American Dynamics

From Tyco Security Products

victor CEM Integration User Guide

version 5.4 and 5.4.1

8200-1147-1192 A0

Notice

The information in this manual was current when published. The manufacturer reserves the right to revise and improve its products. All specifications are therefore subject to change without notice.

Copyright

American Dynamics

60 Congress Avenue

Boca Raton, FL 33487 U.S.A.

Customer Service

Thank you for using American Dynamics products. We support our products through an extensive worldwide network of dealers. The dealer through whom you originally purchased this product is your point of contact if you need service or support. Our dealers are empowered to provide the very best in customer service and support. Dealers should contact American Dynamics at (800) 507-6268 or (561) 912-6259 or on the Web at www.americandynamics.net.

Trademarks

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 sales representative.

License Information

Your use of this product is governed by certain terms and conditions. Please see the detailed license information at the end of this manual.

Contents

Overview

The victor CEM AC2000 Integration driver provides a powerful, flexible and easy to use Graphical User Interface (GUI) for managing and monitoring your CEM AC2000 door access infrastructure through the victor unified client from American Dynamics.

Assumptions

This documentation covers the installation of victor CEM AC2000 Integration and an overview of the AC2000 integration features and benefits. It is assumed that the end users and installers of the CEM AC2000 Integration have relevant experience and a good working knowledge of victor unified platform, Windows operating system and experience configuring Physical Security Environments. Partners, Customers and Resellers configuring Tyco products should have relevant Tyco product training completed.

AC2000 CDC Requirements

This integration uses the AC2000 API to connect to the AC2000 system, through the AC2000 CDC Server. The connection is made to the CDC PostgreSQL ODBC database, so you must configure the network and port settings to allow the connection from the victor application server to the CDC PostgreSQL database.

victor Application Server

The victor Application Server stores all data, operator profiles, roles and event information and video recorder and camera objects.

Dual modes of user authentication allow users to log in using Active Directory credentials or via a ‘Basic’ method that does not require a domain controller. Operator profiles are portable, so that users can move from one victor client to another and their credentials follow them, regardless of the PC.

Restrict what devices and features an operator can access by assigning roles using victor's included policy management. Permissions can be set system wide for fire objects.

Any feature can be limited and updated as situations warrant. victor also journals and tracks what has happened on your systems, such as operator activities, fire alarm and point history, creating an audit trail.

victor unified client

victor unified client connects to the victor Application Server, allowing event management, observation and monitoring.

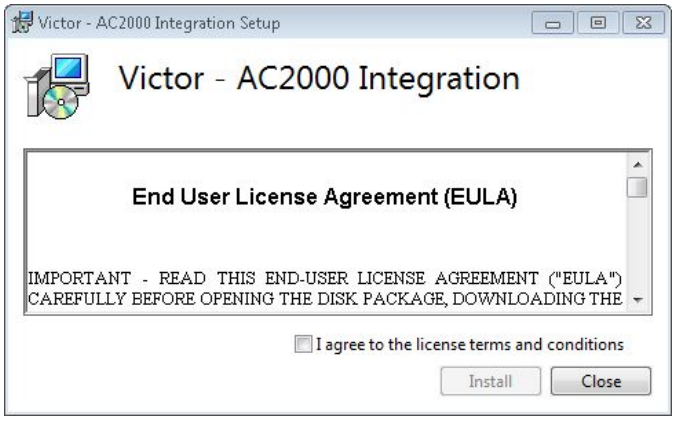
The AC2000 Integration Driver can be installed on the victor Application Server. You can download the integration driver from the American Dynamics website. The AC2000 Driver Service is a licensed option for victor unified client. If you do not have a license for this integration, contact American Dynamics.

Procedure 1 Installing the AC2000 Integration Driver

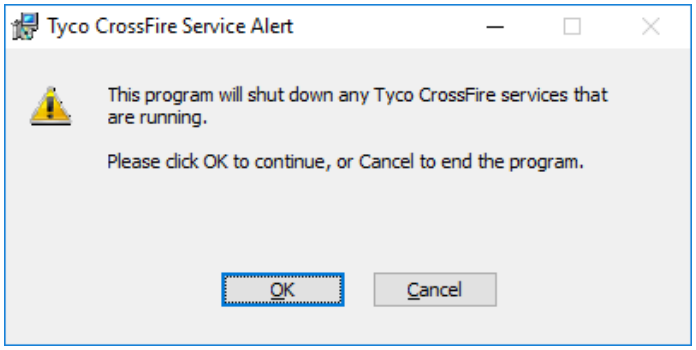
Note:
Before you start this procedure, stop the Crossfire Framework Service and Crossfire Server Component Framework Service, and close the Server Configuration application.

1 Double-click `AC2000_Integration-x.x.x.x_AD.exe` to start the installer.

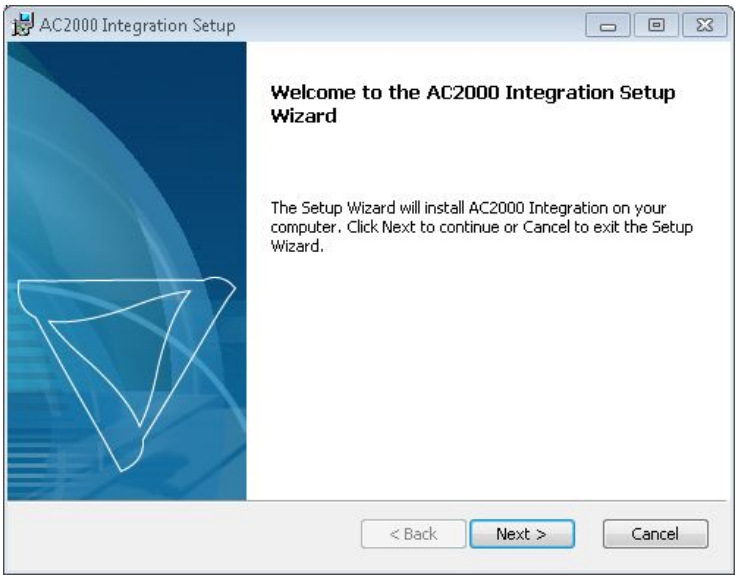
2 Select **Next**. The End User License Agreement (EULA) opens.



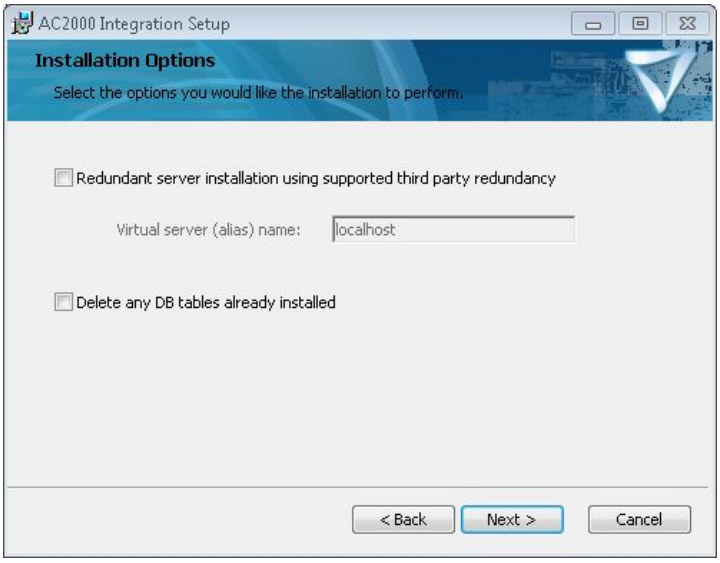
3 Read the EULA, select the **I agree to the license terms and conditions** checkbox, and then click **Next**.



4 In the **Tyco Crossfire Service Alert** dialog box, click **OK** to restart Crossfire services. The **AC2000 Integration Setup** window opens.



5 Click **Next**. The **Installation Options** dialog opens:

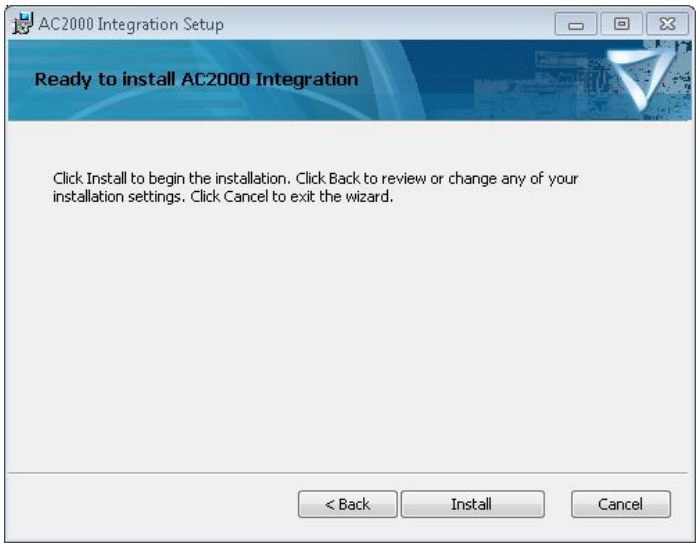


6 If the integration is being installed on a redundant server select the **Redundant Server** option and enter the virtual server name in the **Virtual Server (alias) name** field.

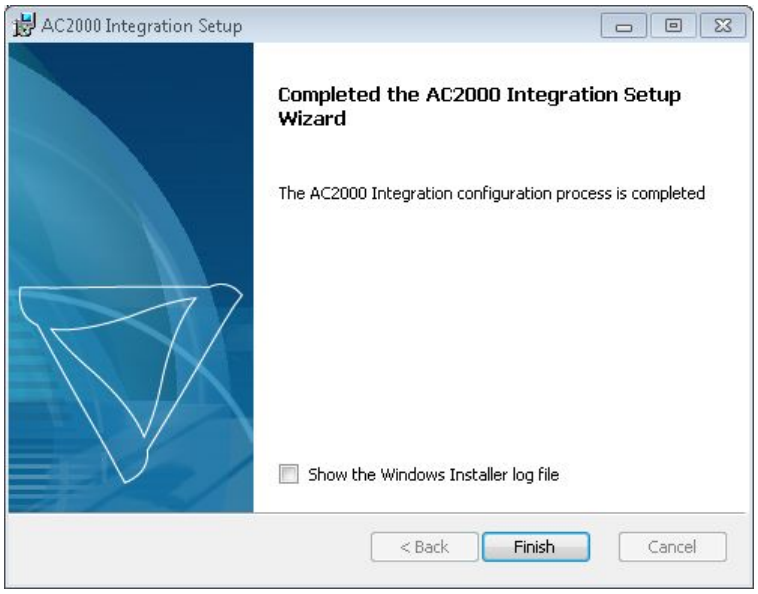
7 Select one of the following options, then click **Next**:

- (Optional) To install a new version of the AC2000 tables and overwrite a current installation, select the **Delete any DB Tables already installed** checkbox.
- If this is a new installation clear the **Delete any DB Tables already installed** checkbox.

8 Click **Install**.



9 After the installation completes, click **Finish**.



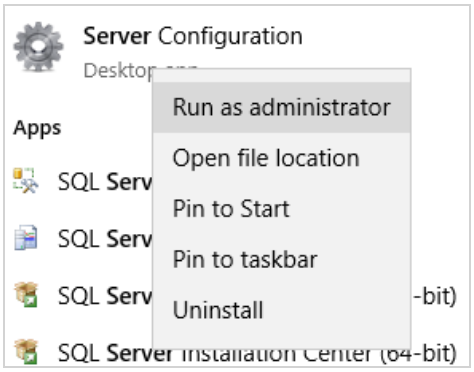
Initial Configuration

Following installation, victor requires some initial configuration before use.

Note:
Services may start automatically following installation depending on Windows configuration.

Procedure 2 Initial Configuration

1 On the desktop, right-click the Server Configuration Application desktop icon and select **Run as Administrator**.



2 Select **Start** next to Crossfire Framework Service and Crossfire Server Component Framework Service. Status changes from **Stopped** to **Start Pending** then **Running**.

3 Once both Crossfire services are displaying as status **Running**, select the **Enabled** checkbox and then select **Start** next to the AC2000 Driver Service. Status changes from **Stopped** to **Start Pending** then **Running**.

4 Select the **Enabled** checkbox and then select **Start** for each Extension Service that corresponds to hardware that is connected to your system. For example, enable the American Dynamics VideoEdge Driver Service for American Dynamics VideoEdge recorders.

5 Close the Server Configuration Application.

6 Enable the victor process (victor Integration) on the AC2000 Server.

7 Double-click victor unified client desktop icon to start victor.

AC2000 Integration Configuration

CEM AC2000 and all underlying hardware configured and connected to AC2000 can be can be added to victor. To add an AC2000 connection to victor, carry out the following steps:

Procedure 3 Creating ODBC DSN Connection to CDC Server PostgreSQL database

The AC2000 Integration driver automatically installs the `PostgreSQLUnicode ODBC 64bit` driver for windows. victor uses this driver to connect to the CEM AC2000 System.

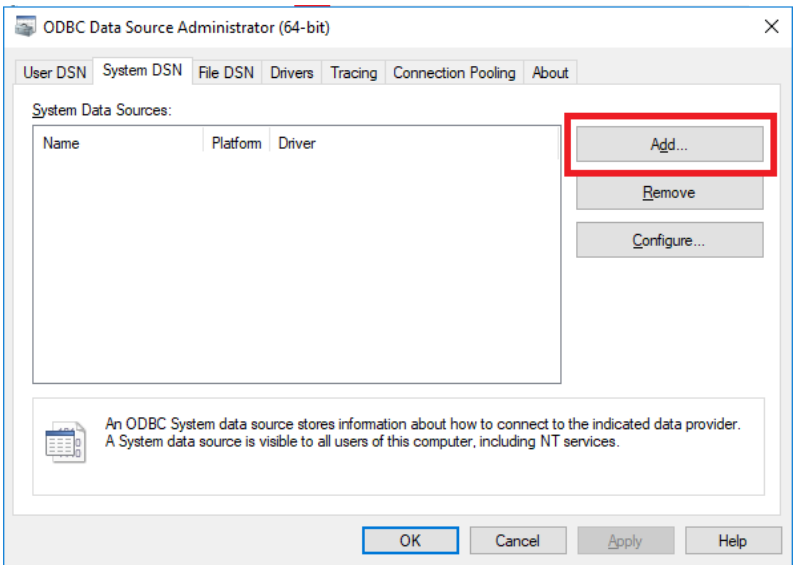
1 Open windows ODBC Data Source Administrator (64-bit).

a Open **Control Panel**, and then click **Administrative Tools**.

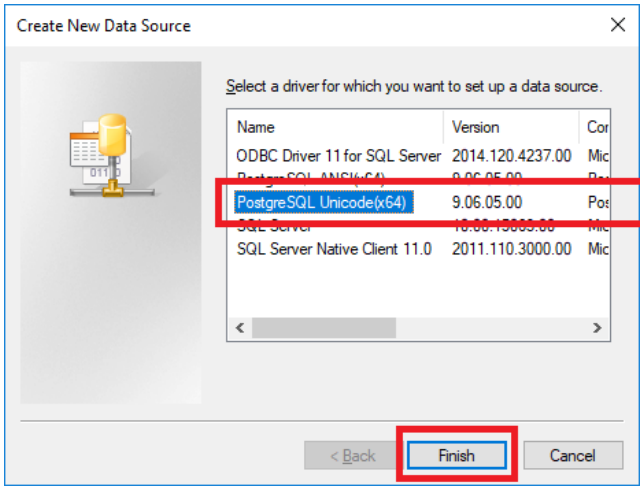
b In the Administrative Tools window, double-click **ODBC Data Sources (64-bit)**.

2 Select the **System DSN** tab.

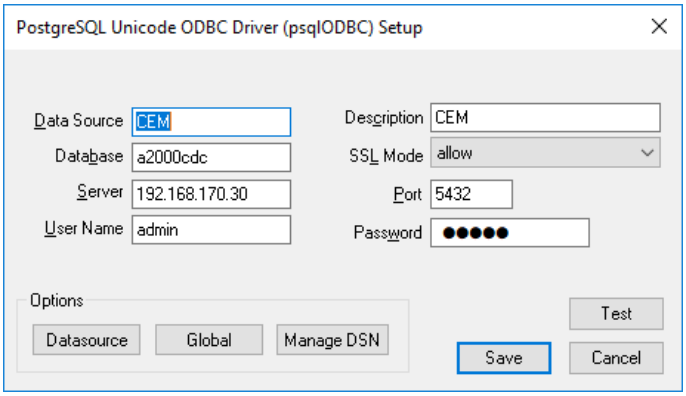
3 Click **Add**.



4 Select the **PostgreSQL Unicode(64)** option and click **Finish**.



5 Enter the connection information to the AC2000 CDC server PostgreSQL database



a In the **Data Source** field, enter the name of the DSN connection. This name must be the exact string used in the next section when entering ODBC DSN Name for the victor AC2000 CDC Server connection parameter.

b In the **Database** field, type `a2000cdc`.

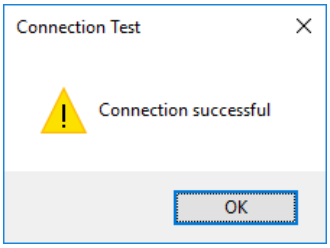
c In the **Server** field, enter the hostname or IP address.

d Set **SSL Mode** to **allow**.

e In the **Port** field, enter the PostgreSQL port number. By default this is 5432, unless changed on the CDC.

f In the **User Name** and **Password** fields, enter the database connection credentials.

6 Click **Test** to test all the connection. If the connection is successful the following message appears:

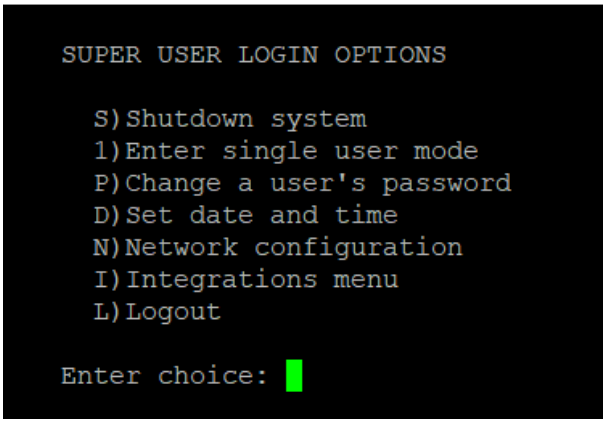


Procedure 4 Enabling the CDC External Interfaces

Note: You must apply the relevant integration licenses before completing the following procedure to successfully activate the integrations.

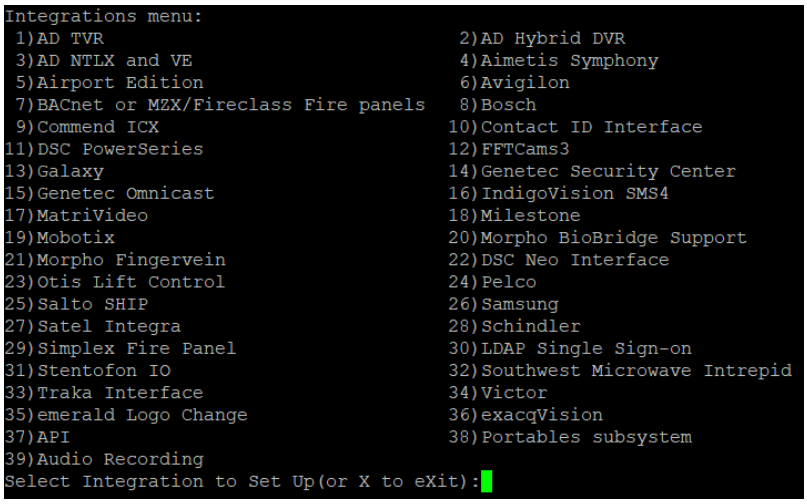
1 On the CDC Server, log in to the command prompt as root user.

The SUPER USER LOGIN OPTIONS page displays.



2 Type I, and then press Enter, to select the Integrations menu.

The Integrations menu displays.



3 Select an integration:

- Type 34, and then press Enter, to enable victor.
- Type 37, and then press Enter, to enable API.

Procedure 5 Adding CEM AC2000 CDC Server within victor

1 Select the **Create new item** icon.

2 Select **AC2000 CDC Server**.

3 Enter a **Name**.

4 (Optional) Enter a **Description**.

5 Select the **Enabled** checkbox.

6 Enter an **ODBC DSN Name** for the server.

Note:
This is the DSN **Data Source** field configured as described in the previous section: See Creating ODBC DSN Connection to CDC Server PostgreSQL database for more information.

7 Set the **Card Swipes Log Display Limit** field to set how many card swipes to store in the database for the Card Swipe transaction display defaults to 100.

8 Set the **Event Poll Interval** field to adjust the rate at which the driver polls the CDC server for updates. Note. Minimum value is 1000ms, the lower the value the quicker updates will be received from CDC but increases the network communication as opposed to higher value which will reduce the network communication. The default value is 2000ms.

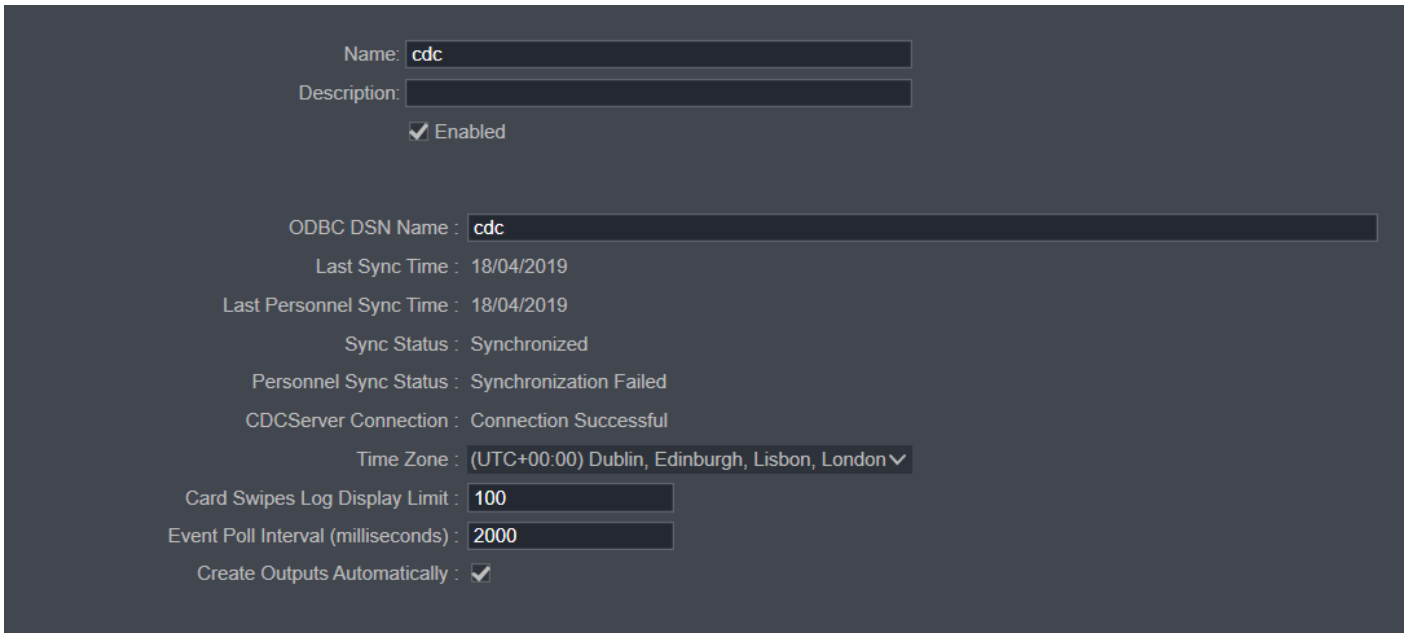
9 To automatically create 2 outputs per reader during device synchronization enable the **Create Output Automatically** option. This can be disabled and Output devices can then be added manually in victor at a later time.

10 To synchronize victor action configuration from the CDC server, enable the **Sync Victor Actions** field. This retrieves settings from CDC External Systems > Victor alarm settings.

