



MCE Sentry®

MCE Sentry provides security administration for MCE iControl elevator installations. Both ¹ETA and Destination Based Dispatching modes are supported.

Sentry defines three administrative roles: Administrator, Manager, and Technician. Once logged on, each role has the ability to view or administer security depending upon the access definitions for that role:

- Administrator: Full system permissions including building security maps, passenger schedules, user administration, and report generation.
- Manager: Passenger schedule administration and report generation. Viewing privileges only for remaining security capabilities.
- Technician: Viewing privileges only.

The PC used by the Administrator, Manager, or Technician is called a Security Client. The Security Client communicates with a Security Manager PC through an Ethernet connection. Real time security processing and application hosting are handled by the Security Manager. The data base containing the security configuration is automatically mirrored by the Security Manager so that if the primary data base is damaged, the secondary data base will assume its place.

When the system is configured, an IP address is assigned to the Security Manager. To log on (establish a connection to the Security Manager), the administrator, manager, or technician launches their web browsing application, enters the Security Manager IP address into the browser URL window, and presses Return. Once the connection is established, a log-in screen appears. The user clicks login, provides a valid user name and password, and is given access to the system.

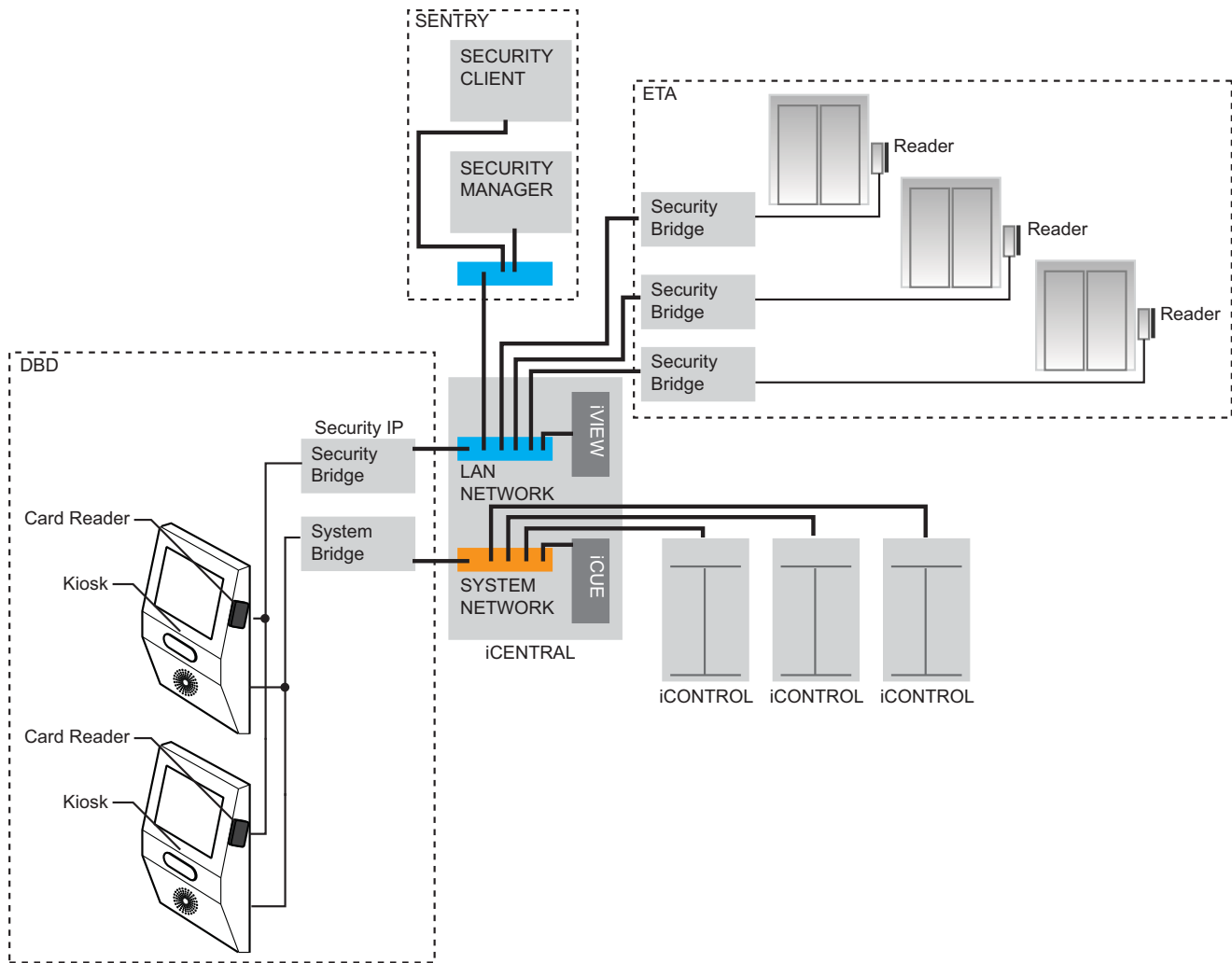
-
1. With ETA dispatching, controlling logic recognizes a hall call demand and assigns a car to answer it based primarily on the cars Estimated Time of Arrival. (The car that can answer the call most quickly is assigned to the call.) ETA dispatching works to assure the shortest possible passenger wait time.

With DBD (Destination Based Dispatching), passengers select their desired destination floor. Controlling logic, primarily by assigning passengers with the same or nearby destinations to the same car, works to achieve the shortest possible in-car travel time and provide the most efficient use of each car.



In the illustration below, the Bridge boards (Security or System) are shown as they are functionally. Physically, Bridge boards are located in the iCentral group cabinet. For more information about Bridge boards, see [Bridge Boards \(HC-MPU-M Board\)](#) on page 25.

