

MOTION CONTROL ENGINEERING, INC.



Sentry v2.3 USER GUIDE



Motion Control Engineering
11380 White Rock Road
Rancho Cordova, CA 95742

voice 916 463 9200
fax 916 463 9201
www.mceinc.com



User Guide

Sentry v2.3

Copyright

This document is owned and copyrighted by Motion Control Engineering. All Rights Reserved. Upon request by Motion Control Engineering, this document must be returned to Motion Control Engineering. ©Motion Control Engineering, 2022.

Trademarks

All trademarks or registered product names appearing in this document are the exclusive property of the respective owners.

Warning and Disclaimer

Although every effort has been made to make this document as complete and accurate as possible, Motion Control Engineering and the document authors, publishers, distributors, and representatives have neither liability nor responsibility for any loss or damage arising from information contained in this document or from informational errors or omissions. Information contained in this document shall not be deemed to constitute a commitment to provide service, equipment, or software by Motion Control Engineering or the document authors, publishers, distributors, or representatives.

Limited Warranty

Motion Control Engineering (manufacturer) warrants its products for a period of 15 months from the date of shipment from its factory to be free from defects in workmanship and materials. Any defect appearing more than 15 months from the date of shipment from the factory shall be deemed to be due to ordinary wear and tear. Manufacturer, however, assumes no risk or liability for results of the use of the products purchased from it, including, but without limiting the generality of the forgoing: (1) The use in combination with any electrical or electronic components, circuits, systems, assemblies or any other material or equipment (2) Unsuitability of this product for use in any circuit, assembly or environment. Purchasers' rights under this warranty shall consist solely of requiring the manufacturer to repair, or in manufacturer's sole discretion, replace free of charge, F.O.B. factory, any defective items received at said factory within the said 15 months and determined by manufacturer to be defective. The giving of or failure to give any advice or recommendation by manufacturer shall not constitute any warranty by or impose any liability upon the manufacturer. This warranty constitutes the sole and exclusive remedy of the purchaser and the exclusive liability of the manufacturer, AND IN LIEU OF ANY AND ALL OTHER WARRANTIES, EXPRESSED, IMPLIED, OR STATUTORY AS TO MERCHANTABILITY, FITNESS, FOR PURPOSE SOLD, DESCRIPTION, QUALITY PRODUCTIVENESS OR ANY OTHER MATTER. In no event will the manufacturer be liable for special or consequential damages or for delay in performance of this warranty.

Products that are not manufactured by MCE (such as drives, CRTs, modems, printers, etc.) are not covered under the above warranty terms. MCE, however, extends the same warranty terms that the original manufacturer of such equipment provide with their product (refer to the warranty terms for such products in their respective manual).

End User License Agreement

This End User License Agreement ("Agreement") grants you the right to use the software contained in this product (the "Software") subject to the following restrictions: You may not: (i) copy the Software, except for archive purposes consistent with your standard archive procedures; (ii) transfer the Software to a third party apart from the entire product; (iii) modify, decompile, disassemble, reverse engineer or otherwise attempt to derive the source code of the Software; (iv) export the Software or underlying technology in contravention of applicable U.S. and foreign export laws and regulations; and (v) use the Software other than in connection with operation of the product.

"LICENSOR'S SUPPLIERS DO NOT MAKE OR PASS ON TO END USER OR ANY OTHER THIRD PARTY, ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY OR REPRESENTATION ON BEHALF OF SUCH SUPPLIERS, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, TITLE, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."

Important Precautions and Useful Information

This preface contains information that will help you understand and safely maintain MCE equipment. We strongly recommend you review this preface and read this manual before installing, adjusting, or maintaining Motion Control Engineering equipment. This preface discusses:

- Safety and Other Symbol Meanings
- In This Guide

Safety and Other Symbol Meanings



Danger

This manual symbol is used to alert you to procedures, instructions, or situations which, if not done properly, might result in personal injury or substantial equipment damage.



Caution

This manual symbol is used to alert you to procedures, instructions, or situations which, if not done properly, might result in equipment damage.



Note

This manual symbol is used to alert you to instructions or other immediately helpful information.

In This Manual:

This manual is the installation and operation guide for the Sentry monitoring application. When viewed online as a pdf file, hyperlinks link to related topics and informational web sites. The manual includes:

- [Contents](#): Table of Contents. When viewed online as a pdf file, hyperlinks in the Contents link to the associated topic in the body of the manual.
- [Section 1](#). General description and installation instructions.
- [Section 2](#). Quick Start: Quick instructions for getting started using Sentry.
- [Section 3](#). Reference: Detailed explanation of screen controls.



Contents

Section 1. Important Precautions and Useful Information

Safety and Other Symbol Meanings	1-iv
In This Manual:	1-iv

Section 1. Sentry

Sentry	1-1
Card Readers	1-2
Integrated Access Control Companies	1-3
Access Control systems available through BraXos	1-4
Hotel Guest Cards	1-4
Installation	1-5
Determining Hardware Requirements	1-5
Installing Sentry	1-5
Configuring Sentry	1-6
Connection to iCue	1-6
Authorization	1-6

Section 2. Quick Start

Sentry	2-1
Menu	2-2
Service Status	2-2
Browse Data	2-2
Clear Screen	2-3
Settings	2-3
About	2-3
Data Views	2-4
MCE Reader:	2-4
Access Control:	2-5
Turnstile:	2-6
Building Map	2-7
Diagnostic LEDs	2-8
Remote Security Status	2-8

Security Override Status	2-8
Elevator Eligibility Mode	2-8
Connection Status	2-8
Checking Sentry is connected in iView	2-8

Section 3. Reference

Setting Up Security - Elevator Side	3-1
Security	3-2
Security Type	3-3
Sentry Connection Status	3-4
Mapping Readers and Touchscreens	3-5
Default Security Map	3-7
Testing Security	3-8
Override Security	3-8
Active Security Map	3-9
Testing Card Swipes	3-10
Troubleshooting	3-11

Sentry

Sentry is an elevator security interface application that sits between the MCE's iCue elevator dispatcher and one of many non-MCE access control systems. For Sentry to work properly, the access control system must have an integration with MCE's elevator protocol. Sentry runs on the same PC as the iCue dispatcher. It waits for the access control application to connect to it; it then translates messages between iCue and the access control software so that the dispatcher does not need to change every time there is a new access control system introduced.

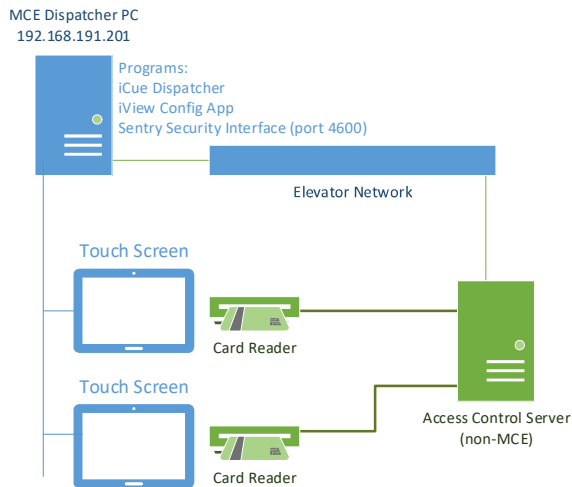
Through Sentry, the access control system may send over which floors require card access, which floors are locked out and which floors are open to the public. Sentry allows for all security schedules to be managed by the access control system instead of trying to synchronize schedules on both the access control and elevator system. Sentry creates a path for the access control system to send over card swipes over a network interface instead of one line per floor relay interface, eliminating much of the wiring between access control and elevator systems. Turnstiles can be implemented so that a card swipe registers a call automatically. Finally, Sentry sends valuable tracking information back to your access control to be logged, such as which elevator was assigned a call and what floor was selected.

Sentry has an intuitive graphical user interface that can be used to see all information shared between the access control system and the elevator system. Sending data over a network interface is much more efficient than over discrete wires, but mechanics may worry that troubleshooting is harder in a black box. Not with Sentry! You will be able to see each card swipe sent to and each acknowledgement from the dispatcher. Sentry keeps these in a local database so any complaints can be investigated even after the fact.

