operator can enter from zero to three letters, such as Aa, C, or cat.
&	Represents a required character. Allows input of Unicode characters (other than control characters) in addition to ASCII letters. **Example:** &&& in a mask means the Operator must enter three characters, such as aAa, C•C, or Yo!.
C	Represents an optional character. Allows input of Unicode characters (other than control characters) in addition to ASCII letters. **Example:** CCC in a mask means the Operator can enter from zero to three characters, such as A, C•, or Yo!.
A	Represents a required Alphanumeric character. Allows input of the ASCII letters a-z and A-Z, and digits 0-9. **Example:** AAAA in a mask means the Operator must enter four characters, such as R2D2, 1234, or 2Pac.
a	Represents an optional Alphanumeric character. Allows input of the ASCII letters a-z and A-Z, and digits 0-9. **Example:** AAAA in a mask means the Operator can enter from zero to four characters, such as R2D2, 4, or Mac.

Table 130: Mask Symbols Definitions (continued)

Symbol	Description
.	Represents a decimal placeholder. The actual display character used will be the decimal symbol appropriate to the system's location. **Example:** 99.9 in a mask means the Operator can enter from zero to three numbers, and the decimal separator is placed appropriately, such as 52.2, 4.0, or 4.8.
,	Represents a thousands placeholder. The actual display character used will be the thousands symbol appropriate to the system's location. **Example:** 9,999 in a mask means the Operator can enter from zero to four numbers, and the thousands separator is placed appropriately, such as 52, 4,000, or 4.
:	Represents a time separator. The actual display character used will be the time separator appropriate to the system's location. **Example:** 0:00:00 in a mask means the Operator must enter five numbers, and the time separator is placed appropriately, such as 5:22:30, 9:00:00, or 4:59:59.
/	Represents a date separator. The actual display character used will be the date symbol appropriate to the system's location. **Example:** 00/00/00 in a mask means the Operator must enter six numbers, and the date separator is placed appropriately, such as 5/22/30, 11/01/09, or 4/10/10.
$	Represents a currency symbol. The actual display character used will be the currency symbol appropriate to the system's location. **Example:** 999$ in a mask means the Operator can enter from zero to three numbers, and the currency symbol is placed appropriately, such as 67$, 999€, or 4¥.
<	Converts all characters to lower case. The actual display character used will be the lower case version of each character entered. **Example:** <LLL in a mask means the Operator must enter three letters. The letters entered are converted to lower case, even if entered as upper case, such as abc, xyz, or ttt.
>	Converts all characters to upper case. The actual display character used will be the uppercase version of each character entered. **Example:** >LLL in a mask means the Operator must enter three letters. The letters entered are converted to upper case, even if entered as lower case, such as ABC, XYZ, or TTT.
|	Disables a previous < (shift to lower case) or > (shift to upper case) so that characters that follow are no longer forced to upper or lower case. **Example:** >LLL|LLL in a mask means the Operator must enter six letters. The first three letters entered are converted to upper case, even if entered as lower case, and the last three are left as typed, such as ABCabc, XYZaBc, or TTTabC.
\	Represents a Escape indicator. This is used to enter a literal character such as L or 9 that usually represents a Mask. For example, if you want the Mask to contain a literal letters or numbers such as "999" or "BIN#" you would need \ to indicate that the "9" characters ("\9\9\9") or the "#" ("BIN\#") should be treated as characters, not as Mask symbols. **Example:** BIN\#999#999 in a mask means the Operator can enter from zero to seven numbers, with a number or space in position four of the entry. The field contents display as BIN#765 124 if the Operator enters 765 124. The "#" after "BIN" is displayed as a text character because it is preceded in the mask by "\".

Table 130: Mask Symbols Definitions (continued)

Symbol	Description
All other characters	Represents a literal character. All non-mask elements appear as themselves within the Masked field. Literals always occupy a static position in the mask at run time, and cannot be moved or deleted by the user. **Example:** IDNumber99999 in a mask means the Operator can enter from zero to five numbers, and the literal text "IDNumber" is displayed in the field and cannot be edited or erased. For example, if the user types 45678, the field displays "IDNumber45678".

Setting Restrictions for a Date Field

Restrictions for a Date field allow you to set a Default Value for the field, including **Now**, which displays as the current date when the field is first edited in the object Editor. You can also specify a **Minimum Value** (the earliest date in time that an Operator can enter in the field) and **Maximum Value**.

To Set Restrictions for a Date Field

1. Create a new Date field or edit an existing Date field. See Accessing the User-Defined Fields Editor on Page 505.
2. Click the **Date Restrictions** tab.
3. To have the field assigned by default the time that the object is created, select **Now**. If you select **Now**, you cannot select a **Default Value** (or an **Initial Value**, if the Date field is Mandatory).
4. To set a date as a **Default Value**, click to open a calendar to select a date.
5. You can use the default **Minimum Value,** or you can click to open a calendar to select a date.
6. You can use the default **Maximum Value,** or you can click to open a calendar to select a date.
7. To save these settings, click **Save**. To close the editor click **Save and Close**.

Date Fields Restrictions Tab Definitions

Table 131 on Page 518 defines the fields on the Restrictions tab for Date fields.

Table 131: Date Fields Restrictions Tab Definitions

Field/Button	Description
Now	This selection displays the date of the creation of the object as a default value when a record is first edited in the object editor. However, the Operator can change the date, and if the record is saved, the value chosen by the Operator is saved.
Default Value (if the field is not Mandatory)	You can set the default value to a specific date. This date is displayed when a record is first edited in the object editor. However, the Operator can change the date, and if the record is saved, the value chosen by the Operator is saved.
Initial Value (if the field is Mandatory)	You must set an **Initial Value** for a Mandatory User-defined Field or you cannot save the field. The **Initial Value** is selected from a calendar drop-down, and is validated against the **Minimum Value** and the **Maximum Value**.
Minimum Value	Represents the earliest date that is considered valid for this field.
Maximum Value	Represents the latest date that is considered valid for this field.

Setting Restrictions for a Date Time Field

Restrictions for a Date Time field allow you to set a **Default Value** for the field (or an **Initial Value**, if the field is Mandatory), including **Now**, which displays as the current date and time when the field is first edited in the object Editor. You can also specify a **Minimum Value** (the earliest date time that an Operator can enter in the field) and **Maximum Value**.

To Set Restrictions for a Date Time Field

1. Create a new Date Time field or edit an existing Date Time field. See Accessing the User-Defined Fields Editor on Page 505.
2. Click the **DateTime Restrictions** tab.
3. To have the field assigned by default the time that the object is created, select **Now**. If you select **Now**, you cannot select a **Default Value** (or an **Initial Value**, if the Date Time field is Mandatory).
4. To set a date as a **Default Value**, click to open a calendar to select a date, and click the cursor in the field to change the time.
5. You can use the default **Minimum Value,** or you can click to open a calendar to select a date, and click the cursor in the field to change the time.
6. You can use the default **Maximum Value,** or you can click to open a calendar to select a date, and click the cursor in the field to change the time.
7. To save these settings, click **Save**. To close the editor, click **Save and Close**.

Date Time Fields Restrictions Tab Definitions

Table 132 on Page 519 defines the fields on the Restrictions tab for Date Time fields.

Table 132: Date Time Field Restrictions Tab Definitions

Field/Button	Description
Now	This selection displays the date and time of the creation of the object a default value when a record is first edited in the Personnel editor. However, the Operator can change the date and time, and if the record is saved, the value chosen by the Operator is saved.
Default Value (if the field is not Mandatory)	You can set the default value to a specific date and time. This date and time is displayed when a record is first edited in the object editor. However, the Operator can change the date and time, and if the record is saved, the value chosen by the Operator is saved.
Initial Value (if the field is Mandatory)	You must set an **Initial Value** for a Mandatory User-defined Field or you cannot save the field. The **Initial Value** is selected from a calendar drop-down, and is validated against the **Minimum Value** and the **Maximum Value**.
Minimum Value	Represents the earliest date and time that is considered valid for this field.
Maximum Value	Represents the latest date and time that is considered valid for this field.

Setting Restrictions for a Decimal Field

Restrictions for a Decimal field allow you to set a Default Value for the field. You can also specify a **Minimum Value** (the smallest numerical value that an Operator can enter in the field), a **Maximum Value**, and the number of digits to the right of the decimal point (to determine the display precision of the field).

To Set Restrictions for a Decimal Field

1. Create a new Decimal field or edit an existing Decimal field. See Accessing the User-Defined Fields Editor on Page 505.
2. Click the **Decimal Restrictions** tab.
3. To set a **Default Value**, click to choose a value, or click in the field a type a value.
4. You can use the default **Minimum Value,** or you can click to choose a value, or click in the field a type a value.
5. You can use the default **Maximum Value,** or you can click to choose a value, or click in the field a type a value.
6. You can use the default **Number of digits to right of decimal,** or you can click to choose a value, or click in the field a type a value.
7. To save these settings, click **Save**. To close the editor click **Save and Close**.

Decimal Fields Restrictions Tab Definitions

Table 133 on Page 520 defines the fields on the Restrictions tab for Decimal Fields.

Table 133: Decimal Field Restrictions Tab Definitions

Field/Button	Description
Default Value (if the field is not Mandatory)	You can set the default value to a specific value. This value must conform to the setting for **Number of digits to right of decimal**. **Example:** If the **Number of digits to right of decimal** setting is 3, and you enter 34.5 as the Default Value, it is formatted with three decimal places (i.e., 34.500). If the field is Unique, **Default Value** is unavailable (you cannot set a **Default Value** for a Unique field).
Initial Value (if the field is Mandatory)	You must set an **Initial Value** for a Mandatory User-defined Field or you cannot save the field. The format of the **Initial Value** is adjusted to conform to the setting for **Number of digits to right of decimal**.
Minimum Value	Represents the smallest numerical value that is considered valid for this field. The format of the **Minimum Value** is adjusted to conform to the setting for **Number of digits to right of decimal**. **Example:** If the **Number of digits to right of decimal** setting is 3, the **Minimum Value** is formatted with three decimal places (i.e., .000).
Maximum Value	Represents the largest numerical value that is considered valid for this field. The format of the **Maximum Value** is adjusted to conform to the setting for **Number of digits to right of decimal**. **Example:** If the **Number of digits to right of decimal** setting is 3, the **Maximum Value** is formatted with three decimal places (i.e., .000).
Number of digits to right of decimal	You can specify the number of decimal places that are displayed in the field.