Figure 1. System Architecture

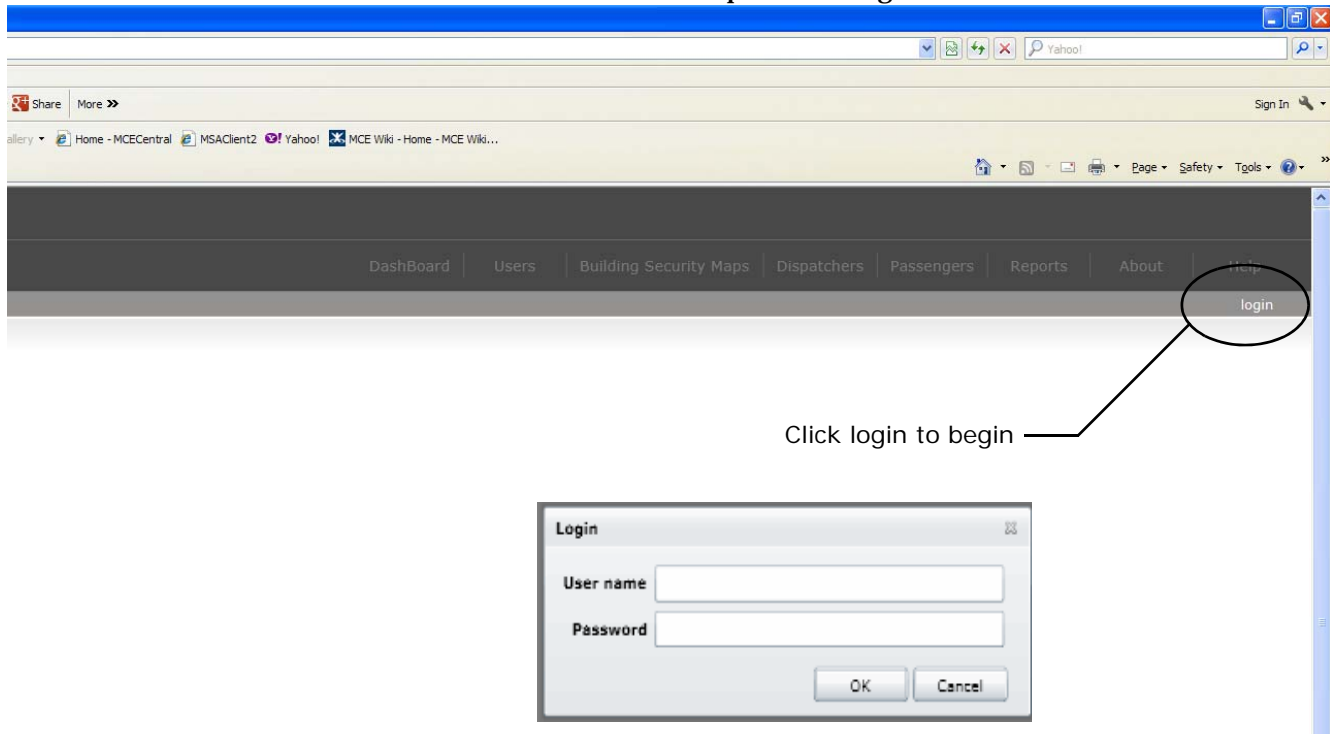


Initial Log On

Launch the Internet Explorer browsing application on the Client Server PC.

- Enter the URL provided by MCE for the web server (residing on the Client Server). For example:
 - <https://mcesentry/msac>

When contact is established, the web server will provide a log on screen.



If you do not yet have a personalized Client Server username and password, you will initially log on the system as:

- Username: admin
- Password: admin

This will log you on with full administrative privileges. For first time users, we recommend you set up a personalized Administrator account with a Username and Password you choose ([Set Up Users on page 4](#)), log off the system, then log back in using your personal information.

After some period of time, when you are comfortable with using the application, we recommend you delete the default admin/admin account.



Security Tools

Dashboard | Users | Building Security Maps | Dispatchers | Passengers | Reports | Settings | About | Help

Security tools are described in order of use for initial system setup:

- Set up users, [page 4](#)
- Set up Dispatchers, [page 7](#)
- Set up Building Security Maps, [page 10](#)
- Add Passengers, [page 15](#)
- Run Reports, [page 20](#)
- Settings (add security cards), [page 20](#)
- Using the Dashboard, [page 21](#)

Informational Items

- About, [page 21](#)
- Help, [page 21](#)
- System terminology, [page 22](#)

Set Up Users

Select the Users menu. User menu tools allow you to create and edit accounts for those individuals who will administer security.



User name	Role	Is locked out	Unlock	Reset password	Edit	Delete
almondjoy	Manager	<input type="checkbox"/>	Unlock			
bill	Manager	<input type="checkbox"/>	Unlock			
cspencer	Administrator	<input type="checkbox"/>	Unlock			
Darnitman	Manager	<input type="checkbox"/>	Unlock			
jcunts	Administrator	<input type="checkbox"/>	Unlock			
jinl	Administrator	<input type="checkbox"/>	Unlock			
JohnDole	Technician	<input type="checkbox"/>	Unlock			

Page 1 of 3

{Added = 0, Modified = 0, Removed = 0}

Add User

Click Add User to create a new security account.

- Enter identifying and contact information for the new account.
 - User name must be a single string of characters with no spaces.
 - Password must be at least seven characters and contain at least one number.
- Select a Role for the account. This will determine the depth of access to the security system. [Please refer to “MCE Sentry®” on page 1.](#)
- Click OK to create the account or click Cancel to close the dialog without accepting any changes.
- Once you click OK, the Save/Reject changes buttons at the bottom of the page will become active. To save your changes, click on the Save changes button.

The 'Add User' dialog box is a light gray window with a title bar. It contains four input fields: 'User name' (a text box), 'Password' (a text box with a small 'i' icon to its right), 'Confirm password' (a text box), and 'Role' (a dropdown menu). At the bottom right, there are two buttons: 'OK' and 'Cancel'.

List of Accounts

The list displays User Name and Role for each account. It also provides controls to reset user passwords, and to edit or delete user profiles. Click on User name or Role headers to sort accounts by that criteria. To move through a long list of Users, you may use the scroll bar to the right of the pane or use the Page controls at the bottom of the pane.

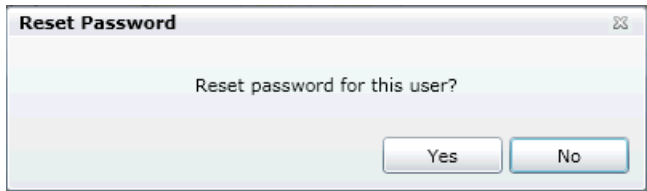
- **Is Locked Out:** Lock out is automatically initiated when a user tries and fails to log on five times inside a ten minute period.
- **Unlock:** If a user is locked out, this button becomes active allowing an Administrator to reset the lock.

Edit User To edit user information, click on the Edit button adjoining that user's name.