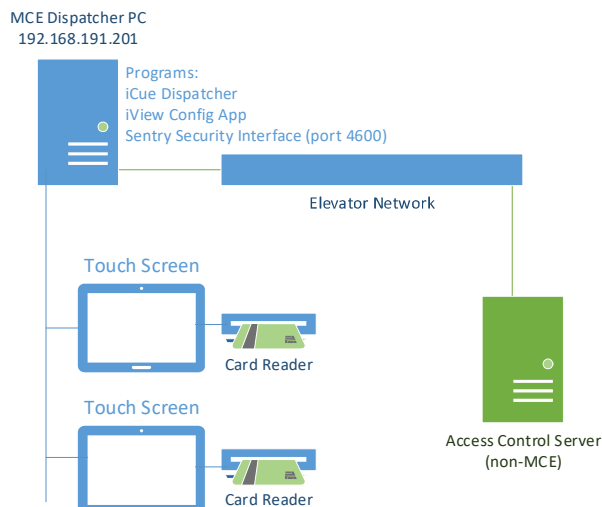
Card Readers

Card readers are the front end interface for the access control system. Through card readers the access control systems are able to control access to elevators and/or floors by allowing or restricting access based on the card holders access privileges programmed on their cards. MCE touch screens can house a variety of supported card readers, which fall into either one of two categories:

Segregated Readers: These readers are housed by MCE touch screen but are powered by and communicate to the access control company directly. Sentry does not see any messages between reader and access control. When access control gets a message, it sends floor destination data to Sentry.



Integrated Readers: In this scenario, MCE installs HID 5127 multipurpose readers into the touch screen housing. These readers are powered by the MCE touch screen and the touch screen communicates directly with the readers over USB. When a card is swiped, the reader sends data to the touch screen, which then uses the existing elevator communication to relay it to the Sentry and Sentry sends a destination floor access request to the access control system. This architecture requires access control system to be able to take card reads from Sentry and saves dozens of extra hours of wiring every single card reader back to a panel board.



Integrated Access Control Companies

Below is a list of access control systems that Sentry has direct integrations with. Please verify with your MCE sales contact the version of access control available at time of sale.

Table 1.1 Integrated Access Control Companies



<https://www.amag.com/>



<https://www.blubox.com/>



<https://braxos.com/>



<http://centennialsecurity.com/>



<https://www.datawatchsystems.com/>



<http://forteksecurity.com/>



<https://www.genetec.com/>



<https://buildings.honeywell.com/us/en/brands/our-brands/security/>



<https://www.ict.co/Solutions>



<https://www.kastle.com/>



<https://www.lenel.com/products/onguard>



http://www.swhouse.com/products/software_CCURE9000.aspx

Access Control systems available through BraXos

MCE can work with BraXos to connect to even more access control systems. BraXos would be provided by the Security Contractor or Building Management. BraXos can integrate to the following companies without any change to Sentry.

- S2
- Siemens

Hotel Guest Cards

BraXos is also needed for Hotel system integration including Assa Abloy (Ving) or Kaba (SafLok).

Installation

Installing Sentry includes:

- Determining Hardware Requirements
- Installing Sentry software
- Configuring Sentry

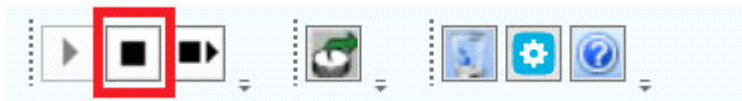
Determining Hardware Requirements

Sentry will normally be installed on the iCue dispatcher PC supplied by MCE. If there is a need to install Sentry on a separate PC, the following configuration is a minimum.

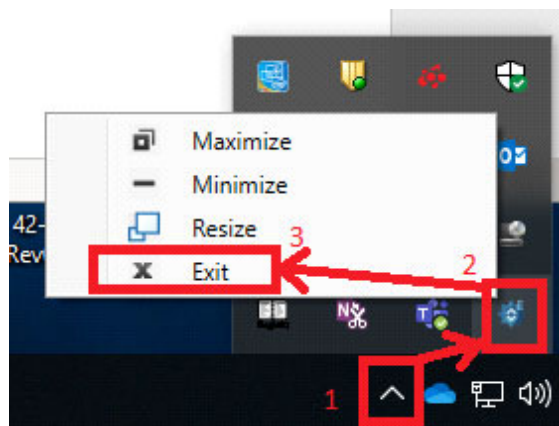
- Microsoft Windows 7 Professional or greater
- 4 GB RAM
- Intel 1.6 GHz i3 processor
- 10/100 Ethernet
- 1280x1024 display

Installing Sentry

1. Stop existing Sentry service, if one is running the MCE Sentry application, by clicking the Stop button in the application window.



2. Exit Sentry GUI application.



3. Uninstall any previous versions of Sentry (see old versions below).
4. Insert new media (CD or USB Stick) with latest Sentry installer.
5. Copy Sentry Software installer to the PC Desktop.
6. Run Setup.exe and follow on screen instructions.

Old Versions:

If you have an older version of Sentry already installed, use Add/Remove Program function from the Microsoft Windows Control Panel to remove it before installing new software.

Configuring Sentry

Any changes to the Sentry configuration require a restart of the Sentry application.

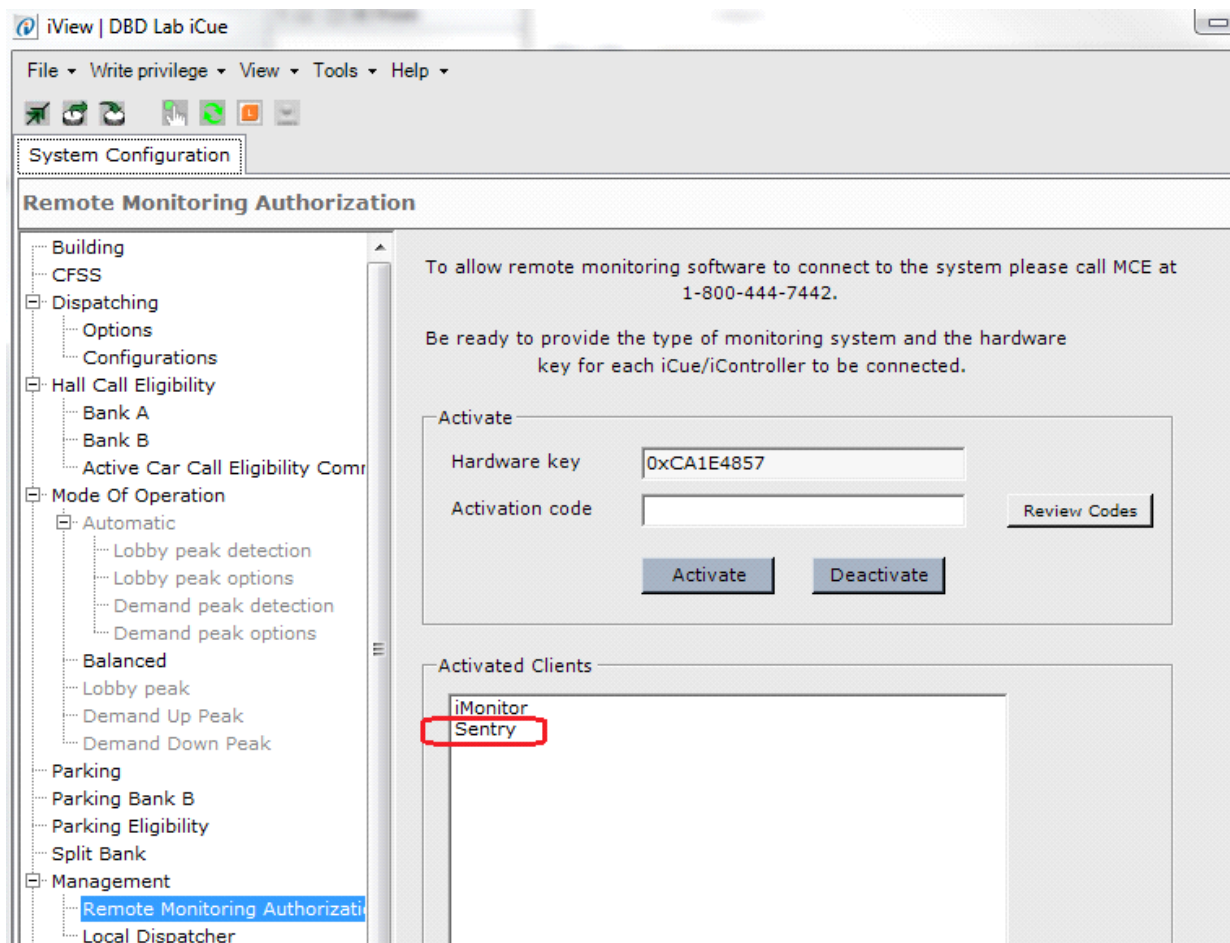
Connection to iCue

Sentry is set up to automatically connect to iCue if it is on the same PC. Sentry connects to only one iCue. If there are multiple elevator banks in the building, each dispatcher will have its own Sentry application running. The access control system is responsible for connecting to multiple Sentry systems.

