

# Crisis Mode / Emergency Management QRG

- Crisis Mode / Emergency Management .....2
  - Administrative Policies and Procedures .....2
  - What is Crisis Mode .....2
  - How does Crisis Mode Work.....2
- Configuring Crisis Mode.....3
  - Designating a Schedule for Crisis Mode Usage.....3
  - Creating a Crisis Mode I/O Group - Quick Steps .....4
  - Assigning a Crisis-Mode IO Group to a Loop/Cluster - Quick Steps.....5
  - Assigning a Crisis Mode Schedule to an Access Group - Quick Steps .....6
  - Assigning a 'Crisis-Mode-enabled' Access Group to a Cardholder - Quick Steps .....7
  - Assigning a Crisis-Mode to a Door - Quick Steps .....8
- Activating & Resetting Crisis Mode .....9
  - Managing Crisis Mode via Toolbar Buttons .....9
  - Managing Crisis Mode via Loop/Cluster Diagnostics.....10
  - Managing Crisis Mode using an Input with Crisis Mode IO Group .....11

# Crisis Mode / Emergency Management

This guide describes how to configure the *Crisis Mode feature* to operate during a predetermined emergency.

## Administrative Policies and Procedures

The System Galaxy software does not dictate what determines a crisis, nor constrain how crisis mode feature is applied to hardware or credentials. It is the responsibility of the system owner to establish the definition of a crisis and to predetermine how the system hardware and credentials will operate – for example which doors/entry points will lock or unlock, and how credentials will be affected (grant or deny access).

## What is Crisis Mode

**Crisis Mode** is a system-wide *access control feature* that changes some or all of the **access rules** during a crisis situation (e.g., system lock-down), based on predetermined configuration. Crisis mode changes the behavior of the hardware and access credentials by changing which access rules are applied during the emergency.

## How does Crisis Mode Work

When **Crisis Mode** is activated, the access control system will automatically change the *system hardware* and the *access credentials* to use the preconfigured '*Crisis Mode Rules*'. **Crisis Mode** uses unique schedules/rules to control the *hardware* and *credentials* in a specific way during a crisis. The system operator will activate crisis mode. Crisis Mode Rules remain in effect while *Crisis Mode* is active. When crisis mode is reset, the *hardware* and *access credentials* will return to normal operating rules.



**Access Rules** use schedules to control how the *system hardware* and users' *access credentials* will work during normal operation.

- lock/unlock doors and access points.
- activate/deactivate inputs, outputs, or other devices.
- grant/deny cardholder access or exit to a door, entry point, or area.



**Crisis Mode Rules** are separate access rules that are applied to hardware and credentials only while Crisis Mode is activated or engaged. These crisis rules can be assigned to *some* or *all* of the hardware and credentials, based on administrative planning/policies.

# Configuring Crisis Mode

To configure Crisis Mode, you must identify the specific *Crisis Mode Time Schedules* you need. Then you will assign them to the cardholder *Access Groups* and system *I/O Groups* and *Door Schedules* you want to apply the Crisis Mode Schedules to. When crisis mode is activated, the system will switch to the crisis mode schedules that are applied throughout your system programming. Be aware that schedules, access groups, i/o groups are managed by Loop/Cluster.

1. **Identify the Crisis Mode Schedule(s)** – like “Never” or “Always” or a Custom Crisis Mode Schedule.
2. **Assign the Crisis Schedule** to an Access Group, I/O Group, or Door in the software screens.
3. **Assign the Crisis Group** – such as Access Group, Crisis I/O Group to the Crisis Mode Droplist in the appropriate screens – such as Loop/Cluster, to I/O Group, Access Group, as needed.
4. **Activate/Reset the Crisis Mode** operation to ensure the system will behave as you intended when crisis mode is engaged. Also verify that the system returns to normal operation when crisis mode is reset.

## Designating a Schedule for Crisis Mode Usage

Schedules are created by Loop/Cluster.