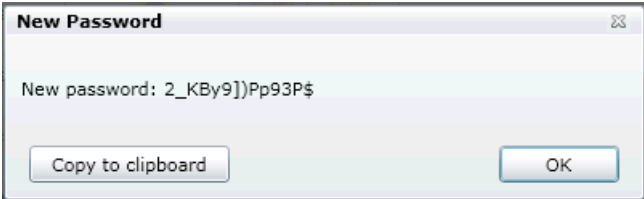
The 'Edit User' dialog box is a light gray window with a title bar. It contains two input fields: 'User name' (a text box containing the text 'cspencer') and 'Role' (a dropdown menu showing 'Administrator'). At the bottom, there are two buttons: 'OK' and 'Cancel'.



Reset Password To reset a user password, click on the Reset password button adjoining that user’s name.



The system will assign the user a new password. A button in the dialog allows you to copy the new password to the computer clipboard, making it available for you to paste it into a word processing or other application for storage.



Delete User You may also delete users from the list by clicking the Delete button adjoining the user’s name.

- Once you click Delete, the user’s name will immediately disappear. The Save/Reject changes buttons at the bottom of the page will become active. To save your changes, click on the Save changes button.

Save/Reject Changes

When changes have been made, these two buttons become active and the message next to them will update to tell you the number of additions, modifications, or removals that are pending.

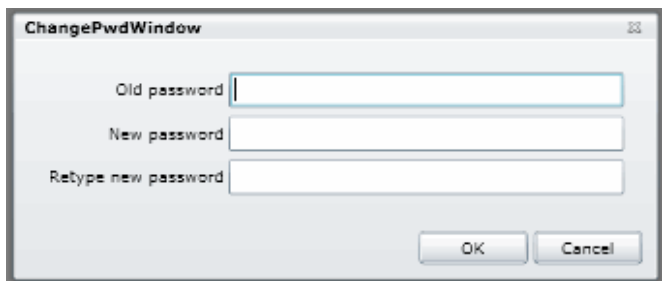
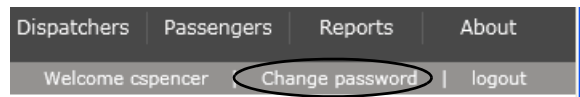
- Save Changes: Click to save/accept changes.
- Reject Changes: Click to reject changes, retaining previously saved information.

Search

If you have a lengthy list of security accounts, activate Search and enter a User Name or an Email address and click Search users to bring up a particular account. You can also click Get all users to display all current accounts.

Change Password

Individual users, once logged on, can change their password at any point through the Change Password cue that appears next to Login/Logout on the initial screen.



Set Up Dispatchers

Select the Dispatchers menu. These tools allow you to add or edit elevator dispatchers.

Dispatchers provide coordinating logic for a group of elevators. Sentry supports iControl, iCue (iCentral) dispatchers. iCue dispatchers are capable of both ETA and DBD dispatching duties.

Add Dispatcher(s)

Click Add Dispatcher to initially configure a new dispatcher in the security system.

The screenshot shows a dialog box titled "Add Dispatcher" with the following fields and controls:

- Name:** A text input field.
- IP address:** A text input field.
- Device type:** A dropdown menu currently showing "iCue".
- OK:** A button to save information.
- Cancel:** A button to close the dialog.

Callouts on the right side of the dialog box point to these elements:

- Name
- Dispatcher IP address, see MCE drawings
- Select device type
- OK to save information
- Cancel to close dialog

Name The name you enter should allow you to easily identify the dispatcher.

IP Address The IP address will be on the MCE drawings for the installation.


Device Type iCue: DBD or ETA dispatching. iBox: ETA dispatching only. Both iCue and iBox dispatchers may have alternate (backup) dispatchers which will take over dispatching logic if the primary dispatcher should be taken off line. Alternate dispatchers are configured through the iView application and, should the primary dispatcher be taken off line, Sentry will locate the alternate dispatcher automatically.




List of Dispatchers




The list displays Name, IP Address, Port, Group ID, and Device Type for each available dispatcher. Click on any of these headers to sort by that criteria.

When a primary dispatcher is selected in the upper list, any associated alternate dispatchers appear in the lower list.






Clicking on any dispatcher  displays ¹Bridge information for that dispatcher.

Search



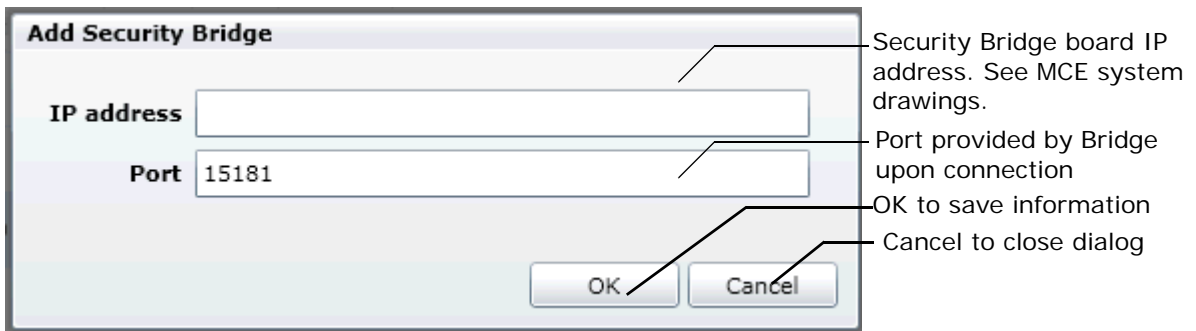
	Name	IP address	Port	Group ID	Device type	Edit	Delete	Add security bridge
+	Group DBD	10.10.52.100	4555	0	iCue			

Page 1 of 1

	Name	IP address	Port	Group ID	Device type	Add security bridge
+	Alt car 1	10.10.52.101	5555	0	iBox Alternate Dispatcher	
+	Alt car 2	10.10.52.102	5555	1	iBox Alternate Dispatcher	
+	Alt car 3	10.10.52.103	5555	2	iBox Alternate Dispatcher	
+	Alt car 4	10.10.52.104	5555	3	iBox Alternate Dispatcher	
+	Alt car 5	10.10.52.14	5555	4	iBox Alternate Dispatcher	

1. A bridge is a device used to translate from one communications protocol to another. An iCue dispatcher requires two bridge units; one to interface destination entries from kiosks (destination input devices); one to interface to security equipment. An iBox requires only a Security interface bridge.

Add Security Bridge Once a dispatcher is initially defined and appears in the list, it can be added to the security system by entering its Bridge IP address. Every dispatcher added to security must have its own Bridge.






