

TX3 Series

MiVISION

MiVision Manual



*Copyright June 2025 Mircom Inc.
All rights reserved.*

MiVision Manual Version 4

Microsoft, MS-DOS, Windows, and Windows 2000/NT/XP/Vista/7/8/10 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Mircom
25 Interchange Way
Vaughan, Ontario
L4K 5W3
905.660.4655
<http://www.mircom.com>

Contents

1	Introducing MiVision 6
1.1	Requirements 6
1.2	Log into MiVision 6
1.3	Real Time Messaging Icon 9
1.4	Advanced Network Setup 9
1.5	Sites 10
1.6	Tools 16
1.7	Language 21
1.8	Help 21
1.9	Log Out 21
1.10	Send the Job 21
1.11	Firmware Upgrade 23
1.12	Commands 25
1.13	Change a Main Node's IP Address 28
2	Monitoring 31
2.1	Dashboard 31
2.2	Access Points 32
2.3	Elevators 33
2.4	Chart 35
2.5	Events 36
2.6	Maps 37
2.7	System 47
3	Touch Screen, Telephone Entry, and Emergency Phone Configuration 50
3.1	Configure a Panel 50
3.2	Touch Screen 60
3.3	Inputs 60
3.4	Outputs 62
3.5	Correlations 63
4	Touch Screen Appearance Configuration 67
4.1	Panels 68
4.2	Layouts 69
4.3	Themes 70
4.4	Videos and Banners 71
4.5	Advertising 77
4.6	Directory Groups 82
4.7	More Options 83
5	Card Access System Panel Configuration 88
5.1	Configure a Panel 88
5.2	Operations 89
5.3	Access Points 91
5.4	Inputs 93
5.5	Outputs 95
5.6	Correlations 97

6	Elevator Restriction Panel Configuration 101
6.1	Add an Elevator Restriction Unit 101
6.2	Operations 102
6.3	Configure Card Access with Elevator Restriction 103
6.4	Configure Residents with Elevator Restriction 108
7	People 112
7.1	View People 112
7.2	Add People 113
7.3	Remove People 113
7.4	View a Person's Profile 114
7.5	Edit Multiple People 121
8	Credentials 122
8.1	View Credentials 122
8.2	Add a Credential 123
8.3	Remove a Credential 124
8.4	Edit a Credential 124
9	Holidays 127
9.1	View Holidays 127
9.2	Add or Edit a Holiday 127
9.3	Remove a Holiday 128
10	Schedules 129
10.1	View Schedules 129
10.2	Add or Edit a Schedule 130
10.3	Delete a Schedule 131
11	Access Levels 132
11.1	View Access Levels 133
11.2	Add or Edit an Access Level 133
11.3	Delete an Access Level 134
12	Floor Groups 135
12.1	View Floor Groups 135
12.2	Add or Edit a Floor Group 135
12.3	Delete Floor Group 136
13	Alerts 137
13.1	View Alerts 137
13.2	Add or Edit an Alert 137
13.3	Send Sample Alert 142
13.4	Delete an Alert 142
14	Reports 143
14.1	Save and Export Reports 143
14.2	Show and Hide Columns 143
14.3	Chart 144
14.4	Event Logs 144
14.5	Residents 146
14.6	Credentials 148
14.7	People 150

14.8	Paper Directory	151
14.9	Panels	154
15	TX3 Networks with MiVision	156
15.1	Overview	156
15.2	MiVision and the Touch Screen	160
15.3	Administrator's Responsibilities	161
15.4	Additional Documentation	161
16	Compatible Products	162
17	Configurable Touch Screen User Interface Elements	163
18	Warranty and Warning Information	169

1

Introducing MiVision

MiVision is a cloud-based configuration and monitoring tool designed for managing all controllers in a TX3 network. It connects to on-site TX3 controllers through the TX3 Cloud Gateway.

This manual provides information about the configuration of MiVision, and must be read in its entirety before beginning any configuration work.

Note: Mircom periodically updates panel firmware to add features and correct any minor inconsistencies. For information about the latest firmware visit the Mircom website at <http://www.mircom.com>.

For information on TX3 networks with MiVision, see section 15.