Setting Restrictions for an Integer Field

Restrictions for an Integer field allow you to set a **Default Value** for the field (or an **Initial Value**, if the field is Mandatory). You can also specify a **Minimum Value** and **Maximum Value**.

To Set Restrictions for an Integer Field

1. Create a new Integer field or edit an existing Integer field. See Accessing the User-Defined Fields Editor on Page 505.

2. Click the **Integer Restrictions** tab.
3. To set a **Default Value** (or an **Initial Value** for a Mandatory field), click  to choose a value, or click in the field a type a value.
4. You can use the default **Minimum Value,** or you can click  to choose a value, or click in the field a type a value.
5. You can use the default **Maximum Value,** or you can click  to choose a value, or click in the field a type a value.
6. To save the settings, click **Save**. To close the editor click **Save and Close**.

Integer Fields Restrictions Tab Definitions

Table 134 on Page 521 defines the fields on the Restrictions tab for Integer fields.

Table 134: Integer Fields Restrictions Tab Definitions

Field/Button	Description
Default Value (if the field is not Mandatory)	You can set the default value to a specific value. If the field is Unique, **Default Value** is unavailable (you cannot set a **Default Value** for a Unique field).
Initial Value (if the field is Mandatory)	You must set an **Initial Value** for a Mandatory User-defined Field or you cannot save the field. The default value is 0.
Minimum Value	Represents the smallest numerical value that is considered valid for this field. The default value is 0. Once you save the Integer User-defined field, the **Minimum Value** can be decreased but it cannot be increased.
Maximum Value	Represents the largest numerical value that is considered valid for this field. The default value (and the largest value allowed) is 2147483647 Once you save the Integer User-defined field, the **Maximum Value** can be increased but it cannot be decreased.

Setting the Initial Value for a Logical Field

The Logical Restrictions tab allows you to set the **Initial Value** for a Logical field.

To Set the Initial Value for a Logical Field

1. Create a new Logical field or edit an existing Logical field. See Accessing the User-Defined Fields Editor on Page 505.
2. Click the **Logical Restrictions** tab.
3. Select either **Checked** (True) or **Unchecked** (False) as the Initial Value for the Logical field.
4. To save the settings, click **Save**. To close the editor click **Save and Close**.

Logical Fields Restrictions Tab Definitions

Table 135 on Page 521 defines the fields on the Restrictions tab for Logical Fields.

Table 135: Logical Field Restrictions Tab Definitions

Field/Button	Description
Checked	Select Checked to represent a Logical True value.
Unchecked	Select Unchecked to represent a Logical False value.

Setting Restrictions for a Multi-Line Field

You can set the maximum character length and the default value for a a Multi-line field.

NOTE A Multi-line field allows Carriage Return (CR) and Line Feed (LF) characters.

To Set Restrictions for a Multi-Line Field

1. Create a new Multi-Line field or edit an existing Multi-Line field. See Accessing the User-Defined Fields Editor on Page 505.
2. Click the **Multi-Line Restrictions** tab.
3. Choose a value for the **Maximum Length** of the Multi-Line field using the  .
4. To specify a default value for the Multi-Line field, type it in the Default Value field.
5. To save the settings, click **Save**. To close the editor click **Save and Close**.

Multi-Line Fields Restrictions Tab Definitions

Table 136 on Page 522 defines the fields on the Restrictions tab for Multi-Line fields.

Table 136: Multi-Line Fields Restrictions Tab Definitions

Field/Button	Description
Maximum Length	The maximum number of characters that the field can contain, including any Carriage Return and Line Feed characters. You can set the **Maximum Length** if you want to restrict the number of characters an Operator can type in to the field. The value for **Maximum Length** must be at least one character and no greater than 10,000 characters. The default value for **Maximum Length** is 1,000 characters. Once you specify a **Maximum Length and** save the field, you cannot subsequently edit the field and reduce the **Maximum Length** value. You can, however, increase the **Maximum Length** value when editing a previously saved Multi-line field.
Default Value	You can specify a default value for a Multi-line field by typing the text you want displayed in the field into the **Default Value** text box. The text you type cannot exceed the **Maximum Length** setting.

Setting Restrictions for a Time Field

Restrictions for a Time field allow you to set a **Default Value** for the field (or an **Initial Value**, if the field is Mandatory), including **Now**, which displays as the current date and time when the field is first edited in the object Editor.

To Set Restrictions for a Time Field

1. Create a new Time field or edit an existing Time field. See Accessing the User-Defined Fields Editor on Page 505.
2. Click the **Time Restrictions** tab.
3. To have the field assigned by default the time that the object is created, select **Now**. If you select **Now**, you cannot select a **Default Value** (or an **Initial Value**, if the Time field is Mandatory).
4. Choose a value for the **Maximum Length** of the Time field using the  .
5. To save the settings, click **Save**. To close the editor click **Save and Close**.

Time Fields Restrictions Tab Definitions

Table 137 on Page 523 defines the fields on the Restrictions tab for Time fields.

Table 137: Time Field Restrictions Tab Definitions

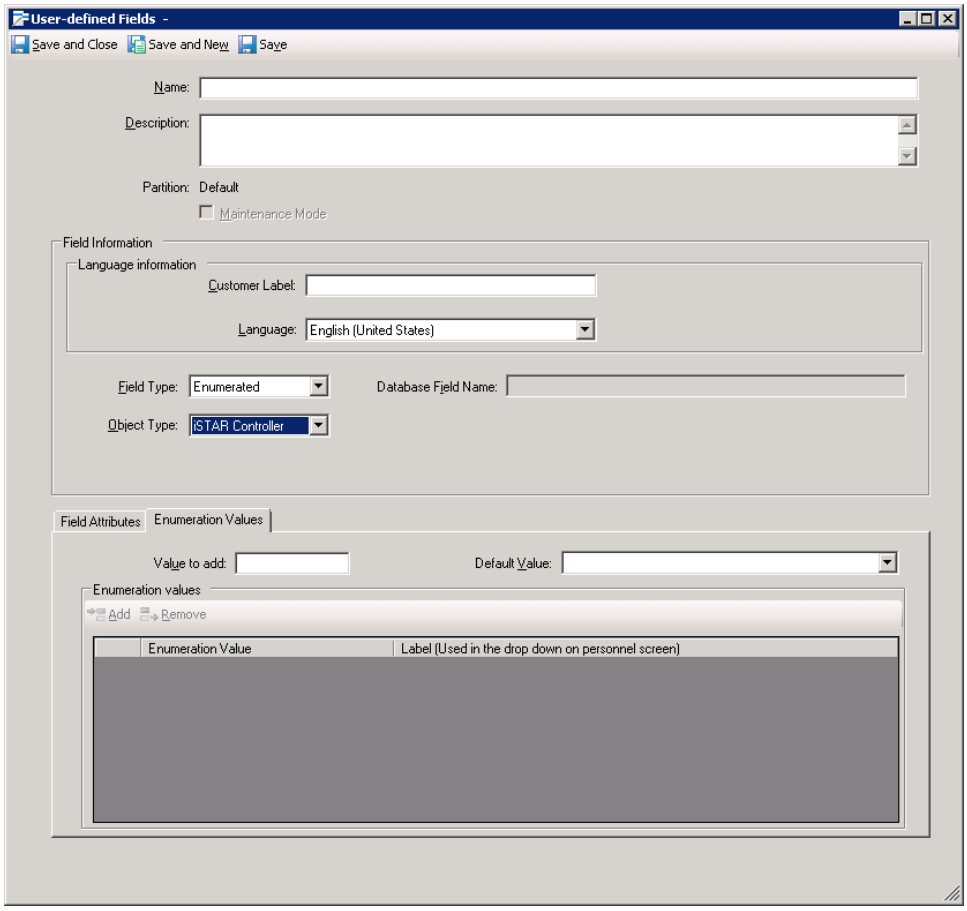
Field/Button	Description
Now	displays the date and time of the creation of the object as a default value when a record is first edited in the object editor. However, the Operator can change the time, and if the record is saved, the value chosen by the Operator is saved.
Default Value (if the field is not Mandatory)	You can set the default value to a specific time. This time is displayed when a record is first edited in the object editor. However, the Operator can change the time, and if the record is saved, the value chosen by the Operator is saved.
Initial Value (if the field is Mandatory)	You must set an **Initial Value** for a Mandatory User-defined Field or you cannot save the field. The **Initial Value** is selected from a calendar drop-down, and is validated against the **Minimum Value** and the **Maximum Value**.
Minimum Value	Represents the earliest date and time that is considered valid for this field.
Maximum Value	Represents the latest date and time that is considered valid for this field.

User-defined Fields Editor Enumeration Values Tab

The Enumeration Values tab allows you to define the list of possible values for an Enumerated User-defined field.

See Enumeration Values Tab Definitions on Page 525 for definitions of all fields and buttons on the Enumeration Values tab. Figure 165 on Page 524 shows the Enumeration Values tab.

Figure 165: Enumeration Values Tab



Enumeration Values Tab Tasks

You can perform the following tasks from the Enumeration Values tab:

- Setting Enumeration Values for an Enumerated Field on Page 524.
- Creating Enumeration Values for Additional Languages on Page 525.