Search If you have a lengthy list of Dispatchers, activate Search and enter a Name or an IP address and click Search Dispatchers to bring up a particular one. You can also click Get All Dispatchers to display all currently available dispatchers.



Set Up Building Security Maps

Select the Building Security Maps menu. These tools allow you to edit or create building security maps, determining which floors/openings are Unsecured, Secured, or Locked for the selected dispatcher by application of the security map. Floors and Openings may be:

- Unsecured:  No security enforced for this floor/opening.
- Secured:  Access from or to this floor/opening will be allowed with accepted identification for passengers whose security maps and schedules authorize their access.
- Locked:  Access from or to this floor/opening is not allowed while Locked status is active.

List of Dispatchers The list displays Name, IP Address, Port, and Device Type for each available dispatcher. Click on any of these headers to sort by that criteria. [Please refer to “Set Up Dispatchers” on page 7](#) if you wish to add a dispatcher.

Name	IP address	Port	Device type
DBD iCue	10.10.52.100	4555	iCue

- To display the Security Maps for a particular dispatcher, click on that dispatcher in the list.
 - The dispatcher must have been previously added.

Adding Maps **Default** source and/or destination maps are active when no other source or destination map is currently being applied. (Currently active maps for the selected dispatcher are displayed on the Dashboard.)

- Source map: Source maps apply security for the departure floor (the floor on which the hall call or destination call is registered). If secured, hall calls or destination selections may not be registered **from** the secured floor without appropriate code entry.
- Destination map: Destination maps apply security for the destination floor (the floor selected on the car operating panel or on the destination entry kiosk). If secured, car calls or destination calls may not be registered **to** the secured floor without appropriate code entry.

- Security settings may be edited here directly for the active map. (Click Save Changes button to activate changes.)

Default: This tab selects the default source map for the selected dispatcher.

Default: This tab selects the default destination map for the selected dispatcher.

Click and select security status per floor and opening

Floor	Front	Rear
17	Secured	unsecured
16	unsecured	unsecured
15	unsecured	unsecured
14	unsecured	unsecured
13	unsecured	unsecured
12	Secured	unsecured
11	Secured	unsecured
10	unsecured	unsecured
9	unsecured	unsecured
8	unsecured	unsecured
7	Secured	unsecured
6	unsecured	unsecured
5	unsecured	unsecured
4	unsecured	unsecured
3	unsecured	unsecured
2	unsecured	unsecured
L	unsecured	unsecured

The **Destination map** tab provides a list of available map-enforcing schedules sortable by Title, Start Time, End Time, and Recurrence Type.

Title	Start time	End time	Recurrence type	Delete
Morning Work Hours	4/22/2014 6:00:00 AM	No end date 6:00:00 PM	Daily	
Evening Non-working Hours	4/22/2014 6:00:00 PM	No end date 6:00:00 AM	Daily	
Weekend	4/22/2014 All day	No end date All day	Weekly	

Schedule: Security Map

Enable Recurrence

Recurrence Pattern

Daily Every 1 day(s)
 Weekly Every weekday
 Monthly Yearly

Range of Recurrence

No end date
 End after 10 occurrences
 End by 5/2/2014

Title: Morning Work Hours

Start Time: 4/22/2014 6:00 AM All day
 End Time: 4/22/2014 6:00 PM

- Select a schedule in the list to view or edit schedule occurrence and/or the security map the schedule enforces.



The **Destination override map** tab displays existing Override Security Maps. An active override map will override all other maps for the period(s) specified. This feature allows you to readily accommodate emergency or unusual needs. [Please refer to “New/Schedule/Security Map” on page 13.](#)

Default source map	Default destination map	Destination map	Destination override map

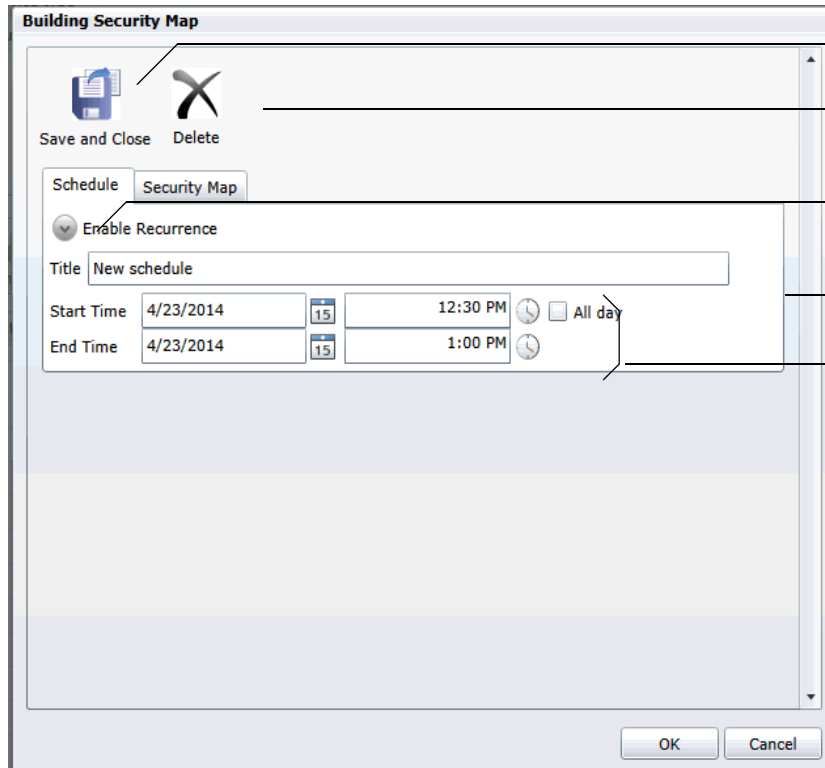
Title	Start time	End time	Recurrence type	Delete
Weekend Schedule	4/21/2014 All day	No end date All day	None	

Schedule	Security Map
<input type="checkbox"/> Enable Recurrence	
Title: Weekend Schedule	
Start Time: 4/21/2014	2:30 PM <input type="checkbox"/> All day
End Time: 4/21/2014	3:00 PM

[Please refer to “Override map” on page 23](#) for detailed information.