Note:
When the device synchronization command is executed and this setting is enabled the AC2000 **Event Configuration** and AC2000 device **Alarms Enabled** option will be set. All alarm types

included in that list will have the alarm type enabled in the victor Event Configuration window and disable all others. All devices that are included in that list will have the Alarms Enabled setting enabled and all other AC2000 devices disabled.

11 The **Site ID** field allows multiple AC2000 servers to be grouped together in the device list under the Site ID parent groups.

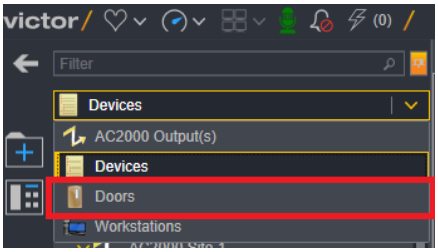


12 Save and close.

13 Select **AC2000 CDC Servers** then **Show All**.

14 Right-click the CDC Server device and select **Synchronize Devices**, and then select **Synchronize Personnel**.

AC2000 devices are displayed in the Devices list in victor unified client. AC2000 reader objects appear in the Door dropdown filter view.



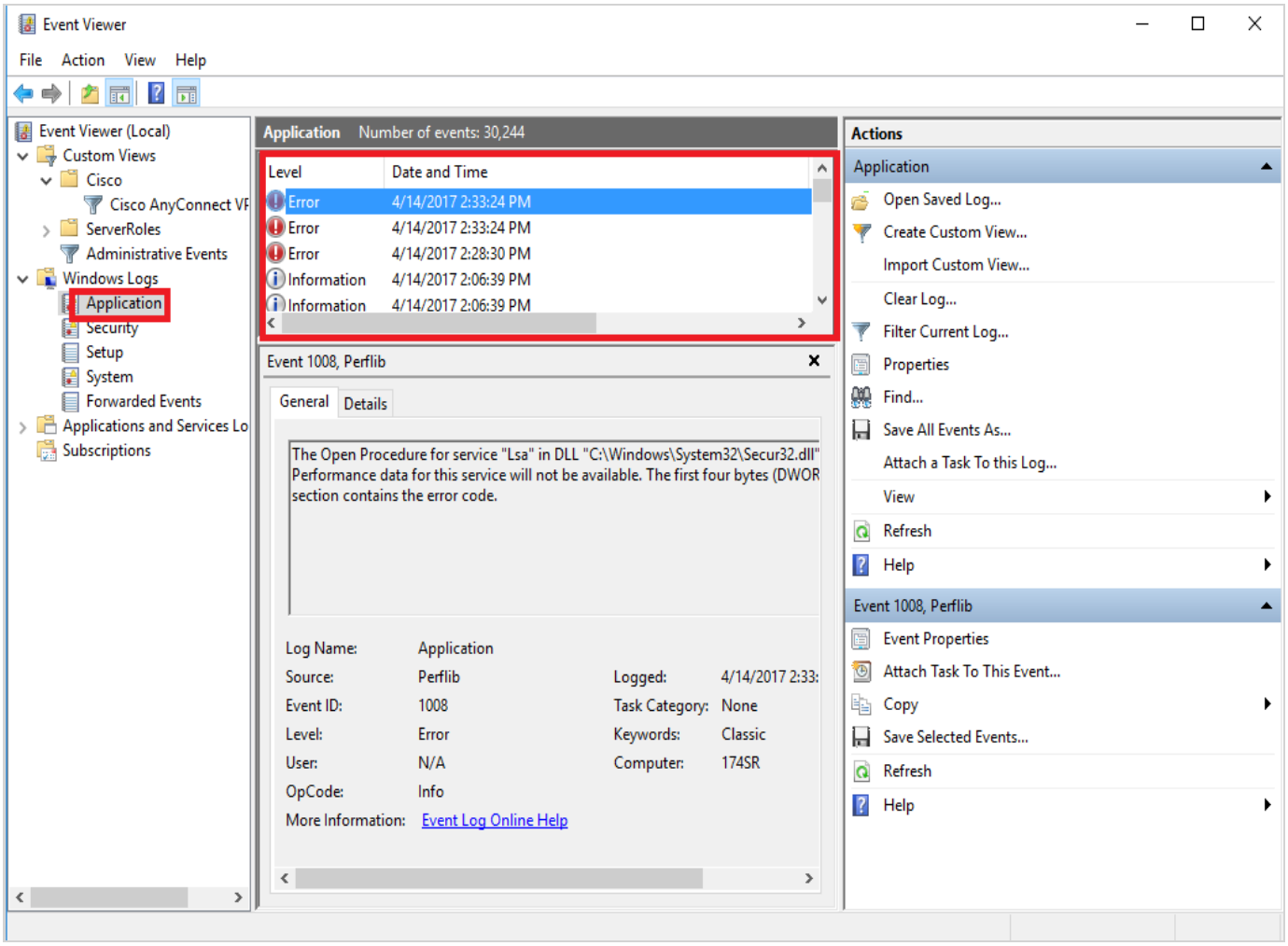
Procedure 6 Testing AC2000 Connectivity

If the device list does not load you can open the Microsoft Event Viewer to check for errors

1 Start the Microsoft Event Viewer.

2 Expand the **Windows Logs** group and then select **Application**.

Note:
See **System Values** section to configure diagnostic logs to appear in the Event Viewer for more information.



3 Check if the AC2000 events appear in the Journal in victor unified client.

a Click the **New Tab** icon.

b Select **Activity Viewer**.

AC2000 Device Configuration

You can configure the following parameter for RTC, input, output, and zone objects:

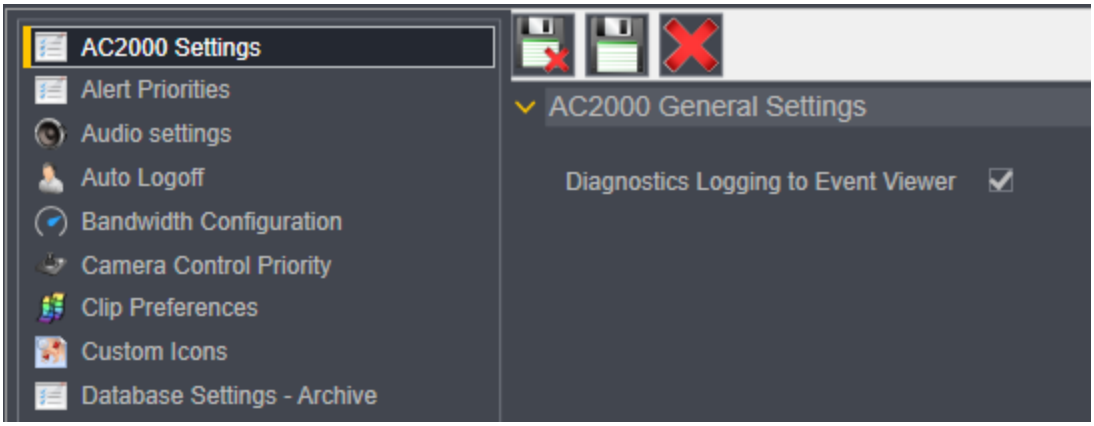
- **Alarms Enabled** – This switch controls all Door alarms to be disabled if required so no alarms received in the AC2000 driver are processed within victor or sent to the victor Journal.

You can configure the following AC2000 settings in victor unified client.

Database Settings- AC2000

AC2000 Settings are Global Integration-wide settings for AC2000 Objects, Select Setup and System Values to display the following configuration options:

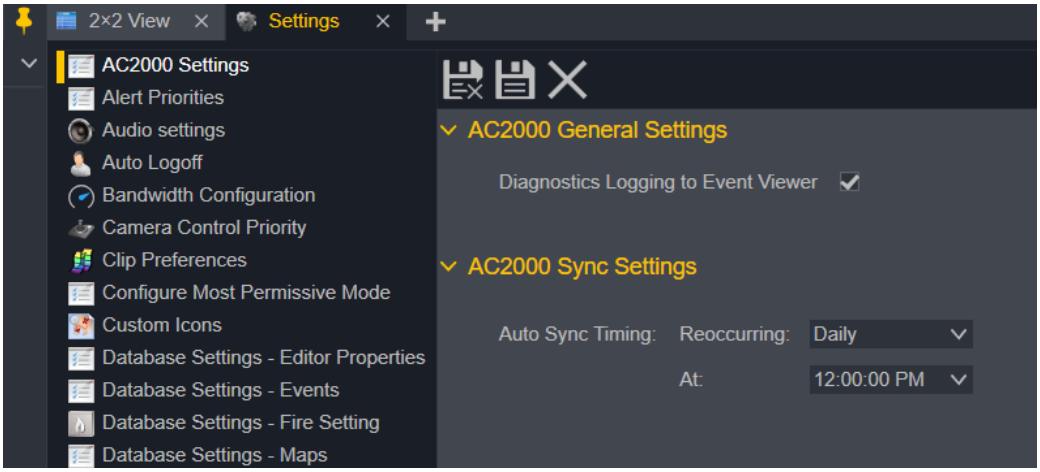
- **Diagnostics Logging to Event Viewer** – This allows users to enable or disable Diagnostic level logging to be viewable from the Windows Event Viewer.



Note:
This setting is dynamic and needed to be only applied once and saved, there is no driver restart required.

Automatic Schedule Setting for Synchronization

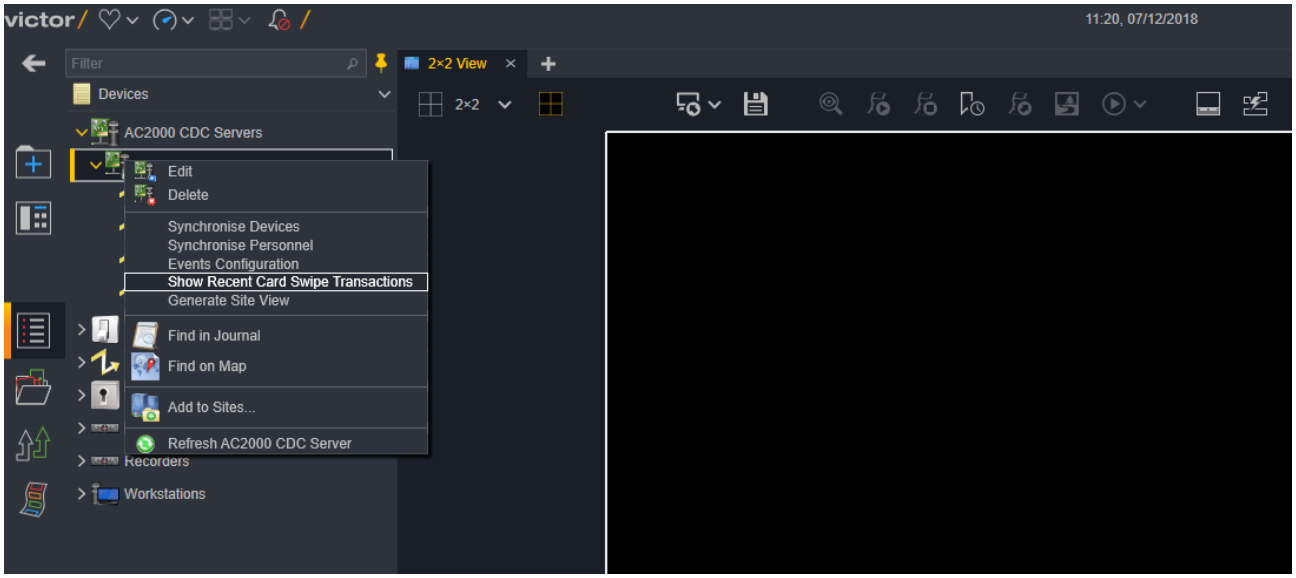
You can configure an automatic schedule to synchronize the Doors and the Personnel of the AC2000 system every day, at the specific time as defined in the settings. This keeps the system in sync with object edits on the AC2000. You can also manually synchronize victor with the AC2000 system from the CDC Server on the victor Devices list.



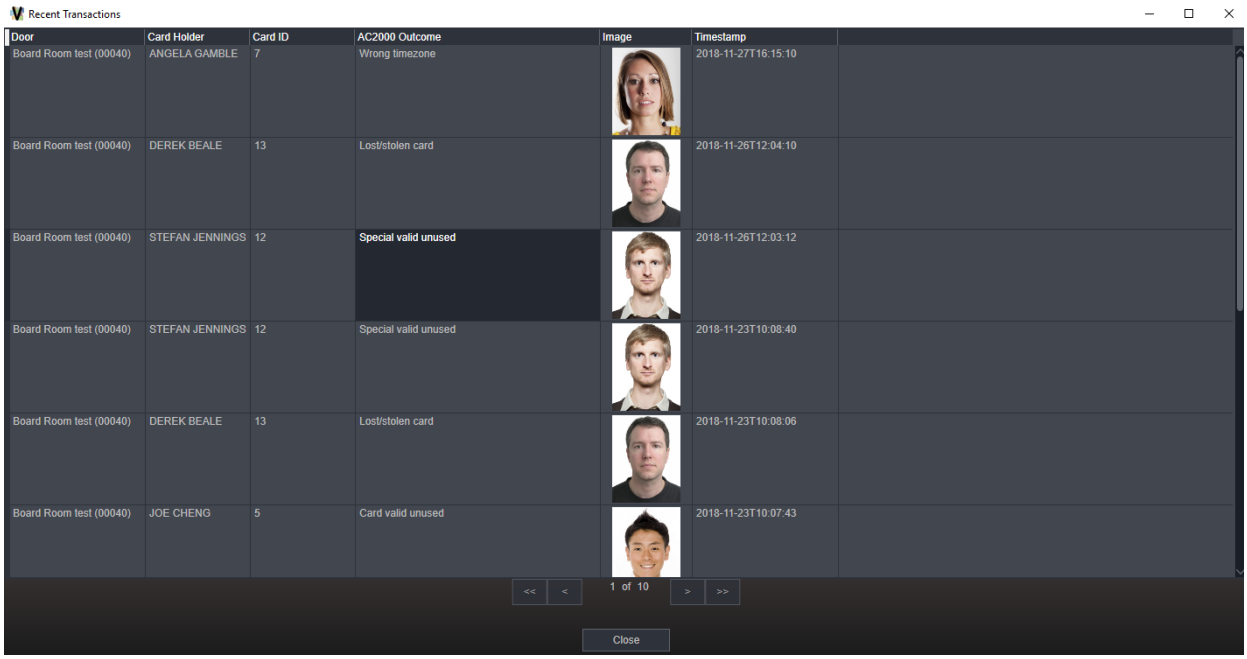
Card Swipe Transactional View

The transactional swipe and show feature allows the victor Client to display the Card access being read live from the Door Readers that are connected to the AC2000 system.

In the **Devices** list, right-click the CDC Server and select **Show Recent Card Swipe Transactions** to open the transactional Swipe & Show window. This window displays the Personnel that are accessing the relevant Doors in the various locations and swipe Card state.



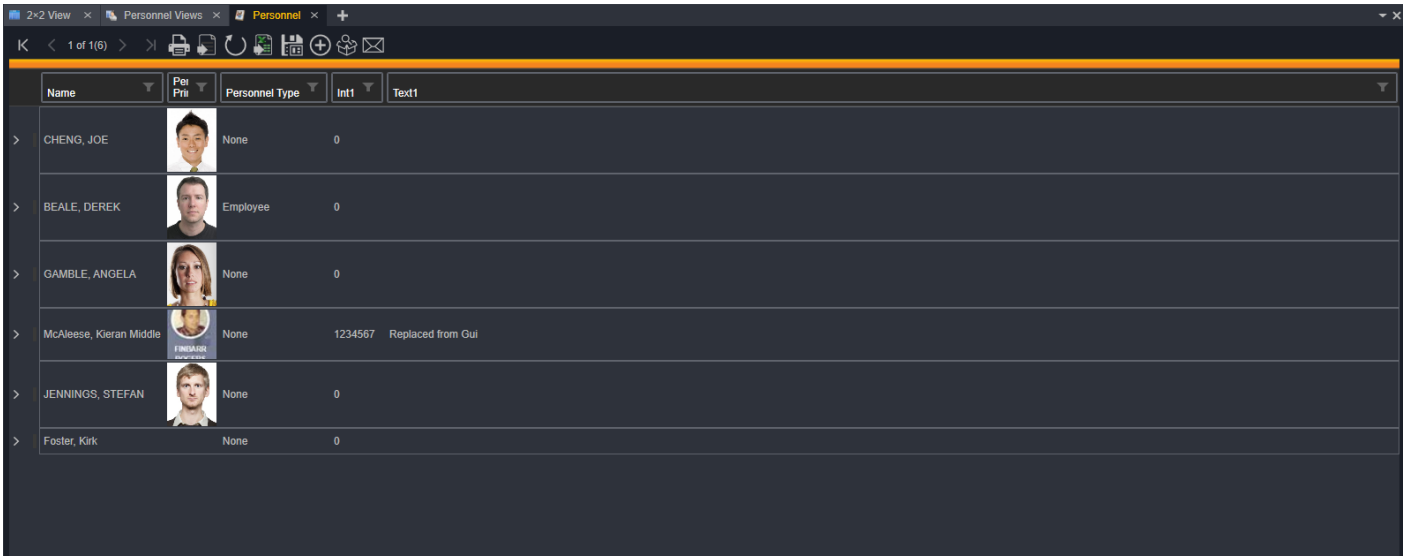
The Card ID is the auto generated ID from AC2000 and cannot be edited within victor but from AC2000.



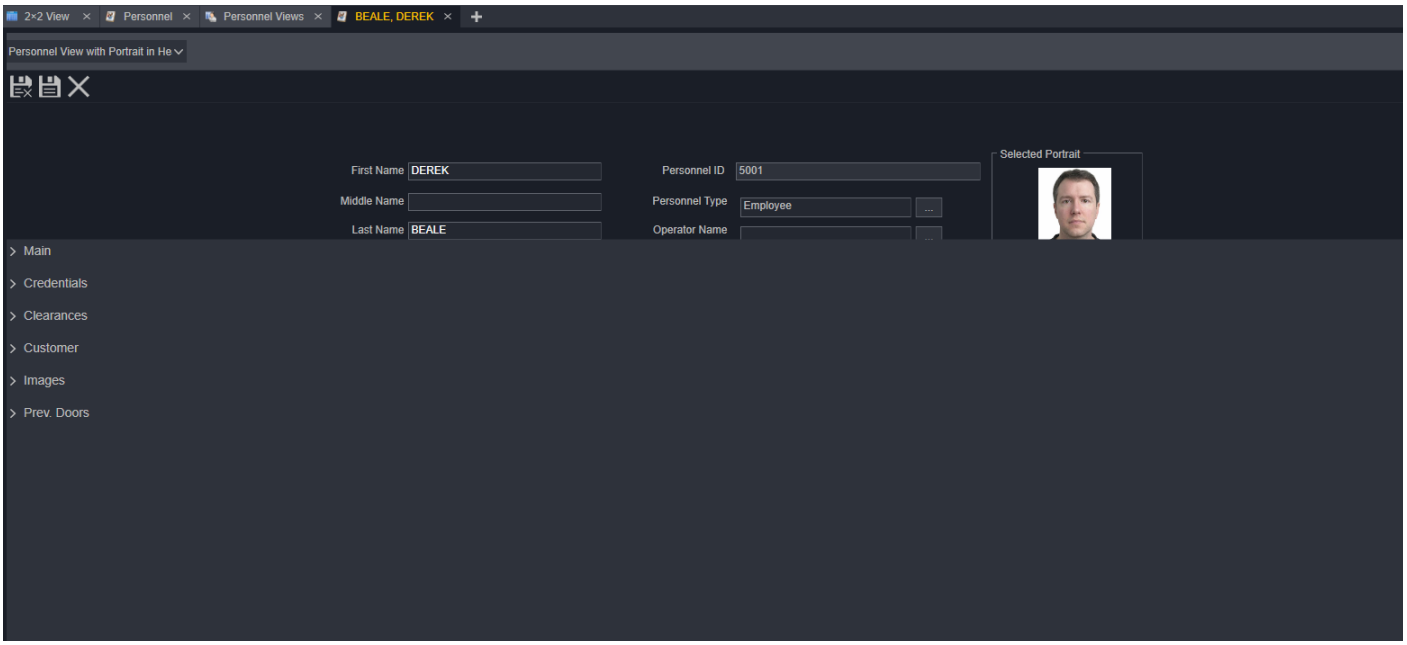
Personnel View

The Personnel can be viewed in a list as obtained from the AC2000 system. This is a read-only list - and any edits made within victor are not synchronized to the AC2000 and are overwritten when you perform a Re-Sync.

The Personnel Type, Integer1 and Text1 are all local fields to victor.



To edit a Personnel record, right-click the highlighted Card and select Edit. Note any changes here can be overwritten when a resync is performed. Therefore all edits should be made within AC2000 Personnel System and then re-synchronize is performed to preserve the changes into victor. The list can also be exported as an Excel spread sheet or an XPS document.



Swipe and Show pane view

From the New Tab page, you can select the Swipe and Show monitor. This monitor has three different types of view that you can select to display.

- **Monitor All Doors for Admits** - This view only shows successful Admission on all the Doors
- **Monitor All Doors for Admits and Rejects** - This view shows Successful and Unsuccessful Admission on all the Doors
- **Monitor all Doors for Rejects** - This view shows Unsuccessful Admission on all the Doors and will be displayed in Red on the main view.