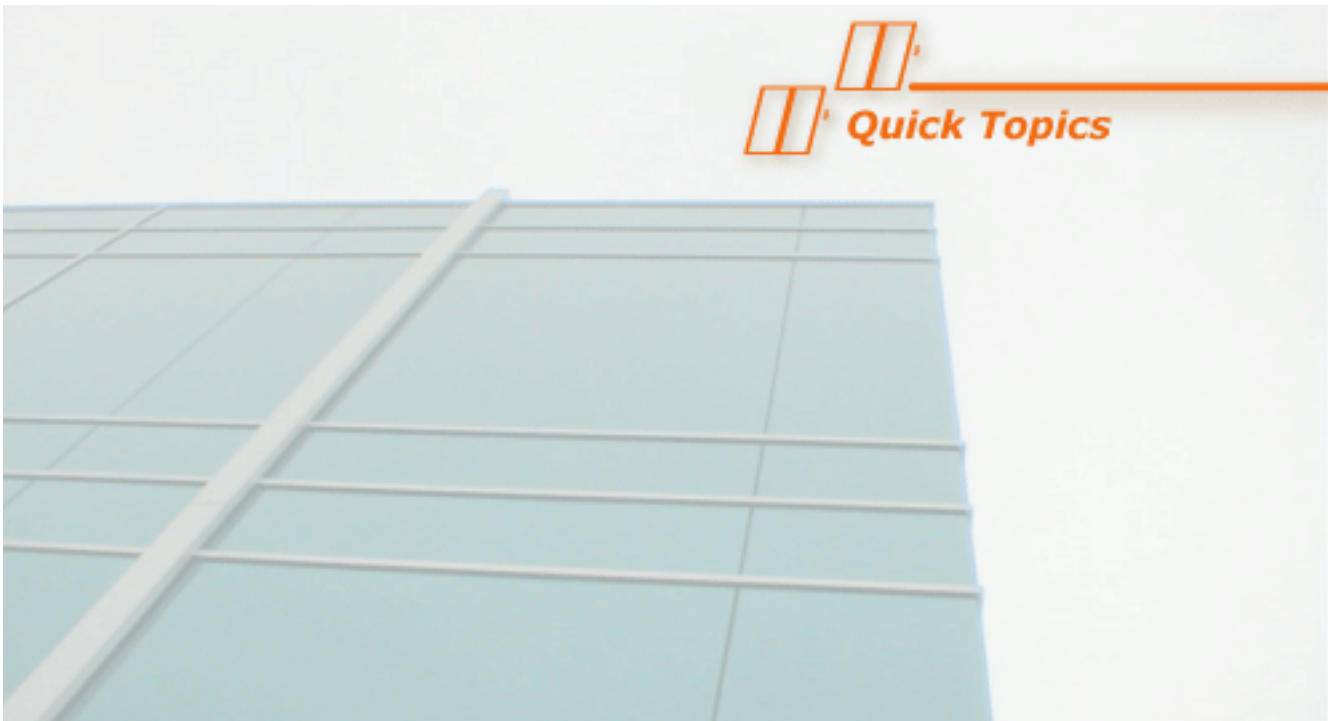
Authorization

The iCue must have a valid Sentry Authorization key enabled before Sentry will be allowed to connect. Use iView to connect to the dispatcher and check that Sentry's authorization key has been accepted.

Connect the iView configuration application to the iCue dispatcher.



First, verify that Sentry is activated on the System Configuration > Management > Remote Monitoring Authorization tab. If you do not see Sentry, contact MCE support to obtain an activation code.



Quick Start

2

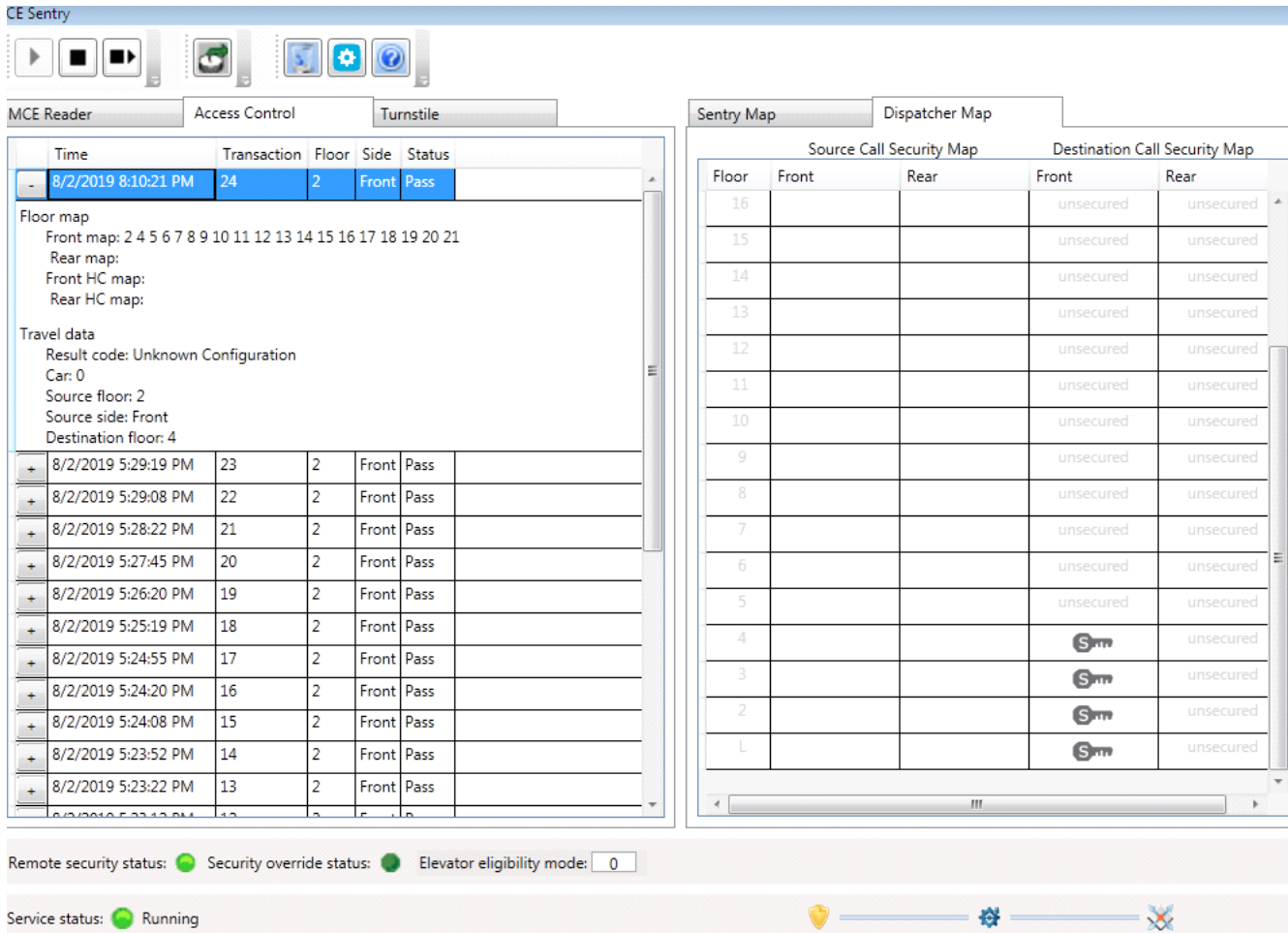
Sentry

Sentry should always be running. If you need to start the graphical user interface:



Double click the desktop icon

The application should automatically come up and connect to iCue.