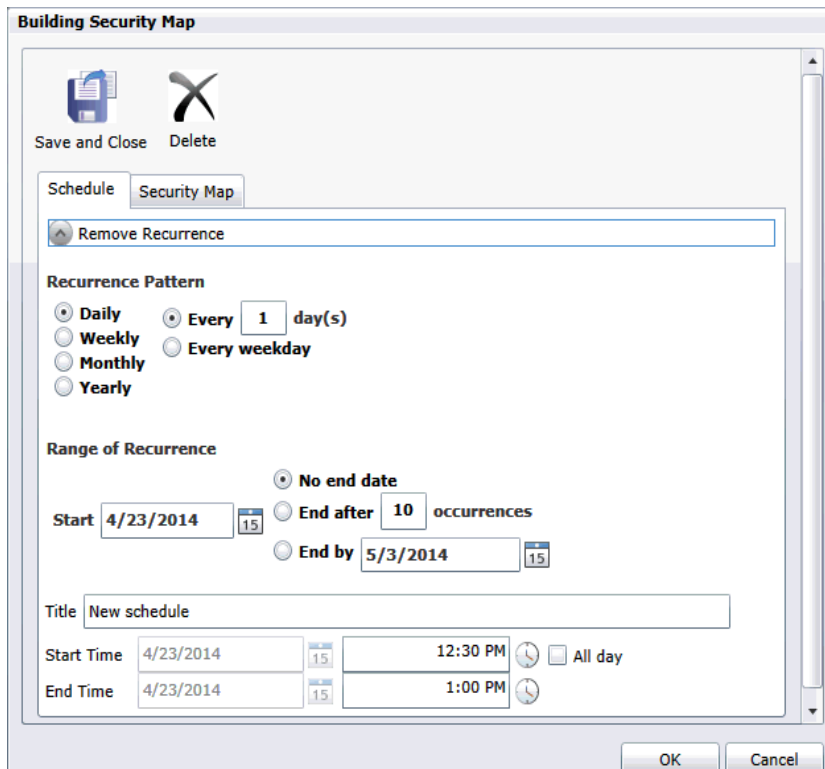
New/Schedule/Security Map If you choose to add/edit a new Security Map or Override map, a dialog will appear to help you:

NON-RECURRING



- When you have made changes, use Save & Close.
- Use Delete to remove the schedule.
- If a schedule is to recur, Enable Recurrence.
- Provide a unique name for the new schedule.
- Start/End Times for non-recurring schedule. See below for recurring.

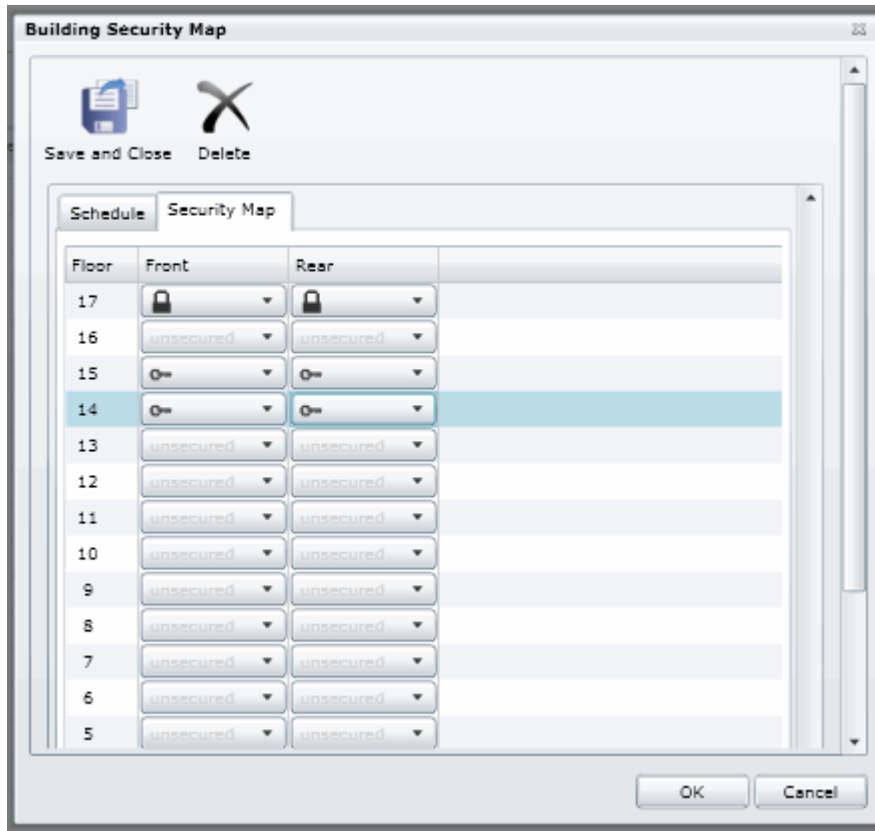
RECURRING



When you select a Recurrence Pattern, the controls will change to appropriate selections for that pattern.



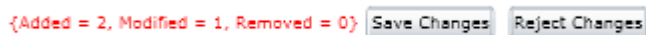
Floors and Openings for the new or edited schedule/security map are set as described previously. Please refer to “Set Up Building Security Maps” on page 10.



- Click OK to enter schedule/map changes or Cancel to exit.

Save/Reject Changes When changes have been made, these two buttons become active and the message next to them will update to tell you the number of additions, modifications, or removals that are pending.

- Save Changes: Click to save/accept changes.
- Reject Changes: Click to reject changes, retaining previously saved information.



Search If you have a lengthy list of Dispatchers, activate Search and enter a Name or an IP address and click Search Dispatchers to bring up a particular one. You can also click Get All Dispatchers to display all currently available dispatchers.

Add Passengers

Select the Passengers menu. These tools allow you to add passengers to the system and assign security attributes to passengers/passenger IDs per elevator dispatcher.

List of Passengers The list displays First and Last Names for each defined passenger. A passenger must have been previously added to the system for their map to appear. Click on a header to sort by that criteria.

Add passenger
Add source security map
Add destination security map

Photo	First name	Last name	Edit	Delete
	test1	123		
	may1	123		
	EditingTimer	123		
	EditingTimer2	123		

First name: test1
 Last name: 123
 HID: 14789
 Location: 123
 Phone:

Select dispatcher: [All]

Source map | Destination map

Title	Start time	End time	Delete
test1's schedule	4/21/2014 4:30:00 PM	No end date 4:00:00 AM	

Schedule | Security Map

Dispatcher security map applies to: iCue Varrick

Floor	Front	Rear
17	<input type="checkbox"/>	<input type="checkbox"/>



Add Passenger Click Add Passenger(s) to add a new passenger to the security system.