Setting Enumeration Values for an Enumerated Field

You can create a list of values for the Enumerated field using the **Enumerated Values** tab. You can define the value and label for each enumeration, and a Default Value for the field.

To Set Enumeration Values for an Enumeration

1. Create a new Enumeration field or edit an existing Enumeration field. See Accessing the User-Defined Fields Editor on Page 505.

2. Click the Enumeration Values tab.
3. For each Enumeration Value that you want to add to the Enumerations for the field:
   a. Type the Enumeration Value in the **Value to add** field. Each Enumeration Value must be unique within the Enumeration.
   b. Click **Add** to add the value to the Enumeration Values table.
   c. You can click in the **Label** column if you want to change the **Label** that is displayed to represent the field in the Personnel editor.

NOTE Once you click **Add** to add a value to the list, you cannot edit that Enumeration Value, only its label. If you need to make a change to an Enumeration value, you must select that row in the Enumeration Values table, click **Remove** to remove that value from the table, and then recreate the value.

4. In the **Default Value** field, select one of the values you have added as the default value for this Enumerated Field when it appears in a Personnel View. Click to open a list of the Enumeration values, and click on the value you wish to assign as a **Default Value**.
5. To save these settings, click **Save**. To close the editor click **Save and Close**.

Creating Enumeration Values for Additional Languages

You can create translated Labels for an Enumerated list by changing the language in the **Language** drop-down.

You can only make language changes for language versions currently residing on your system. When you choose a language from the **Language** field drop-down list, the list only contains the languages for which language resources already exist on your system. See Selecting a Language on Page 509 for more information.

If you do not translate a label in the Enumerated Value list, the label for the default language appears in the Enumerated Field drop-down list when the field is viewed in the object editor.

To Create Enumeration Values for a Language

1. Create a new Enumeration field or edit an existing Enumeration field. See Accessing the User-Defined Fields Editor on Page 505.
2. Select the Language that you want to create labels for from the **Language** drop-down list.
3. Click the Enumeration Values tab.
4. For each label you want to translate, double-click in the **Label** field for that Enumeration Value and type the translated label.
5. You can also set a separate Default Value for the field in the selected Language by clicking to open a list of the Enumeration values, and clicking on the value you wish to assign as a **Default Value**.
6. To save these settings, click **Save**. To close the editor click **Save and Close**.

Enumeration Values Tab Definitions

Table 138 on Page 526 defines the fields on the Enumeration Values tab for Enumerations.

Table 138: Enumerations Values Tab Definitions

Field/Button	Description
Value to Add	Type a text name for the enumeration then click **Add** to add the Value to the list of Enumerations. Its length can not exceed 15 characters. The text you type into this field is stored in the database to identify this enumeration. This value must be unique within the enumeration (you can not have two or more of the same enumeration values in the list).
Default Value	You can select the default value for this field from a drop-down list that includes the labels of all the enumerations from the grid. The names that appear in the list are the labels in the selected language. (If there is no translation in the selected language, the enumeration value is displayed).
Add	Click this button to add an enumeration value. The button is unavailable when **Value to Add** is blank or contains a non-unique value, or when the language is not set to the base language.
Remove	Click this button to remove one or more enumeration values. You can select multiple Enumeration Values in the list using **Ctrl+Shift** or **Ctrl+Left-Click**. If you remove values that are assigned to existing objects, an error message appears when you attempt to save the User-defined field - you cannot save such changes to a User-defined because it would leave invalid values in some existing objects. You need to edit those existing objects to select a different value for the field (use a Query to find objects that contain the enumerated value).
Enumeration Value	When you click **Add**, the **Value to Add** is added to this field in the Enumeration Values list. This field is Read Only. This is the value stored in the User-defined Field, and in an XML file if the object is exported to .XML.
Label	Type in the text that you want to be displayed for this Enumeration value in the object editor drop-down list of this User-defined Enumerated field.

21

Workstation

This chapter explains the C•CURE 9000 Workstation objects.

In this chapter

Workstation

A **Workstation** object appears in a C•CURE 9000 server automatically when an operator logs on to the same C•CURE 9000 server from a different computer using the following applications:

- the **Administration Workstation** application
- the **Monitoring Station** application
- the **victor** application
- the **Visitor Kiosk** application

Other clients such as: **C•CURE Portal**, **C•CURE Web** Client, and **C•CURE Go** do not create **Workstation** objects if the operator accesses them from different computers, but are associated with the pre-defined workstation object called "Default Workstation" created at the time of installation.

Operators can delete **Workstation** objects. Operators should use the delete operation in the case a workstation system has been modified or the operators have removed the actual computer from the network. However, if the operator attempts to use the computer which associates to a deleted **Workstation** object again, the server recreates that former **Workstation** object. It is therefore recommended to disable the unwanted workstation instead of performing a deletion.

Operators cannot import **Workstation** objects because each computer that runs a C•CURE 9000 Client can register in the system as a **Workstation** object automatically.

Standard behavior of the Workstation object's privileges include:

- The operator can view and modify the Workstation objects based on their user privileges.
- If a Workstation object has the **Enabled** property disabled, users cannot log in from that Workstation.
- If an operator does not have read access to a Workstation, they can still log into the system from that Workstation.
- The system creates a new Workstation object automatically at the time an operator uses the computer or tablet for the very first time, the workstation is created in the default partition of the server at that time.

NOTE The System Administrator must move the Workstation objects into proper partitions after they are created in the system in case of the multi-tenant customers. This is due to newly created Workstations objects being created in the Default partition where any operator can view them. It might not be acceptable for the multi-tenant use case.

If an operator performs a particular action in the system, such as clicking the **Assistance Request** button in the Personnel editor, the system logs the name of the associated **Workstation** where the operation is performed.

By right-clicking and viewing the context menu of the object, operators can use **Find in Audit Log** and **Find in Journal** queries and find all the records that are associated with that particular workstation.

NOTE Prior to 2.7 a SAS user was able to login to a MAS and modify their existing SAS based objects but starting with 2.7, this is no longer be possible without the Administrator modifying user privileges.

For more information about configuring Workstation objects, refer to:

- Table 139 on Page 529 describes the Dynamic View of **Workstation** objects.
- Modifying a Workstation on Page 529 for the procedure to edit values of a Workstation.
- Restricting Access to a Workstation on Page 530 to restrict access to a Workstation.

Fields of Workstation Dynamic View

Table 139 on Page 529 describes the fields of the **Workstation** Dynamic View.

Table 139: Workstation Dynamic View fields

Field	Description
Name	The name of the Workstation. By default, this populates automatically at the time when an operator logs in and you can change through the editor or Set Property executor. NOTE: It is advised that you use a meaningful naming convention when naming Workstations so the names are unique as these are the names that appear in Journal and Audit Log messages.
Enabled	The status of the workstation. By default, this status is set to true and the check box appears selected. NOTE: If you clear the check box and set the status to false, all connections from the disabled Workstation are blocked.
Description	The description that you assign to the workstation. You should provide a meaningful name to each object.
Last Known Operator	The name of the operator to last access the workstation.
Last Known Connections	The details of the last connections of the workstation. This includes the name and software version of the connection.
Partition	The partition of the workstation. This is created in the partition of the Operator who runs a supported C•CURE 9000 client on a particular computer for the first time.
Internal Name	This is the exact name of the computer. This field is read-only and you cannot edit.

Modifying a Workstation

You can access the **Workstation** dynamic view from the **Configuration** pane of C•CURE 9000 Administration Station. You can edit properties of a **Workstation** object through the editor or through the Set Property executor. In the Set Property executor of the **Workstation** objects, you can edit the **Description**, **Name**, **Set Partition**, and **Enabled** values.

NOTE The System Administrator must move the Workstation objects into proper partitions after they are created in the system in case of the multi-tenant customers. This is due to newly created Workstations objects being created in the Default partition where any operator can view them. It might not be acceptable for the multi-tenant use case.

Setting Properties of Workstations through Set Property Executor

1. In the Navigation pane of the Administration Workstation, click **Configuration** to open the **Configuration** pane.
2. From the **Configuration** pane drop-down list, select **Workstation**. Click the arrow beside the drop-down list to open a Dynamic View.
3. Right-click the object in the list for which you want to set the property and select **Set Property** from the context menu. The Set Property box appears.
4. In the **Property** field, click the ellipsis to see a list of properties and select the property you want to modify.
5. Edit the **Value** field as appropriate and click **OK**. You can view the changes of the object in the **Workstation** Dynamic View.

Setting Properties of Workstations through Workstation Editor

1. In the Navigation pane of the Administration Workstation, click **Configuration** to open the **Configuration** pane.
2. From the **Configuration** pane drop-down list, select **Workstation**. Click the arrow beside the drop-down list to open a Dynamic View.

3. Double-click the object in the list for which you want to edit. The Workstation editor appears.
4. Make the edits you want to the Workstation object and click **Save and Close**.

Restricting Access to a Workstation

Users can be restricted from interacting with Workstations in the C•CURE 9000 system for several reasons:

- The Workstation is disabled.
  - The Administrator can disable the Workstation by clearing the **Enabled** check box for a Workstation in the editor or Set Property executor. This prevents any user logging in and using the particular Workstation. Refer to Modifying a Workstation on Page 529 for information on the procedure to edit a workstation.
- User privileges are restricted.
  - If a user logs in from a previously created Workstation that exists in the same Partition as the 'Access To Common Objects' privilege (Default Partition), they are able to login successfully. This also means that users that do not have the 'Access To Common Objects' privilege, are not able to login from any of their existing Workstations unless their existing privileges have been updated to give them at least READ access to the applicable Workstation.
- New Workstations are prohibited.
  - Every time a user logs in, they create a workstation. The user that logs in from the Workstation has to have a privilege that gives them, at minimum, READ access to the Workstation object. When they login for the first time, the Workstation object is created in the same partition as the user. If another user logs in from the same Workstation, they too must have a privilege that gives them READ access to the Workstation object and applies to the same Partition that the Workstation object was previously created in.