You can select the following window pane views for the Swipe and Show monitor:

- Single
- Dual
- Quadrant
- Carousel

After you select a pane view, card swipes appear in the Swipe and Show tab. Each card swipe includes the Card ID, User Image, and Door reader location. The card swipe's background color is highlighted as follows:

- Red for Card Unsuccessful - Reject
- Yellow for Incorrect PIN - Reject
- Green for Card Successful - Admit

Figure 1: Quadrant Pane style

Figure 2: Carousel Pane Style

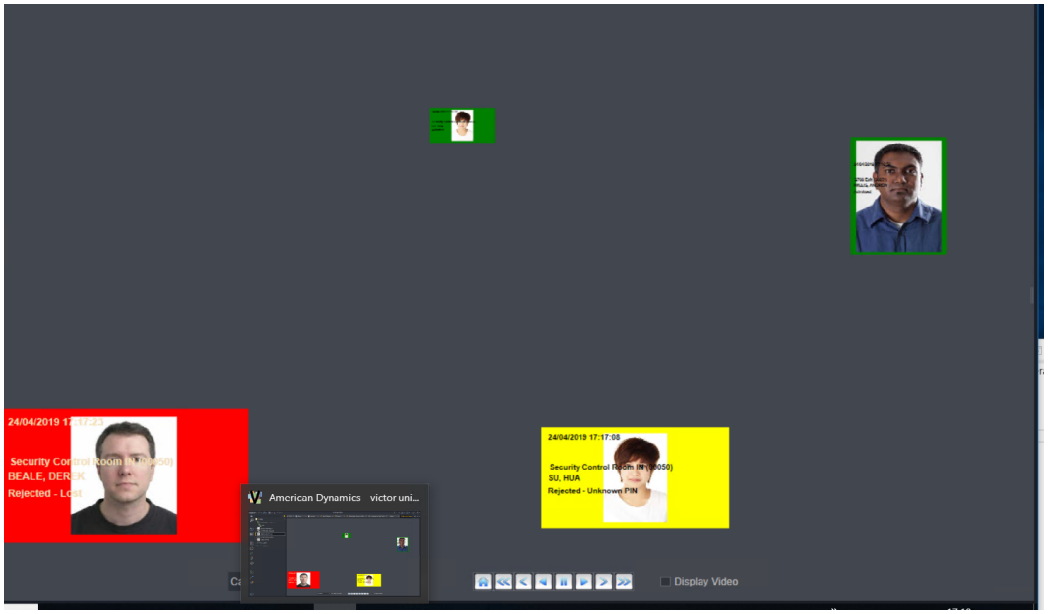
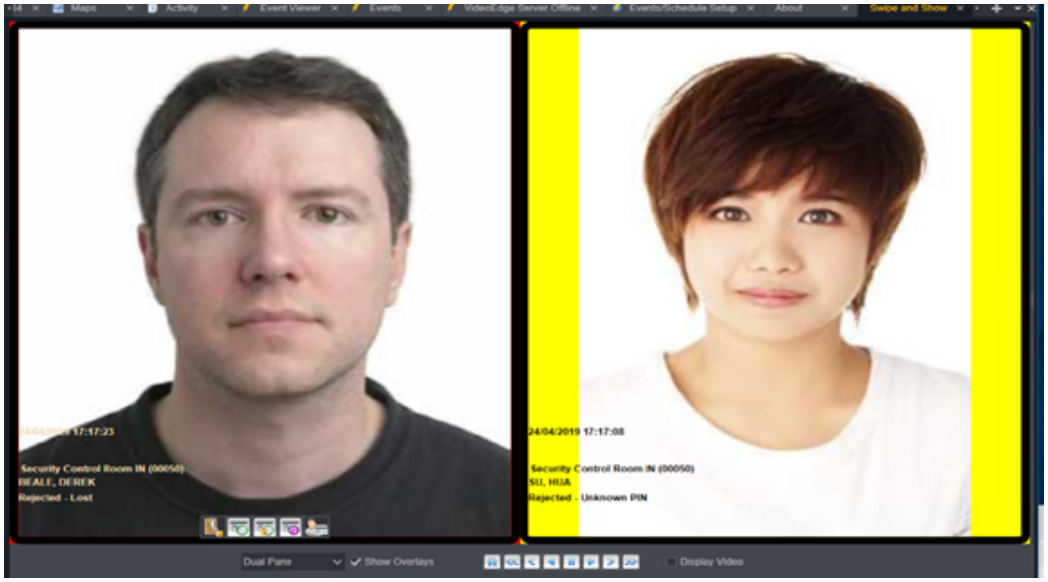


Figure 3: The Dual Pane View

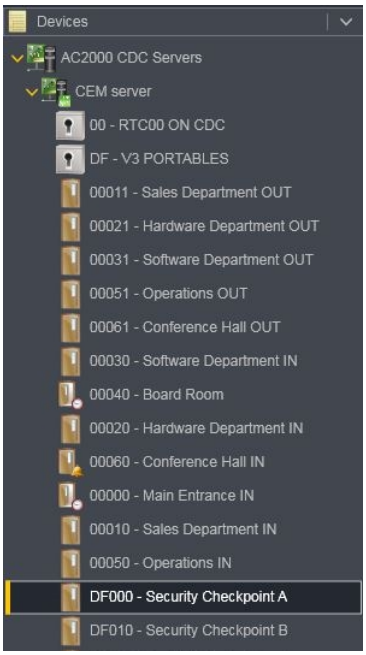


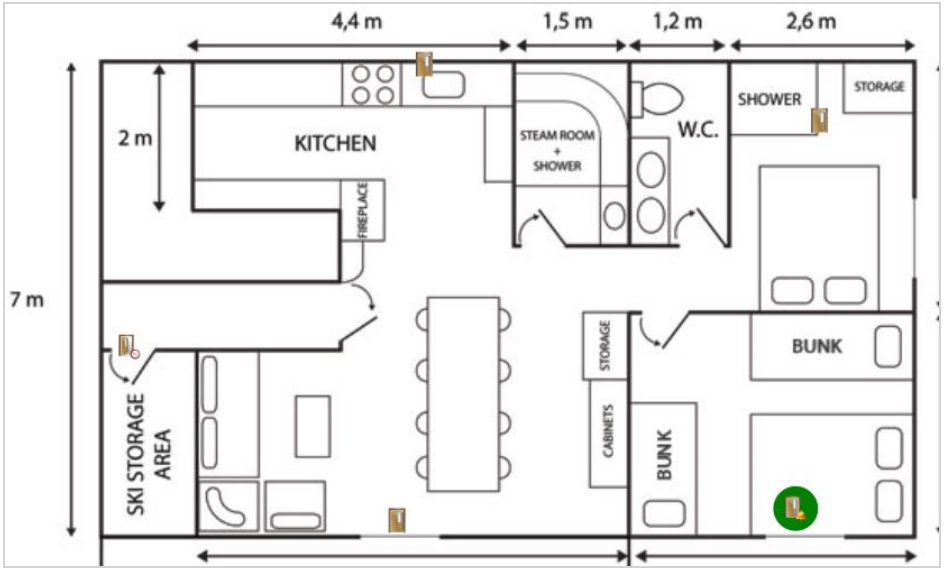
AC2000 Commands

This section describes the AC2000 commands that victor can issue to AC2000 objects.

- CDC Server Commands
- Reader Commands
- RTC Commands
- Output Commands
- Input Commands
- Broadcast Zone Commands
- Action AC2000 Commands
- Broadcast Action Command
- Output Command
- Input Command
- Door Command

In victor unified client, you can access AC2000 commands from the Devices list or from maps:





CDC Server Commands

Command	Description
Synchronize Devices	Synchronizes all supported devices (readers/outputs/inputs/broadcast zones) from the AC2000 CDC Server into Victor as AC2000 objects.
Synchronize Personnel	Synchronizes all AC2000 cardholders/users from the AC2000 CDC Server into victor as victor personnel. User images are also imported in the process as set as primary victor personnel image for that user.
Events Configuration	This command opens the event configuration window for the selected AC2000 server.
Show Recent Card Swipe Transactions	The command opens the card swipe transaction display.

Reader Commands

Command	Description
One-shot	Send one-shot command to reader.
Broadcast open relay 0	Send broadcast open to first reader output/relay (reader output 3).
Broadcast close relay 0	Send broadcast close to first reader output/relay (reader output 3).
Broadcast open relay 1	Send broadcast open to second reader output/relay (reader output 4).
Broadcast close relay 1	Send broadcast close to second reader output/relay (reader output 4).
Suppress Alarms	Disable AC2000 alarms for this device in victor.
Reactivate Alarms	Enable AC2000 alarms for this device in victor.

RTC Commands

Command	Description
Suppress Alarms	Disable AC2000 alarms for this device in victor.
Reactivate Alarms	Enable AC2000 alarms for this device in victor.

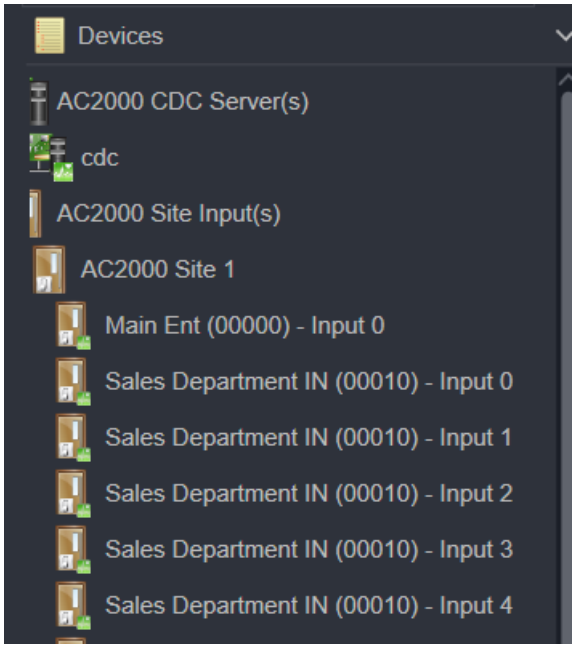
Output Commands

Command	Description
Open	Send open command to the output
Close	Send close command to the output
Suppress Alarms	Disable AC2000 alarms for this device in victor.
Reactivate Alarms	Enable AC2000 alarms for this device in victor.

Input Commands

You can configure AC2000 Inputs to appear in victor's Devices list.

Figure 4: Inputs



You can disable and enable an Input's alarms from the Devices list. Right-click the Input and select the Suppress or Reactivate command.

Table 1: Input Alarm commands

Command	Description
Suppress Alarms	Disable AC2000 alarms for this device in victor.
Reactivate Alarms	Enable AC2000 alarms for this device in victor.

Broadcast Zone Commands

You can use Broadcast Zone Commands to trigger state changes for multiple doors. You can assign multiple doors to a Zone. When you issue a Broadcast Zone command to a Zone, the command affects each door in that Zone.

To open the Broadcast Zone menu, select the New Tab icon from the Navigation bar, and then select the AC2000 Broadcast Zone icon.

Figure 5: The New Tab menu

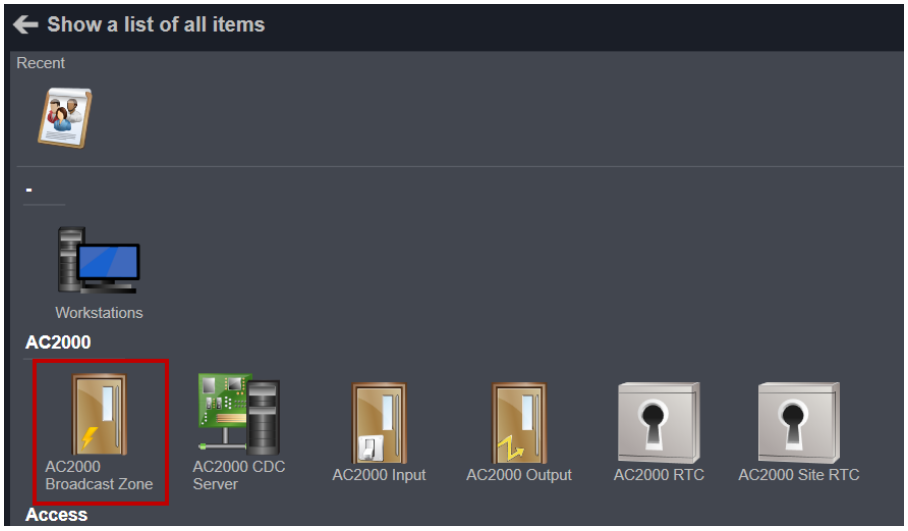
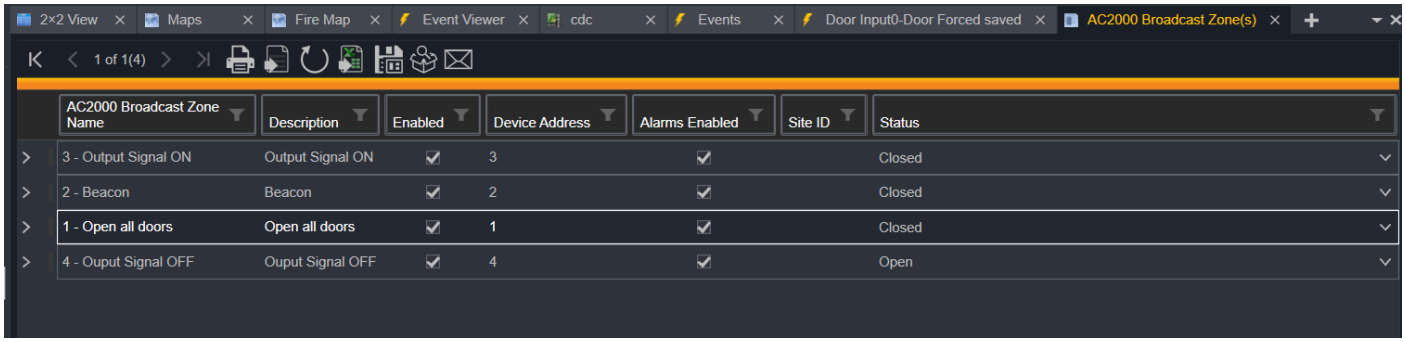


Figure 6: The Broadcast Zone menu



New Broadcast Profiles are initially created in AC2000 and are accessible from victor. The Broadcast's state appears in the Status column. To change a broadcast's state, right-click the Broadcast's profile and then select the command that you want to issue.

Figure 7: Issuing a Broadcast Zone command

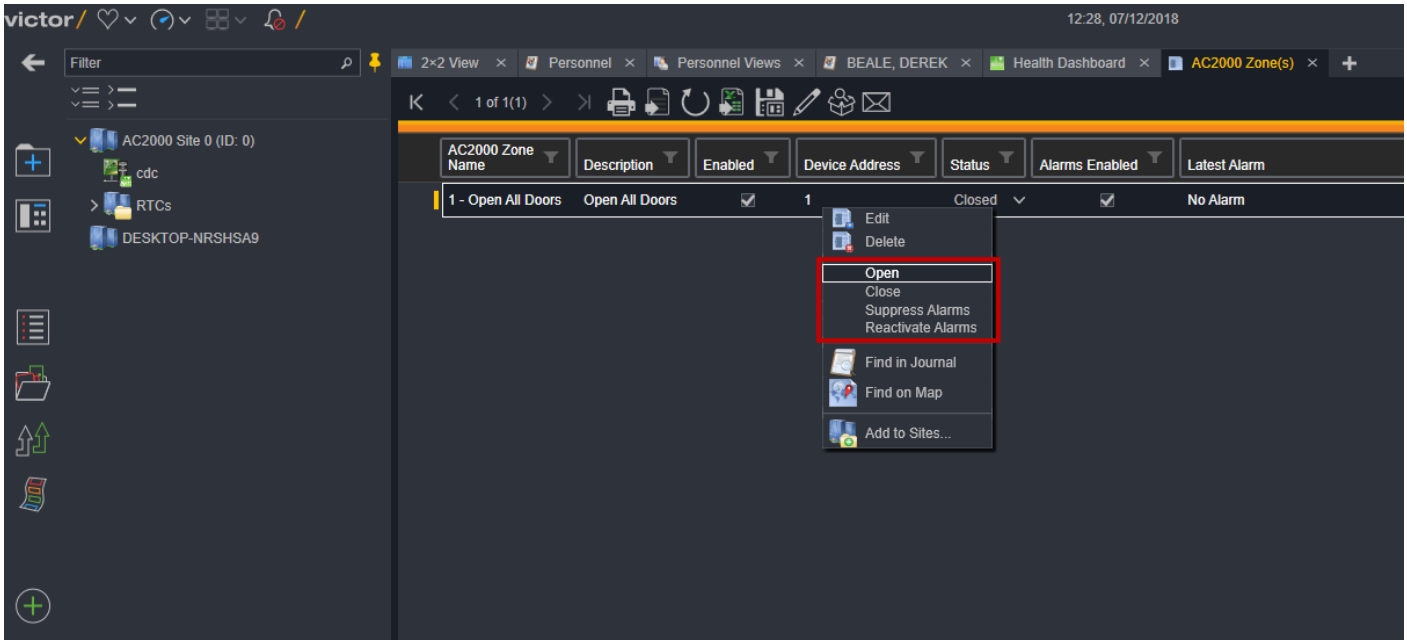


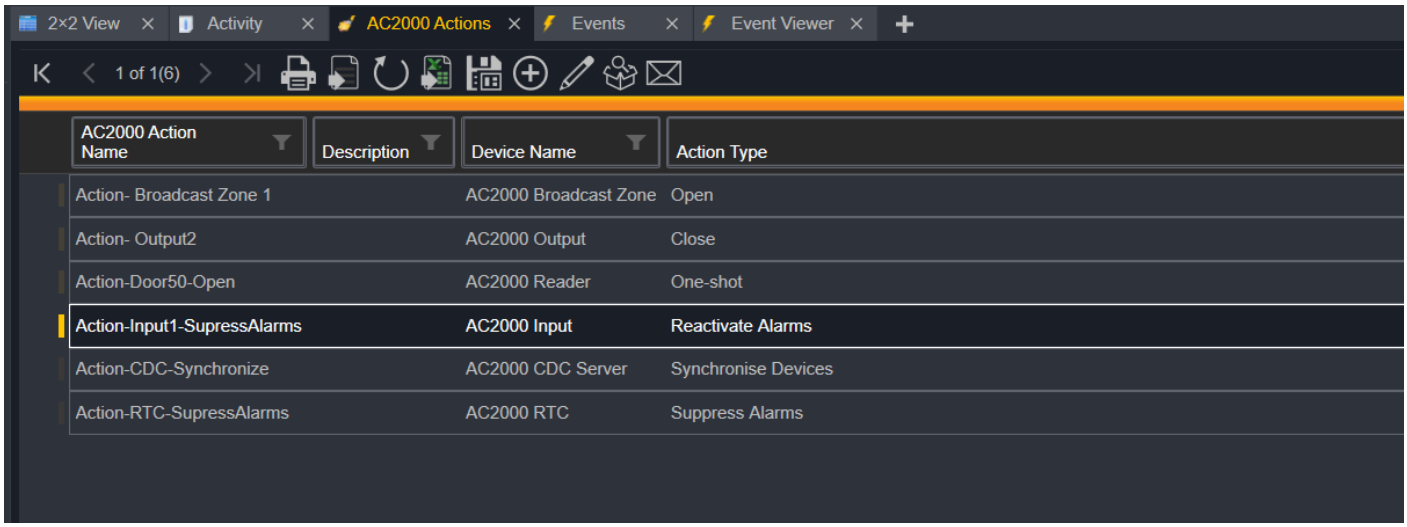
Table 2: Broadcast Zone commands

Command	Description
Open	Send open command to the broadcast zone
Close	Send close command to the broadcast zone
Suppress Alarms	Disable AC2000 alarms for this device in victor.
Reactivate Alarms	Enable AC2000 alarms for this device in victor.

Action AC2000 Commands

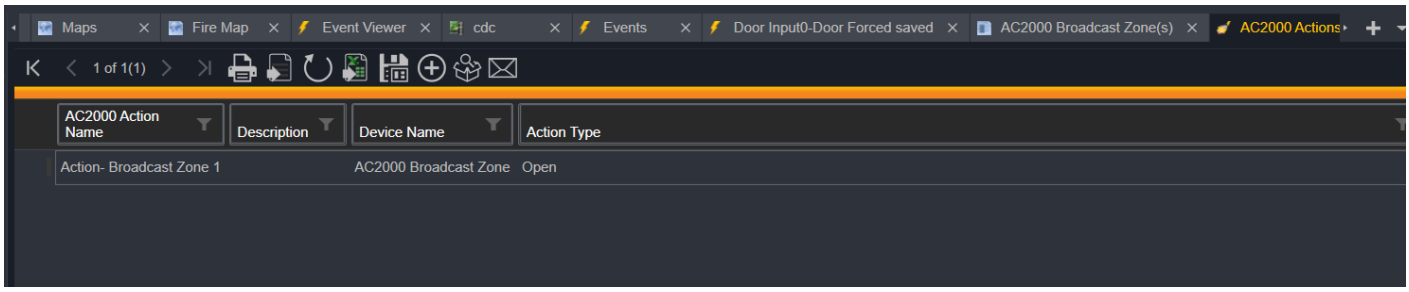
You can configure the following actions to issue the following commands:

- Broadcast Zone
- Output Command
- Input Command
- Door Command



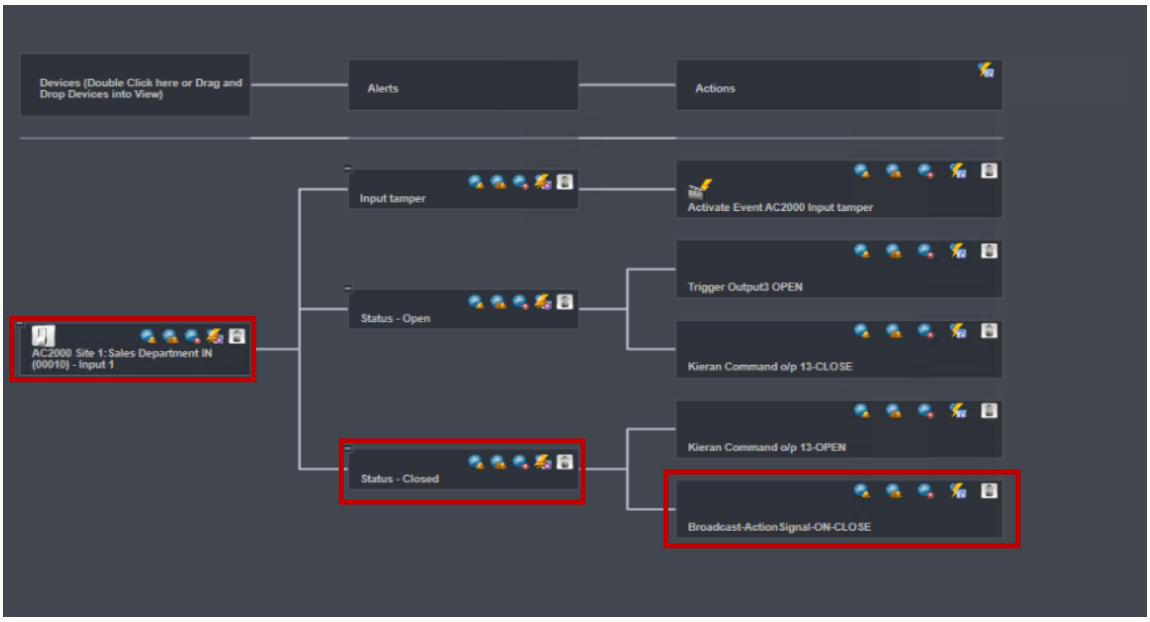
Broadcast Action Command

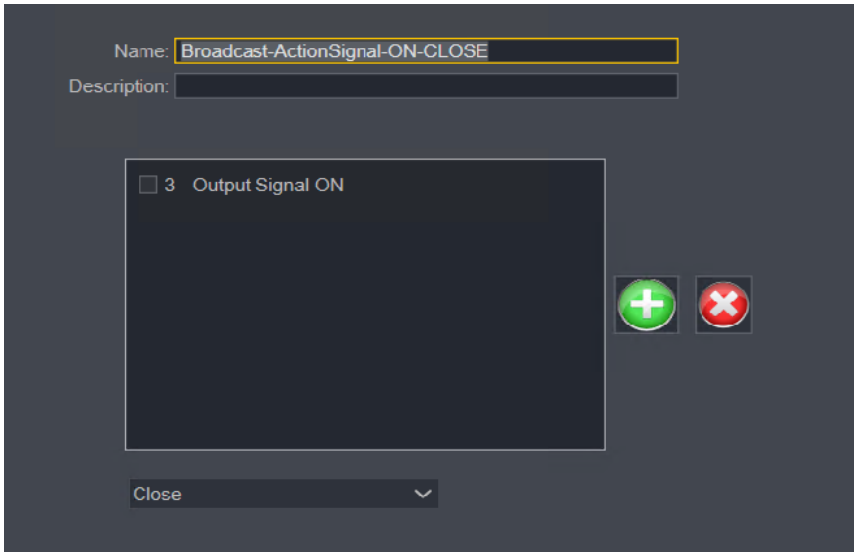
You can create an Action that causes the doors in Zone 1 to open or close, as shown below.



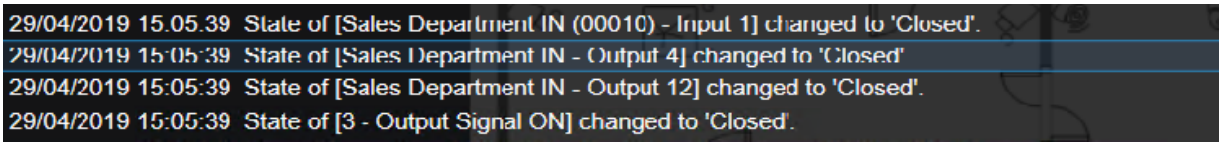
You can add the Zone Broadcast to a map, so that you can manually trigger the Zone Broadcast by clicking on the Icon or Automatic activation from the Action. The state is displayed accordingly.

In the following example When Door 10 (Sales Department) is closed, an Event activates. This Event triggers the Broadcast-ActionSignal-ON-CLOSE action, which triggers 3-Output Signal ON. Its good practice to put the state in the Name of the action so it is self explanatory.