CE Sentry

MCE Reader Access Control Turnstile

Time	Transaction	Floor	Side	Status
8/2/2019 8:10:21 PM	24	2	Front	Pass
8/2/2019 5:29:19 PM	23	2	Front	Pass
8/2/2019 5:29:08 PM	22	2	Front	Pass
8/2/2019 5:28:22 PM	21	2	Front	Pass
8/2/2019 5:27:45 PM	20	2	Front	Pass
8/2/2019 5:26:20 PM	19	2	Front	Pass
8/2/2019 5:25:19 PM	18	2	Front	Pass
8/2/2019 5:24:55 PM	17	2	Front	Pass
8/2/2019 5:24:20 PM	16	2	Front	Pass
8/2/2019 5:24:08 PM	15	2	Front	Pass
8/2/2019 5:23:52 PM	14	2	Front	Pass
8/2/2019 5:23:22 PM	13	2	Front	Pass

Floor map
Front map: 2 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
Rear map:
Front HC map:
Rear HC map:

Travel data
Result code: Unknown Configuration
Car: 0
Source floor: 2
Source side: Front
Destination floor: 4

Sentry Map Dispatcher Map

Source Call Security Map Destination Call Security Map

Floor	Front	Rear	Front	Rear
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			S-m	unsecured
3			S-m	unsecured
2			S-m	unsecured
L			S-m	unsecured

Remote security status: Security override status: Elevator eligibility mode: 0

Service status: Running

Menu

Service Status

The Sentry background service is the software that does all the translating to access control system. Check that the service is running by looking at the lower left corner of the application.

Service status: Running

If the Service Status is showing stopped, start the service with the play button at the upper left of the ribbon.



Play = Start Sentry

Stop = Stop Sentry

Stop/Start = Restart the Sentry service. Do this after making any changes to the Sentry parameters.

Browse Data



In cases where you want to view data that has already transitioned off screen, select this button to pick a data set and time window.

Clear Screen



This button will clear out the data view so you can watch for new swipes or turnstile commands. Data cleared is still in the data base.

Settings



This button will open the settings menu.

1. iCue IP Address: IP address of MCE iCue dispatcher. Use 127.0.0.1 if the MCE Sentry is on the same PC as the iCue dispatcher.
2. Sentry Port: TCP port that Sentry is listening for an access control connection to connect on. Default is 4600.
3. Enable Heartbeats:
 - Checked: If Sentry does not see a heartbeat from the access system it will close the connection (Default).
 - Unchecked: Sentry does not look for access control heartbeats.
4. Heartbeat Receive Timeout: How long Sentry will wait before closing a connection if watchdog option is checked (Default = 30 seconds).
5. Heartbeat Send Frequency: Number of seconds to send a application heartbeat to the access control system if no other data is sent. May need to be 3 seconds for BraXos connections.
6. Sentry treats passenger maps as source maps:
 - No - map sent due to card swipe tells elevator system where passenger can go (Default).
 - Yes - map sent due to card swipe tells elevator system where passenger can leave from.
7. Card swipe bit value to allow access:
 - 0 - access control sends a 0 to indicate passenger can go to a floor (Default).
 - 1 - access control sends a 1 to indicate passenger can go to a floor.
8. Source floor base: What number does the access control system consider the bottom floor for messages about source floors (usually 0 or 1) Default is 1.
9. Destination floor base: What number does the access control system consider the bottom floor for messages about destination floors (usually 0 or 1) Default is 1.
10. Home floor: Used by some access control systems to specify which floors this Sentry should use for global turnstiles. For example, if there are two groups of elevators low rise and high rise, the access control system could encode 0-20 as floors the low rise serves and 21-40 as floors the high rise serves. This Sentry can be set to 21-40 to ignore any turnstile messages with floor set to 0-20. If it sees a floor of 33, it will subtract 21 to get an offset of 12 and Sentry will know that the turnstile message is for the 12th floor.

Note

Restart Sentry for the setting changes to take effect.

About



Displays Sentry version information and MCE contact information.

Data Views

MCE Reader:

If the job has integrated MCE readers, this screen will show the data flow for each card from MCE to the access control, then what floors the card can access, and finally the travel data back from the elevator. This tab shows data from integrated readers (MCE card readers).

MCE Reader							
Access Control				Turnstile			
	Time	Transaction	Floor	Side	KioskId	Num of bits	Bridge board
+	9/13/2019 3:17:48 PM	37	L1	Front	2	26	192.168.191
+	9/13/2019 12:47:53 PM	36	7	Front	1	26	192.168.191
-	9/13/2019 12:18:57 PM	35	7	Front	1	26	192.168.191
Card data							
64-81-87-00-00-00-00-00-00-00-00-00-00-00-00-00							
Floor map							
Front map: 3 9 10 11							
Rear map:							
Front HC map:							
Rear HC map:							
Travel data							
Result code: Timed Out							
Car: 0							
Source floor: L1							
Source side: Front							
Destination floor: L1							
+	9/13/2019 12:15:38 PM	34	L1	Front	2	26	192.168.191
+	9/13/2019 12:15:29 PM	33	7	Front	1	26	192.168.191

The Top Level shows the time, the transaction ID linking the MCE swipe with the access control system, the floor the reader is on, the side, the kiosk ID, the number of bits MCE read from the card, and the address of the bridge board the read came in on. The Card data shows the raw card number that MCE sent to the access control system. The Floor map is the data returned by the access control system for the passenger. This shows the floors the passenger is cleared to use. The Travel data is the information sent back to the access control system for logging. This includes the result of the swipe, car assigned, and floor traveled to.

Access Control:

This tab shows data from a segregated system (reader communicates to access control directly).

MCE Reader		Access Control		Turnstile	
Time	Transaction	Floor	Side	KioskId	Status
+ 9/13/2019 3:18:04 PM	38	7	Front	1	Pass
+ 9/13/2019 3:17:48 PM	37	L1	Front	2	Pass
Flags Vip: <input checked="" type="checkbox"/> Hospital: <input type="checkbox"/> Handicap: <input type="checkbox"/> Visitor: <input type="checkbox"/> Floor map Front map: 3 9 10 11 Rear map: Front HC map: Rear HC map: Travel data Result code: Pass Car id: 2 Source floor: L1 Source floor id: 0 Source side: Front Destination floor: 3 Destination floor id: 0					
+ 9/13/2019 3:03:09 PM	0	L1	Front	0	Pass
+ 9/13/2019 3:03:02 PM	0	L1	Front	0	Pass
+ 9/13/2019 3:02:57 PM	0	L1	Front	0	Pass

2

Each record can be expanded to show what floor map was sent by access control system (floors the passenger was able to go to). Travel data is also paired to see which car was assigned and which floor the passenger selected.

Note

Floor refers to floor label and Floor ID refers to the landing offset, with 0 (zero) being the bottom floor.

Turnstile:

This tab shows data when a turnstile call is registered automatically from the access control system.

MCE Reader		Access Control		Turnstile				
	Time	Transaction	Floor	Side	Status	Dest. floor	Dest. side	Flags
+	8/2/2019 8:13:35 PM	3359	3	Front	Pass	5	Front	0
-	8/2/2019 8:13:30 PM	3359	3	Front	Pass	12	Front	0
Travel data Result code: Pass Car: 0 Source floor: 2 Source side: Front Destination floor: 0								
+	8/2/2019 8:13:24 PM	3359	3	Front	Pass	6	Front	0
+	8/2/2019 8:13:13 PM	3359	3	Front	Pass	8	Front	0
+	8/2/2019 8:12:52 PM	3358	3	Front	Pass	8	Front	0

Each record can be expanded to see the travel data associated.

Note

Floor refers to floor label and Floor ID refers to the landing offset, with 0 (zero) being the bottom floor.

Building Map

Sentry shows the current building map on the right side of the program. This map is set by the access control system to define floors and being either:





- Locked out (no one can access) - Padlock icon
- Require card access (secured) - S Key icon
- Open to the Public (unsecured) - Unsecured text

Destination maps control which floors you can select in an elevator.

Source maps control which floors you can call an elevator from.

Note


These maps are intended for display only. Use the access control system to change any values.

Sentry Map		Dispatcher Map		
Source Call Security Map			Destination Call Security Map	
Floor	Front	Rear	Front	Rear
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
3				unsecured
2				unsecured
L				unsecured

Sentry shows its current map from the access control application as well as the current map being used by the dispatcher for troubleshooting. These should always match.