Using Display as Feedback with a Workstation

You can use **Display as Feedback** to ensure that, when the actions **Display Message** and **Display Viewer** are executed, only the **Workstation** which activated the event will display a message or an object.

To modify the message displayed when the Display as Feedback action is executed

1. From the Event editor, click the Event Action tab.
2. Click **Add** to add an Event Action. See Event Action Tab on Page 293.
3. Select Display Message from the **Action** drop-down list.
4. Customize your message in the Message box at the bottom of the tab.
5. Click the **Display as Feedback** check-box to ensure that this is displayed only on the Workstation which activated the event.
6. Click **Save and Close** to save the event

22

Two Factor Authentication

This chapter explains how to configure Two Factor Authentication in C•CURE 9000.

In this chapter

Two Factor Authentication Overview

The two factor authentication feature provides a further level of security for your C•CURE 9000 system, credentials, and access requests. With this feature, you can gain access to a protected door using a second, additional manner of authentication before access is granted by the reader. By configuring two factor authentication in your system, you can avoid cloned credentials from being used without the knowledge of the original owner of the credential. This software-only security feature is a solution that does not require the deployment of new hardware devices.

The two factor authentication feature in your C•CURE 9000 platform is applied through Duo services. This third party company and its APIs are integrated to provide you with the utmost security from the beginning to the end of access requests by providing the following services:

- Signals a mobile phone that a new authentication request is pending.
- An application or automated call on the mobile phone that you can use to approve or deny the authentication request.

There are two ways Duo services perform the second authentication process for two factor authentication:

- When the cardholder swipes at a two factor authentication protected door and enabled reader, they receive a notification on their mobile phone requesting approval. They can approve or deny the request from the Duo application.
- If a user does not have the Duo application but has a registered phone, they receive an automated call prompting them to press a key to approve the request or terminate the call to deny the request.

Prerequisites

The following components are required to apply two factor authentication to your C•CURE 9000 system and security objects:

- You need to add a license to the server you are using to host the two factor authentication plugin that has:
  - Tyco Web Bridge enabled.
  - 2-Factor Mobile Authentication per Door Annual Subscription License option enabled.
  - The limit you require for the number of doors that participate in the two factor authentication process.
- A valid account with Duo that requires access to both the Auth API and Admin API. The Admin API is not available unless you request it directly from Duo.
  - For more information see Enabling Two Factor Authentication for C•CURE through Duo APIs on Page 534.

Two factor authentication in an Enterprise environment

Two factor authentication is initiated by the Satellite Application Server (SAS) that is connected to hardware and the approved access requests are directed to this connected hardware. Therefore, if you are using an Enterprise system, you need to run the two factor authentication services on each SAS which requires them. All servers in an Enterprise environment can share a single Duo account.

Supporting hardware

Two factor authentication depends on the firmware version applied to the iSTAR family devices you are using in your system. Table 140 on Page 533 lists the devices and firmware versions that support the use of the two factor authentication feature. If the device is not listed, it does not support two factor authentication.

Table 140: Supported Hardware

Device	Firmware version
iSTAR Ultra	v6.5.2 or greater.
iSTAR Ultra SE	v6.5.2 or greater.
iSTAR Ultra LT	v6.5.2 or greater.
iSTAR Edge/eX	v6.2.6 or greater.
iSTAR Pro	v5.2.D or greater

Enabling Two Factor Authentication for C•CURE through Duo APIs

To enable two factor authentication for C•CURE through Duo APIs you must establish a Duo account, request the Admin API from Duo, set up the Admin API and the Auth API, and then, configure the C•CURE Web Bridge Configuration file.

NOTE Ensure you have the prerequisites outlined in Two Factor Authentication Overview on Page 532 before enabling doors to use two factor authentication.

Setting up a Duo account and Duo APIs

1. Set up a Duo account.
   - For information about setting up a Duo account, refer to https://Duo.com/docs/getting-started.
2. Request the Admin API from Duo Support.
   - For more information about the Admin API, refer to https://Duo.com/docs/adminapi#first-steps.
3. Set up the Auth API.
   - Log in to the Duo Admin Panel.
   - Navigate to **Applications**, then click **Protect an Application** and locate the Auth API.
   - Click **Protect this Application** to get the **Integration Key**, **Secret Key**, and **API hostname** for the Auth API. You can use these to securely communicate between the C•CURE host and Duo for the two factor authentication process.
   - For more information about the Auth API, refer to https://Duo.com/docs/authapi#first-steps.
4. Set up the Admin API.
   - Log in to the Duo Admin Panel.
   - Navigate to **Applications**, then click **Protect an Application** and locate the Admin API.
   - Click **Protect this Application** to get the **Integration Key** and **Secret Key**. These are different to the Auth API but the **API hostname** is the same.
   - In the Permissions section, grant read permissions at a minimum. Grant write permissions if your C•CURE host is going to create and remove new users as you enable them for two factor authentication.
   - For more information about the Admin API, refer to https://duo.com/docs/adminapi#first-steps.

NOTE If you are not using Active Directory sync with Duo you can choose the radio button for Simple in the Username normalization section. This provides you with greater flexibility in establishing how C•CURE personnel maps to a Duo user.

Configuring the Web Bridge Configuration file

1. Navigate to the configuration file located here: **C:\Program Files (x86)\Tyco\CrossFire\ServerComponents\ACVS.Enterprise.WebBridge.exe.config**
2. Right click the **ACVS.Enterprise.WebBridge.exe.config** configuration file, select **Open With** from the context menu, then select **Notepad**. The file opens in **Notepad**.
3. Add your **Duo API**, **Integration Key**, **Secret Key**, **Admin Integration Key** and **Admin Secret Key** to the configuration file as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
<appSettings>
<add key="TYCOWebPortalUrlURL" value="" />
```