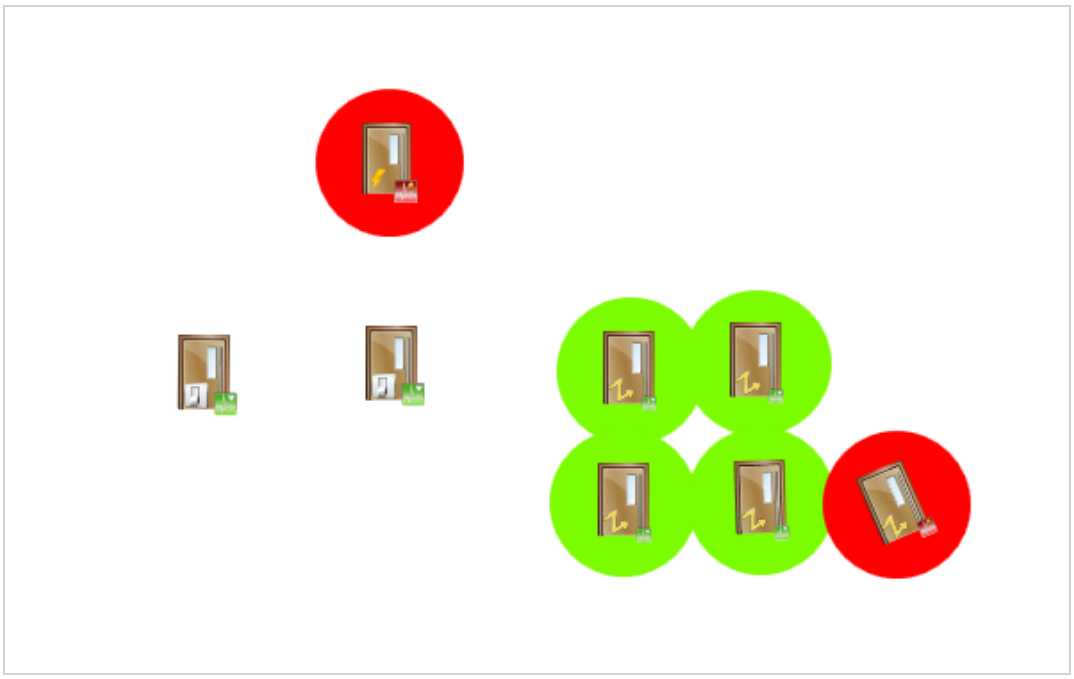




The State of the Action is recorded in the Journal as shown below:

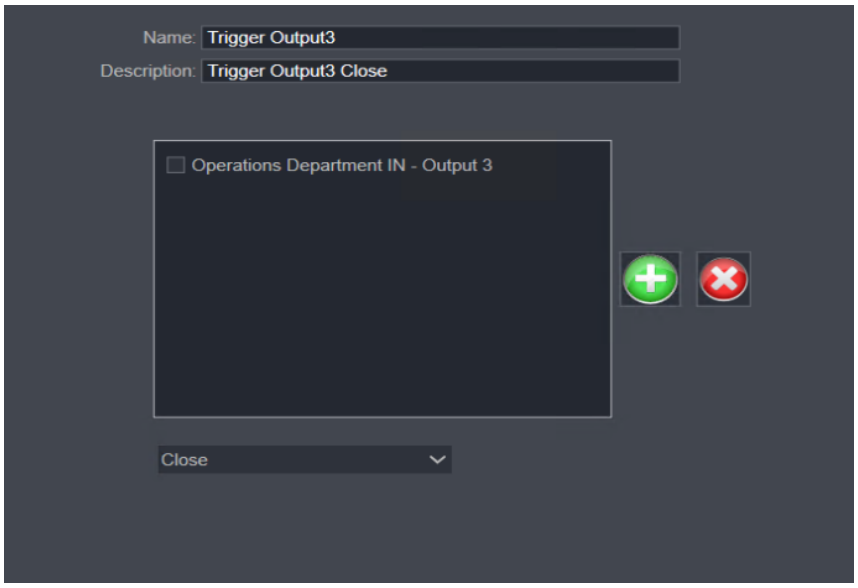


As can be seen on the Map the Broadcast Outcome can also be displayed with the closed State in Red Annunciation.

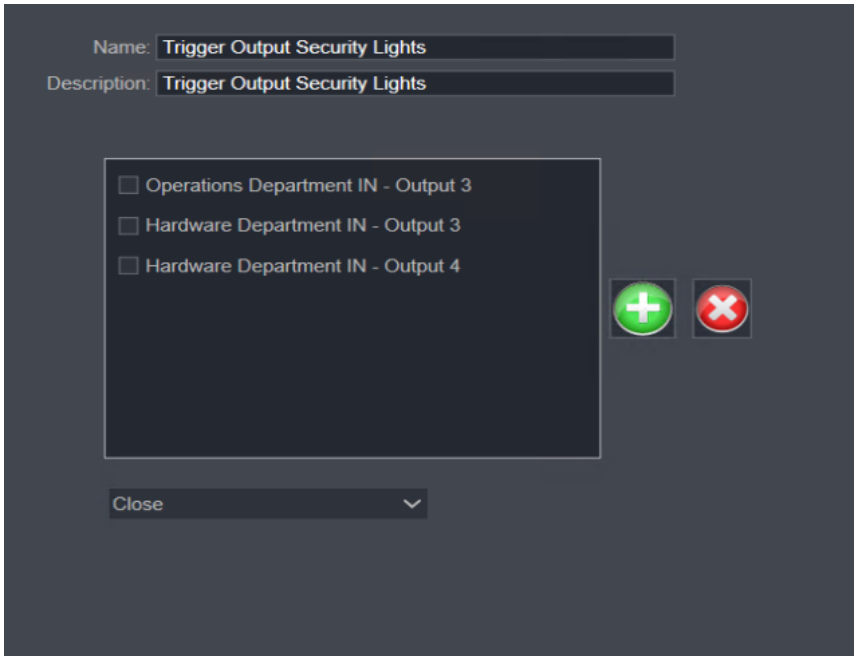


Output Command

Single or multiple Output Actions can be triggered as shown below for this single Output 3 can be triggered dependent upon a certain event or Input state. Therefore allowing complex Business logic and outcome to be set up during certain events.

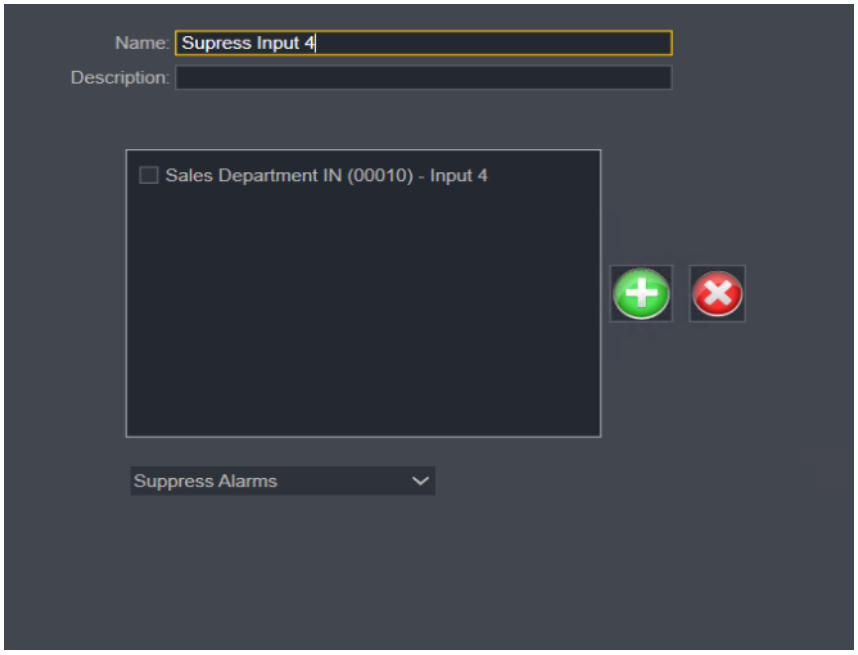


Multiple Outputs can be configured to trigger as shown below to turn on the Security Lights, in the various Door Locations.



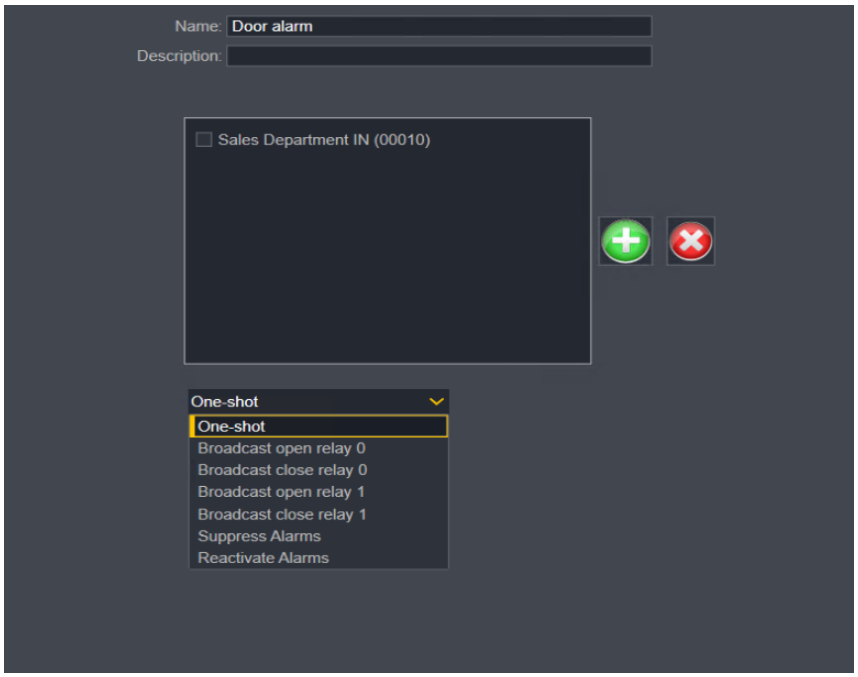
Input Command

You can also configure an Input Command to trigger the Suppression or Activation of that Alarm.



Door Command

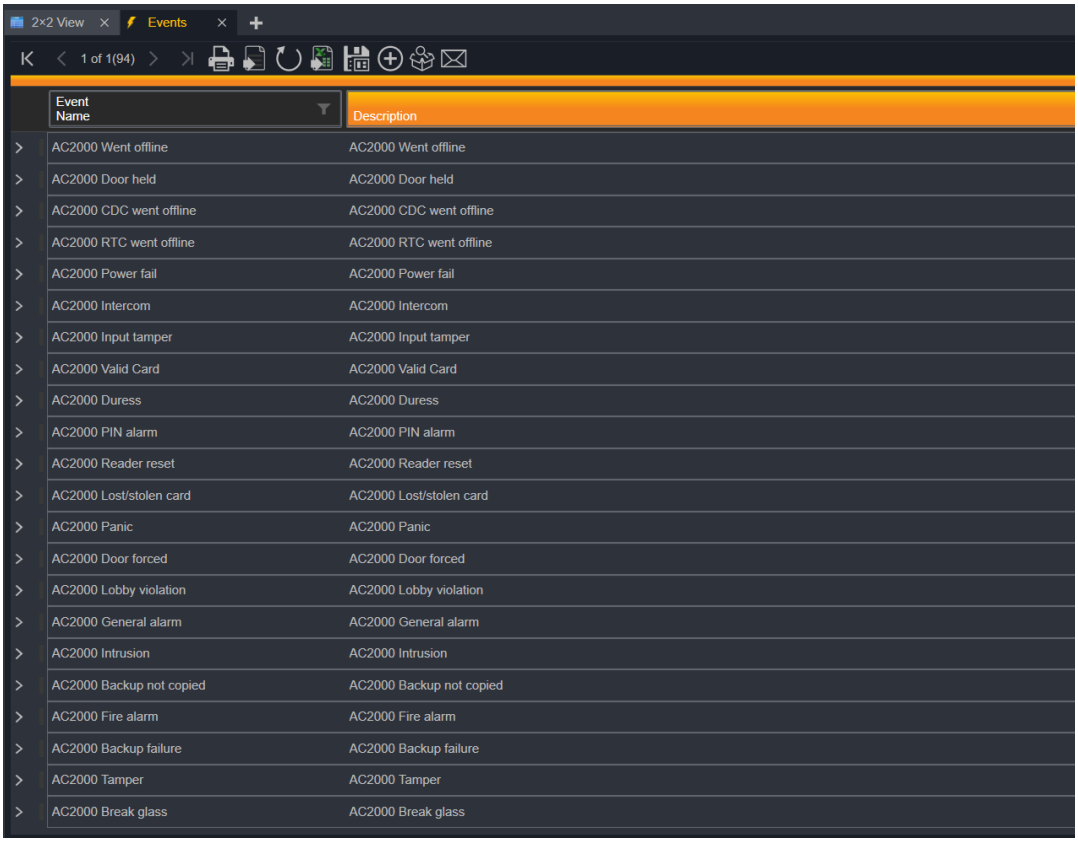
The Door command can be set up to one shot i.e. momentarily open the Door, or send a Broadcast to Open or Close Door permanently using the first two relays 0 or 1 on the Door Reader. If the Open state is sent to Relay 0 this will hold the Door in a permanent OPEN state until closed.



The CEM AC2000 integration includes functionality that allows alarm type configuration at the victor integration level. For example, you can enable and disable alarm types for a server and you can also enable or disable alarms for individual devices. This affects the alarm processing within the victor AC2000 driver level. Incoming alarms are filtered in the driver based on this configuration and either journalled or not journalled into victor.

Pre-configured AC2000 Events are available for use within the victor Event List with a prefix name AC2000 to help deploy the Door Alarm mappings quickly and easily.

Figure 8: AC2000 events in victor



CEM custom alarms

In the CEM system, you can create custom alarm types to use in the CEM system and in victor. You can create custom alarms from the Alarm Configuration page.

When you create a custom alarm, you can select an internal or external alarm source. Internal type alarms are triggered by readers, and external type alarms are triggered by reader inputs. In the image below, CustomAlarm3 and CustomAlarm4 are internal type alarms and CustomAlarm5 is an external type alarm that is associated with a reader input.

Figure 9: Alarm Configuration page

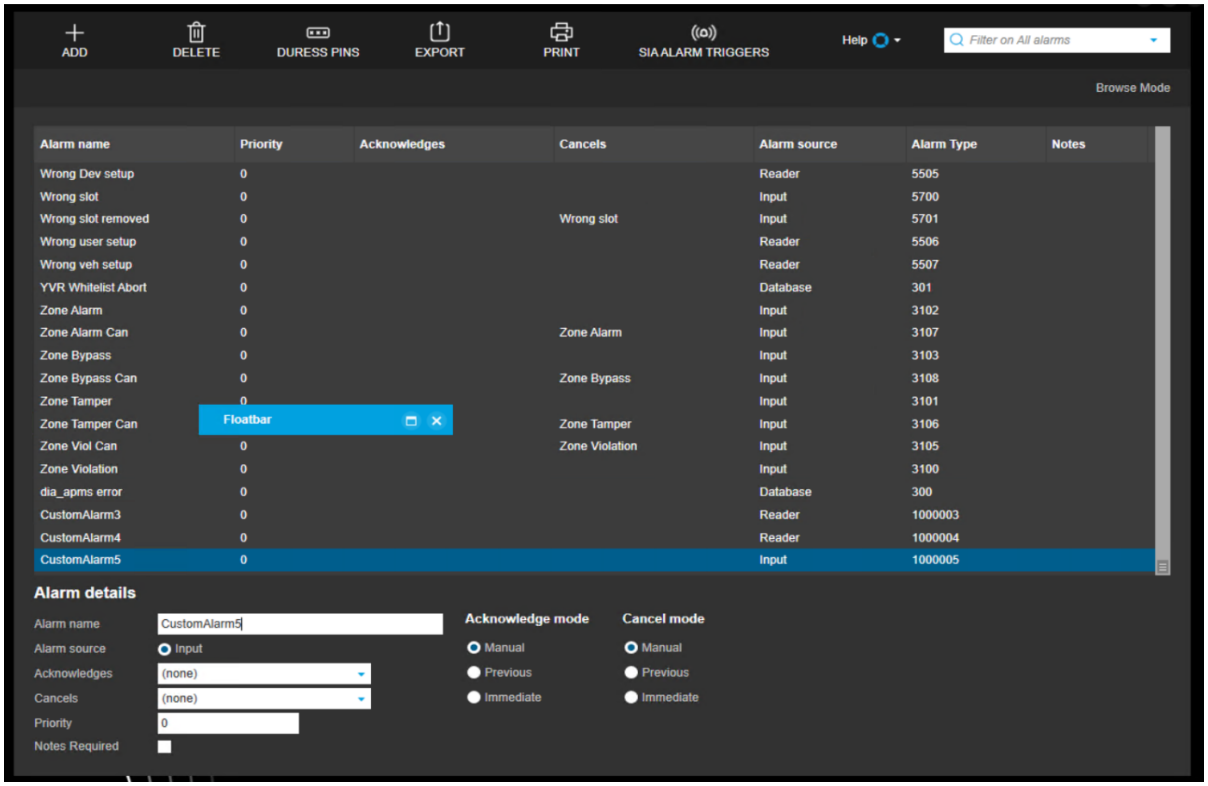
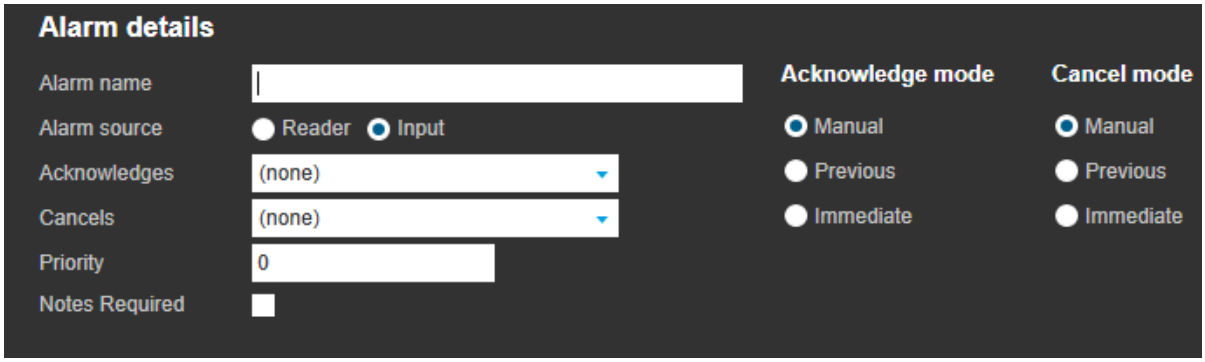


Figure 10: Alarm details pane



Note:
The CEM System starts the custom Alarm ID from 1000000 and increments this value when you add new custom alarms. When you map custom alarms to victor, victor maps the first ID:1000000 as Custom1

Procedure 7 Creating a custom alarm in AC2000

1 Log on to AC2000.

2 Click **Alarm and Event Monitoring**, and then click **Alarm Configuration**.

3 From the **Alarm Configuration** page, click **Add**.

4 From the **Alarm Details** pane, configure the alarm parameters. Refer to the table, CEM Alarm parameters, below.

Table 3: CEM Alarm parameters

Parameter	Description
Alarm name	The name of the alarm.
Priority	The alarm's priority. Priority 0 is the least important, and priority 1000 is the most important. In the Security Hub, the most important alarms are displayed first.
Notes Required	This option defines whether the user must enter a note before they can acknowledge the alarm.
Alarm source	Defines whether the alarm was triggered by a reader or an input to the reader.
Acknowledges	Defines the alarm that is acknowledged in Security Hub when the alarm being configured is triggered.
Cancels	Defines the alarm that is canceled in Security Hub when the alarm being configured is triggered.
Acknowledge mode	Defines how the alarm must be acknowledged.
Cancel mode	Defines how the alarm must be canceled.

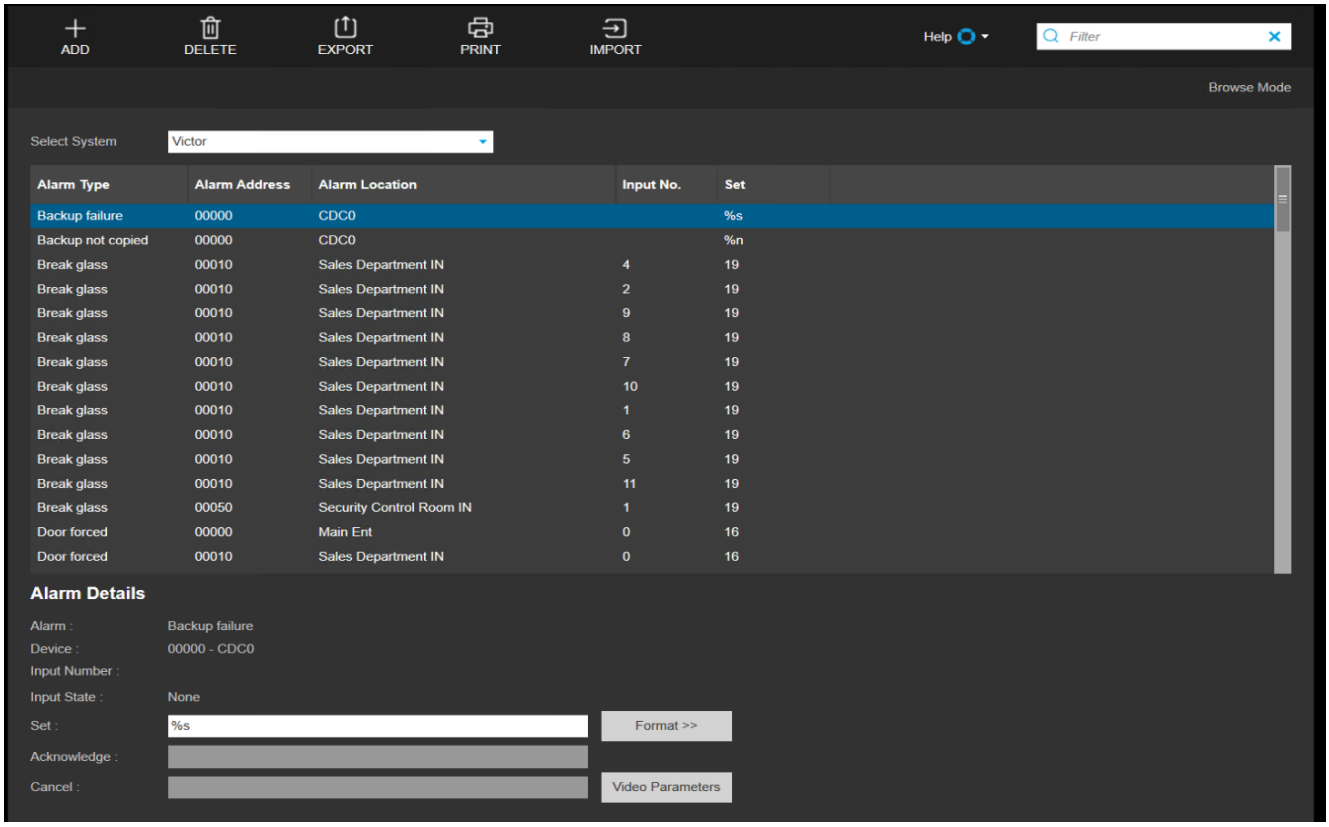
For more information about custom alarms, refer to the *Alarm Configuration* section of the *System Configuration Guide* for AC2000. You can download this manual from the CEM Systems website.

Procedure 8 Exporting custom alarms to victor

After you define the Custom Alarm types, you must configure them in the CEM External Alarm Table for communication to the Victor System, as shown below.

victor will then be able to receive these new custom alarm types both within Doors (Internal) or Door Inputs (External) and use these within the Event Manager to trigger an Event and Map Annunciation or an Action.