You can use the **fixed schedules** (“always” & “never”), or you can create a **custom crisis mode schedule**.



**Fixed Schedule:** a system-default schedule whose time-intervals cannot be changed/edited. System Galaxy has 2 fixed schedules per Loop/Cluster, called “Never” and “Always”.

- “Always” schedule: a 24-hour time-period where all (15-min.) time-intervals are active.
- “Never” schedule: a 24-hour time-period where all (15-min.) time-intervals are inactive.



**Custom Schedule:** a user-defined schedule whose time-intervals can be changed (active/inactive). System Galaxy supports up to **254 custom schedules** per Loop/Cluster.

- **Schedule:** a 24-hour time-period that is divided into 15-minute time-intervals\* which can be set to active or inactive.
- **Custom Schedule (Normal):** a user-defined combination of active and inactive time-intervals; used for normal operation.
- **Custom Crisis Mode Schedule:** user-defined combination of active and inactive time-intervals; used only for crisis mode.



### Do Not Mix/Reuse a *Normal Custom Schedule* with a *Crisis Mode Schedule* ...

If you need a **Custom Crisis Mode Schedule**, you should name/designate it for “crisis mode” and document where you are using it. Do not reuse/borrow a *custom schedule* that is created for *normal operation* in the system, because when someone alters the normal operation, the crisis mode will be adversely affected.

## Creating a Crisis Mode I/O Group - Quick Steps

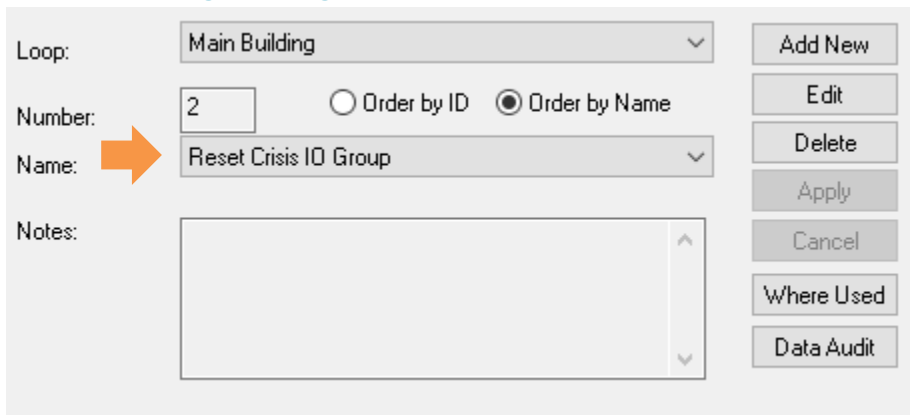
You need a Crisis Mode IO Group and a Crisis Mode Reset IO Group if you are going to implement controls through inputs and outputs. An IO Group links the hardware Inputs and Outputs through the software programming. Crisis Mode IO Groups are the same – they link inputs and outputs together that are specifically designated for managing Crisis Mode.

Crisis I/O Groups are created on a Cluster-by-Cluster basis. They are assigned in the Loop/Cluster Programming screen.

Open the *IO Groups screen* from the menu: [Configure > Hardware > I/O Groups](#)

1. Choose a *Cluster Name* from the [Loop] droplist.
2. Click Add New button.
3. Enter a name that distinguishes this as the Crisis Mode IO Group
4. Click **Apply** to save.

### I/O Groups Programming screen



The screenshot displays the I/O Groups Programming screen. On the left, there are four fields: 'Loop:' with a dropdown menu set to 'Main Building'; 'Number:' with a text input containing '2'; 'Name:' with a dropdown menu set to 'Reset Crisis IO Group' and an orange arrow pointing to it; and 'Notes:' with a large empty text area. On the right side, there is a vertical stack of buttons: 'Add New', 'Edit', 'Delete', 'Apply', 'Cancel', 'Where Used', and 'Data Audit'.