```
<add key="TYCOWebPortalAccount" value="99999" />
<add key="CheckWorkInterval" value="5000" />
<add key="ClientSettingsProvider.ServiceUri" value="" />
<add key="DuoAPIHostName" value="<Enter the Duo API here>" />
<add key="DuoIntegrationKey" value="<Enter the integration key for Duo Authentication here>" />
<add key="DuoSecretKey" value="<Enter the secret key for Duo Authentication here>" />
<add key="DuoAdminIntegrationKey" value="<Enter the Integration Key for Duo Administration here>"
/>
<add key="DuoAdminSecretKey" value="<Enter the secret key for Duo Administration here>" />
</appSettings>
```

NOTE The information contained in the Web Bridge Configuration file is sensitive and should only be access by trusted personnel

Configuring Fallback to One Factor Authentication

There may be situations when your C•CURE host and the two factor authentication provider, or your C•CURE host and the access control panel fail to communicate. In these situations, you may need to configure a contingency plan so that your security system falls back to using one factor authentication.

You can define a trigger and event to maintain security while communications are being fixed in order to do this.

Configuring fallback when the C•CURE host and two factor authentication provider fail to communicate

The C•CURE host periodically confirms connectivity to the two factor authentication provider. If communication fails for any reason the value in the **Web Bridge State** field of the **Application Server Dynamic View** does not appear as **Connected** and the **Web Bridge Connected** check box is clear, which means it is false and not connected.

Configuring fallback to one factor authentication when the C•CURE host and two factor authentication provider fail to communicate

1. Click the **Configuration** pane and select **Event** from the drop-down list.
2. Click **New** to create a new panel event.
3. In the **Event** editor, click the **Action** tab.
4. Click Add to add a row for the action you want to configure.
5. In the Action drop-down list, select **Set Clearance Filter to Level <x>**, where **x** is a level below the pre-configured **Clearance Filter Level** the reader uses for two factor authentication.
6. In the **Reader** field, click the ellipsis and select the reader you want to apply this action to if there is communications loss between C•CURE and the access control panel.
7. Complete any other configuration options in the **Event** editor you want to pair with this event in the situation it is triggered. Ensure that you select the **Enable** and **Armed** check boxes.
8. Click **Save and Close**. You have created an event that sets the chosen reader to a lower clearance level. To finalize this configuration, you must apply this event to the Application Server in case there is a communication failure.
9. Open the editor for your Application Server and click the **Triggers** tab.
10. In the **Property** section, select **Web Bridge Connected** or **Web Bridge State**. This depends on which field you want to base this trigger on.
11. In the **Value** section, select the value you want to use to trigger the event you configured.
    - If you choose **Web Bridge State** you can choose several options such as, but not limited to: **Disconnected** or **Not Licensed**.
    - If you choose **Web Bridge Connected** you can choose the check box value of selected, **True**, or clear, **False**.
12. In the **Action** section, select **Activate Event**.
13. In the **Event** field, click the ellipsis and select the event that you configured which lowers the **Clearance Filter Level** of the reader.
14. Click **Save and Close**. The Application Server is now configured to trigger an event that lowers the clearance level of a reader in case the server has a connection problem.

Configuring fallback to one factor authentication when the C•CURE host and the access control panel fail to communicate

1. Click the **Configuration** pane and select **Event** from the drop-down list.
2. Click **New** to create a new event.
3. In the **Event** editor, click the **Action** tab.
4. Click **Add** to add a row for the action you want to configure.
5. In the **Action** drop-down list, select **Set Clearance Filter to Level <x>**, where x is a level below the preconfigured **Clearance Filter Level** the reader uses for two factor authentication.
6. In the **Reader** field, click the ellipsis and select the reader you want to apply this action to if there is a communication loss between C•CURE and the access control panel.
7. Complete any other configuration options in the **Event** editor you want to pair with this event in the situation it is triggered. Ensure that you select the **Enable** and **Armed** check boxes.
8. Click **Save and Close**. You have created an event that sets the chosen reader to a lower clearance level. To finalize this configuration, you must apply this event to the access control panel in the case there is communication failure.
9. Open the editor for your access control panel cluster and click the **Triggers** tab.
10. Click **Add** to add a row to the **Triggers** section.
11. In the **Property** section, select **Primary Communication Status**.
12. In the **Value** section, select **Offline**.
13. In the **Action** section, select **Activate Event**.
14. In the **Event** field, click the ellipsis and select the event that you configured which lowers the **Clearance Filter Level** of the reader.
15. Click **Save and Close**. The access control panel is now configured to trigger an event that lowers the clearance level of a reader in case the panel has an offline status.

Two Factor Authentication Behaviors

When a cardholder approaches a two factor authentication protected door and swipes their card, the outcomes in the Table 141 on Page 538 are possible.

Table 141: Two Factor Authentication Behaviors

Card swipe is valid or not valid	Clearance Filter Level of the cardholder	Two factor authentication request	Result
Not valid	n/a	n/a	Entry is rejected.
Valid	Equal to or higher than the reader.	n/a	Entry is allowed.
Valid	Less than the reader	Two factor authentication request initiated.	• The request is approved and the door is used. • The request is approved but the door is not used. • The request is denied. The door is never unlocked. • The user is not enrolled with Duo and two factor authentication. The door is never unlocked.

A

Setting Up Import/Export Data Formats

This appendix provides the structure of the different data formats used by the C•CURE 9000 Import and Export processes.

In this appendix

Data Objects

The major components that make up the C•CURE 9000 system, its hardware, configuration schemas, and data are represented logically to users of the system as *Objects*. Consequently, the Import/Export features for the C•CURE 9000 system also function on the object level.

In general, the *export* process can be described as taking a set of data objects stored in the system and serializing them into an external XML document. The *import* process can be described as taking an XML document, de-serializing it into a set of data objects defined in system, and storing these objects in the server's database.

The common functionality provided by Import and Export combines with definitions provided by each object type supported by the system.

Fields

For each object, the user can select a particular subset of fields to be imported/exported. Object IDs and fields marked as not importable are read-only and are not modified during import, although they can be exported.

The Import process tries to parse string values stored in the XML document to convert them into proper types specified by the properties of the imported object. If the conversion fails, the entire record is rejected.

The rules shown in Table 142 on Page 540 are used for serialization of field values during import and export.

Table 142: Rules for Serialization of Field Values

Field Type	XML Representation
Integer	String representation of the number
Boolean	True/False values
Enumeration	Internal (English) name of the enumerated constant (with no spaces between words)
Type	String with a full type name (namespace plus the name of the type), such as: SoftwareHouse.NextGen.Common.SecurityObjects.Personnel
Local Date/Time	String using the date/time format for the current culture (See Attribute 'culture-info' on Page 550.)
UTC Date/Time	String using the date/time format for the current culture with the appended GMT time zone information (See Attribute 'culture-info' on Page 550.)
Binary array	Encoded base-64 string
Images	Encoded base-64 string
GUID	A string in the format where 'd' represents a hexadecimal number ('-' between groups is required): ddddddddd-dddd-dddd-dddd-ddddddddddddd NOTE: Import shall also recognize the format (32 hexadecimal numbers with leading '0x' and without '-' between the groups) 0xddddddddddddddddddddddddddddddddd

Table 142: Rules for Serialization of Field Values (continued)

Field Type	XML Representation
Object Reference (ObjectKey)	Name or GUID of the referenced object • If the system has more than one partition defined, the name of the referenced object is combined with the object's partition name in double brackets. - $$Default$$ references the system Default partition, regardless of its name. - In an Enterprise environment, $$Global$$ references the Global partition, regardless of its name • GUID is placed within double {} brackets **Examples:** Contractor [[My Partition]] Employee [[$$Default$$]] {{c5327a42-7dbe-4f25-9af8-6fe9732409b0}}
XML Strings	Strings converted into well formatted values of XML tags (where special symbols like & and > are converted into XML entities such as & and >)

These are general rules. Some individual properties have their own custom rules. See Special Fields on Page 552.

Validation

The same validation rules apply to an imported object as apply to one added to C•CURE 9000 through the user interface.

Object Relations

C•CURE 9000 has many different object types, which may be related.

- Parent-child relations often exist between different object types.

  If an object of type B cannot exist in the system unless it is linked to an object of type A, that is considered a parent/child relation between objects. In this case, A is a parent of B or B is a child of A. When the system deletes an object, it also deletes all its child objects without additional requests.

  Example:

  The Personnel object can have a collection of Credential objects. Credential is considered a child object of a Personnel object.

- References are another type of relation between objects.

  If deleting object A does not lead to the deletion of object B and deleting object B is not allowed until all the objects which reference B are deleted (or the references are removed), that is considered a reference relation.

  In this case, it is also possible that A exists without referencing any object B, and B exists without any objects that reference it.

  Example:

  A Report object can have a reference to a Query object and a Personnel object always has a reference to a Personnel Type value.

- An object type is called a top-level object (if it has no parent object type or if its parent is optional

  Example:

  An Image object can be used as a child of a Personnel object or it can be used as an independent object without any parent. Consequently it is also a top-level object.

Exporting Objects

When the system exports an object, all the child objects related to it can also be exported as tags nested into the main tag of the exported object. Regardless of the preceding, if the exported object references any other objects, these references are placed into the output file as values containing the names of the referenced objects.

NOTE The referenced objects are not included in the output document, only their names. In a partitioned system, the name is also appended by the name of the Partition in double brackets.

It is possible to export any object the C•CURE 9000 can display in the Dynamic Views. However, if the exported object is not a C•CURE 9000 top-level object, it cannot be imported back.

Importing Objects

When the system tries to import a document, it is assumed that all the child objects of each object to be imported are listed as its nested tag elements. Child objects cannot be imported without being nested into their parent object. Only top-level objects can be used as the top-level tags in the XML document to be imported.

If the system is importing a document with an object that contains a reference to another object, the import tries to resolve the reference by name. It fails if the referenced object does not already exist in the system.

Export Integrity

The Export process allows operators to export any subset of fields for any user- selectable object type. This can be a quick way to make an XML version of a report on a particular object set. Such an export can also be used later for importing data into another application such as Excel and manipulating the data.

NOTE Not every set created by the Export process can be imported back into a C•CURE 9000 system. See the examples on the next two pages.

There are several rules to follow when configuring an export if its purpose is the creation of an XML document that can be successfully imported by another C•CURE 9000.

1. The top-level object type selected for export in the 'Export schema selector' list must be a top-level object type. Otherwise the import process will reject it during import.

   Example:

   It is possible to export a list of Credential objects, but the only way to make a proper export that can later be imported into a C•CURE 9000 system is to first select the Personnel object and then the Credential objects as its children. (A standalone Credential object is rejected during import because it cannot be linked with a proper parent Personnel object, and a Credential object cannot be created without such a relationship.)

2. The set of fields selected for export for a particular object type must be complete in terms of the object's validation. Some objects have fields that do not have default values, but these are required for a new object to be created.

   Example:

   An ISC Board object requires the IP address to be defined. If such a required field is not defined in the exported document (because the configuration excludes it from the exported field set) and the file is used for importing new objects into a different C•CURE 9000, all the objects new to the system will be rejected. (However, this might work for updating existing objects.)

3. The set of fields selected for export for a particular object type must be complete in terms of the object's matching. If the fields that help the C•CURE 9000 system uniquely identify an object are not included in the exported XML document, the system will not be able to update the objects during import. (However, this might work for creating new objects in the system).

4. The order in which object types are listed in the export is also important because of cross-references between objects.

Example:

A hardware object such as an ISC Controller can reference the hardware folder where it was created. Consequently this hardware object will be rejected when imported into a different C•CURE 9000 system where that referenced (by name) hardware folder does not exist.

To correct this problem, either such a folder will have to be created manually before importing the ISC controllers, or else the hardware folder will need to be exported before exporting the ISC controller.

The Export process does not have enough information to validate that a currently defined export object can be used for importing data into a different C•CURE 9000.

Software House therefore recommends that before making a full-scale export, you experiment with a small subset of data to verify that the export definition contains all the information required by the import.

Selecting a proper top-level object type and exporting all of its fields and its child objects is usually sufficient to create a proper export definition.

Internal and External Document Formats

The Export process creates files in the format recognized by the Import module without any modifications (internal document format). The files are well-formatted XML documents of a particular structure.

However, the Import process can understand a wider spectrum of document formats (external document format) through the conversion available during importing.

The easiest way to create a document with an external format is to export an object in the internal document format and rename the tags of the fields

Example:

Personnel object – rename as follows:

FirstName tag into First_Name
LastName into Last_Name

If the external document format is still a well-formatted XML document, it can be converted back into a proper internal document format by using one or more Import Converters during the import. For more information, see Data Conversion on Page 43 and Data Import Data Conversion Tab on Page 89.

The Import process also supports CSV file format as a special kind of external document format. Importing CSV files requires configuring an Import object using a special CSV File Source. It also requires configuring a proper Field Conversion to define the type of objects contained in the CSV file, and optionally to rename the columns in the CSV file as field names recognized by C•CURE 9000 for that object type.

The Import/Export Process

Import Matching Rules and Validations

The import process evaluates each record in the import file individually:

- No matching is performed for the add-only-mode imports. (Records can still be rejected, but only if the database rules—such as the uniqueness of the object's name—are violated by the newly created object.)
- For update-existing-records-mode imports,
  - All fields designated as match fields for a top-level object must match only one record in the database for the import process to consider a record a match. If more than one record is found, the record is rejected and an error message logged.
  - All fields designated as match fields for a child object must match only one record in the parent's container (collection of child objects of the specified type).
- Every field is validated for valid type, length, etc., and rejects reported. Optionally, rejected records are sent to the same location as the imported file, so they can be modified and re-imported after the errors are resolved.
- During the import of system objects that reference other objects in the system, C•CURE 9000 validates the existence of the referenced objects. If they do not exist, the record update is rejected, and a report that identifies the missing references issued.

NOTE Validating the existence of referenced objects during import either follows the matching rules (for contained objects), or the system's normal reference checking and validation (for object IDs).

- Validating field data type and length is performed during formatting when the imported data is converted to the C•CURE 9000 predefined structures, as well as during the process of saving the data.
- Read-only fields and fields marked as not importable, if there are any in the import file, are always ignored.

Import Transactions

Every import operation has each record as a transaction boundary that determines whether the record is written to the system, or is not when—the operation fails.

Example:

If a Credential record being imported as part of a Personnel record is rejected for any reason, the entire Personnel record is rejected.

Logging

Each import or export operation generates a special historical log that operators can view called Data Import result or Data Export result. This log contains a summary of the completed import or export, including information such as the following:

- Date/time the operation was initiated
- Import or export type
- Number of records exported, added, deleted, or updated

C•CURE 9000 also generates an error log for import operations to aid in troubleshooting failed imports. This file is stored locally on the server, and can be accessed on the client from the Data Import Results Dynamic View by clicking Popup View from the right-click context menu For each error during the import process, the log contains the following:

- Description of the error

- Record that caused the error

Rejected records can also be sent to the client that initiated the import. This allows the client to form a special file with the rejected records that can later be reviewed, corrected, and re-imported.

NOTE Records stored in the error log file may have a format or structure different from the original file if the import process applied any data conversion to the original data.

Import/Export File Format (IEFF)

The combination of the items described in the preceding sections of this appendix (rules, selected objects and their fields, input and output files, etc.) make up a definition for importing to or exporting from C•CURE 9000.

Example:

A definition for exporting personnel data could consist of the following:

- A set of export rules defined by a query for all personnel whose first name starts with 'S'
- An output file location

This definition can then be saved in the system and used later.

Because the export definition is very flexible, the format of the result file varies. There are, however, characteristics common to any file generated by the system.

Common IEFF Structure

An IEFF is an XML document with the root tag 'CrossFire' where each top- level tag represents a single C•CURE 9000 object—with perhaps nested child objects. The name of the top-level tag is the full name of the object's type followed by the attribute **ImportMode** that defines the operation to be executed on the object when it is imported back to the system.

The tags nested into the top-level tag represent the properties of that top-level object. If the nested tag has the attribute **ImportMode**, the tag represents a nested child object of the top-level object. In this case, the name of the tag must be the full name of the child object's type.

The structure of the child object tags is the same as the structure of the top-level tag: each child object can have its own child objects. See the example of the object in the following sample:

Example:

The following sample contains two top-level objects:

- One named 'CompanyName' has the type HardwareFolder
- Another named '370 Basset Road 'has the type ISCController.

  The object ISCController has a nested child object of the type ISCBoard, while the board has a child object of the type Input.