Figure 11: CEM External Alarm table



1 Log on to AC2000, click **Device Configuration**, and then click **External Systems**.

2 From the **Select System** list, select **Victor**.

3 Click **Add**.

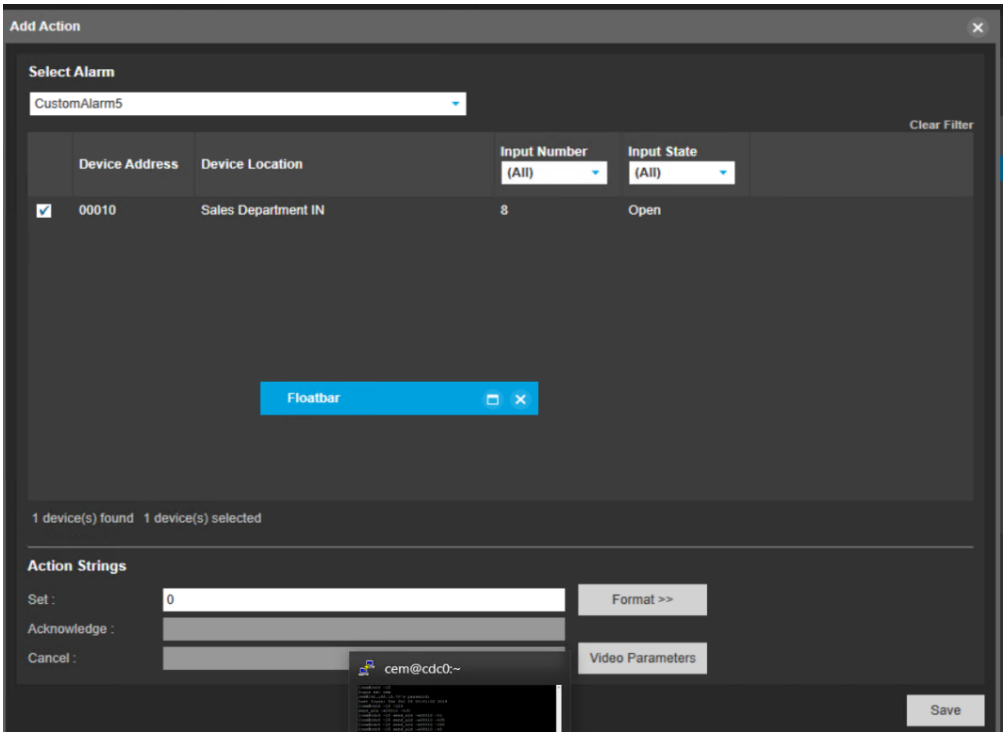
4 From the **Select Alarm** list, select an alarm.

5 From the list of devices, select the door that you want to link to the alarm.

6 (External alarms only) Assign the alarm to an **Input Number**.

In the image below, CustomAlarm5 is assigned to Door 10 Input 8.

Figure 12: Linking an alarm to a door



7 In the **Action Strings** pane, configure the Set string that is sent to the external system when the alarm triggers on AC2000.

Note:
For more information, refer to the *Configuring the Set string* section of the *System Configuration Guide* for AC2000. You can download this manual from the CEM Systems website.

8 In the **Acknowledge** field, type the command string that is used to acknowledge the alarm.

9 In the **Cancel** field, type the command string that is used to cancel the alarm.

10 Click **Save**.

11 When complete, click **OK** to save the configuration.

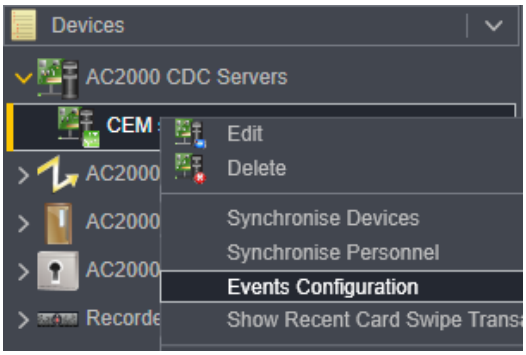
Note:
In victor, you can define any undefined alarm types as custom, to match any alarms that you map from the AC2000 system . There are 20 custom alarms that you can use in victor to generate victor events.

Procedure 9 Enabling AC2000 events in victor

In victor, you can enable or disable AC2000 events from the Devices list.

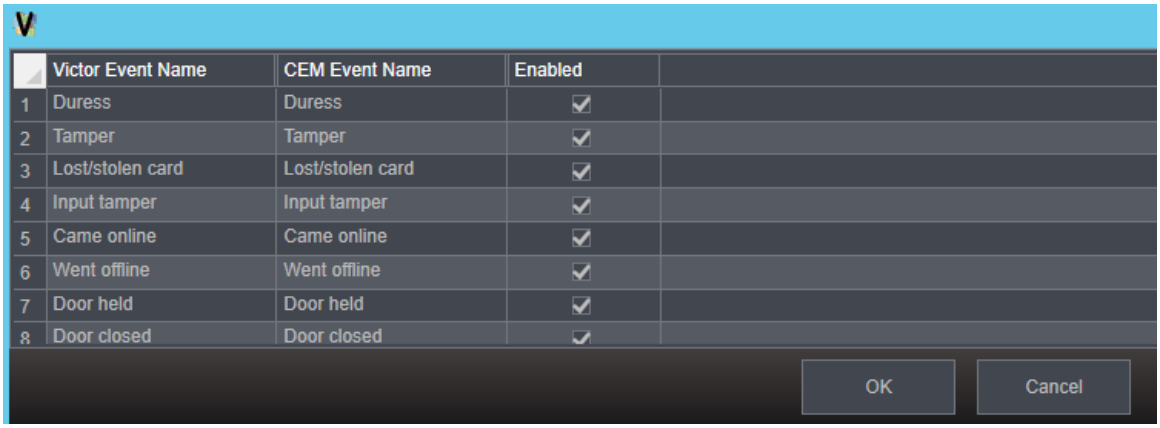
1 In the **Devices** list, right-click the AC2000 CDC Server object and select **Events Configuration**.

Figure 13:



2 Select the **Enabled** checkbox for any AC2000 alarms that you want to enable, and then click **OK**.

Figure 14: The Events Configuration menu



Procedure 10 Enabling and disabling alarms for AC2000 devices

From victor, you can enable or disable alarms for any AC2000 device (Reader/Input/RTC/Output/Zone). If you disable a device's alarms, victor does not create journal entries for that device. You can perform this procedure from the Devices list, from a dynamic view, or from a map.

1 Right-click an AC2000 device.

2 Select one of the following options:

- Click **Suppress Alarms** to disable the device's alarms.
- Click **Reactivate Alarms** to enable the device's alarms.
- Click **Edit** and select or clear the **Alarms Enabled** checkbox for individual device alarms.

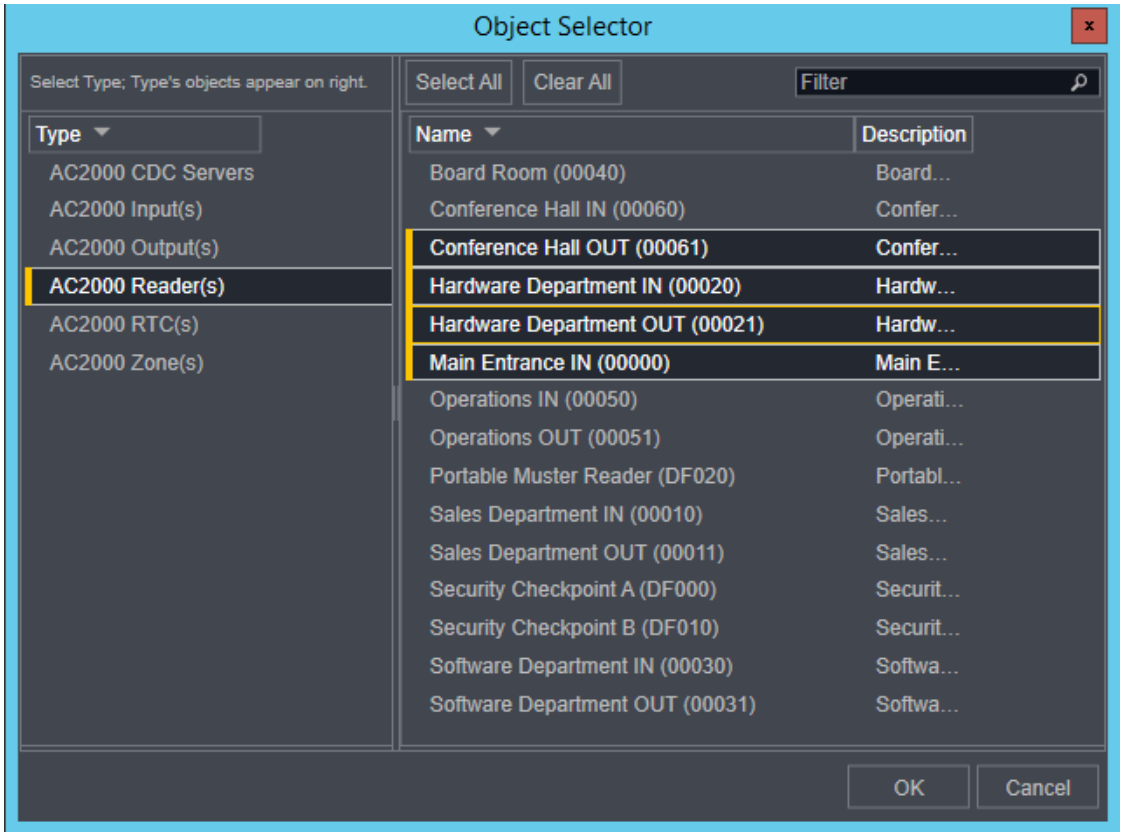
Procedure 11 Creating an AC2000 action

Users can create AC2000 Actions to trigger various types of Events. Integration specific actions to tie together system events with actions you wish to trigger.

1 Click the **Create new item** icon, and then click **AC2000 Action**.

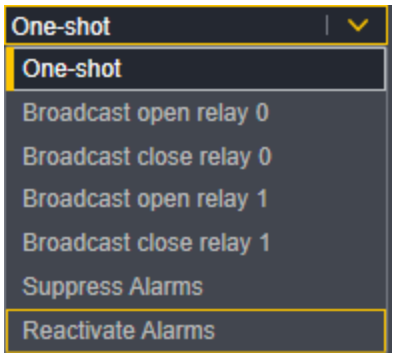
2 Enter a **Name** and **Description**.

3 Click  and use the object selector to add devices to this action.



4 Select the action to execute.

For example, you can select one of the following actions for a reader:



5 Select **Save**.

Linking actions and events to devices

Using the Event Setup Editor and the Event/Action pairing editor you can build multiple event configurations quicker and easier than building single event configurations one at a time for AC2000 objects.

Event/Action Pairing Editor

Use the Event/Action pairing editor to link system events with actions. Use this editor to link an AC2000 action to an event.

Note:
Event/Action association can only be made in this editor.

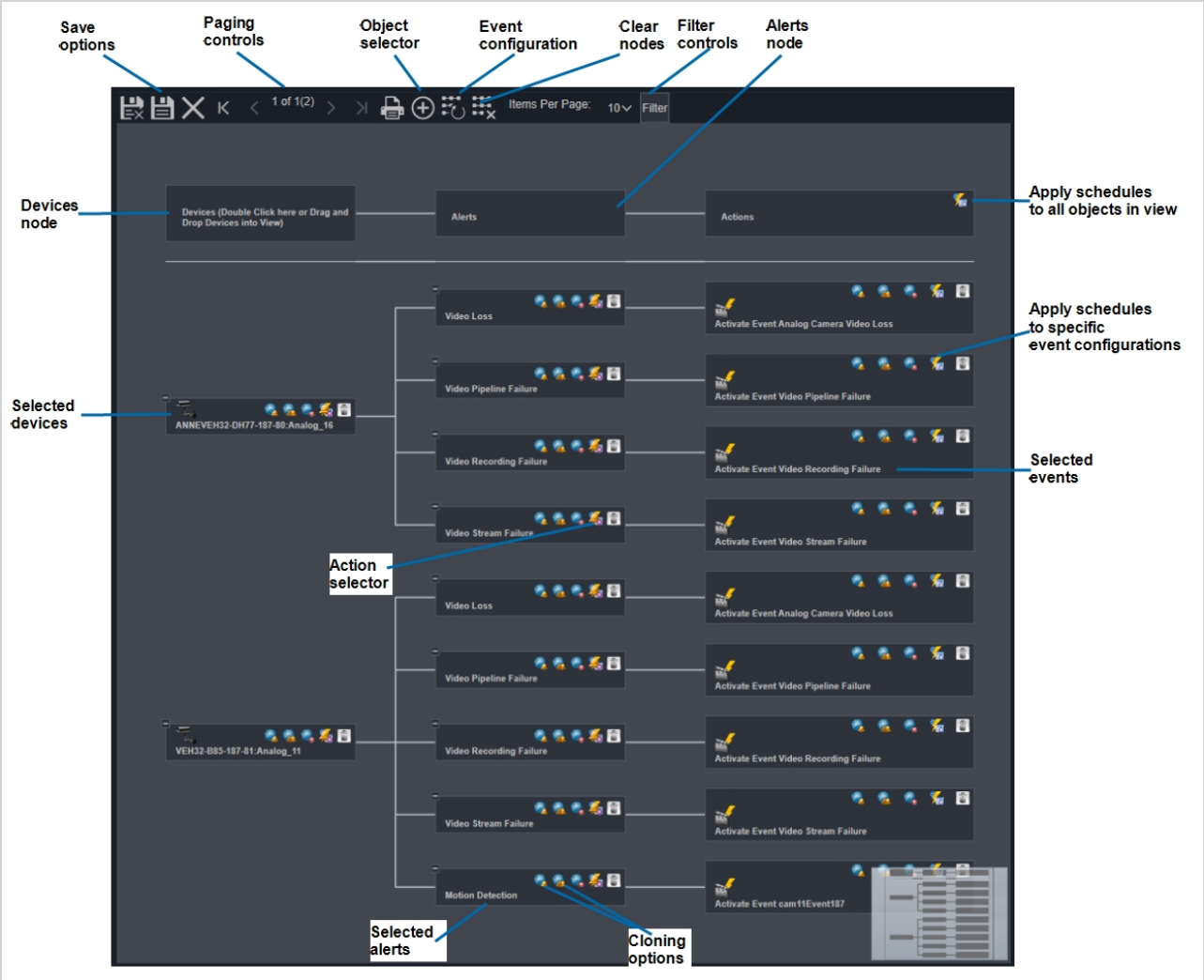
Procedure 12 Pairing an event with an action

1. Click the **System Configuration** icon, and then click **Event/Action Pairing**.
2. Click the **Events** node and use the object selector to select events as required.
3. In the Event node, click  and use the object selector to assign actions to the event.
4. (Optional) Click  to remove an action from an event.
5. Click **Save**.

Event/Schedule Setup

The Event/Schedule setup editor provides a dynamic, visual method of batch linking device alerts to actions or events, as well as to set up event scheduling. Use the Event/Schedule setup editor to link AC2000 device alerts to system events. For more information about the Event/Schedule setup editor, refer to the *victor Unified Client / victor Application Server Administration and Configuration Guide*.

Figure 15: The Event/Schedule setup editor



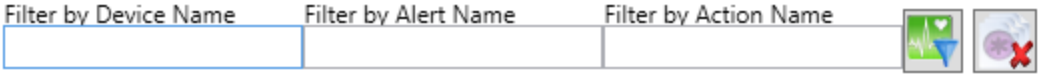
Procedure 13 Linking a device alert to an event

1 Click the **System Configuration** icon, and then click **Event/Schedule Setup**.

2 Use one of the following methods to add a device to the Event/Schedule Setup editor:

- Double-click the **Devices** node and use the object selector to select an AC2000 device
- Drag an AC2000 device from the **Devices** list onto the editor.

Note:
To configure all system objects of a single type, select the **Search for Event Configurations** icon from the top toolbar, and filter the search results by the required type:



3 Configure the device's alerts:

a In the device's node, click the **Select alert type** icon.

b In the **Select Alerts** list, select the checkboxes for the alerts that you want to enable.

c Click **Add Alerts**. Selected alerts are displayed under the Alerts node.

4 Assign events to the device's alerts:

- Click  in an alert node and use the object selector to assign events to the alert.
- Repeat as required.

5 (Optional) Click the **Remove** icon to remove an alert or an event from a device.

6 (Optional) Use merge and clone options to copy configurations:

Icon	Name	Description
	Clone Merge	Merge and clone target configuration
	Clone Duplicate	Duplicate source configuration to all targets
	Clone Remove	Remove configuration on source and target

7 (Optional) Apply a schedule to an event:

a Click  to open the **Schedules** list.

b Select the checkboxes for any schedules that you want to apply.

c Clear the checkboxes for any schedules that you want to remove.

d Click **Apply Schedules**.

Note:
For more information about Schedules, refer to the *victor unified client / victor Application Server Administration and Configuration Guide*.

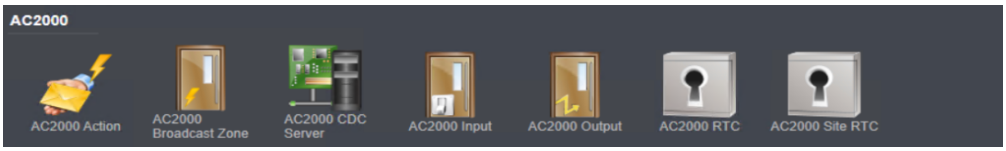
---

8 Select **Save**.

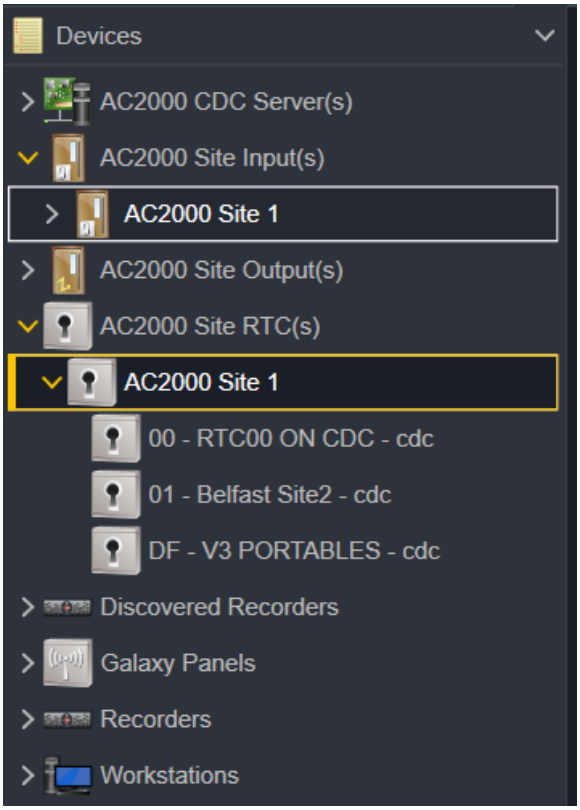
AC2000 Device States

You can use the AC2000 victor integration to control the following AC2000 objects.

- CDC Server
- RTC
- Doors
- Broadcast Zone
- Inputs
- Outputs



Within each object you can view the states that are supported by each of the AC2000 object types in victor, and the object state icons that are supported. From the Devices list, you can view AC2000 objects. The object icons update to show their current state.



CDC Server States

The CDC Server can be monitored for any loss of Connection or state change and subsequent Events can then be triggered if this is required.

State	State Values
Devices Sync Status	Synchronization Status Unknown Synchronization Failed Synchronizing Synchronized Backup Failure Backup Not Copied
Connection Status	Connection Status Unknown Connection Failed Connecting Connection Successful Disconnected

CDC Server State Images

State	Image
Connected	
Connection Failed/Disconnected	
Default	

RTC States

The RTC Server can be monitored for any loss of Connection or state change and subsequent Events can then be triggered if this is required.

State	State Values
Latest Alarm	See List of supported Alarms in AC2000 Alarms type section

RTC State Images

State	Image
Default	

Door Reader States

The Door Readers can be monitored for any loss of Connection or state change and subsequent Events can then be triggered as when required.

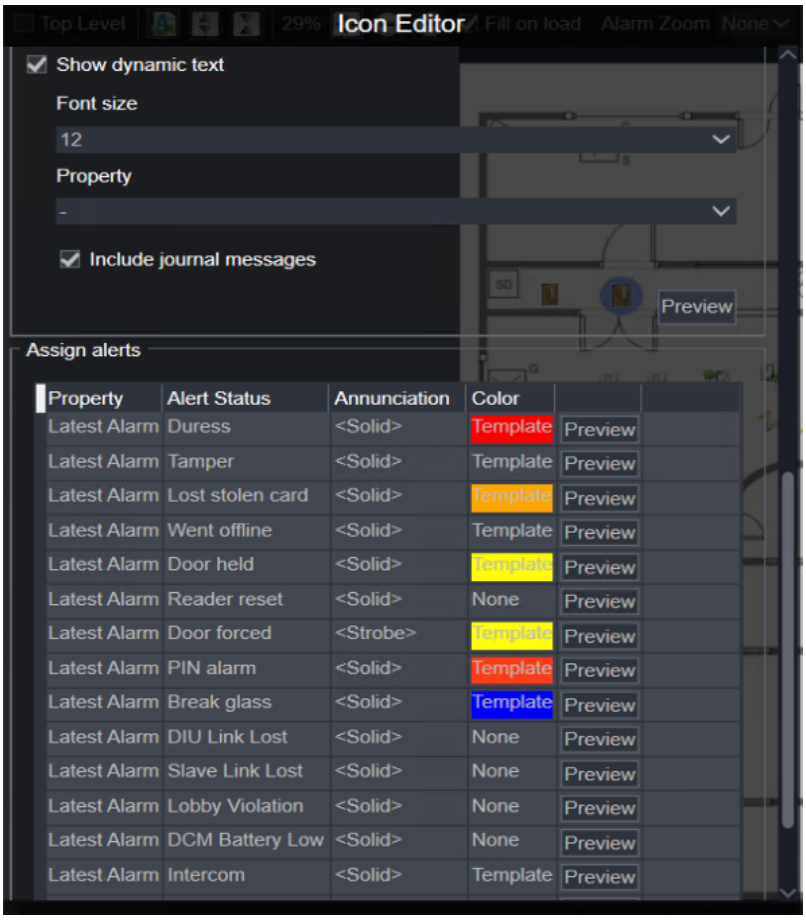
State	State Values
Latest Alarm	See List of supported Alarms in AC2000 Alarms type section

Door Reader State Images

State	Image
Door Forced	
Door Held Open	
Door Lock Engaged	
Door Other Alarm	
Default	

Door Alarm Type Annunciations

The Door Alarm Type can be displayed on the Map with the annunciation being set with the appropriate colors for the Duress- RED Lost/Stolen Card- Orange Door Forced- Yellow etc.



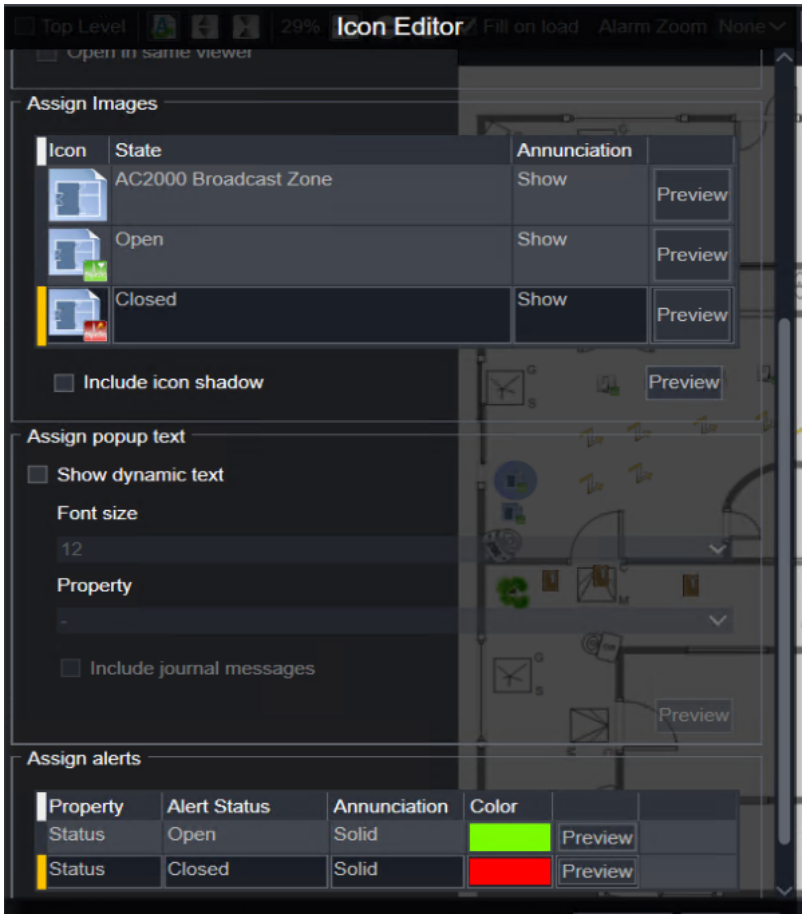
Broadcast Zone States

State	State Values
Latest Alarm	See List of supported Alarm types in AC2000 Alarms Type section
Status	Open Closed

Zone State Images

State	Image
Open	
Closed	
Default	

The broadcast zone state can be displayed on the Map with the annunciation being set to Red for Closed State and Green for Open.