NOTE: The Edit Passenger window does not include the schedule or destination security map information.

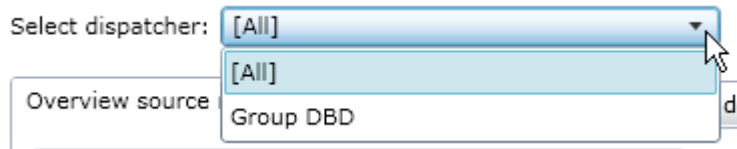
- Fill out name fields
- Location: Resident/working floor number for passenger.
- Phone/Email: Provide passenger contact information.
- Provide card information — [Please refer to “Settings” on page 20.](#)
- Card type: Select previously entered type (Settings) from dropdown menu.
- Card ID: From card or, if the card has been scanned (Settings), automatically generated.
- Factory ID: Select previously entered ID (Settings) from dropdown menu.
- HID: Generated by scanning the card into the HCE2 scanner
- Load Photo (Webcam): If Load Photo button is present, click to browse to and load a digitized user photo (recommend 500k or smaller).
- Webcam (Load Photo): If webcam icon is visible, clicking it will activate the camera connected to the system and import the image into the Sentry application.

Once you click OK, the passenger will be added to the passenger list. Their schedule (following page) and destination security maps ([page 18](#)) will become available to set up.

Add Security Map When a passenger is highlighted in the list, their personalized security schedules/maps for the currently selected Dispatcher will appear (if any have been created).

To view the security map for a selected passenger on a specific dispatcher:

- Select the Dispatcher. You may select a single dispatcher or all dispatchers.



Information for that passenger and dispatcher combination will appear (if previously created). If no Security Maps exist for this passenger, you may create a new one by clicking on the Add Source Security Map or Add Destination Security Map buttons. The security map you create will apply to the selected passenger on the selected Dispatcher. [Please refer to “New/Edit Passenger Security Map” on page 18.](#)



Source or Destination schedule/Map information for a selected passenger will appear and may be directly edited.

Title	Start time	End time	Delete
Pepsi's schedule	10/11/2012 1:00:00 PM	10/11/2012 4:00:00 PM	

Select to set Schedule

Select to set Map



New/Edit Passenger Security Map You can open a schedule for editing in Detailed view by right-clicking on the schedule and selecting Edit Schedule from the popup menu. You can click on an Add Security Map button to create a schedule from scratch. (The popup menu also provides the option to Delete Schedule. You may also delete a schedule by selecting it and pressing the Delete key on the computer keyboard.)

When a schedule is opened, the controls used to configure application of that schedule will change depending upon whether it is recurring or single use.

NON-RECURRING

Annotations for Non-Recurring mode:

- Recurrence not enabled
- Name this schedule
- Select starting and ending dates and times.

RECURRING

Annotations for Recurring mode:

- Select to set schedule
- Select to set map
- When you select a Recurrence Pattern, the controls will change to appropriate selections for that pattern.
- Name this schedule

Passenger Access Per Schedule Scroll down the Passenger Security Map to set the secured floor access permitted the passenger when this schedule is active.

Schedule		Security Map	
Dispatcher security map applies to: DBD iCue			
Floor	Front	Rear	
17	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
16	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
15	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
14	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
13	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Click to select/deselect.

Checked openings are available to this passenger while this schedule is active after validation of security credential.

Access permission affects ONLY SECURED FLOORS. Please refer to "Set Up Building Security Maps" on page 10.

Save/Reject Changes When changes have been made, these two buttons become active and the message next to them will update to tell you the number of additions, modifications, or removals that are pending.

- Save Changes: Click to save/accept changes.
- Reject Changes: Click to reject changes, retaining previously saved information.

{Added = 2, Modified = 1, Removed = 0}

Search If you have a lengthy list of passenger security maps, activate Search and enter a First Name, Last name, or an HID (identification from security card/badge) and click Search Passengers to bring up a particular one. You can also click Get All Passengers to display all defined passenger maps.



Run Reports

These tools allow elevator system security reports to be generated:

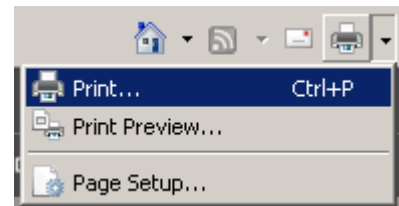
- **Travel Data:** Time, Passenger, Dispatcher, Car, Source Floor, Source Side, Destination Floor, Destination Side, Status, and Location. Click on any of these headers to sort the list by that criteria.
- **Swipe Data:** Time, Card ID, Group ID, Bank Designation, Riser Designation, DID Type, Source Floor Type, Location, Source Floor number, and Side. Click on any of these headers to sort the list by that criteria.
- **Dispatcher Events:** Time, Dispatcher, IP Address, and Event code. Click on any of these headers to sort the list by that criteria.
- **Bridge Board Events:** Time, IP Address, Dispatcher, and Event code. Click on any of these headers to sort the list by that criteria.
- **User Activities:** Login/Logout data, Passenger information, Dispatcher information — all with times, dates, and associated information.

To initiate a report:

- Select the report type.
- Set start and end dates.
- Set filtering criteria.
- Click Refresh.

To print a report, use the browser printing controls:

- To print immediately, select Print.
- To preview and set up, then print, select Print Preview.
- To establish page layout before printing, select Page Setup.



Settings

The Settings tab is accessible to Administrators only.

- **Factory codes:** The factory code is generally printed on or included in the box of cards received from the security consultant. Key it into the entry box, then click Add Factory Code. To delete an existing code, click the X button next to that code.
- **Card Types:** i.e. “26 bit standard.” Tells Sentry how to interpret card swipes in order to produce a Card ID.
- **(Bit) Format:** Again provided with the cards.

Factory codes

23	X
8	X

Factory code: **Add factory code**

Card types

26 Bit Standard XXXX XXPI IIII IIII IIII IIII FFFF FFFP	X
---	---

Card type name:

Format:

Add card type

Save changes **Reject changes**

Using the Dashboard

The Dashboard provides a way for you to quickly select a Dispatcher, view the status of dispatcher to security server communication, view the status of bridge board to security server information, and view the currently active building security map.