## Assigning a Crisis-Mode IO Group to a Loop/Cluster - Quick Steps

When Crisis Mode is active, the Cluster will use the **Crisis Mode IO Group**. When crisis mode is reset, the Cluster will return to using the **Reset Crisis Mode IO Group**. Behavior of inputs and outputs are based on programming.

Open the **Loop/Cluster Properties** screen from the menu: [Configure > Hardware > Loop/Cluster](#)

1. Optionally, from the *Hardware Tree* you can right-click on the **Loop/Cluster branch** and select the *Properties* option from the shortcut menu.
2. Click **Edit** and select the *Card Settings Tab*,
3. Set the **[Activate Crisis Mode IO Group]** droplist to your Crisis Mode IO Group.
4. set the **[Reset Crisis Mode IO Group]** droplist to your Reset Crisis Mode IO Group
5. Click **APPLY** to save changes.

### Loop/Cluster Programming screen

The screenshot shows the 'Loop/Cluster Programming screen' with the 'Card Settings' tab selected. The interface includes several configuration sections:

- ABA Options:** Start digit: 1, Stop digit: 60, Encode long codes:
- Reader Disable Options:** Disable after # of invalid attempts: 0, Min:Sec: 0:0, Disable reader for: 0:0
- Wiegand Options:** Start Bit: 0, Stop Bit: 255
- Cardax Options:** Start Bit: 34, Stop Bit: 59

The 'Activate Crisis Mode I/O Group' and 'Reset Crisis Mode I/O Group (635 Panels)' dropdown menus are highlighted with an orange box. The 'Activate Crisis Mode I/O Group' dropdown is set to 'Crisis IO Group', and the 'Reset Crisis Mode I/O Group (635 Panels)' dropdown is set to 'Reset Crisis IO Group'. An orange arrow points to the 'Card Settings' tab.

## Assigning a Crisis Mode Schedule to an Access Group - Quick Steps

Open the **Access Groups** screen from the menu: **Configure > Cards > Access Groups**

5. Choose a *Cluster Name* from the [Loop] droplist.
6. **Select your Access Group ...**
  - a) Choose an existing *Access Group* and click [Edit] button.  
~ OR ~
  - b) Click the [Add New] button and enter (type) a name for your new Access Group.
7. In the **Crisis Mode droplist**, choose from one of the following ...
  - To restrict access during Crisis Mode = set to "NO ACCESS" (system default Access Group)
  - For unrestricted access during Crisis Mode = set to "UNLIMITED ACCESS" (system default Access Group)



NOTICE: **Crisis Mode** is a "Latching" setting which means the system hardware will remain in Crisis Mode even after the triggering condition has ceased. **Crisis Mode** must be reset manually by issuing an Operator command from the SG Toolbar (green button), or by resetting the affected controllers from the Loop Diagnostics screen.

8. (optional) Configure the Activation & Expiration Date/Time – as needed.
9. On the *Access Privileges* tab, configure the normal Access Privileges as follows ...

*You can move one door at a time and link the desired schedule, or move some (or all) of the doors at the same time and link the same schedule. Use Shift+Click to choose multiple doors at the same time, then click the arrow button to move them.*

  - a) Move the desired doors into the "Authorized Readers" List
  - b) When prompted, select the desired Schedule for the selected doors for normal operation.  
(This designates the doors and times a cardholder will have normal access once this access group is assigned on the Card Settings tab of the Cardholder screen.)
  - c) When the doors are added to the "Authorized" List, the schedule names will be displayed. You can change which schedule is assigned by clicking on the *Schedule Name* in the list area.
10. Click [Apply] to save the Access Group on the selected Loop/Cluster.

### Access Groups Programming screen

Unauthorized for Readers	Authorized for Readers	Time Schedule
Test Room - prox Brd: 1, Sect: 1-0	LAB ENTRY : Brd: 1, Sect: 2	ALWAYS

## Assigning a 'Crisis-Mode-enabled' Access Group to a Cardholder - Quick Steps



NOTICE: If you already have Cardholders programmed with Access Groups, simply add Crisis Mode to the Access Groups that are already in use, by editing the Access Group Properties (screen).