Diagnostic LEDs

Remote Security Status

Remote security status: 

This LED indicates that the elevator dispatcher is configured to use Sentry as a remote security interface. If this LED is off, make sure the security type in iCue is set to Remote Security. Please refer to “Security” on page 3-2.

Security Override Status

Security override status: 

This LED indicates that the elevator SECURITY OVERRIDE is active so the elevator system is not going to use any security data from the access control system. If this LED is on, make sure the iCue > Security configuration is set to Active. Please refer to “Security Type” on page 3-3.

Elevator Eligibility Mode

Elevator eligibility mode:

This diagnostic shows which hall call eligibility map the iCue is currently using.

Connection Status



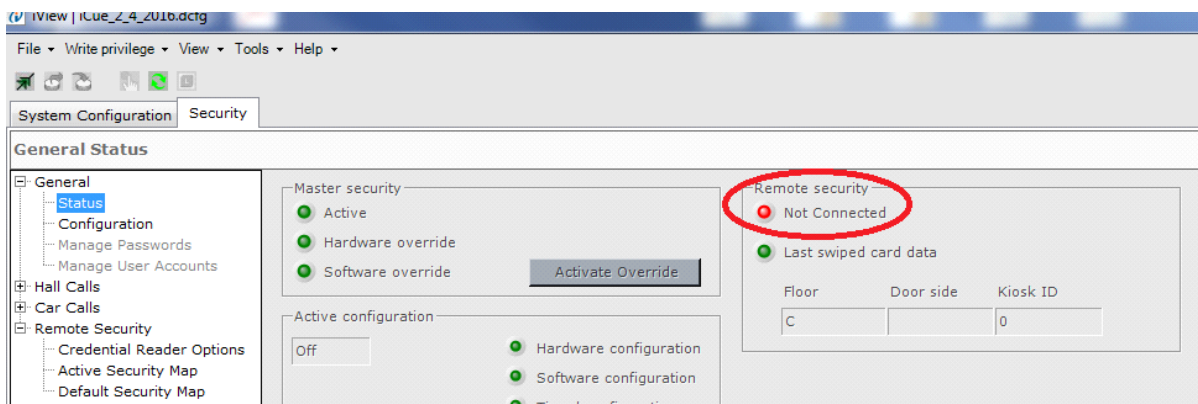
This diagnostic shows the connection status between the access control software (shield) and Sentry (gear) as well as connection status between Sentry (gear) and iCue elevator dispatcher (diamond). If connection is lost a red X will be displayed on the line.



Checking Sentry is connected in iView

You can open the Security > Status screen in iView to check that Sentry is connected. Please refer to “Sentry Connection Status” on page 3-4. The color of the LED circled indicates status:

- Red: Sentry is not connected
- Yellow: Sentry is connected, but access control is not connected to Sentry
- Green: Both access control and Sentry are connected.





Reference

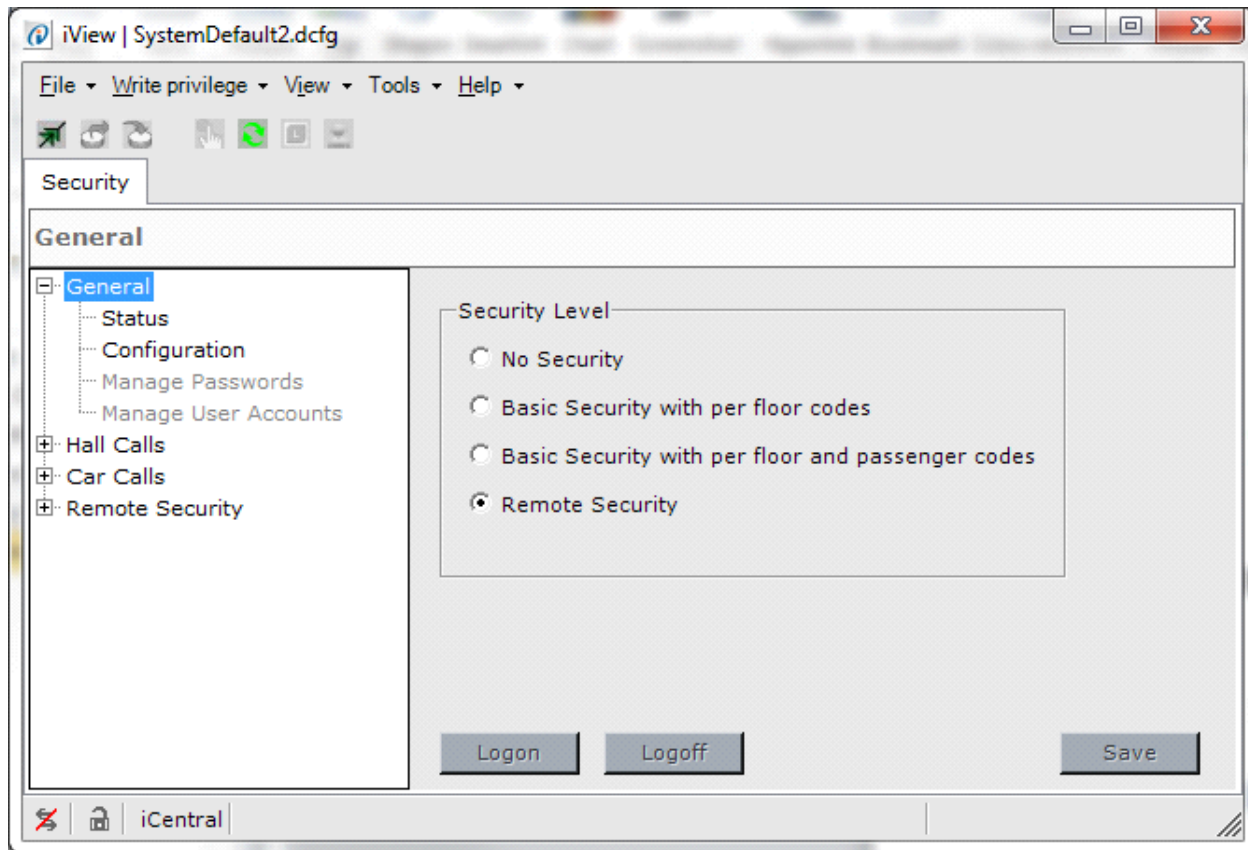
Setting Up Security - Elevator Side

Connect iView configuration tool to the iCue Dispatcher.