Currently selected Dispatcher: iCue Varrick

IP Address	Status
10.10.52.100	CONNECTED

** IP address & * status of bridge boards

IP Address	Status
10.10.52.60	CONNECTED
10.10.52.111 (Alt car 1)	NOT CONNECTED
10.10.52.112 (Alt car 2)	NOT CONNECTED
10.10.52.113 (Alt car 3)	CONNECTED

Active source map

Floor	Front	Rear
17	unsecured	unsecured
16	unsecured	unsecured
15	unsecured	unsecured
14	unsecured	unsecured
13	unsecured	unsecured
12	unsecured	unsecured
11	unsecured	unsecured
10	unsecured	unsecured
9	unsecured	unsecured
8	unsecured	unsecured
7	unsecured	unsecured
6	unsecured	unsecured
5	unsecured	unsecured
4	unsecured	unsecured
3	unsecured	unsecured
2	unsecured	unsecured
L	unsecured	unsecured

Last card swipe data

Time	Name	HID	Kiosk ID	Floor

Secured

Locked

Active destination Map

Floor	Front	Rear
17	SM	unsecured
16	SM	unsecured
15	SM	unsecured
14	SM	unsecured
13	SM	unsecured
12	SM	unsecured
11	SM	unsecured
10	SM	unsecured
9	SM	unsecured
8	SM	unsecured
7	SM	unsecured
6	SM	unsecured
5	SM	unsecured
4	SM	unsecured
3	SM	unsecured
2	SM	unsecured
L	SM	unsecured

Current destination map

Front	Rear
SM	unsecured
unsecured	unsecured
SM	unsecured
SM	unsecured
SM	unsecured
unsecured	unsecured
unsecured	unsecured
unsecured	unsecured
unsecured	unsecured
unsecured	unsecured
unsecured	unsecured
unsecured	unsecured
unsecured	unsecured
unsecured	unsecured
unsecured	unsecured
unsecured	unsecured
unsecured	unsecured
unsecured	unsecured
unsecured	unsecured

Current Maps: Visible when the destination map schedule changes but has not take effect yet. Once settings take effect, this will become the Active destination map and the "current" map will no longer be visible.

- * Status of dispatcher to security server communication.
- ** Status of bridge board to security server communication.

- Active Building Maps: Actual source and destination security map status at this time.
- Override Maps: When active, Override maps override all other maps.

About

About provides Sentry application software version and access to online documentation.

Help

Access on-line help by clicking on the Help menu.



Terminology

The following table defines proprietary terms used in this application.

Table 1. Terminology

Term	Definition
Access Denied	Status message indicating a passenger credential was not accepted for the desired destination/opening.
Bank Designation	A number identifying the bank to which an elevator belongs. (Dispatching groups may be subdivided into smaller groups (banks)).
Bridge (board)	A device used to translate between one communications protocol to another. One bridge is used to interface DID floor entries to the elevator System network. A second type of bridge, the Security Bridge, is used to interface security data to the elevator LAN network. The IP address of this second bridge is identified as the Ethernet source of the security information. Adding a Security Bridge board to a security system authorizes security entries from DIDs associated with that bridge.
Card ID/HID	The identifying number associated with a passenger credential (card).
DBD	Destination Based Dispatching. Elevator system for which the passenger enters their desired destination floor and is assigned a specific car.
Destination Floor	The desired floor entered by the passenger on a DID (Destination Input Device).
Destination Side	For "walk through" doors, the "side" on which a destination floor was entered.
DID	Destination Input Device. A kiosk through which the passenger enters their desired Destination Floor.
Dispatcher	AKA "group control." An overall dispatching and parking control in charge of a number of elevators.
Group ID	The numerical identifier assigned to a group of elevators directed by the same dispatcher.
IP Address (Internet Protocol)	A unique numeric identifier assigned to a device communicating over Ethernet networks. The IP Address allows messages to and from the device to be properly routed.
IsLockedOut	A security user may be temporarily locked out of system access through the IsLockedOut function. Lock out is automatically initiated when a user tries and fails to log on five times inside a ten minute period.
IsUnlocked	A locked out security user may be allowed system access through the IsUnlocked function.
Location	Floor location for a tenant/passenger.

Table 1. Terminology

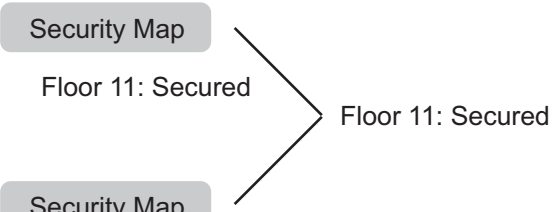
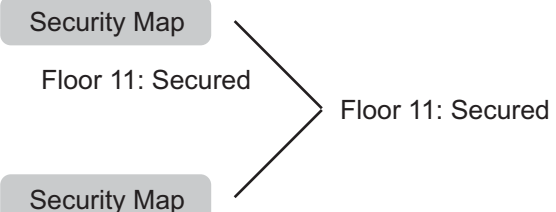
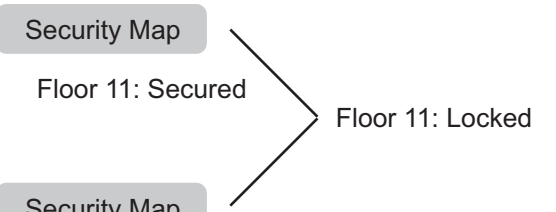
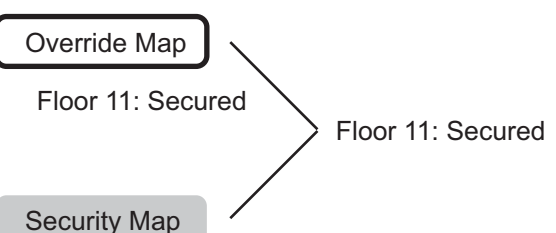
Term	Definition
Override map	<p>An override schedule is different from a regular schedule in that an override schedule security map replaces that of regular schedules and is not or'd with them. This allows you to create exceptions to regular schedules. Example: There is a regular daily schedule between 1:00 PM and 6:00 PM that secures floors 5 through 10 and you would like to change this schedule for floor 10 for this coming Saturday because there is a meeting scheduled and that floor should be made unsecured. You would not be able to do this with regular schedule because all schedules that overlap would have their maps or'd together (when "secured" and "unsecured" are or'd together, the result is "secured"). An override schedule would allow such a schedule exception.</p>
<div style="display: flex; justify-content: space-around;"> <div style="width: 45%;"> <p>Simultaneously Active Maps</p>   </div> <div style="width: 45%;"> <p>Simultaneously Active Maps</p>  <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p>Override Map: The settings of all other simultaneously active maps are overridden, regardless of the selection made there. <u>Only one</u> Override map may be active at a time.</p> </div> </div> </div>	