Open the **Cardholder** screen from the menu: [Configure](#) > [Cards](#) > [Cardholders](#)

### 1. Select a Cardholder ...

a) Choose an existing *Cardholder Name* and click **[Edit]** button.  
~ **OR** ~

b) Click the **[Add New]** and enter (type) a name for your new Cardholder.  
You need to enter a first and last name. Add any other data and photo, etc - as needed

2. Select the *Card/Badge Settings Tab* and enter any card data - as needed.

### 3. On the *Loop/Cluster Settings Tab*, do the following ...

a) Click **[Edit Loops]** button and choose/add the desired Cluster(s).

b) Select the *Cluster Name* in the [Authorized Loops] droplist

c) Select (assign) the **Access Group** that contains the desired crisis mode programming.

*The crisis mode rules assigned to the Access Group will be based on the policies and planning of your administrative group and how they define a crisis situation and want things to work.*

d) Now the *access credentials* will operate normally under normal system conditions, but the credentials will switch to **Crisis Mode Rules** when Crisis Mode is activated.

e) Repeat steps B and C for each Cluster you assigned to the cardholder.

4. Click **APPLY** to save your changes.

### Cardholder Programming screen

The screenshot displays the 'Cardholder Programming' interface. The 'Card/Badge Settings' tab is selected and highlighted with an orange box. The 'Loop/Cluster Settings' section is also highlighted with an orange box, showing the 'Select Access Groups' dropdown menu with 'Employee Access (M/F)' selected. Two orange arrows point to the 'Auxiliary Function Enabled' checkbox and the 'Expire Date' field, which are currently set to 'No Expiration'. The interface includes various input fields for card data, options, and settings, along with buttons for 'Edit Loops', 'View Audit', and 'Add/Delete T/A Punches'.

## Assigning a Crisis-Mode to a Door - Quick Steps

When Crisis Mode is active, the door will use the **Crisis Mode Unlock Schedule**. When crisis mode is reset, the door will return to using the *Auto Unlock schedule*. Choosing NEVER would typically cause the unlocked doors to lock down.



NOTICE: This option is only available for 600/635-series controllers on systems running SG 10.4.8 or higher.

Open the **Door Properties** screen from the menu: [Configure > Hardware > Doors/Readers](#)

1. From the *Hardware Tree* you can expand the **Loop/Cluster branch** until you can see the reader/doors.
2. Right-click on a **Door/Reader Name** and select the *Properties* option from the shortcut menu.
3. On the *Timing/Schedules Tab*, and select a schedule in the **[Crisis Mode Unlock Schedule]** droplist.
4. Click **APPLY** to save changes.

### Door/Reader Programming screen

The screenshot shows the 'Door/Reader Programming screen' with the 'Timing/Schedules' tab selected. The 'Crisis Mode Unlock Sch.' dropdown menu is highlighted with an orange box, showing the option '\*\* NEVER \*\*'. Other settings include 'Auto Unlock Sch.' set to '\*\* ALWAYS \*\*', 'PIN Required Sch.' set to '\*\* NEVER \*\*', 'Disable Forced' set to '\*\* NEVER \*\*', and 'Disable Open Too Long' set to '\*\* NEVER \*\*'. The 'PIN Mode' is set to 'High Security'. The 'Require Valid Card before auto unlock' checkbox is unchecked. The 'Apply' and 'Cancel' buttons are visible in the top right corner.