3

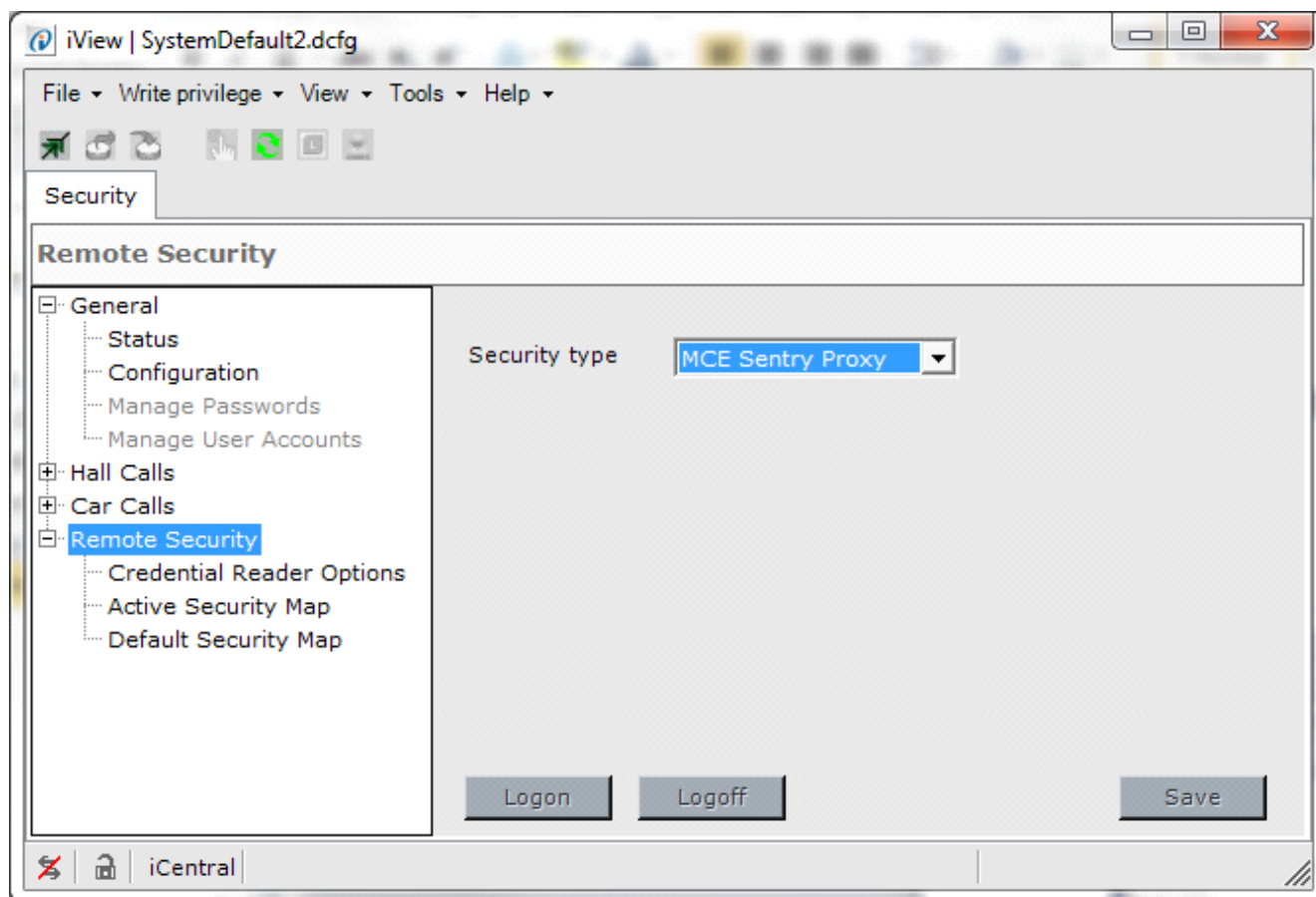
Security

Go to View > Configuration > Security and logon. Default password is **manager**



Under the General tab, make sure that the Security Level is set to **Remote Security**.

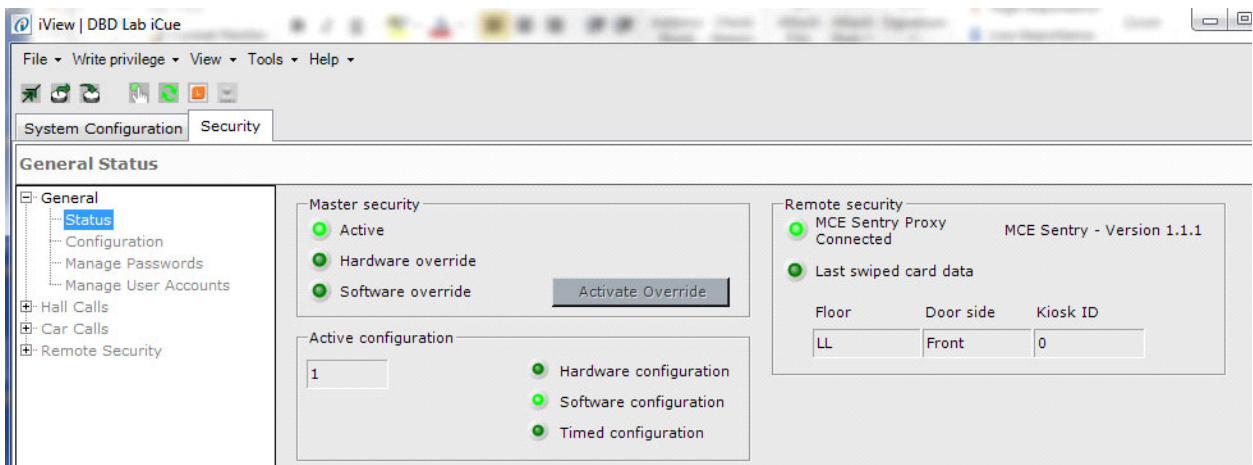
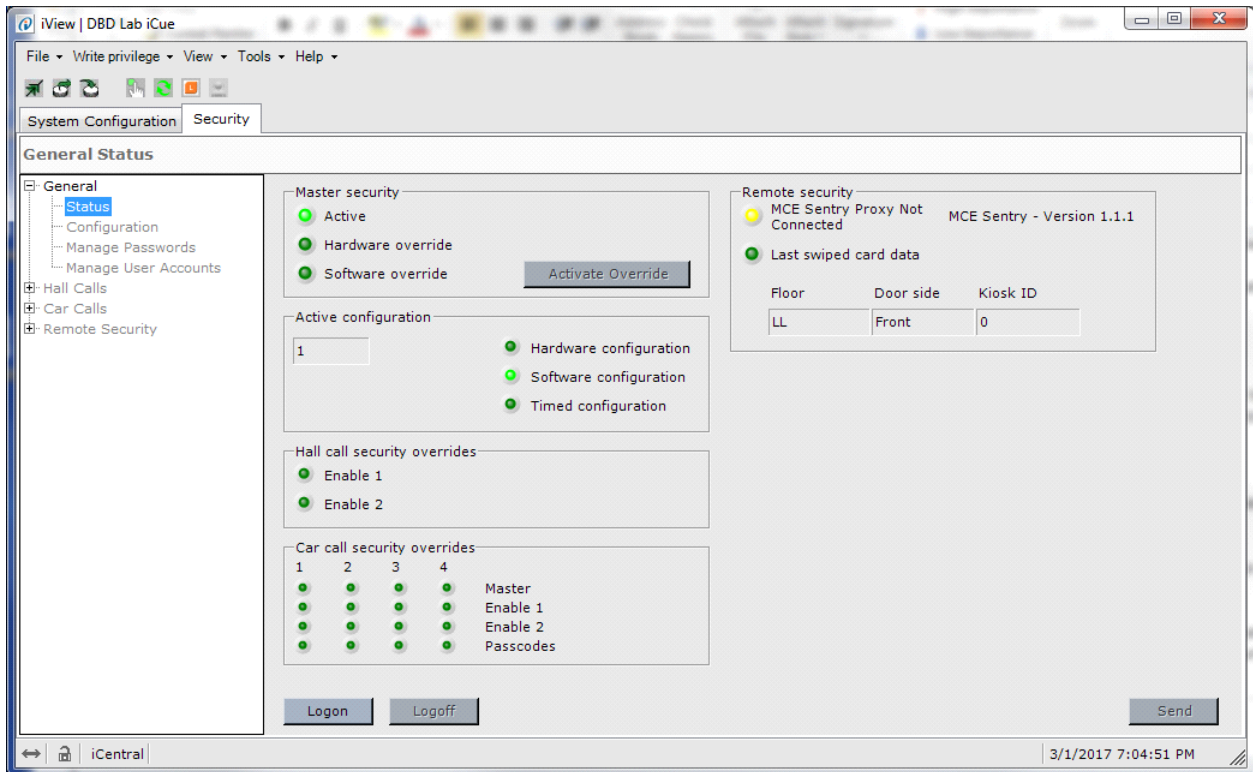
Security Type



3

On the Remote Security tab, make sure the Security Type is set to ***MCE Sentry Proxy***.

Sentry Connection Status



On the Status tab, verify that the Remote security LED is Green and you have a version for MCE Sentry.

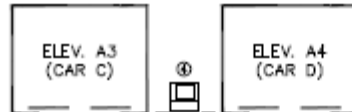
- **Red LED** = No connection between iCue and Sentry - check that Sentry is running.
- **Yellow LED** = iCue is connected to Sentry, but Sentry is not connected to the access control system. Verify access control system is running and can PING the PC running Sentry. Verify access control is configured properly from their manufactures documentation.
- **Green LED** = iCue is connected to Sentry and Sentry is connected to access control system.

Mapping Readers and Touchscreens

The most crucial part of setting up a third party access system is mapping the card readers to the right touch screens.