```
<CrossFire culture-info="en-US">
    <SoftwareHouse.NextGen.Common.SecurityObjects.HardwareFolder ImportMode="Default">
        <Name>CompanyName</Name>
         <Description>Company Name</Description>
         <GUID>7a6bb3ea-87e5-4d24-85e9-736fbd412026</GUID>
         <PartitionKey>Default</PartitionKey>
    </SoftwareHouse.NextGen.Common.SecurityObjects.HardwareFolder>
    <SoftwareHouse.NextGen.Common.SecurityObjects.ISCController  ImportMode="Default">

         <Name>370 Basset Road</Name>
         <ACFailTroubleStatus>Unknown</ACFailTroubleStatus>
         <AutomaticDownloadFlag>False</AutomaticDownloadFlag>
         <BatteryChargerTroubleStatus>Unknown</BatteryChargerTroubleStatus>
         <BatteryTroubleStatus>Unknown</BatteryTroubleStatus>
         <BufferLimit>80</BufferLimit>
         <CardTroublesCountStatus>0</CardTroublesCountStatus>
         <VersionMismatchTroubleStatus>0</VersionMismatchTroubleStatus>
        <SoftwareHouse.NextGen.Common.SecurityObjects.ISCBoard ImportMode="Default">
            <Name>RM1-NHV Annex Office</Name>
```

```
        <BoardType>ISC2Reader</BoardType>
        <ControllerID>5000</ControllerID>
        <GUID>db5f1abb-a8af-485d-aef8-edbdd2bc0721</GUID>

      <SoftwareHouse.NextGen.Common.SecurityObjects.Input ImportMode="Default">
          <Name>NHV-Annex Cafe Ent - DOOR SWITCH</Name>
           <ActivateOnSupervision>True</ActivateOnSupervision>
           <ActiveStatus>Inactive</ActiveStatus>
           <Annunciate>True</Annunciate>
           <GUID>17fb6415-e24e-4633-9eac-2e404d62bfa1</GUID>
           <InputType>DoorSwitch</InputType>
           <IsAlarmed>False</IsAlarmed>
           <iSTARInputHWStatus>Unknown</iSTARInputHWStatus>
           <LastModifiedByID>5001</LastModifiedByID>
           <LastModifiedTime>7/16/2007 2:55:09 PM GMT-04:00</LastModifiedTime>
           <MonitorState>Unknown</MonitorState>
           <NormalMode>Open</NormalMode>
      </SoftwareHouse.NextGen.Common.SecurityObjects.Input>
    </SoftwareHouse.NextGen.Common.SecurityObjects.ISCBoard>
</SoftwareHouse.NextGen.Common.SecurityObjects.ISCController>
```

Attribute 'ImportMode'

The attribute **Import Mode** serves two purposes:

- It indicates that the tag represents an object. (If a tag does not have this attribute, it represents an object's property.)
- It defines the operation that the import process should perform when importing the object.

NOTE This attribute overrides the Default Import Mode configured on the **Data Import Editor General** tab.

The following values are allowed for this attribute—these values are case sensitive:

- Default – the action on the object is defined by the Default Import Mode parameter specified in the Import object that is importing the file.
- Unknown – same as **Default**.
- Add – indicates that the object must be added to the system. (If the object already exists in the system, the record is rejected.)
- Update – indicates that the object must be updated in the system. (If the object does not exist in the system, or two objects match the specified matching rule, or a matching rule does not exist for the object, the record is rejected.)
- Set – if the object does not exist in the system, the attribute acts the same as **Add** and the object is appended to the database; otherwise, the object is updated, but the operation fails if a matching rule is not defined.
- Delete – tries to find a single object that matches the matching rules and delete that object and all its child objects. If the object does not exist, the record is ignored; if more than one object matches the rules or a matching rule is not defined, the record is rejected.
- DeleteAll – deletes all the child objects of the specified type. If used for a top-level object, acts the same as **Delete**—a single object is deleted if matched by the rules, or the record is rejected.

NOTE

The **ImportMode** attribute is valid for both top-level objects and their child objects. They act independently, although not each combination of the attribute values makes sense.

Example:

If the top-level object has the **ImportMode** set to **Add**, it does not make sense to use **Update** or **Delete ImportMode** in the child records (even though this combination is not restricted) unless Import Template rules are configured.

The action provided by **ImportMode** also depends on the matching rules defined.

Example:

This example requires updating a personnel record by removing one of its clearances. The Personnel record is matched by **GUID**, and the Clearance record is matched by **Clearance name**.

```
<CrossFire culture-info="en-US">
     <SoftwareHouse.NextGen.Common.SecurityObjects.Personnel ImportMode="Update">
        <GUID>fa34ac4f-97cf-4f41-b8c2-80f6817fe734</GUID>
        <SoftwareHouse.NextGen.Common.SecurityObjects.PersonnelClearancePair ImportMode="Delete">
             <ClearanceKey>iSTAReX51013c Clearance</ClearanceKey>
         </SoftwareHouse.NextGen.Common.SecurityObjects.PersonnelClearancePair>
    </SoftwareHouse.NextGen.Common.SecurityObjects.Personnel>
</CrossFire>
```

Example:

The example following on the top of the next page requires updating a personnel record by removing all of its existing clearances and appending two new clearances, **Clearance 01** and **Clearance 02**. It is assumed that the personnel record is matched by the field, **GUID**.

```
<CrossFire culture-info="en-US">
    <SoftwareHouse.NextGen.Common.SecurityObjects.Personnel ImportMode="Update">
        <GUID>fa34ac4f-97cf-4f41-b8c2-80f6817fe734</GUID>
        <SoftwareHouse.NextGen.Common.SecurityObjects.PersonnelClearancePair ImportMode="DeleteAll" />
        <SoftwareHouse.NextGen.Common.SecurityObjects.PersonnelClearancePair ImportMode="Add" />
             <ClearanceKey>Clearance 01</ClearanceKey>
        </SoftwareHouse.NextGen.Common.SecurityObjects.PersonnelClearancePair>
         <SoftwareHouse.NextGen.Common.SecurityObjects.PersonnelClearancePair ImportMode="Add" />
            <ClearanceKey>Clearance 02</ClearanceKey>
        </SoftwareHouse.NextGen.Common.SecurityObjects.PersonnelClearancePair>
    </SoftwareHouse.NextGen.Common.SecurityObjects.Personnel>
</CrossFire>
```

NOTE

Where child records with the **DeleteAll** and **Delete** attributes are located within the parent record is significant since child records are applied one by one.

Consequently, if the record with the **DeleteAll**, **ImportMode** is located at the end of the parent record, all the child records appended during import are also deleted, as shown in the following example.

Software House recommends putting the records with the **DeleteAll** attribute before all the other child records.

Example:

This example deletes all the existing clearances from the specified personnel record. It does not add any new clearances because they are located before the record with the **DeleteAll** attribute, as described in the preceding note.