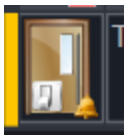


Input States

The Door Controller inputs can be monitored for any state change and subsequent Events can then be triggered as when required.

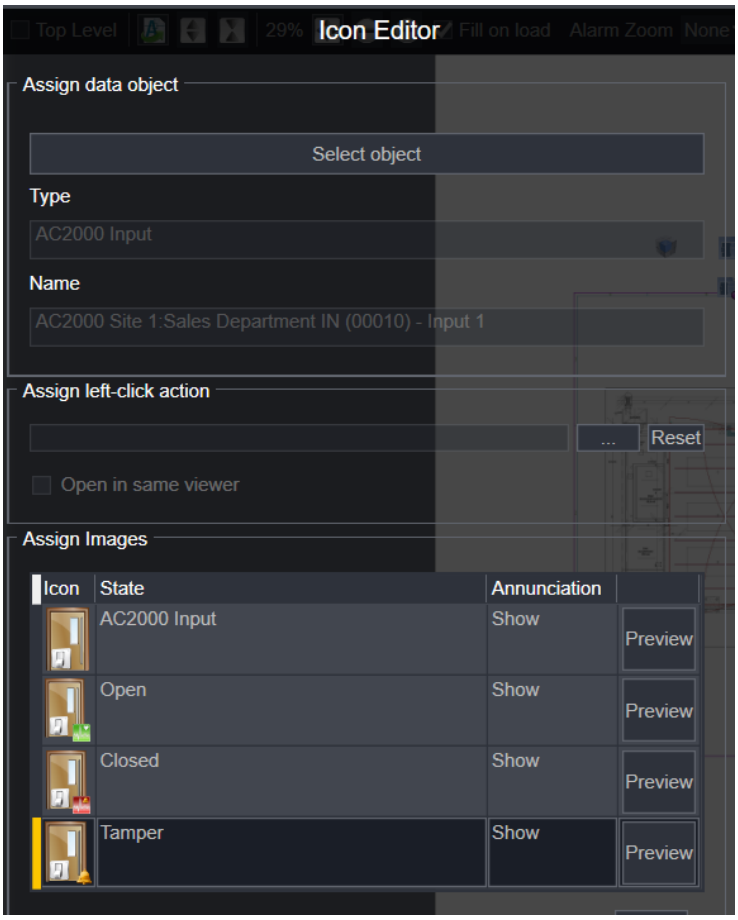
State	State Values
Latest Alarm	See List of supported Alarms in AC2000 Alarms Type section
Status	Open Closed Tamper (Note: This property is only updated when you synchronize devices)

Input State Images

State	Image
Open	
Closed	
Tamper	

Input Alarm Type Annunciations

The input Alarm Type can be displayed on the Map with the annunciation being set to RED for Closed State and Green for Open State and Orange for Tamper State.



Output States

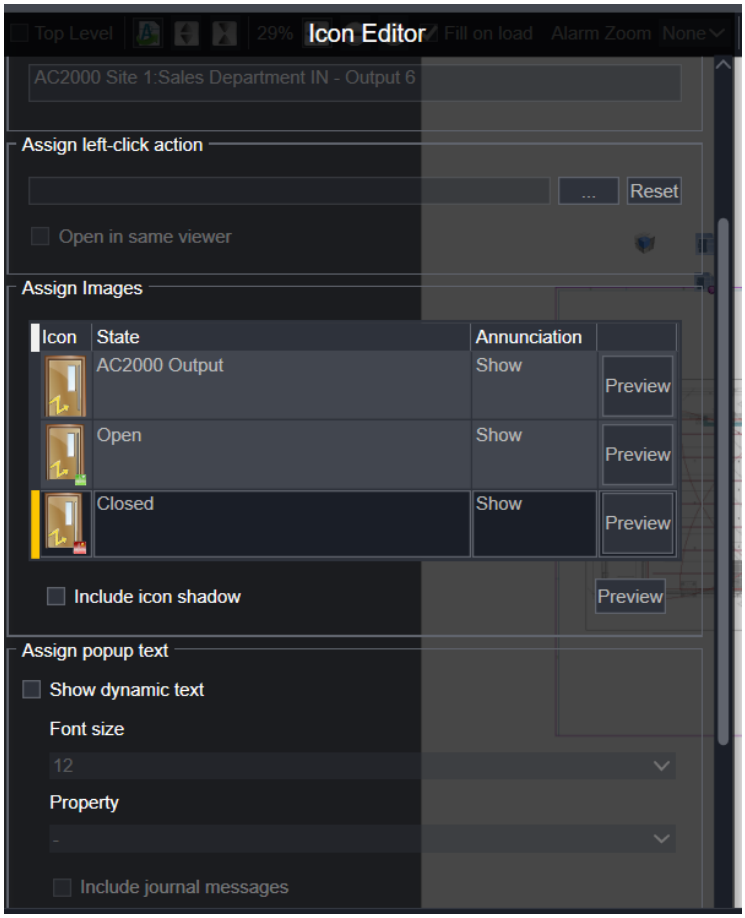
The Door Controller outputs can be monitored for any state change and subsequent Events can then be triggered as when required.

State	State Values
Latest Alarm	See List of supported Alarms in AC2000 Alarms Type section

Output State Images

State	Image
Open	
Closed	

The Door outputs are Dual State and can Display both the physical state and the Alarm type as can be seen on the Map with the annunciation Red/Green for Switch State and the Alarm Type with the previous template defined color.



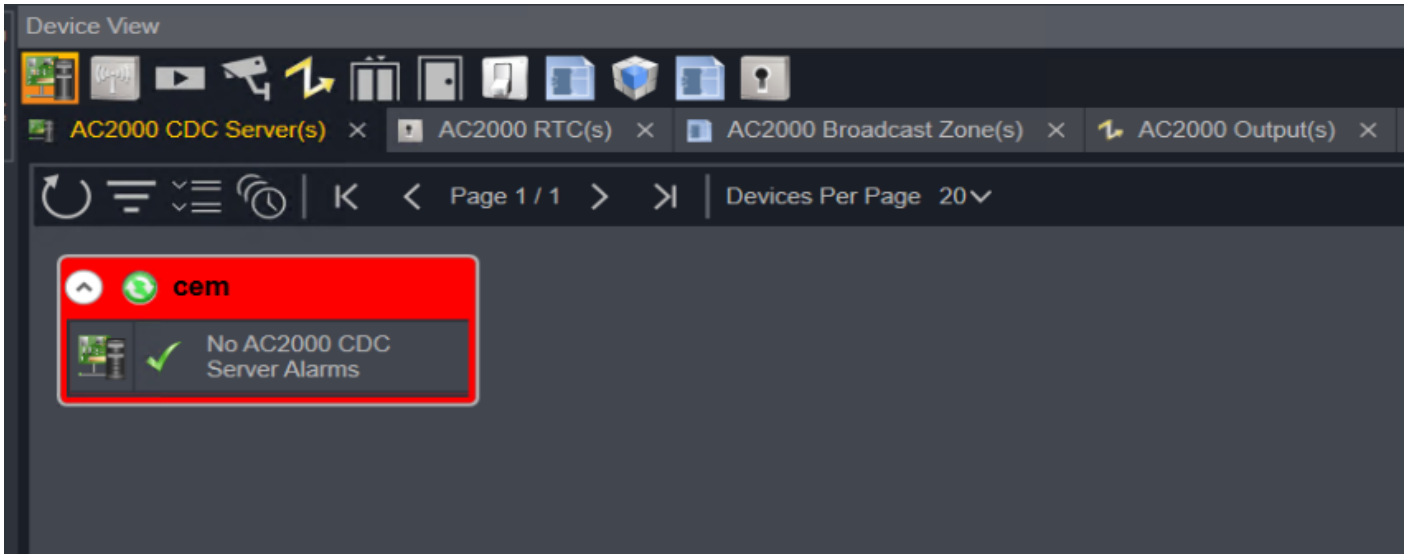
Introduction to Health Status

You can open the Health dashboard from the New Tab menu. From the Health dashboard you can monitor the status of the CDC AC2000 System. This includes Health status of the following:

- CDC Controllers
- Doors
- Inputs
- Outputs
- RTC's
- Broadcast Zones

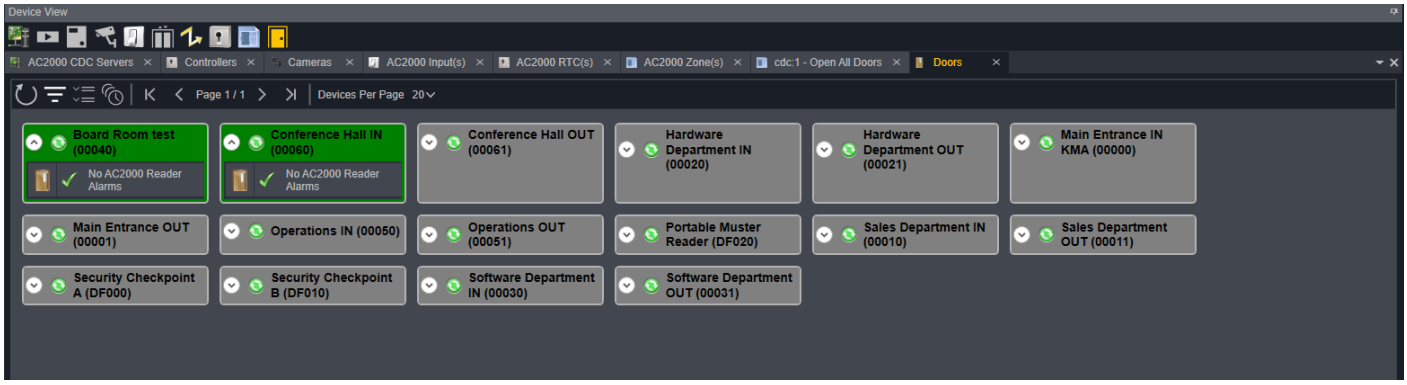
CDC Server Status

The CDC Server Status can be monitored for health and the overall status displayed for any alarms.

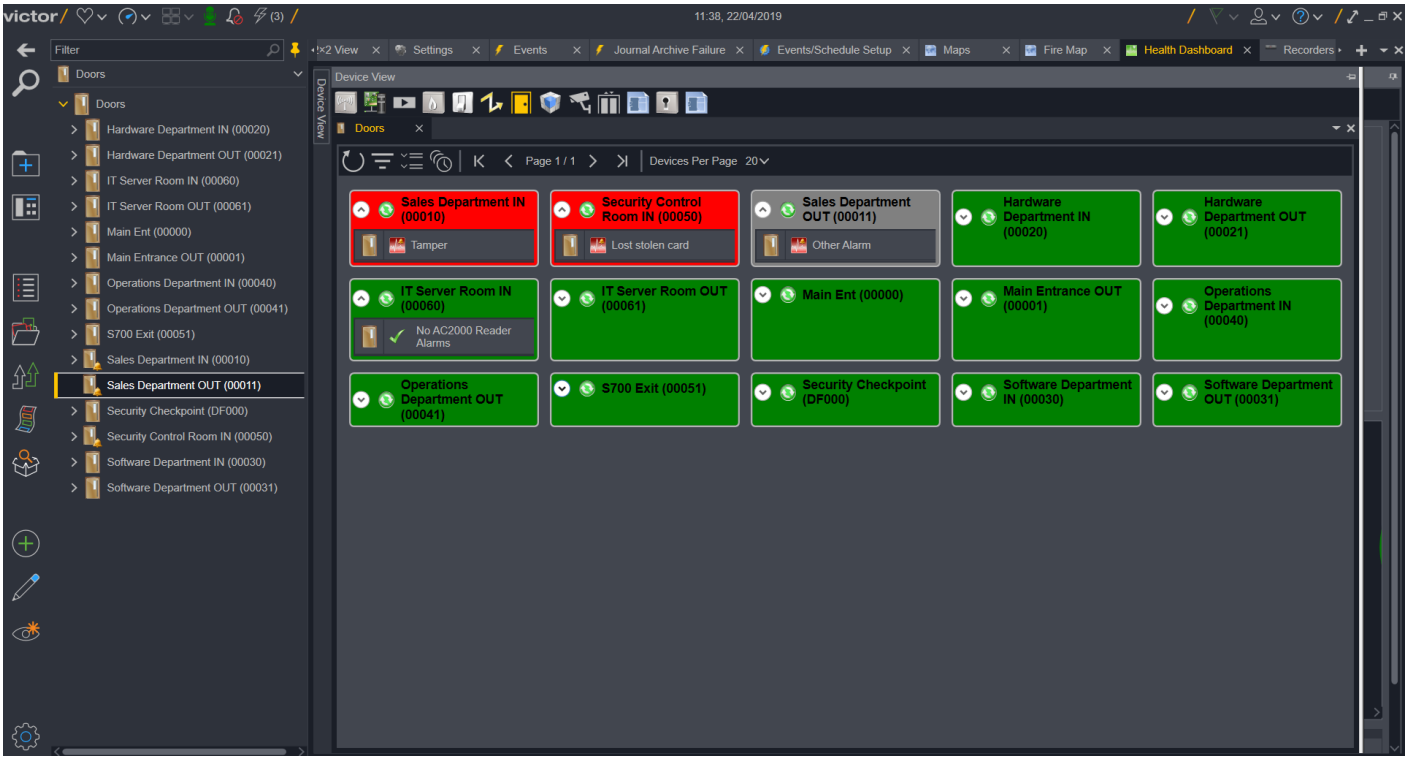


Door Health Status

The Door Status can be monitored for health and the overall status displayed for any alarms

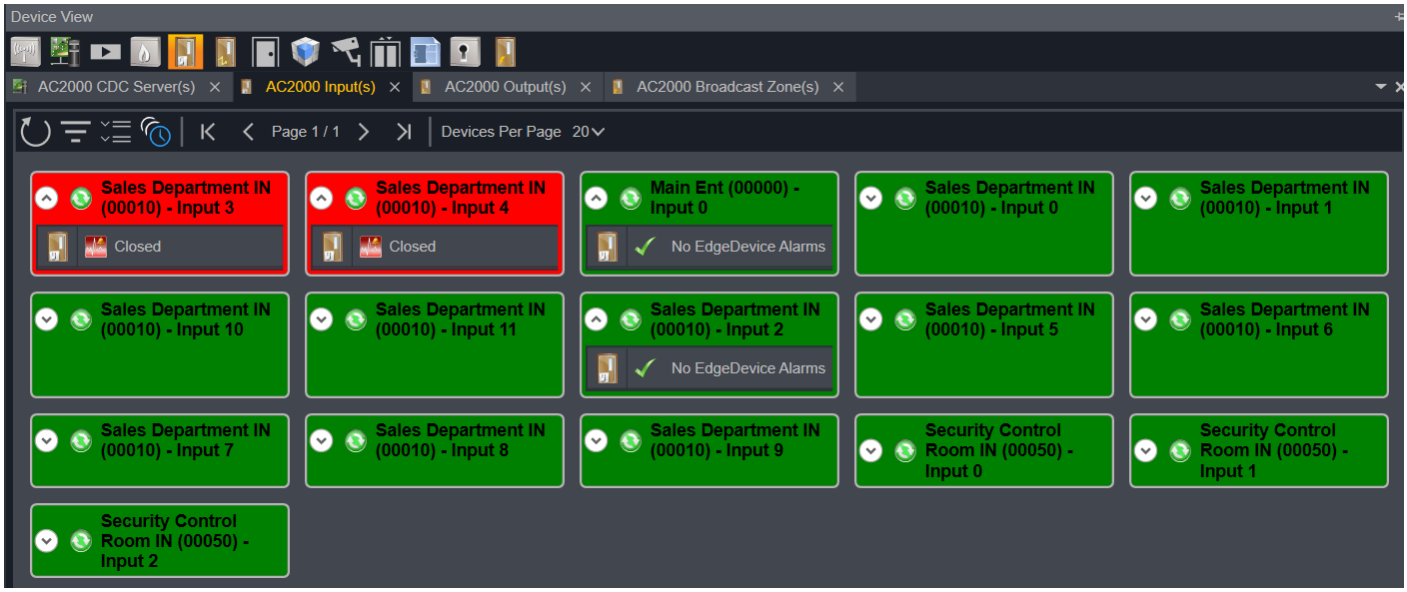


If any Alarms are triggered then they will appear as highlighted in Red along with the Alarm type as defined in the drop down box.



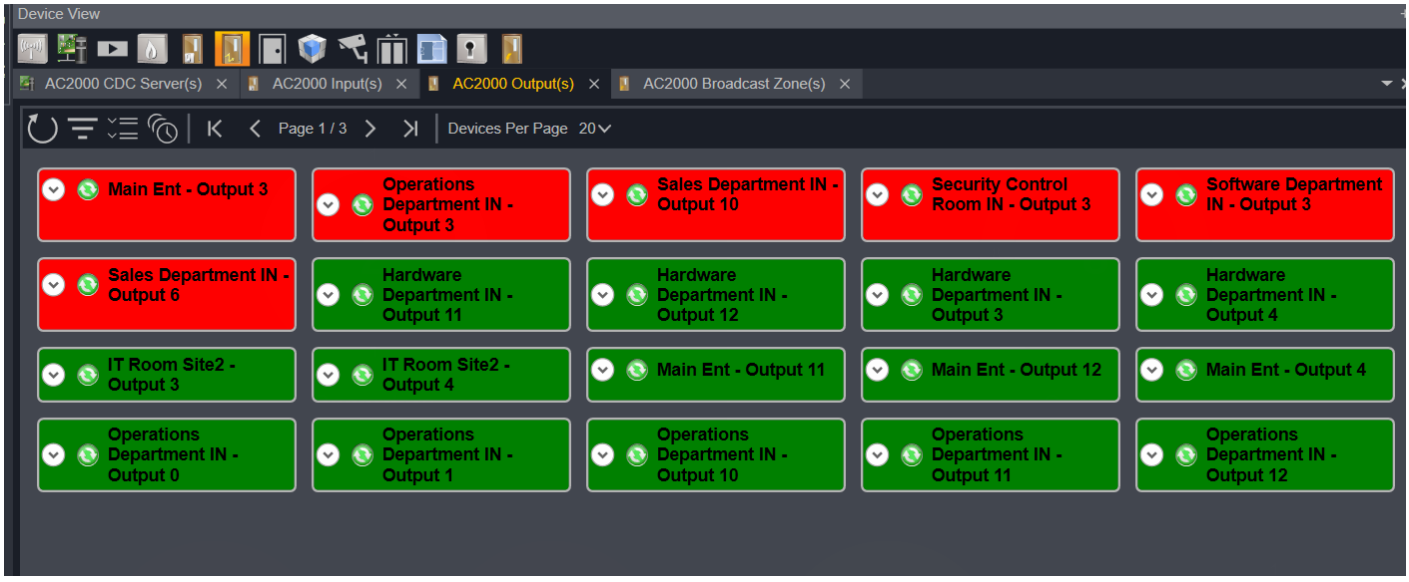
Input Health Status

The Door Inputs can be monitored for health and the overall status displayed for any alarms



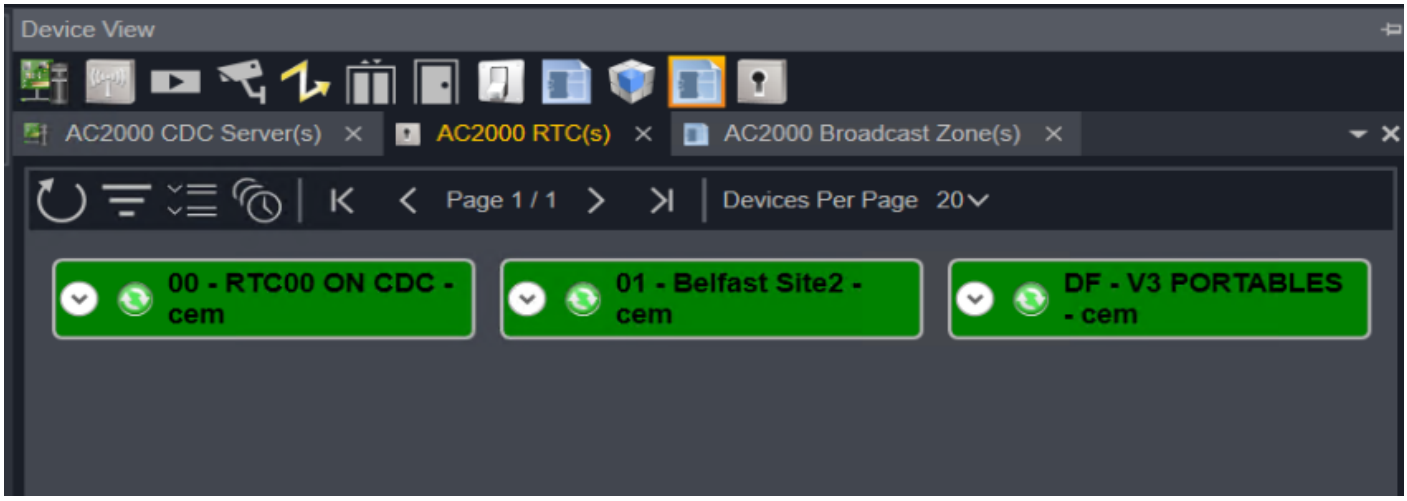
Output Health Status

The Door Outputs can be monitored for health and the overall status displayed for any alarms



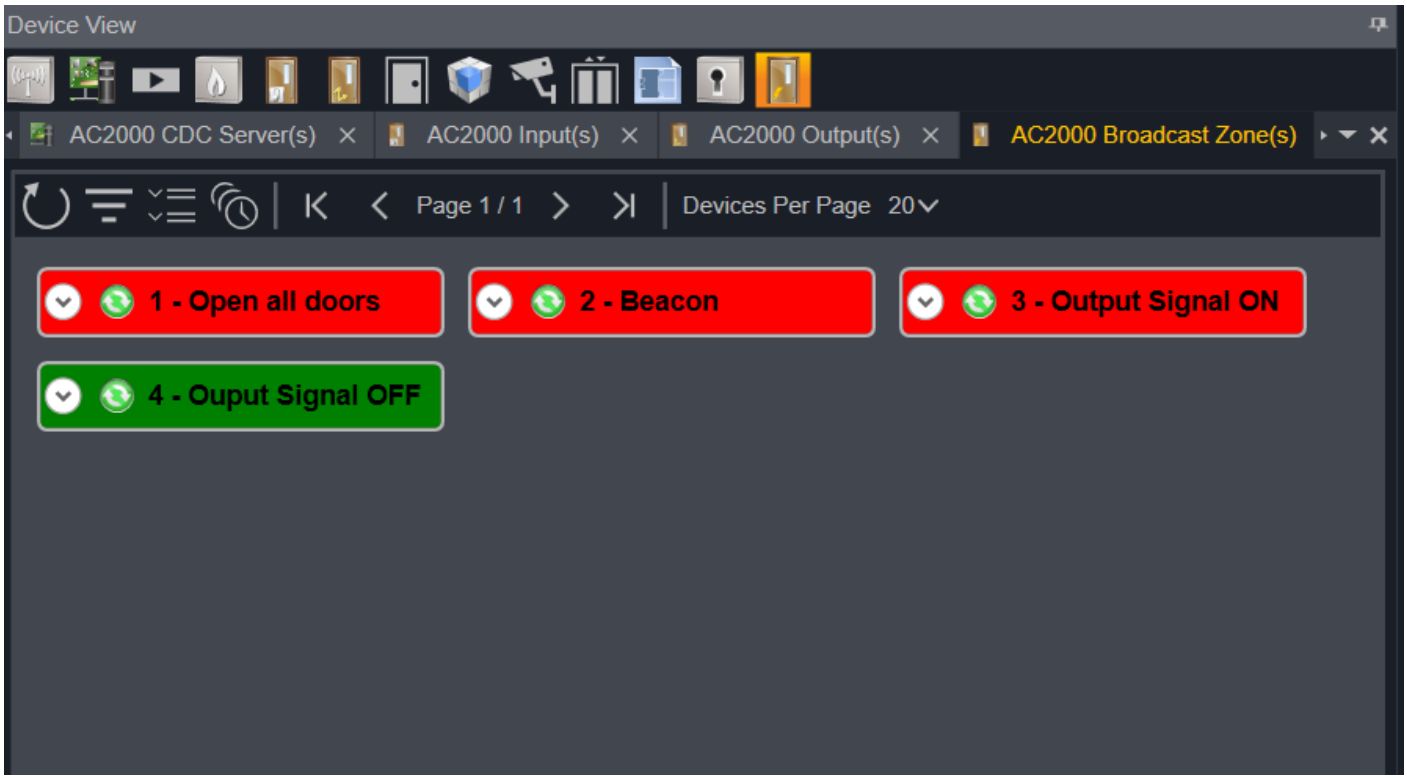
RTC Server Health Status

The RTC Server can be monitored for health and the overall status displayed for any alarms.