KIOSK ID AND KIOSK TO CAR WALK TIMES

KIOSK ID	WALK TIME FROM KIOSK (SEC.)			
	ELEV. A1	ELEV. A2	ELEV. A3	ELEV. A4
4	-	-	2	2



TOP LANDING (FLOOR LABELED "PH")

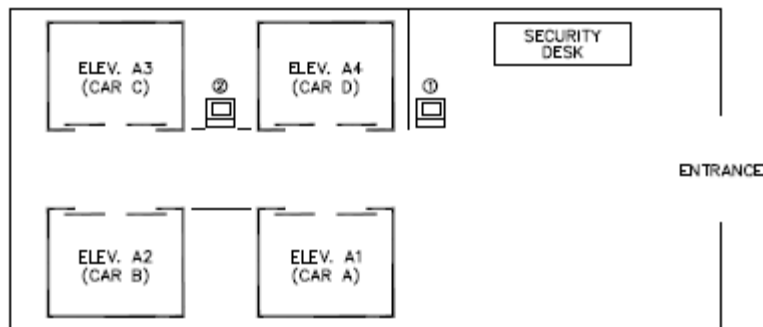
KIOSK ID	WALK TIME FROM KIOSK (SEC.)			
	ELEV. A1	ELEV. A2	ELEV. A3	ELEV. A4
3	4	4	2	2



5th THRU 15th LANDING (FLOOR LABELED "6" THRU "16")

3rd AND 4th LANDING ARE FALSE FLOORS

KIOSK ID	WALK TIME FROM KIOSK (SEC.)			
	ELEV. A1	ELEV. A2	ELEV. A3	ELEV. A4
1	2	4	2	2
2	4	4	2	2



2nd LANDING (FLOOR LABELED "1")

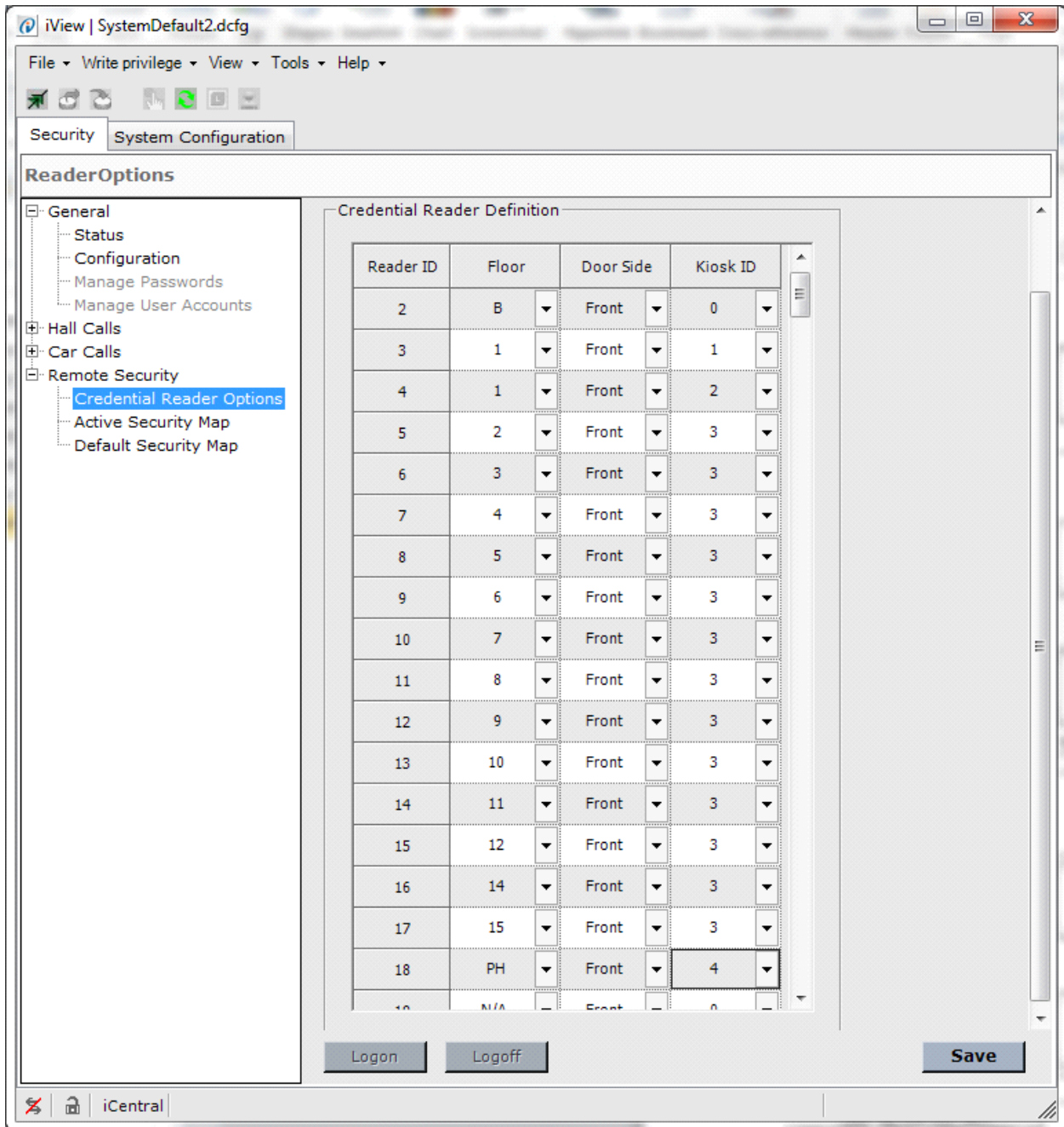
KIOSK ID	WALK TIME FROM KIOSK (SEC.)			
	ELEV. A1	ELEV. A2	ELEV. A3	ELEV. A4
0	-	-	-	2



BOTTOM LANDING (FLOOR LABELED "B")

Above is a sample print showing kiosk (touch screen) IDs as numbers in circles. Notice that multiple floors may have the same kiosk ID if the relationship between the kiosk and car doors is the same.

In this example, kiosk ID 0 is at "B", kiosk IDs 1 and 2 are at floor "1", kiosk ID 3 is used for all middle floors, and finally, kiosk ID 4 is used at "PH" the top floor.



Go into Remote Security > Credential Reader Options and verify the mapping matches job prints for floor, side, and Kiosk ID. The order and Reader ID is not important for the elevator side but is important depending on how the access control system sends over data. Consult the access control system documentation for instructions on matching Reader ID.

Default Security Map

If security is activated, but the link between the access control and elevator system is broken, you can configure the iCue to either use the last known security map (any secured floors end up becoming locked out because there is no way to get card swipes), or you can set up a default security map to go to. Again, any secured floors will end up being locked out because there is no way to read a card swipe.

iView | SystemDefault2.dcfg

File Write privilege View Tools Help

Security System Configuration

DefaultSecurityMap

- General
 - Status
 - Configuration
 - Manage Passwords
 - Manage User Accounts
- Hall Calls
- Car Calls
- Remote Security
 - Credential Reader Options
 - Active Security Map
 - Default Security Map**

If communication to the security manager fails:

☐ Use last received map from security manager

☒ Use default security map

Floor label	Source Call Security Map		Destination Call Security Map	
	Front	Rear	Front	Rear
PH				
16				
15				
14				
12				
11				
10				
9				
8				
7				
6				
5				
4				
3				
2				
1				
B				

Set Selection

Logon Logoff Save

iCentral

3

Go to Default Security map and set Use Default Map. Make sure to unsecure any floors that need to be serviced if security link is broken. NOTE: Unsecured floors mean anyone has access to them; they become public. Most offices will choose to make floors public if the security link is broken, while laboratories, banks, or government buildings may choose to lock sensitive floors down.