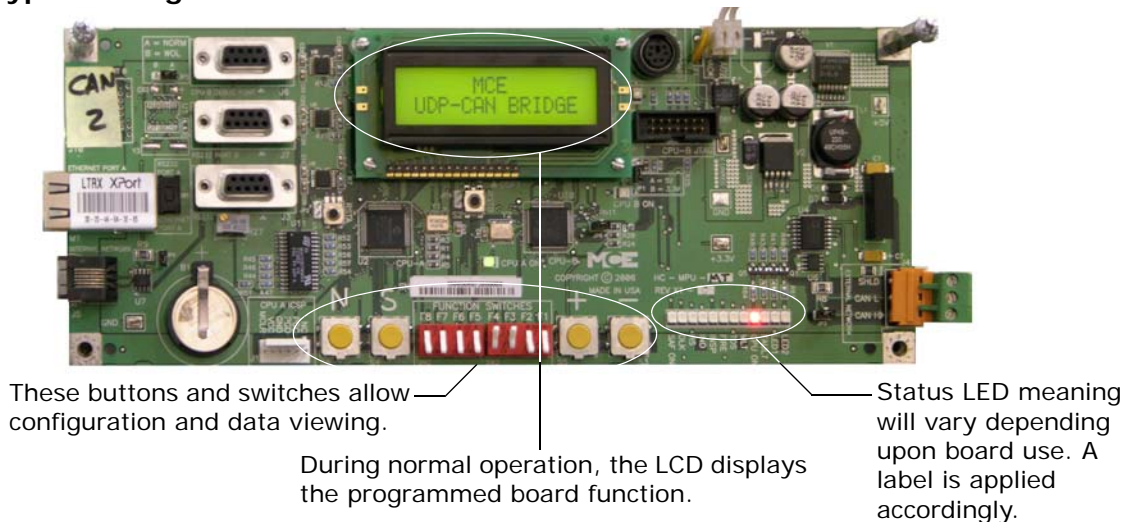
Table 1. Terminology

Term	Definition
Pass	Status message indicating a passenger credential was accepted for the desired destination/opening.
Port	An Ethernet connection may support one or more Ports. A Port further subdivides the IP address. Generally, the Port is defined by the associated device.
Riser Designation	A label identifying the riser (front, rear) associated with the DID through which a desired destination/opening was registered.
Role	Persons allowed to access MCE Sentry are defined by the system as belonging to one of three Roles (Administrator, Manager, or Technician). Please refer to "MCE Sentry®" on page 1.
Source Floor	The floor on which a DBD call was registered.
Source Floor Type	Identifier for a floor type.
Source Side	When multiple risers are used, i.e., front and rear doors on a car, the "side" on which a destination floor was entered.
Status	The outcome of an action or the condition of a device.
Timed Out	Status message indicating a passenger failed to register proper credentials within the allotted period of time.
Unknown	Status message displayed when a presented credential is unknown to the system.

Bridge Boards (HC-MPU-M Board)

Bridge boards are microprocessor controlled circuit boards that provide translation to/from one communication format and another. They are very flexible in their application because the microprocessor can be programmed according to specific requirements.

Figure 2. Typical Bridge Board



IP Address

IP addresses are assigned to each bridge board at the factory using a Lantronix utility. The address of each board is shown in your job prints for proper wiring. IP addresses may be changed in the field if required (contact MCE customer support).

Default DIP Switch Settings

As shipped from MCE, bridge board DIP switch settings are:

- System Bridge (orange cable to System Ethernet): F3, F4 = ON. All others: OFF.
- Security Bridge (blue cable to LAN Ethernet): F5 = ON. All others: OFF

Board Programming

Function switches: (in the UP position)

- F8: Bridge menu active
- F7: No function
- F6: No function
- F5: Kiosk message filtering (ON = kiosk messages blocked)
- F4: Security message filtering (ON = security messages blocked)
- F3: iCue Protocol select - ON = 1.3.6 or lower; OFF = 1.3.6 or higher
- F2: Timeout (ON = Timeout on)
- F1: DISP HB (ON = Enabled [require dispatcher heart beat signal])

Button action after F8 Function selected (Bridge menu entered):

- Press N to cycle through menu
- Press S to select
- Use S to move cursor
- Use +/- to change selection
- Press N to go to save menu
- Press S to save



F8 Menu Screens

Software Version

- Version (software): i.e., 002.000.000

Data Stream, C=CAN, N=NET, R=RECEIVE, S=SEND. Messages sent and received should remain in sync. Provides a way to see that communication is occurring properly.

- CR 0 0
- NS 0 0

Data Stream

- NR 0 0
- CS 0 0

Message Volume (Peak = highpoint of messages in the buffer; 9520=max cap in buffer).

- Curr CAN Q: 0 (number of messages currently in the buffer)
- Peak: 0/9520

Message Volume (See above.)

- Curr NET Q: 0
- Peak: 0/9520

Receive State Flags (1 in any position indicates a message failed and the reason. From the left to the right, First byte was not the header; Second section did not match MCE protocol; Third section did not match MCE protocol; fourth section did not match MCE protocol.)

- RCV STATE FLAGS
 0 0 0 0

Time Out Errors (Number of messages dropped because full message not found within one second.)

- TIME OUT ERRS
 0000

Reset Ethernet Port (Provides a way to reset the Ethernet port if NET communications are presenting a problem.)

- RESET XPORT?
- YES = S, NO = N

Switch State Menus —

- F1: DISP HB: ON = No HB, OFF = HB - In the ON position, a heart beat signal is required from the elevator dispatcher to validate its function. Used for factory test. Default = OFF.
- F2: TIMEOT: ON = Allow Timeout - In the ON position, enables the system to drop incomplete messages after one second and continue processing. Default is OFF. If system has excessive latency, setting this to ON may help prevent communications “hanging.”
- F3: PROTCL: ON = <= 1.3.6, OFF = >= 1.3.6 - Set according to the iCue software version.
- F4: FILTER: ON = ONLY security messages - ON for Security bridge boards.
- F5 FILTER: ON = ONLY kiosk messages - ON for System bridge boards.
- F6: No function
- F7: No function
- F8: Bridge Menu entry