```
<CrossFire culture-info="en-US">
    <SoftwareHouse.NextGen.Common.SecurityObjects.Personnel ImportMode="Update">
        <GUID>fa34ac4f-97cf-4f41-b8c2-80f6817fe734</GUID>
        <SoftwareHouse.NextGen.Common.SecurityObjects.PersonnelClearancePair ImportMode="Add" />
             <ClearanceKey>Clearance 01</ClearanceKey>
```

```
        </SoftwareHouse.NextGen.Common.SecurityObjects.PersonnelClearancePair>
        <SoftwareHouse.NextGen.Common.SecurityObjects.PersonnelClearancePair ImportMode="Add" />
            <ClearanceKey>Clearance 02</ClearanceKey>
        </SoftwareHouse.NextGen.Common.SecurityObjects.PersonnelClearancePair>
        <SoftwareHouse.NextGen.Common.SecurityObjects.PersonnelClearancePair ImportMode="DeleteAll" />
    </SoftwareHouse.NextGen.Common.SecurityObjects.Personnel>
</CrossFire>
```

Attribute 'MatchingFields'

The attribute **MatchingFields** allows the XML document to overwrite the matching rule defined in the import object. It is a comma-delimited string. Each element of the string represents the name of the property that must be used to match this particular object during an Update or Delete operation. If the attribute is used with the Add operation, it is ignored.

The matching fields specified by the attribute are **not** applied to nested child objects defined in the document. Each imported object (child or parent) must define its own set of matching fields; otherwise the default matching rule specified in the import object is applied.

Example:

This example requires updating a personnel record by removing one of its clearances. The personnel record is matched by **LastName** and **FirstName**, and the clearance record is matched by **Clearance name**. Matching rules, as specified in the import object for these types, are ignored. The example also requests an update of the person's portrait using the matching rule specified in the import object.

```
<CrossFire culture-info="en-US">
    <SoftwareHouse.NextGen.Common.SecurityObjects.Personnel
                ImportMode="Update"MatchingFields="LastName,FirstName">
        <GUID>fa34ac4f-97cf-4f41-b8c2-80f6817fe734</GUID>
    <SoftwareHouse.NextGen.Common.SecurityObjects.PersonnelClearancePair
              ImportMode="Unknown" MatchingFields="ClearanceKey">
            <ClearanceKey>iSTAReX51013c Clearance</ClearanceKey>
        </SoftwareHouse.NextGen.Common.SecurityObjects.PersonnelClearancePair>
        <SoftwareHouse.NextGen.Common.SecurityObjects.Images ImportMode="Default">
         <ImageFilePath>ExternalFile.jpg</ClearanceKey>
         <ImageType>Portrait</ImageType>
            <Name>Portrait</Name>
        </SoftwareHouse.NextGen.Common.SecurityObjects.Images>
    </SoftwareHouse.NextGen.Common.SecurityObjects.Personnel>
</CrossFire>
```

Attribute 'culture-info'

The **culture-info** attribute defines the locale to be used to interpret certain values placed into the XML document. The value of the attribute is any valid .Net culture name, such as **en**, **en-UK**, or **en-US**.

- The **Export** process automatically enters the culture info value that matches the locale of the system exporting the data.
- The **Import** process reads the information from the **culture-info** attribute, and uses it to determine the culture of the document it is importing. This culture is used when converting the values of the properties from XML strings into .Net values. If the **culture-info** attribute is omitted, the current culture of the system is used.

Currently, the only properties sensitive to the value of the **culture-info** attribute are Date/Time properties and properties containing Decimal Numbers. The culture defines the format used to convert a Date/Time or Decimal Number value to a string and back.

Example:

- The **en-US** culture uses the month/day/year format (12/23/10), while the **en-UK** culture uses the day/month/year format (23/12/10).
- The e**n-US** culture uses the dot (.) for Decimal Numbers (1.01), while the **fr** culture uses the comma (,) for Decimal Numbers (1,01).

The **culture-info** attribute allows the export of data from a C•CURE 9000 system with European settings and the import of that data to a system with U.S. settings without confusion of the Date/Time or Decimal Number values.

Attributes 'platform-version' and 'product-version'

The 'platform-version' attribute indicates the version of the Crossfire platform code used to generate the exported XML document, while the 'product-version' attribute indicates the version of the C•CURE 9000 code used to generate the exported XML document.

These attributes are reserved for providing backward compatibility with future version of the Crossfire platform and C•CURE 9000 system.

Handling UTC Date/Time Values

C•CURE 9000 has two types of Date/Time values, defined by each object's property:

- Absolute (UTC) values
- Relative values

Exporting

The Export object always puts date/time values into the output file using the current system's culture.

- Relative values are placed into the file without conversions.
- If the date/time value is absolute, it is converted to the time zone of the system currently performing the export and the value appended with the information about the time zone.

Example:

```
<LastModifiedTime>9/13/2007 3:27:09 PM GMT-04:00</LastModifiedTime>
```

Importing

When the Import object reads a date/time value and detects that the value has an appended time zone parameter, it converts the date/time value from the specified time zone to the time zone of the system currently performing the import.

- If this conversion is done to a property stored as a UTC value, the system makes the proper conversion when the object is saved.
- If the time zone information is appended to a value of a property stored as a relative date/time value, only the conversion to the local time zone of the system performing the import occurs.

If the time zone information is **not** appended, the value is assumed to be in the time zone of the system performing the import.

Special Fields

The following types of C•CURE 9000 Objects have special fields:

- Personnel (Credential) Objects – see Special Fields of the Personnel (Credential) Objects on Page 552
- Image Objects – see Special Fields of the Image Objects on Page 555
- Document Objects – see Special Fields of the Document Objects on Page 556

Special Fields of the Personnel (Credential) Objects

Personnel objects have the following special non-exportable, write-only fields:

Field Internal Name	Field Label
ClearancesAll	Clearances (Replace All)
ClearancesChanged	Clearances (Replace All)
CardNumberForMatching	Card Number (for matching only)
PrimaryPortraitImageData	Primary Portrait
PrimaryPortraitImageFile	Primary Portrait File Path

Personnel and Credential objects also have the following read/write field with a special behavior:

Field Internal Name	Field Label
ImportedDecodedPIN	Imported Decoded PIN
GroupsChanged	Groups Changed
GroupsAlll	Groups All

ClearancesAll and ClearancesChanged

These fields allow modifying a collection of clearances assigned to a personnel record without making nested PersonnelClearancePair records within the top-level Personnel record. This technique is mostly useful for importing data from CSV and LDAP data sources that, by default, do not support nesting.

NOTE

If both the 'ClearancesAll' and 'ClearancesChanged' properties are used within a single record that is being imported, they are applied one by one. This makes it difficult to predict the result of the import. Consequently, Software House recommends that you **not** use both properties in the same record.

In addition, 'ClearancesAll' and 'ClearancesChanged' do **not** operate properly if clearances have names that start with a minus sign '-' or a pipe sign '|'. So Software House also recommends that you **not** use either symbol in the clearance names.

'ClearancesChanged' – this field accepts a string with pipe-delimited names of clearances.

Example:

```
'+Clearance 01|-Clearance 02|Clearance 09'
```

Each value element in the string represents a name of a clearance. Clearances listed in the string are appended to the personnel records.

- If a clearance name has the prefix '-', it is removed from the record (if it existed in the list before the import).
- A special value '-*' means that all the clearances must be removed.
- The code also accepts the prefix '+', indicating that the clearances must be appended (it can be omitted).

The preceding example instructs the import to remove a clearance with the name 'Clearance 02' and add two clearances, named 'Clearance 01' and 'Clearance 09'

ClearancesAll – this field has the same format as the **ClearancesChanged** property. The only difference is that it assumes that all the existing clearances of the personnel record (if any) must be removed before assigning the new values.

In the following example, the value in line #1 assigned to the property **ClearancesAll** works the same way as the value in line #2 assigned to the property **ClearancesChanged**: all clearances are removed from the personnel records, and three clearances "Clearance 01", "Clearance 02", and "Clearance 03" are assigned.

Example:

```
 "Clearance 01|Clearance 02|Clearance 03" #1 "-*|Clearance 01|Clearance 02|Clearance
03" #2
```

Card Number (for matching only)

This field allows you to specify a card number to find a particular Personnel record in the C•CURE 9000 database. This field is only used for matching and is not used to create a new card number for a record.

Primary Portrait and Primary Portrait File Path

These fields allow an import to either update the existing primary portrait for a Personnel record or to add a new primary portrait to a Personnel record.

The external personnel record can have a field with the full path to a JPG, BMP, GIF, or PNG file that can be used as a primary portrait for the personnel record being imported.

The PrimaryPortraitImageFile field accepts a string value with the full path to an image file, while the PrimaryPortraitImageData field accepts a byte array containing an image that is encoded using base64 encoding.

ImportedDecodedPIN

This field can be in both the Personnel and the Credential objects.

'ImportedDecodedPIN' is a read/write field with a special behavior. While the field can always be included in export and/or import definitions, both its value and validation rules depend on the current settings of two of the Personnel System Variables (accessed from the Options & Tools pane). For information, see the *C•CURE 9000 System Maintenance Guide*.

Table 143: Impact of System Variable Value on 'ImportedDecodedPIN' Property

System Variable Value	Impact on Field
Display PIN = true	If exported/imported, the field contains the decoded value of the PIN (for both Personnel and Credential records). • For export – If the Personnel record does not have an assigned PIN, the value is 0. • For import – once imported: - Value is encoded before being stored in the database. - If field contains the value "-1", the entire record is rejected.

Table 143: Impact of System Variable Value on 'ImportedDecodedPIN' Property (continued)

System Variable Value	Impact on Field
Display PIN = false	• If exported, the field contains the value "-1". • If imported, the value in the field is ignored, which means: - Newly added personnel/credential records will have no PIN assigned. - Updated personnel records will retain the old value assigned PIN.
Use General PIN for PIN Only Access = true	The value of this field for Personnel records is ignored if the import record has a Credentials record with the Pin Only Access flag set. In this case, the value of the PIN field of the Credentials record is copied into the PIN field of the Personnel record before the record is saved.
Use General PIN for PIN Only Access = false	Values for this field in the Credentials records are imported independently from the values in the parent Personnel record.

Credentials records have the following additional restrictions when the 'ImportedDecodedPIN' is used:

- Only one Credentials record in the Personnel record can have an assigned PIN.
- The Credentials record with the non-zero value in the property must have a special CHUID 'PIN only' format assigned.
- The value of a PIN assigned to a Credentials record must be unique in the system.

GroupsAll and GroupsChanged

These fields allow an import to add or remove specified Personnel to a group of Personnel from a Personnel record. GroupsAll removes a record from all groups before adding the record to a set of new groups. GroupsChanged adds a Personnel record to a group without removing it from groups that it is currently a member of.

NOTE You do not need to know what groups a Personnel record is assigned to before using GroupsAll or GroupsChanged.

Table 144 shows examples the GroupsChanged and GroupsAll fields, where pg1, pg2, and pg3 are variable group names.

Table 144: Examples of GroupsChanged and GroupsAll fields

Keyword	Impact
`<GroupsChanged>+pg1</GroupsChanged>`	Adds a personnel record to the personnel group called pg1.
`<GroupsChanged>+pg1|+pg2</GroupsChanged>`	Adds the personnel record to groups pg1 and pg2.
`GroupsChanged>-pg1</GroupsChanged>`	Removes the personnel record from group pg1.
`<GroupsChanged>+pg1|+pg2|-pg3</GroupsChanged>`	Adds the personnel record to groups pg1 and pg2 and removes the record from group pg3.

Table 144: Examples of GroupsChanged and GroupsAll fields (continued)

Keyword	Impact
<GroupsChanged>-*|+pg1</GroupsChanged>	Removes the personnel record from all groups and adds the record to group pg1.
<GroupsAll>+pg1</GroupsAll>	Removes the personnel record from all groups that it is currently a member of, and adds it to group pg1.
<GroupsAll>+pg1|pg2</GroupsAll>	Removes the personnel record from all groups that it is currently a member of, and adds it to group pg1 and pg2.

Special Fields of the Image Objects

The object 'Image' has a special non-exportable, write-only field, 'ImageFilePath'. The field expects a string that is interpreted as a path to an image file. If the tag 'ImageFilePath' exists in the tag Images, as shown in the following example, an external file is accessed when assigning the field to the 'Image' object. This file then replaces the current content with the new portrait image from the file.

Example:

```
<CrossFire culture-info="en-US">
    <SoftwareHouse.NextGen.Common.SecurityObjects.Personnel ImportMode="Update" MatchingFields="GUID">
        <GUID>fa34ac4f-97cf-4f41-b8c2-80f6817fe734</GUID>
        <SoftwareHouse.NextGen.Common.SecurityObjects.Images ImportMode="Default">
           <ImageFilePath>ExternalFile.jpg</ImageFilePath>
           <ImageType>Portrait</ImageType>
                <Name>Portrait</Name>
        </SoftwareHouse.NextGen.Common.SecurityObjects.Images>
     </SoftwareHouse.NextGen.Common.SecurityObjects.Personnel>
</CrossFire>
```

If both of the following tags are specified for the same Image object, the tag listed last wins—overriding the current value:

- <Image> – the one containing an embedded binary representation of an image
- <ImageFilePath> – a reference to an external file.

The Image type can be any one of the following:

- Portrait
- Signature
- Fingerprint

Special Fields of the Document Objects

The object ‘Document’ has a special non-exportable, write-only field, ‘ExternalFilePath’. This field allows you to import Documents from an external source to add to the C•CURE 9000 system for use with Personnel records or with Events (as part of the Assess Events feature).

The field expects a string that is interpreted as a path to a document file. If the tag ‘ExternalFilePath’ exists in the tag Document, as shown in the following example, an external file is accessed when assigning the field to the ‘Document’ object. This file then replaces the current content with the new document from the file.

Example:

```
<CrossFire culture-info="en-US">
    <SoftwareHouse.NextGen.Common.SecurityObjects.Personnel ImportMode="Update" MatchingFields=”GUID”>
        <GUID>fa34ac4f-97cf-4f41-b8c2-80f6817fe734</GUID>
        <SoftwareHouse.NextGen.Common.SecurityObjects.Documents ImportMode="Default">
           <DocumentFilePath>ExternalFile.doc</DocumentFilePath>
        </SoftwareHouse.NextGen.Common.SecurityObjects.Documents>
     </SoftwareHouse.NextGen.Common.SecurityObjects.Personnel>
</CrossFire>
```

If both of the following tags are specified for the same Document object, the tag listed last wins—overriding the current value:

- <DocumentData> – the one containing the document content.
- <ExternalFilePath> – a reference to an external file.

B

Personnel Data Types and Conversion

The table in this appendix lists the ODBC and C•CURE data types and possible conversion errors.

In this appendix

C•CURE Data Types

The key for the table is as follows:

- **OK** indicates a successful conversion
- **F** indicates format errors
- **T** indicates truncations
- **O** indicates overflow

NOTE Parentheses **( )** enclosing the letters, **F/T/O** indicate that only the format errors: truncations and overflow are *possible*.

Data Types

(ODBC Data Types)	Character	Integer	Logical	Date	Time	Date/time
SQL_CHAR	OK	(F,T,O)		(F,T)	(F,T)	(F,T)
SQL_VARCHAR	OK	(F,T,O)		(F,T)	(F,T)	(F,T)
SQL_LONGVARCHAR	OK	(F,T,O)		(F,T)	(F,T)	(F,T)
SQL_TINYINT	OK	OK				
SQL_SMALLINT	OK	OK				
SQL_INTEGER	OK	OK				
SQL_BIGINT	OK	(O)				
SQL_DECIMAL	OK	(T,O)				
SQL_NUMERIC	OK	(T,O)				
SQL_BIT	OK	OK	OK			
SQL_REAL	OK	(T,O)				
SQL_FLOAT	OK	(T,O)				
SQL_DOUBLE	OK	(T,O)				
SQL_DATE	OK			OK		OK
SQL_TIME	OK				OK	OK
SQL_TIMESTAMP	OK			T	T	T

NOTE The following ODBC data types are not supported:

- SQL_BINARY
- SQL_VARBINARY
- SQL_LONGVARBINARY

C

Custom Stylesheet (XSLT) Sample

The sample stylesheet in this appendix allows you to convert data exported from the C•CURE 800 for import into C•CURE 9000.

In this appendix

Custom Stylesheet Sample

The stylesheet in this appendix allows you to convert data you exported from C•CURE 800 and import it into C•CURE 900. You can copy the text in this stylesheet and then paste it into the Data Import Custom Stylesheet Editor using the right-click context menu. For more information, see Custom Stylesheet Editor on Page 114.

```
<?xml version ="1.0" encoding="utf8" ?>
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
<xsl:output method="xml" version="1.0" encoding="UTF-8" indent="yes" />

<!-- Parameters assigned at runtime. -->
<xsl:param name="paramCurrentTimestamp">20001231173010</xsl:param>
<xsl:param name="paramCurrentDT" >12/31/2000 5:30:10 PM</xsl:param>
<xsl:param name="paramCurrentCulture">en-US</xsl:param>

<!-- Specific 800 mapping. -->

   <!-- Convert all the "clear_id*" fields like "clear_id11" into "ClearanceAll" -->
   <xsl:template match="*[starts-with(name(), 'clear_id')]">
      <xsl:element name="ClearanceAll">
         <xsl:value-of select="."/>
   </xsl:element> </xsl:template>

   <!-- Rename "Partition_ID" into "PartitionKey" mapping "$Standard Partition" of 800 into
   "Default" partition on 9000 -->
   <xsl:template match="Partition_ID">
      <xsl:element name="PartitionKey">
         <xsl:choose>
            <xsl:when test="text()='$Standard Partition'">$$Default$$</xsl:when>
            <xsl:otherwise><xsl:value-of select="."/></xsl:otherwise>
         </xsl:choose>
      </xsl:element>
   </xsl:template>

   <!-- Split values of the "Person_type" 800 field into "PersonnelType" and "EscortOption" of 9000
   -->
   <xsl:template match="Person_type[text()='1']">
      <xsl:element name="PersonnelType">None</xsl:element>
   </xsl:template>

   <xsl:template match="Person_type[text()='4']">
      <xsl:element name="PersonnelType">Contractor</xsl:element>
```

```
    </xsl:template>

    <xsl:template match="Person_type[text()='5']">
        <xsl:element name="PersonnelType">Employee</xsl:element>
    </xsl:template>

    <xsl:template match="Person_type[text()='2']">
        <xsl:element name="EscortOption">Escort</xsl:element>
    </xsl:template>

    <xsl:template match="Person_type[text()='6']">
        <xsl:element name="EscortOption">EscortedVisitor</xsl:element>
    </xsl:template>

    <xsl:template match="Person_type[text()='3']">
        <xsl:element name="EscortOption">Visitor</xsl:element>
    </xsl:template>

<!-- The transformation below provides trivial default copy of everything. -->
<xsl:template match="*|@*">
    <xsl:copy>
        <xsl:apply-templates select="*|@*|text()"/>
    </xsl:copy>
</xsl:template>

<xsl:template match="@*">
    <xsl:copy /> </xsl:template>
<!-- End of customizable area. -->

</xsl:stylesheet>
```