Testing Security

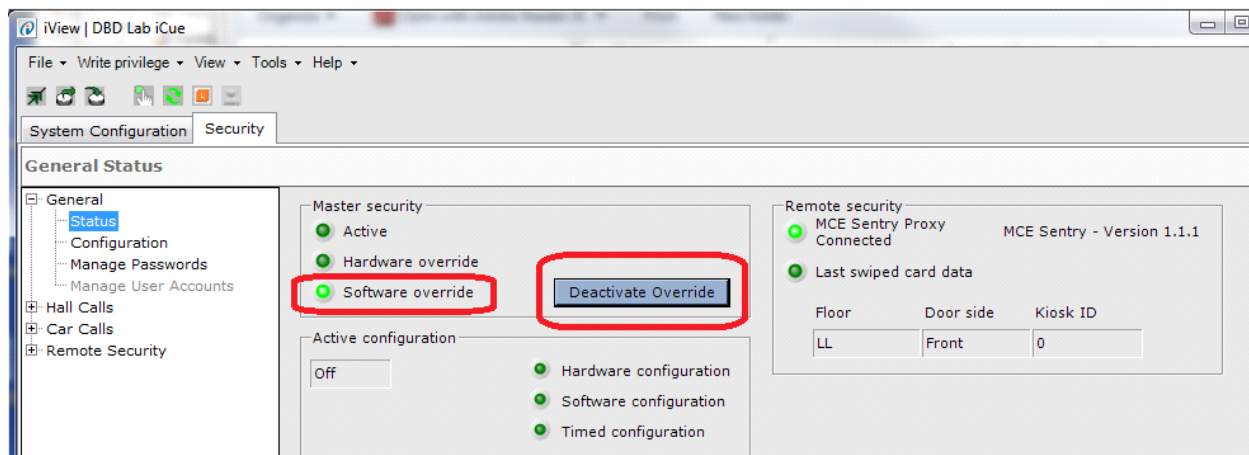
Once the third party access system is connected to Sentry and it is connected to iCue (green LED on Security Status page), we can start testing security features.

Override Security

To override security go into the Status tab and click the Activate Override button. Once clicked it will turn into a Deactivate Override button and software override LED will light. During this time all floors will be treated as public.

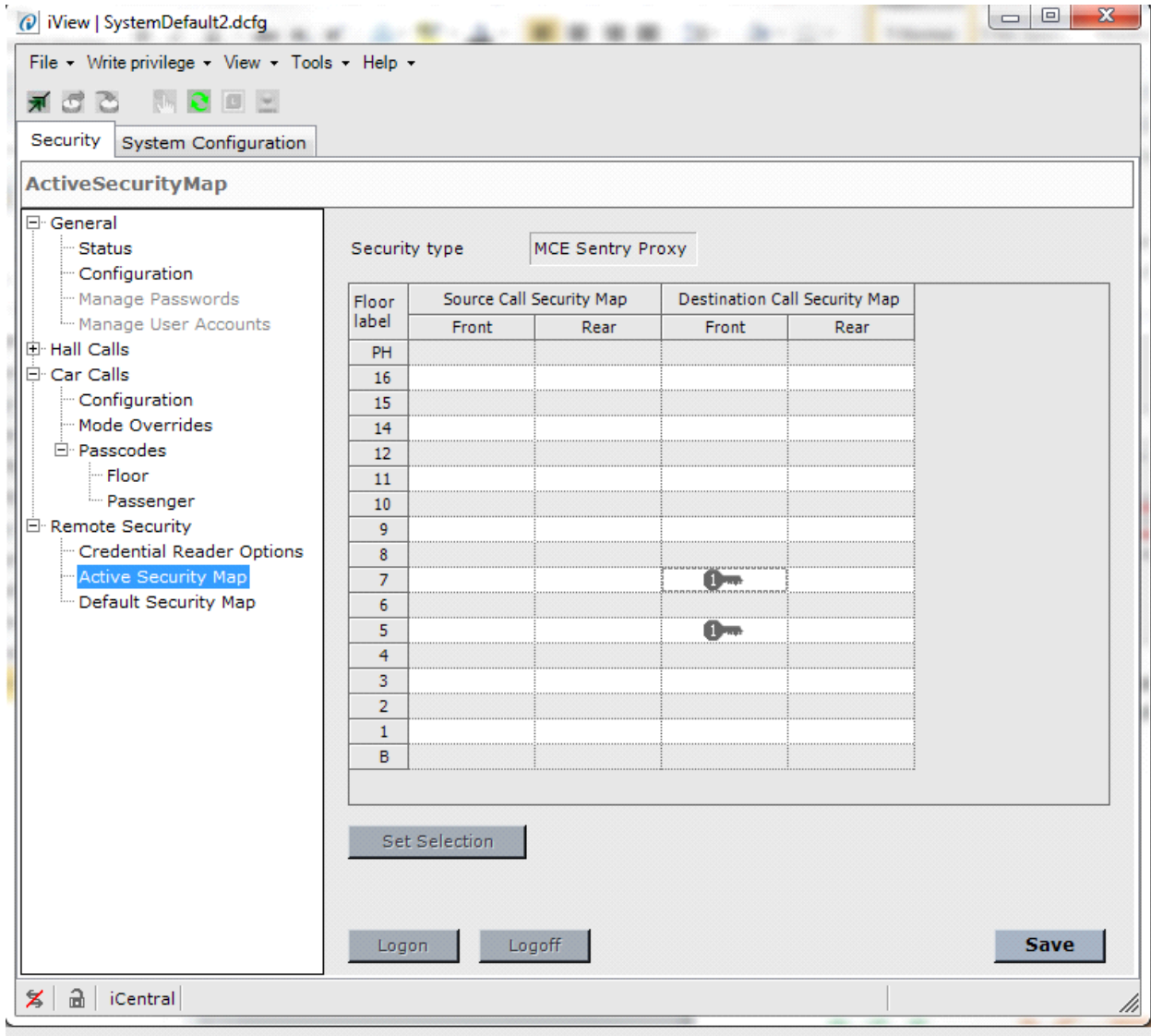
Note

It may be a good idea to override security while testing so testing does not interrupt passenger traffic. This decision depends on the type of building.



Active Security Map

The first thing the access system should do after connecting to the elevators is send over a map telling the elevators which floors will need card access and which are public. Verify this is correct in the Active Security Map.



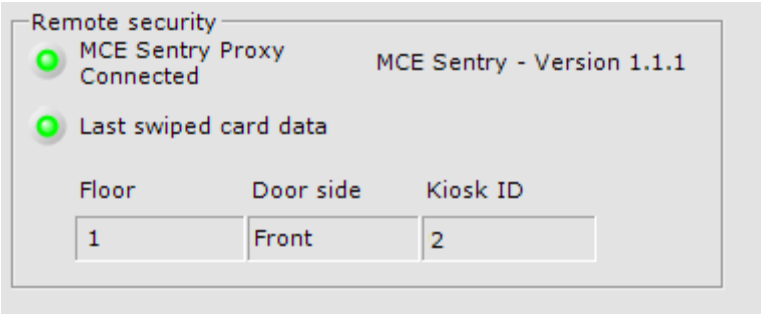
This map is populated by the access control system. This example shows that the access control system is telling the elevator system that a card is required to go to floor 5 or 7. Notice that there are maps for both source and destination.

Securing a Source floor means that no one can call an elevator to pick them up at that floor without a card. This is unusual and used only when an elevator serves public floors like outside unmanaged parking levels.

Securing a Destination floor means you have to have a card with valid access to travel TO that floor. This is the common type of security used in buildings.

Testing Card Swipes

iView will show the last card swipe the dispatcher received. You can use this function to double check that swiping a card is seen by the elevator system and that the mapping between kiosk and reader is properly done.



The Last swiped card data LED will blink when a new swipe is seen. The data below the LED will show the floor, side and kiosk ID sent.

Troubleshooting

Here are a couple of tips on troubleshooting the system if it is not working.

1. The Access Control system will not connect to Sentry.
 - Confirm Sentry is installed and running (at least a yellow LED).
 - Confirm that Sentry is an authorized client in Remote Monitoring Authorization .
 - Confirm that Sentry is the latest version from MCE.
 - Confirm Access system can ping the PC IP address Sentry is running on.
 - Confirm connection settings on the Access system are correct.
 - Confirm there are no firewalls blocking a connection.
2. The Access Control System is connected, but will not send an Active Map.
 - Review Access Control documentation for how to set up the elevator map and schedule changes based on timer tables.
3. Card swipes are not working.
 - Confirm Green Status light on iView Security Status menu.
 - Confirm kiosks are configured with kiosk IDs correctly.
 - Confirm reader mapping on Access Control side is set up correctly.
 - If multiple readers at same floor, try swiping each and then placing call from same kiosk.
 - If swiping has opposite effect (passenger can only go to floors they are not supposed to have access to and cannot go to floors they are set up to have access to), this indicates opposite polarity in bitmasks between Sentry and Access Control. Sentry has an option to flip on our side. Go to Settings button on Sentry GUI and check the option "**Passenger has access if Bitmask is**" parameter. Change and restart Sentry to try.
4. Passengers can go to any floors, even ones that show up as secured in the Active Map.
 - Confirm that Security Override is not set on the iView Security Status page.