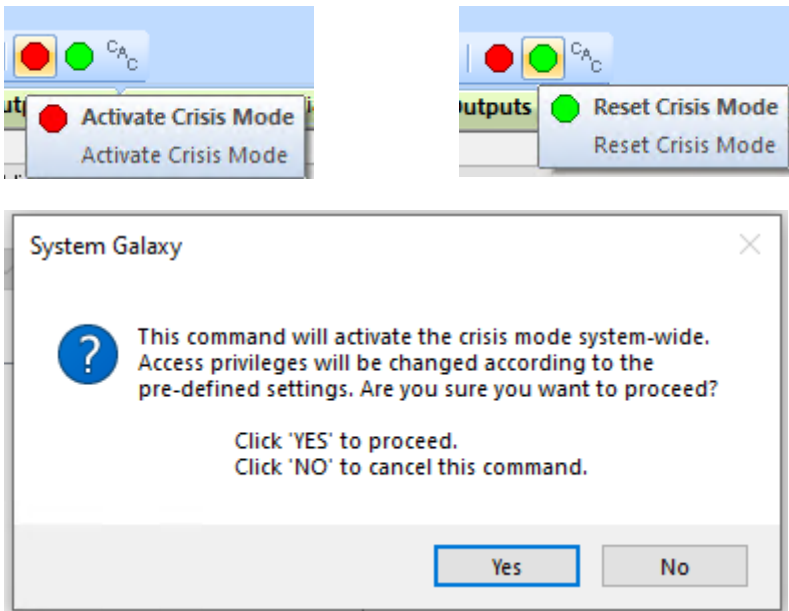
# Activating & Resetting Crisis Mode

Crisis mode can be activated and reset from the System Galaxy Toolbar (system-wide), the Loop Diagnostics screen, or using an input button (panic button) that is linked to IO Groups to trigger the Crisis Mode.

## Managing Crisis Mode via Toolbar Buttons

Click the Crisis Mode buttons to Activate or Reset Crisis mode across all loops/clusters system-wide. The system will require you to confirm your action.

- Red button activates Crisis Mode
  - Green button resets Crisis Mode
1. Open the **System Galaxy software** and sign in with your *user name* and *password*.
  2. You can control Crisis Mode from the SG Toolbar as follows ...
    - a. Click the **Red Crisis Mode button** to activate Crisis Mode.
    - b. Click the **Green Crisis Mode button** to reset Crisis Mode
  3. Click **YES** to continue the action when prompted. (Clicking NO will cancel the command.)



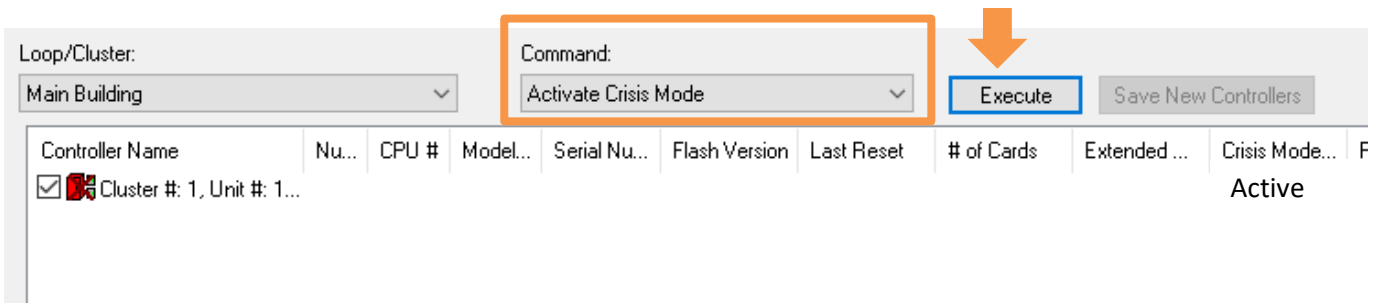
## Managing Crisis Mode via Loop/Cluster Diagnostics

Click the Crisis Mode commands to *Activate* or *Reset* Crisis mode for the chosen Loop/Cluster. The system may require you to confirm your action.