Broadcast Health Status

The Broadcast Zone can be monitored for health and the overall status displayed for any alarms.



Introduction to Maps

The Maps feature provides a dynamic view of physical security objects within a visual representation of their environment. Physical objects are represented by icons to form an integrated, unified view allowing monitoring and reaction to state changes in real time. You can also link map actions to events, to provide real-time visualization of event activity.

Supported Image files are:

- *.dwg / *.dxf (Vector)
- *.png / *.jpg (Raster)

Note:
• victor automatically converts vector graphics to .jpg and stores them in the database.
• CAD Layers: Only CAD Layers visible at the time of import are visible within the image in victor. However, once imported, new layers can be added to the converted CAD image and used to configure icons. The actual CAD layers do not exist in victor.
• Map Image files can be updated without disassociating the icons which were previously placed on the map.
• victor supports image files up to 20 MB

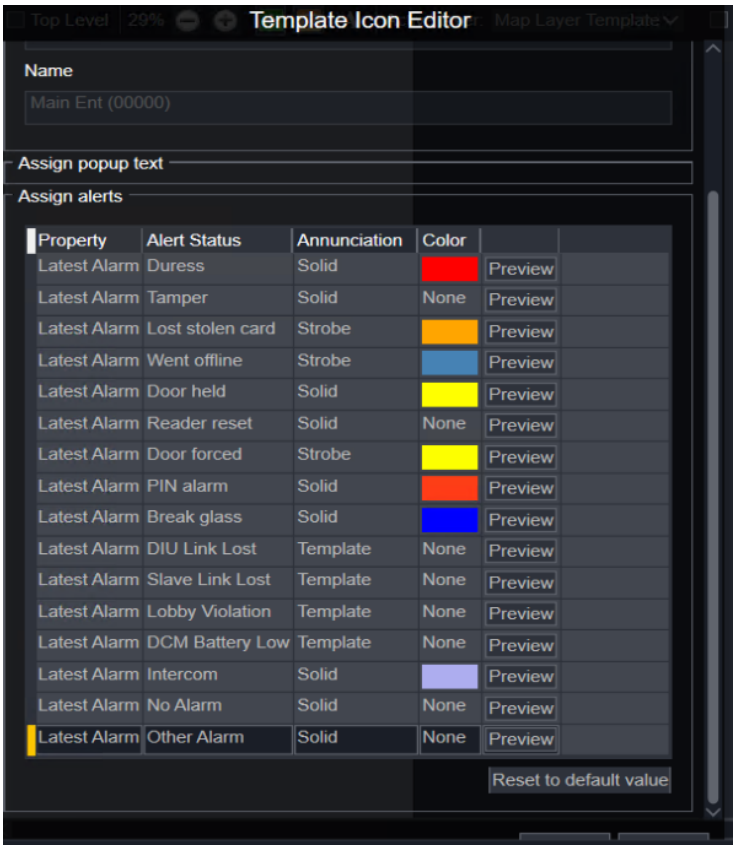
Map Template

Use the Map Template to create and configure template icons. Any icon created in the Map Template becomes a template for icons of the same type on all maps in your system. The annunciation and alert color settings from the template icon replace the default annunciation and alert color settings for new icons of that type added to any map.

Procedure 14 Configure a Template Icon

1. Select **Map** from the **Show All Items** tab.
2. Right-click the Map Template and select **Edit**.
3. In the Map editor, click 
4. From the **Icon Selector** menu, click an object icon to add that object to the map.
5. Right-click the icon and select **Drop on Map**.

   The Template Icon Editor opens.
6. Click **Select Object**.
7. Select an object from the list and click **OK**.
8. In the **Assign Alert** section, configure the icon's annunciation settings.



a Select the **Annunciation** type for an alert.

b In the **Color** cell, select **Custom** from the list.

c Select one of the following options:

- Select an alert color from the menu.
- Select **Advanced**, select a color from the advanced color menu, and then click **OK**.

Note:
Object annunciation and color settings are applied to new icons of the same type added to a map. Other template settings are not applied to new icons.

---

9 (Optional) Click **Reset to default value** to restore the default annunciation and color settings for the object.

10 Click **OK**.

11 Select **Save**.

Procedure 15 Importing a map image

A map image must be imported and the points added manually. Map image can be *.dwg / *.dxf (Vector) or *.png / *.jpg.

1 From the **Add New Item** tab, select **Map**.

2 Enter a name for the map in the **Name** textbox.

3 Enter a description for the map in the **Description** textbox.

4 The **Enabled** checkbox is selected by default, deselect to disable the map.

5 Select  - Browse window displays.

6 Browse to and select the required image file.

7 Select **Open**.

8 (CAD files only) To set a compression level for the file, enter **Height** and **Width** values.

9 Click **Import**. File imports and displays in map editor.

10 Select **Save**.

Add/Configure Icons

After you import an image to create a map, you can add icons to the map. Icons are added to maps to represent victor objects. Various icon properties can be configured depending on the object type they represent.

Procedure 16 Adding and configuring icons

1 Open the map in edit mode.

2 Select  . The icon selector displays.

3 Select the icon that you want to add to the map.

4 Move the icon to the required position on the map. Right-click the icon and select **Drop on Map**. The Icon Editor displays.

5 Select **Object**. The Object Selector will display.

6 Select the object to link to the icon and click **OK**.

Note:
If **Not in map** is selected in the Object Selector only items which have not yet been added to the map will be displayed. Clear this checkbox to display all items.

---

7 Select **OK**.

8 Assign characteristics in the Icon Editor if required.

9 Select **Save**.

Add/Configure icons Using Drag and Drop

Icons are added to maps to represent victor objects. Various icon properties can be configured depending on the object type they represent.

Procedure 17 Add and Configure Icons using drag and drop

1 Drag victor objects from the Devices list into the Map editor. An icon appears on the map, linked to the victor object.

Note:
You can also drag objects onto maps from Site lists, Call ups and Object lists.

---

2 Configure an icon's characteristics:

a Right-click the icon.

b Select **Edit**.

c Assign characteristics in the Icon Editor.

d Click **OK**.

3 Select **Save**.

Cloning icons

You can use an existing icon as a template from which to configure a new icon.

Procedure 18 Cloning an icon configuration

1 From the map editor, select the icon that you want to clone from.

2 Drag and drop a victor object from Device List. The icon (with original icons configuration) will be added to the map.

3 Right-click the new icon and edit as required.

Configuring areas

Procedure 19 Configure an Area

You can configure areas on victor Maps to group icons. If any icons related to an area go into Alert status, the entire area will highlight. This applies to icons where annunciation is set to Strobe, Pulse, Blink, Fade, Ripple, Wave or Flash.

1 From the Map editor, hold the Shift key and draw the required area using your mouse.

Note:
To access the Map editor, select **Maps** from the **Show All Items** tab, then selecting **Maps**. Right-click the map to be edited and select **Edit**.

2 Use the grab handles to manipulate the area.

3 You can further manipulate the drawn area can by right-clicking and selecting from:

- Select all related icons
- Clear all related icons
- Hide this shape drawing
- Remove this shape drawing
- Send to back
- Bring to front
- Display automatically when in view mode
- Priority Animation (select to alert the area with the highest priority alert from all objects within the area)

Polygon Shapes

A Polygon Shape can be added to a map icon placed onto another map to increase the annunciation area when the icon goes into alert (Strobe, Pulse, Blink, Fade, Ripple, Wave, Flash or Solid only). When the polygon shape goes into

alert, the entire alerting area can be selected, drilling down to the lower level map.

Procedure 20 Adding a polygon shape to a map

1 Configure an icon on a map.

2 Right-click the map icon, select **Polygon Shape**, and then click **Add**. Triangle displays.

3 The area can be manipulated by using the grab handles. Move and resize the triangle as required to represent the area covered by the detailed (building) map. Various right-click options are available for the shape including:

- Hide this shape drawing
- Remove this shape drawing
- Send to back
- Bring to front
- Display automatically when in view mode

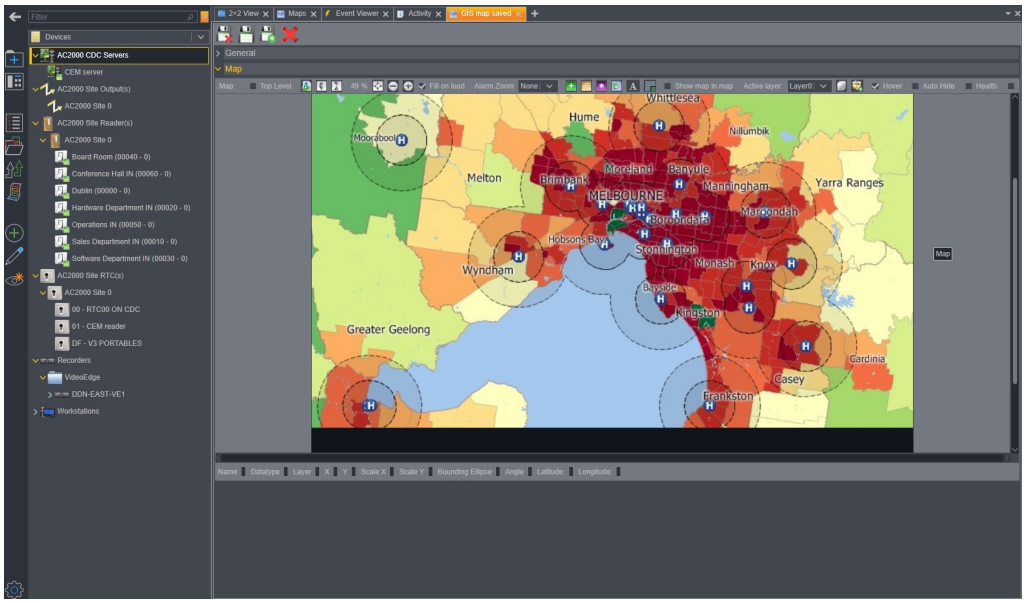
4 To add an additional grab handle, right-click an existing grab handle and select **Add New Point**. This will allow further manipulation of the shape of the Polygon Shape.

5 Select **Save**.

GIS Level Maps

GIS Level Maps can be used in a scenario where an overview of your facility or site is required. For example, a GIS Level Map could be used to show all buildings on a corporate campus, with each building being represented by an individual Map. Clicking on each building would 'drill down' to show an overview of that building with further 'drill down' to show each floor or area.

Selecting the GIS Level checkbox when creating a GIS Level Map will improve navigation performance by using caching to reduce load time.

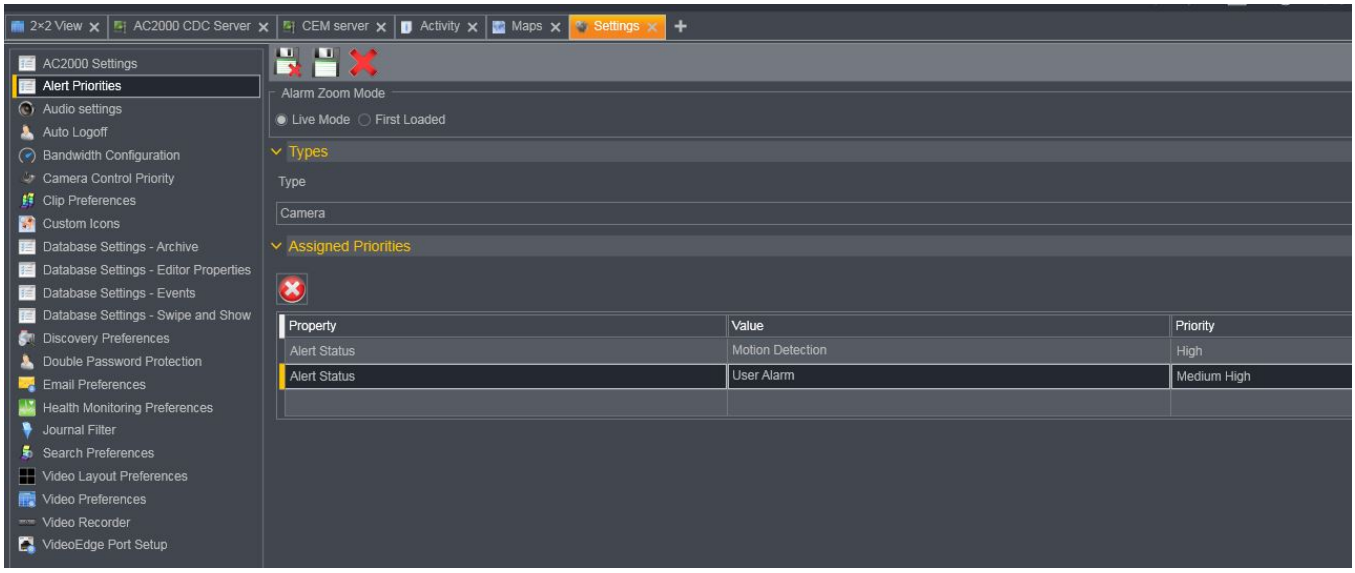


Alarm Zoom

When an object goes into alarm, it will annunciate based on configuration in the Icon Editor. The Alarm Zoom setting enables the Map to zoom to the alarming object. If Alert Priorities are configured (System Configuration > Settings > Alert Priorities), the Map will zoom to the current highest priority alarming object.

Select settings from the Alarm Zoom dropdown:

- None turns Alarm Zoom off
- High, Medium and Low sets the zoom level with high being the maximum zoom level and low the minimum.

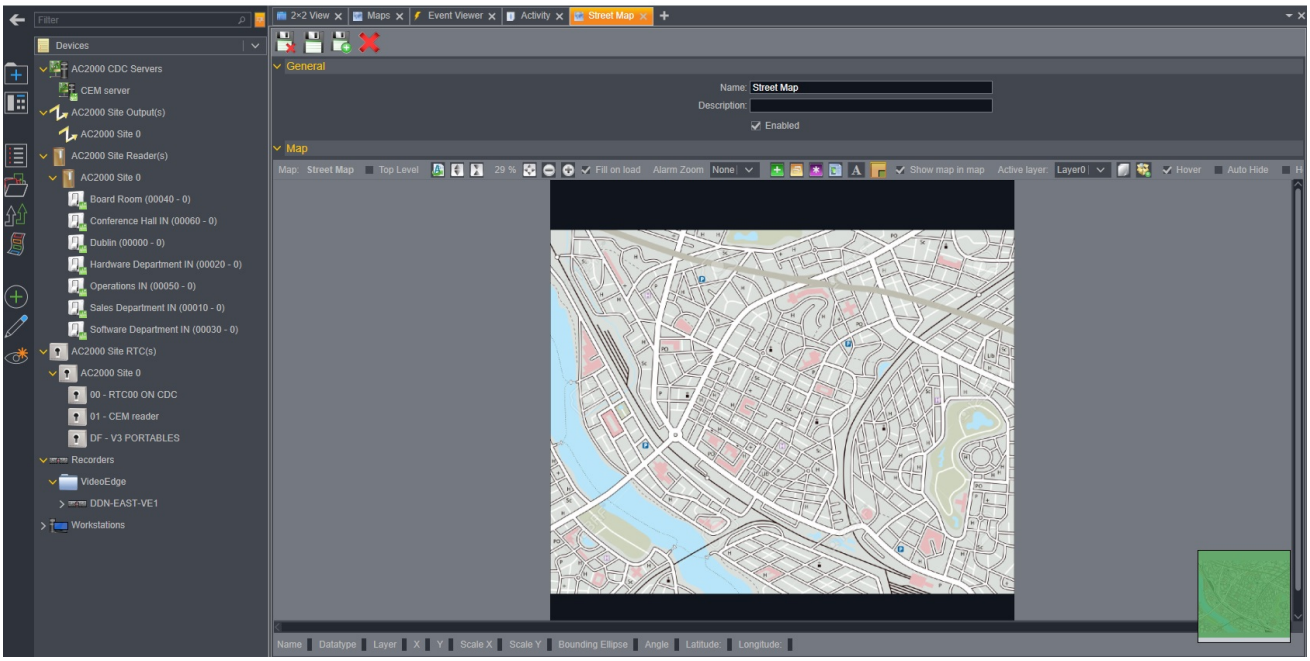


Live Mode vs. First Loaded

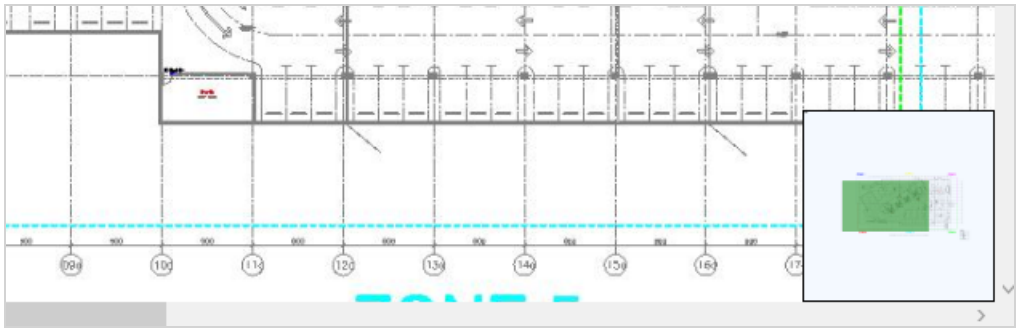
By default, the Alarm Zoom will zoom to the first or highest priority alarming object (First Loaded). System Values>Alert Priorities allows configuration of Live Mode which means the Map will zoom to all new alarms as they are activated.

Map in Map

Map in Map shows the current zoom level and position within a map. It can be toggled on or off using  in the Map toolbar. Default is off.



When creating/editing a Map, checking the Show Map in Map checkbox will show Map in Map by default for the current Map.



Viewing Maps

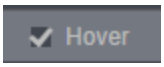
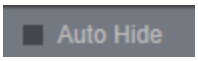
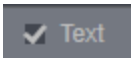
Once a map has been created and saved, it can be viewed directly from the Show All Items tab.

Procedure 21 View Maps

1 Select **Maps** from the **Show All Items** tab.

2 Select the map that you want to view.

3 Use the toolbar buttons to manipulate the map.

Element	Details
	Zoom controls - displays current zoom level percentage along with Fit to Window and Zoom Out/In buttons
	Hide Icon Types - opens the Hide Type editor which allows selection of icon types to hide, e.g. Cameras or Recorders
	Show All Icons from All Layers - shows and highlights all icons from all visible layers. Note: icons that are on layers that have been hidden using the Map Layers editor will not be displayed
	Show All Shapes from All Layers - shows all configured areas from all visible layers. Right-click to display FoV or Shapes only. Note: areas that are on layers that have been hidden using the Map Layers editor will not be displayed
	Activity List - opens a map specific Activity List that displays the 100 most recent activities relating to objects on the map. Icon will display with a red border when there are unread items in the Activity List. Right click and select Clear to clear the activity list. Select the padlock icon to freeze the Activity List for 30 seconds
	Show Map in Map - opens a Map in Map image in the bottom right of the Map Viewer, indicating current zoom level.
	Layers - opens Map Layers editor allowing selection of map layers to show/hide
	Save to Incident – Allows users to save map detail to an incident report.
	Hover Mode - select to enable hover mode. When enabled, hovering over objects will display additional information. For example, hovering over a camera will open a pop-up surveillance pane within the map view, displaying live video from the camera. Other cameras can be dragged and dropped into the pop-up windows
	Auto Hide- this works in conjunction with Hover Mode. When auto hide is enabled the surveillance pane will close automatically when the mouse is moved off the icon that initiated surveillance pane. If hover mode is disabled, auto close cannot be selected. This works in both edit and view mode.
	Health Mode - select to enable health mode. When enabled, icons will be highlighted with their health status. When enabled with hover mode, hovering over icons will display the objects health dashboard within the map view
	Show Text shapes - select to show all text shapes on the map. This option is selected by default.

Note:

• When viewing a map, the toolbar will display green. If the toolbar displays orange, this means that the map has been edited and saved since it was opened. Select  to update.

• When viewing a map, drag any icon onto any surveillance pane to view its associated video.

Editing Maps

Once a map has been created and saved, its properties can be edited.

Procedure 22 Edit Maps (Map)

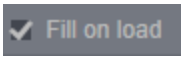
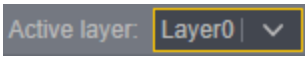
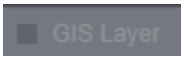
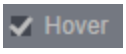
1 Select **Maps** from the **Show All Items** tab.

2 Right-click the map to be edited.

3 Select **Edit**. Map editor opens.

4 Edit the map **Name**, **Description**, and **Enabled** status as required.

5 Use the toolbar button to edit the map:

Element	Details
	Import a map - re import the map image
	Increase/Decrease height of map window
	Fill image in window - fit map to window
	Fill on load - when the map loads, fit map to window
	Add Object Icon - add an object icon to the map
	Copy Icon to Active Layer - copy an icon to the current active map layer
	Show all icons from all layers - displays all icons from all layers of the map
	Show all shapes from all layers - displays all shapes from all layers of the map. Right-click to display FoV or Shapes only
	Active layer - the current active map layer
	Add Text - Displays a field enabling free text input. Font size/colour/type can be changed as required. Text boxes can be copied to other areas of the map.
	Show Map in Map - opens a Map in Map image in the bottom right of the Map Viewer, indicating current zoom level.
	GIS Layers – Make this map a GIS Map.
	Hover - Enable/Disable hover in the map editor

6 Edit map elements as required

7 Select **Save**.

Procedure 23 Edit Maps (Map Icons)

Once an icon has been added to a map, its properties can be edited or copied to create a new map icon. Available options vary depending on map icon type.