Open the *Loop/Cluster Diagnostics* screen from the menu: [View > Loop/Cluster Diagnostics](#)

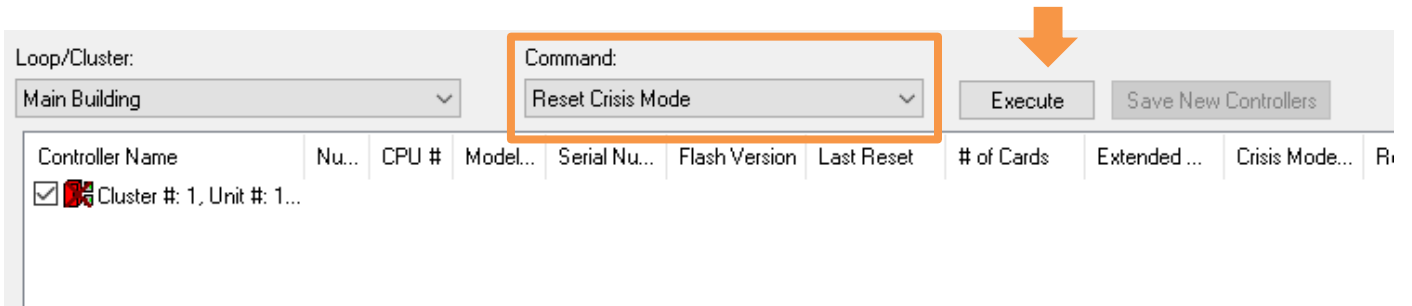
1. Select the **Loop/Cluster Name** you want to manage.
2. Choose the Crisis Mode Command in the **[Command]** droplist.
  - a. Activate will activate crisis mode for the selected loop/cluster
  - b. Reset will deactivate crisis mode for the selected loop/cluster
3. Click **Execute** button to issue the command. Click YES if prompted to continue with action.

### Activate Crisis Mode Command



The screenshot shows the 'Loop/Cluster Diagnostics' interface. The 'Loop/Cluster' dropdown is set to 'Main Building'. The 'Command' dropdown is set to 'Activate Crisis Mode'. The 'Execute' button is highlighted with a blue border and an orange arrow points to it from above. Below the command area is a table with columns: Controller Name, Nu..., CPU #, Model..., Serial Nu..., Flash Version, Last Reset, # of Cards, Extended ..., Crisis Mode..., and F. The first row shows a checked checkbox, a red icon, and the text 'Cluster #: 1, Unit #: 1...'. The 'Crisis Mode...' column for this row is 'Active'.

### Reset Crisis Mode Command



The screenshot shows the 'Loop/Cluster Diagnostics' interface. The 'Loop/Cluster' dropdown is set to 'Main Building'. The 'Command' dropdown is set to 'Reset Crisis Mode'. The 'Execute' button is highlighted with a blue border and an orange arrow points to it from above. Below the command area is a table with columns: Controller Name, Nu..., CPU #, Model..., Serial Nu..., Flash Version, Last Reset, # of Cards, Extended ..., Crisis Mode..., and Ri. The first row shows a checked checkbox, a red icon, and the text 'Cluster #: 1, Unit #: 1...'. The 'Crisis Mode...' column for this row is empty.

## Managing Crisis Mode using an Input with Crisis Mode IO Group

Crisis mode can be activated and reset using hardware inputs in conjunction with IO Groups. You must have done the needed programming and created your Activate and Reset IO Groups and assigned them to your Loop/Clusters.

In this scenario, when the Crisis Input is triggered (such as a panic button), the Activate Crisis IO Group will be activated, and the system will respond as it is configured to do.

When the Reset Input is triggered (such as a reset button), the Reset Crisis IO Group will be activated, and the system will respond as it is configured to do.

- See the Loop/Cluster Programming section in this guide for that programming.
- You can use the *Loop/Cluster Diagnostics screen* to **Get Information** and confirm whether Crisis Mode is active or reset for the loop/cluster.