1 Select **Maps** from the **Show All Items** tab.

2 Right-click the map to be edited.

3 Select **Edit**. Map editor opens.

4 Right-click the icon that you want to edit.

5 Select the required option from the contextual menu.

6 Edit the icon settings.

Note:
Selecting Copy from the right click menu will copy both the icon and all its properties (e.g. assigned object and assigned left click action)

7 Select **Save**.

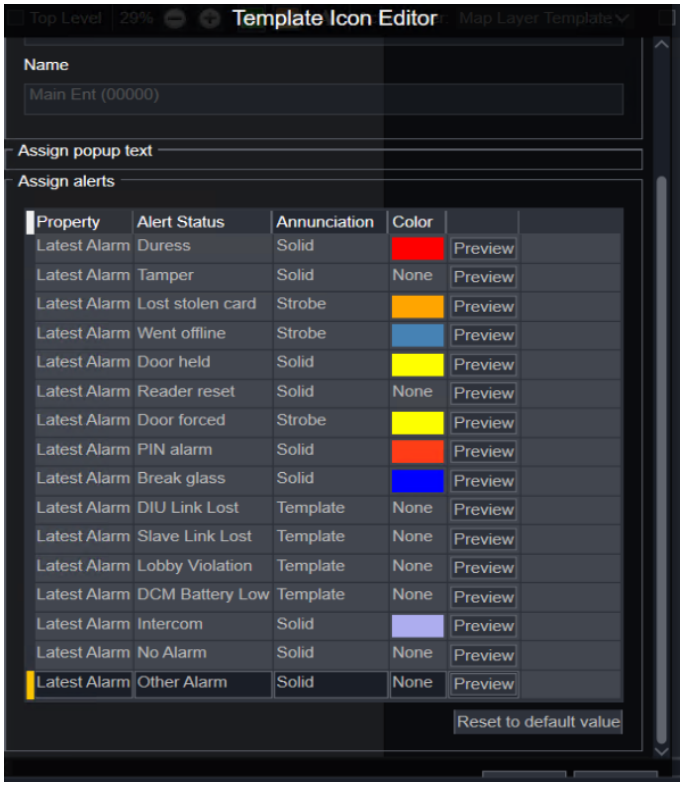
Creating a door map layout

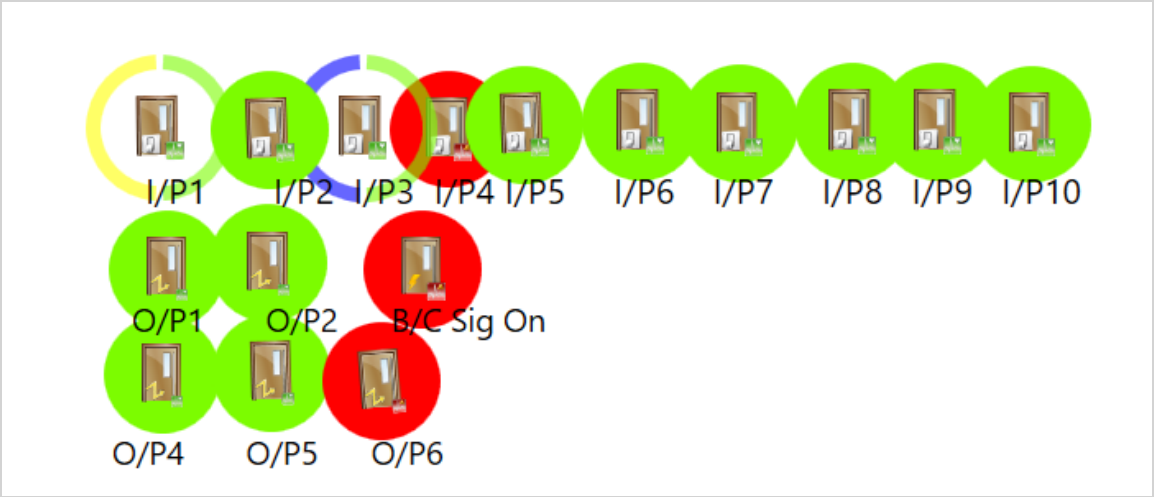
Upon creation of your Building Map which can have various Door Objects placed on it. The Door Inputs can show a dual state, an Alarm Type and a Physical switch state. For example, Open/Closed as can be seen in the Door Input for a Green Open State and Purple for Input Alarm Type = Panic if required

You can configure the different Door Color annunciations to identify different Alarm types.

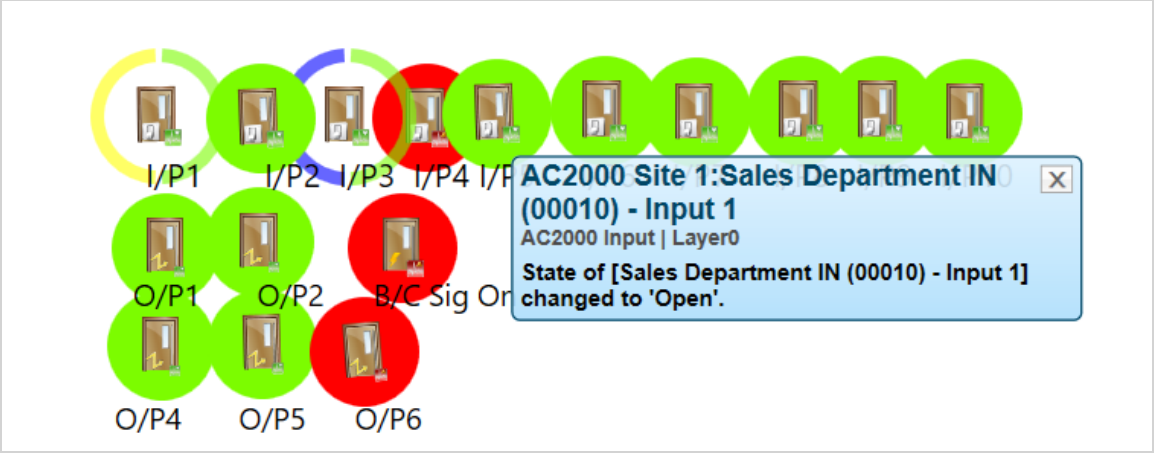
For example:

- Blue = Breaking Glass Alarm
- Yellow = Door Forced
- Purple = Intercom Call





The Door inputs and outputs can be displayed with the popup box Identification also displayed if required.



You can also add the broadcast action to the Map to identify the state of the Broadcast in the various Door Zones.

AC2000 Defined Alarm Types

The following CEM defined Alarm types are used by Victor. The Alarms are defined in four Owner groups. The Alarms can be triggered automatically by the system or manually by the various External states associated with the Inputs. This enhances the logic and complex Business needs to deliver a flexible Door and Building Management system.

- CDC - CDC system Alarms
- DEV- Internal system Alarm types
- EXT- External system Alarm types
- RTC- RTC System Alarm Types

Reserved Internal Input Alarms

Internal Input Alarms are alarms which are automatically generated by the CEM DCM 350 control board which are assigned to reserved Inputs addresses as defined below. Each of these alarms have been preconfigured by CEM Systems to be activated on particular internal events. For example the alarm Door Held; this alarm will be automatically generated by the system when a door which has been opened fails to close in the pre-defined period.

Input Address No	OPEN	CLOSE
5	Master Read head Power failed	Master Read head Power restored
6	DCM Battery Low	DCM Battery restored
7	Mains Power failed	Mains Power restored
D	Slave Read head Power failed	Slave Read head Power restored

CDC System Alarms

Alarm ID	Description	Auto/Manual	Priority	Owner
20	CDC went offline	A	0	CDC
49	System failed over	A	0	CDC
56	Replication failure	A	0	CDC
58	Backup failure	M	0	CDC
59	Park limit reached	M	0	CDC
60	CCTV conn failed	A	0	CDC
73	Split-brain	A	0	CDC
75	Account Locked	M	0	CDC
76	Heartbeat failure	A	0	CDC
84	Backup not copied	M	0	CDC
85	CCTV Service failed	A	0	CDC
87	Bad Shutdown	M	0	CDC

Alarm ID	Description	Auto/Manual	Priority	Owner
88	Disk failure(drbd)	A	0	CDC
90	Translog Big	A	0	CDC
92	System Restore	M	0	CDC
93	Translog too Big	A	0	CDC
300	dia_apms error	M	0	CDC
301	YVR Whitelist Abort	M	0	CDC
1301	Schindler offline	A	0	CDC
3200	Permaconn Offline	A	0	CDC
3202	Permaconn CMS Offln	A	0	CDC
3204	Permaconn Mains Fail	A	0	CDC
3206	Permaconn Batt Low	A	0	CDC
3208	Permaconn Tampered	A	0	CDC
3300	Lift System Offline	A	0	CDC
5501	OFSGMS Unreachable	A	0	CDC
5503	Identec Unreachable	A	0	CDC
5508	Tag not Validated	M	0	CDC
5510	Customs Msg Timeout	M	0	CDC
5512	Customs Unreachable	A	0	CDC
5514	KPIZGMS Offline	M	0	CDC
5516	CustVLP Unreachable	A	0	CDC

Internal System Alarms

Alarm ID	Description	Auto/Manual	Priority	Owner
0	Duress	M	0	DEV
1	Tamper	M	0	DEV
2	Lost/stolen card	M	0	DEV
5	Went offline	A	0	DEV
6	Door held	A	0	DEV
8	Shunt enabled	A	0	DEV
9	Shunt opened	A	0	DEV
14	Went on battery	A	0	DEV

Alarm ID	Description	Auto/Manual	Priority	Owner
16	Power tamper	M	0	DEV
18	Reader reset	M	0	DEV
31	Check-in enabled	A	0	DEV
33	Check-in equip fail	M	0	DEV
34	PIN alarm	M	0	DEV
39	Battery low	A	0	DEV
41	Lock failure	M	0	DEV
42	REX closed too long	A	0	DEV
44	DIU link lost	A	0	DEV
46	Slave link lost	A	0	DEV
48	Lobby violation	M	0	DEV
51	Special grant alarm	M	0	DEV
63	CCTV request	M	0	DEV
81	Soft Anti-passback	M	0	DEV
82	Intercom	A	0	DEV
95	SI whitelist access	M	0	DEV
120	Video Manual Rec	M	0	DEV
121	Video Analytics	M	0	DEV
122	Video Adv Motion	M	0	DEV
123	Video Light Change	M	0	DEV
124	Video Alarm Input	M	0	DEV
125	Video Perimeter	M	0	DEV
126	Video Motion	M	0	DEV
127	Video Loss	A	0	DEV
129	Network Loss	A	0	DEV
201	Tour started	M	0	DEV
202	Tour not started	M	0	DEV
203	Tour finished	M	0	DEV
204	Tour timed out	M	0	DEV
205	Tour broken	M	0	DEV
206	Tour suspended	M	0	DEV
207	Tour not resumed	M	0	DEV

Alarm ID	Description	Auto/Manual	Priority	Owner
208	Tour resumed	M	0	DEV
209	Tour continued	M	0	DEV
210	Tour early	M	0	DEV
211	Tour not finished	M	0	DEV
1000	Unknown Zone	M	0	DEV
1001	Movement/Vibration	M	0	DEV
1002	Threshold	M	0	DEV
1003	Stealth	M	0	DEV
1004	Fibre Break	M	0	DEV
1005	Unknown System	M	0	DEV
1006	Controller Shutdown	M	0	DEV
1007	Laser Off	M	0	DEV
1008	SOP Off	M	0	DEV
1009	FOSS Degraded	M	0	DEV
1010	Locator Fault	M	0	DEV
1011	Laser Temp Warning	M	0	DEV
1012	Laser Shutdown	M	0	DEV
1013	Loss Of Comms	M	0	DEV
1014	Channel Disabled	M	0	DEV
1015	Locator Disabled	M	0	DEV
1016	System Shutdown	M	0	DEV
1017	FFT Edit Mode	A	0	DEV
1019	Digital Input	M	0	DEV
1020	Intrusion	M	0	DEV
1021	OpticalPowerDegraded	M	0	DEV
1022	FFT Maintenance	M	0	DEV
1023	FFT SOP Alarm	M	0	DEV
1024	FFT System Error	M	0	DEV
1025	External Alarm Mask	M	0	DEV
1026	FFT Leak Alarm	M	0	DEV
1027	External Alarm	M	0	DEV
1028	Rdn.Group Degraded	M	0	DEV

Alarm ID	Description	Auto/Manual	Priority	Owner
1029	Rdn.Group Disabled	M	0	DEV
1030	Rdn.Group Alarm Mask	M	0	DEV
1031	Temp. Warning	M	0	DEV
1032	Temp. Shutdown	M	0	DEV
1033	FoTech Laser Off	M	0	DEV
1034	Power supply Degrade	M	0	DEV
1035	Mobile Alarm	M	0	DEV
1036	Mobile Alarm Mask	M	0	DEV
1037	FFT Walk	M	0	DEV
1038	FFT Vehicle	M	0	DEV
1039	FFT Digging	M	0	DEV
1040	FFT Mech Digging	M	0	DEV
1041	FFT Fence Climb	M	0	DEV
1042	FFT Fence Cut	M	0	DEV
1043	FFT Fence Disturbed	M	0	DEV
1044	FFT Heavy Equip	M	0	DEV
1045	FFT Generic Event	M	0	DEV
1046	FFT Train	M	0	DEV
1047	FFT Broken Rail	M	0	DEV
1048	FFT Flat Wheel	M	0	DEV
1049	FFT Gas Leak	M	0	DEV
1050	FFT Lid Lift	M	0	DEV
1051	FFT Rockfall	M	0	DEV
1052	FFT Theft	M	0	DEV
1060	Low Voltage	A	0	DEV
1062	Line Break	A	0	DEV
1064	Compromised	A	0	DEV
1066	Comms Failed	A	0	DEV
1068	Cell Alarm	A	0	DEV
1070	Cable A Fault	A	0	DEV
1072	Cable B Fault	A	0	DEV
1074	UIST Active	A	0	DEV

Alarm ID	Description	Auto/Manual	Priority	Owner
1077	Microwave Alarm	A	0	DEV
1079	Align Path Alarm	A	0	DEV
1081	Service Alarm	A	0	DEV
1083	Config out of Sync	A	0	DEV
1087	RPM Device Tamper	A	0	DEV
1200	ExpnCard Failure	A	0	DEV
1202	Station Alarm	A	0	DEV
1204	Invalid Door Code	M	0	DEV
1205	Door Ringing	M	0	DEV
1206	Intercom Line Fault	A	0	DEV
1209	SIP Call Recv	M	0	DEV
1210	SIP Call Busy	M	0	DEV
1211	SIP Call End	M	0	DEV
1250	Station No License	M	0	DEV
1251	Station Not Auth	M	0	DEV
1252	Station Board Issue	M	0	DEV
1253	Station Offline	A	0	DEV
1255	Node Offline	A	0	DEV
1257	No SDK Connection	M	0	DEV
3004	DSC PS Fire Key	M	0	DEV
3005	DSC PS Aux Key	M	0	DEV
3006	DSC PS Panic Key	M	0	DEV
3007	DSC PS Battery Low	A	0	DEV
3008	DSC PS A/C Off	A	0	DEV
3009	DSC PS Panel Offline	A	0	DEV
3110	Integra Offline	A	0	DEV
3302	Lift Car Alarm	A	0	DEV
3304	Lift Security Alarm	A	0	DEV
3400	Neo Unknown	A	0	DEV
3401	Neo Burglary	A	0	DEV
3402	Neo 24 Hr Super	A	0	DEV
3403	Neo Fire	A	0	DEV

Alarm ID	Description	Auto/Manual	Priority	Owner
3404	Neo Fire Super	A	0	DEV
3405	Neo CO	A	0	DEV
3406	Neo Gas	A	0	DEV
3407	Neo High Temp	A	0	DEV
3408	Neo Low Temp	A	0	DEV
3409	Neo Medical	A	0	DEV
3410	Neo Panic	A	0	DEV
3411	Neo Waterflow	A	0	DEV
3412	Neo Water Leak	A	0	DEV
3413	Neo Pendant	A	0	DEV
3414	Neo Tamper	A	0	DEV
3415	Neo RF Jam	A	0	DEV
3416	Neo HW Fault	A	0	DEV
3417	Neo Duress	A	0	DEV
3418	Neo Personal Emer	A	0	DEV
3419	Neo Hold-up	A	0	DEV
3420	Neo Sprinkler	A	0	DEV
3421	Neo Quick Bypass	A	0	DEV
3422	Neo General	A	0	DEV
3446	Neo Partition Armed	A	0	DEV
3448	Neo Panel Offline	A	0	DEV
4000	Fire Panel Alarm	M	0	DEV
4001	Fire Panel Fault	M	0	DEV
4002	Fire Panel Override	M	0	DEV
4003	Fire Panel OoS	M	0	DEV
4004	Fire Panel Day Mode	M	0	DEV
4005	Fire Panel Night Md	M	0	DEV
4006	Fire Panel Silenced	M	0	DEV
4007	Fire Panel Sounding	M	0	DEV
4008	Fire Sounders Silent	M	0	DEV
4009	Fire Sounders Active	M	0	DEV
4010	Fire Evacuation	M	0	DEV

Alarm ID	Description	Auto/Manual	Priority	Owner
4112	Simplex Cold Start	M	0	DEV
4113	Simplex Warm Start	M	0	DEV
4114	Simplex Offline	A	0	DEV
5000	Gen-Archive-Full	M	0	DEV
5001	Gen-Archive-NoWrite	M	0	DEV
5002	Gen-Archive-Load	M	0	DEV
5003	Gen-Archive-Stop	M	0	DEV
5004	Gen-Archive-Data	A	0	DEV
5006	Gen-VidSig-Noisy	M	0	DEV
5007	Gen-VidSig-Blurry	M	0	DEV
5008	Gen-VidSig-Global	M	0	DEV
5009	Video Bookmark	M	0	DEV
5010	Gen-Face-Detect	M	0	DEV
5013	Gen-Audio-Detect	M	0	DEV
5016	Gen-Object-Left	M	0	DEV
5017	Gen-Object-Removed	M	0	DEV
5050	Aime-Auto PTZ	M	0	DEV
5051	Aime-Video Unstable	M	0	DEV
5052	Aime-Item Moved	M	0	DEV
5053	Aime-Video Activity	M	0	DEV
5100	Not Responding	A	0	DEV
5102	Archive Unavailable	A	0	DEV
5104	Disabled	A	0	DEV
5106	External Event	M	0	DEV
5107	Output Deactivated	A	0	DEV
5109	Disk Space Low	M	0	DEV
5110	VID_SVR-ON MASTER	M	0	DEV
5111	VID_SVR-ON BACKUP	M	0	DEV
5112	VID_SVR-NORMAL	M	0	DEV
5113	Network Loss Second	A	0	DEV
5150	Passive IR Event	M	0	DEV
5151	Missing Config	A	0	DEV

Alarm ID	Description	Auto/Manual	Priority	Owner
5153	Camera Mic Event	M	0	DEV
5154	Camera Temp Event	M	0	DEV
5155	Camera Activity	M	0	DEV
5156	Time out of Sync	M	0	DEV
5500	CardSwipeTimeout	M	0	DEV
5505	Wrong Dev setup	M	0	DEV
5506	Wrong user setup	M	0	DEV
5507	Wrong veh setup	M	0	DEV
5509	OFS Response Timeout	M	0	DEV
5511	Missing Customs Msg	M	0	DEV
5515	GMS Resource Issue	M	0	DEV
5518	Swipe No RFID	M	0	DEV
5520	Banned Vehicle	M	0	DEV
5521	Unknown Vehicle	M	0	DEV
5703	Power failure	M	0	DEV
5707	Item undetectable	A	0	DEV
5708	No transaction	M	0	DEV
5709	Allowance exceeded	M	0	DEV
5710	Traka alarms full	M	0	DEV
5711	Traka trans full	M	0	DEV
5713	Unrec item removed	A	0	DEV
1000000	Unknown Card	M	0	DEV
1000001	Valid Card	M	0	DEV

External System Alarms

Alarm ID	Description	Auto/Manual	Priority	Owner
3	Input tamper	A	0	EXT
12	Lock not engaged	A	0	EXT
13	Panic	M	0	EXT
19	Door forced	M	0	EXT
30	General alarm	M	0	EXT
35	Break glass	M	0	EXT

Alarm ID	Description	Auto/Manual	Priority	Owner
36	Fire alarm	M	0	EXT
37	Power fail	A	0	EXT
40	DIU tamper	M	0	EXT
52	Head current limit	M	0	EXT
53	DCM Battery low	M	0	EXT
54	Panic exit request	M	0	EXT
55	Panic exit opened	M	0	EXT
64	SIA Tamper	A	0	EXT
66	SIA Holdup	A	0	EXT
68	SIA Panic	A	0	EXT
70	SIA Burglary	A	0	EXT
72	SIA/Galaxy	M	0	EXT
1085	Sup Input Alarm	A	0	EXT
1208	SIP Call	M	0	EXT
3000	DSC PS Zone Alarm	A	0	EXT
3001	DSC PS Zone Tamper	A	0	EXT
3002	DSC PS Zone Fault	A	0	EXT
3003	DSC PS Duress Alarm	M	0	EXT
3100	Zone Violation	A	0	EXT
3101	Zone Tamper	A	0	EXT
3102	Zone Alarm	A	0	EXT
3103	Zone Bypass	A	0	EXT
3104	Partition Armed	A	0	EXT
3423	Neo Zone Unknown	A	0	EXT
3424	Neo Zone Burglary	A	0	EXT
3425	Neo Zone 24 Hr Super	A	0	EXT
3426	Neo Zone Fire	A	0	EXT
3427	Neo Zone Fire Super	A	0	EXT
3428	Neo Zone CO	A	0	EXT
3429	Neo Zone Gas	A	0	EXT
3430	Neo Zone High Temp	A	0	EXT
3431	Neo Zone Low Temp	A	0	EXT

Alarm ID	Description	Auto/Manual	Priority	Owner
3432	Neo Zone Medical	A	0	EXT
3433	Neo Zone Panic	A	0	EXT
3434	Neo Zone Waterflow	A	0	EXT
3435	Neo Zone Water Leak	A	0	EXT
3436	Neo Zone Pendant	A	0	EXT
3437	Neo Zone Tamper	A	0	EXT
3438	Neo Zone RF Jam	A	0	EXT
3439	Neo Zone HW Fault	A	0	EXT
3440	Neo Zone Duress	A	0	EXT
3441	Neo Zone Pers Emer	A	0	EXT
3442	Neo Zone Hold-up	A	0	EXT
3443	Neo Zone Sprinkler	A	0	EXT
3444	Neo Zone Quik Bypass	A	0	EXT
3445	Neo Zone General	A	0	EXT
3447	Neo Zone Open	A	0	EXT
3449	Neo Zone Bypassed	M	0	EXT
3499	Neo Zone Unbypass	M	0	EXT
4011	Fire Zone Alarm	M	0	EXT
4012	Fire Zone Fault	M	0	EXT
4013	Fire Zone Override	M	0	EXT
4014	Fire Zone OoS	M	0	EXT
4015	Fire Point Alarm	M	0	EXT
4016	Fire Point Fault	M	0	EXT
4017	Fire Point Override	M	0	EXT
4018	Fire Point OoS	M	0	EXT
4100	Simplex Fire Alarm	A	0	EXT
4102	Simplex Pri2 Alarm	A	0	EXT
4104	Simplex Supv Alarm	A	0	EXT
4106	Simplex Ctrl Alarm	A	0	EXT
4108	Simplex Utility Alm	A	0	EXT
4110	Simplex Trouble	A	0	EXT
5700	Wrong slot	A	0	EXT

Alarm ID	Description	Auto/Manual	Priority	Owner
5702	Unauthorised return	M	0	EXT
5704	Unauth item taken	M	0	EXT
5705	Res item taken	M	0	EXT
5706	Emergency release	M	0	EXT
5714	Remote release	M	0	EXT
5716	Item overdue	A	0	EXT
5718	Illegal handover	M	0	EXT
5719	Item rem manually	M	0	EXT
5720	Res item not taken	M	0	EXT
5721	Illegal key removed	M	0	EXT
1000002	Key switch Active	M	0	EXT

RTC System Alarms

Alarm ID	Description	Auto/Manual	Priority	Owner
27	NCN tamper	M	0	NCN
28	NCN went on battery	A	0	NCN
79	NCN went offline	A	0	NCN
22	RTC tamper	M	0	RTC
24	RTC went offline	A	0	RTC
25	RTC went on battery	A	0	RTC
1101	Visiowave offline	A	0	RTC