For warranty and special notices, see section 18.

1.1 Requirements

MiVision works with all browsers but the following browsers are recommended:

- Microsoft Edge on Windows
- Google Chrome on Windows

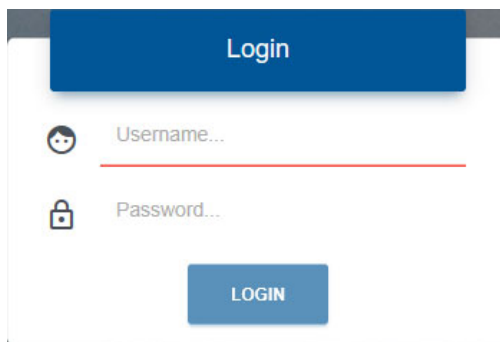
See section 16 for a list of compatible TX3 products.

Note: In order to connect MiVision to a TX3 network, the TX3 Cloud Gateway must be installed and activated as described in LT-6773 TX3 Cloud Gateway Installation Manual, available on <http://www.mircom.com>.

1.2 Log into MiVision

1. Open a Web browser on your computer.
2. Type **mivision.mircom.com** and then press **Enter**.

The **Login** page appears.



The login page features a blue header with the word "Login". Below it, there are two input fields: "Username..." with a user icon and "Password..." with a lock icon. A blue "LOGIN" button is positioned at the bottom right of the form.

Figure 1. Login page

3. Enter the username and password for MiVision.

The list of sites appears.

Click on the arrow icon ➤ to the right of the site that you want to open.

The MiVision Dashboard appears.

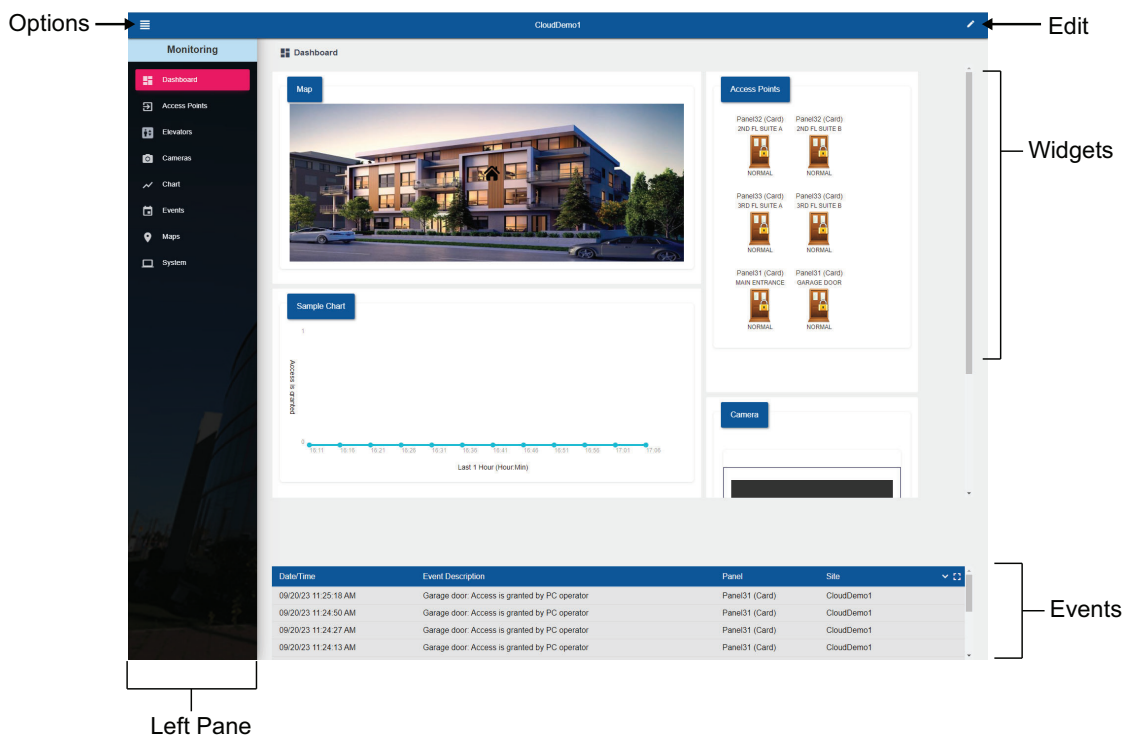


Figure 2. MiVision Dashboard

By default MiVision is in **Monitoring** mode. Click the **Options** menu in the upper left corner to access these options:

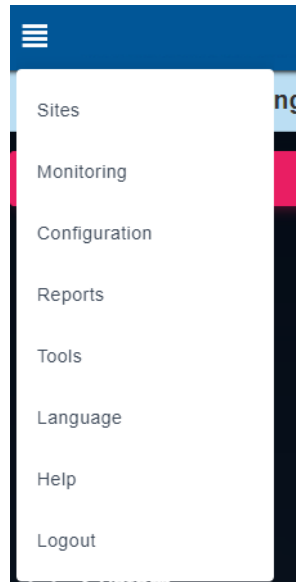


Figure 3. Options Menu

- Sites - section 1.5
- Monitoring - section 2
- Configuration:
 - Touch Screen, Telephone Entry, and Emergency Phone Configuration- section 3
 - Touch Screen Appearance Configuration - section 4
 - Card Access System Panel Configuration - section 5
 - Elevator Restriction Panel Configuration - section 6
 - People - section 7
 - Credentials - section 8
 - Holidays - section 9
 - Schedules - section 10
 - Access Levels - section 11
 - Floor Groups - section 12
 - Alerts - section 13
- Reports - section 14
- Tools - section 1.6
- Language - section 1.7
- Help - section 1.8
- Log Out - section 1.9

1.3 Real Time Messaging Icon


The **Real Time Messaging** icon is at the bottom of the left pane. A green icon means that MiVision is receiving events from the panels in real time. The events are displayed in the Events pane.

A red icon means that MiVision is not receiving events from the panels.

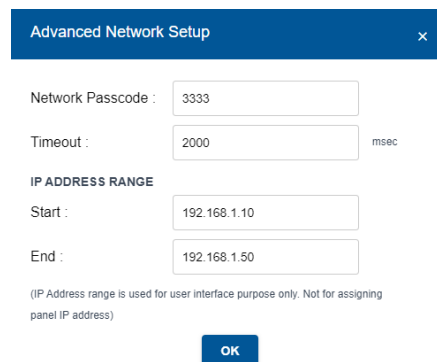


Figure 4. Real Time Messaging Online

1.4 Advanced Network Setup

1. Click the **Options** menu, then click **Configuration**.
2. Click the small gear icon  in the lower right corner.

The **Advanced Network Setup** window appears.



The image shows a screenshot of the 'Advanced Network Setup' window. It has a blue title bar with the text 'Advanced Network Setup' and a close button (X). The window contains several input fields: 'Network Passcode' with the value '3333', 'Timeout' with the value '2000' and a unit 'msec' to its right. Below these is a section titled 'IP ADDRESS RANGE' with two sub-fields: 'Start' with the value '192.168.1.10' and 'End' with the value '192.168.1.50'. At the bottom, there is a small note in parentheses: '(IP Address range is used for user interface purpose only. Not for assigning panel IP address)'. An 'OK' button is located at the bottom center of the window.

Figure 5. Advanced Network Setup

Network passcode. The network passcode is used for logging into each panel. All panels on the network must use this passcode as their highest level passcodes.

Timeout. The timeout is the time the software will wait for each panel to respond to a communication command. Increasing this value may help when there are many communication errors.

IP Address Range. If you are using a range of IP addresses in your network, enter the following parameters:

- **Start.** Starting IP address of your network.
- **End.** Ending IP address of your network.

1.5 Sites

A site is a set of configuration data that uniquely describes and controls a set of networked TX3 control panels. The models of panels in MiVision must match the models that MiVision is connecting to. For example, if your TX3 panels consist of a TX3-TOUCH-S15-E, a TX3-CX-2, and a TX3-2000-4U-C, then the site in MiVision must contain **TX3 Touch**, **TX3-CX-2 (2 doors 2 readers)**, and **TX3-2000-4 (4x20 LCD)**.

Most of this manual is dedicated to configuring a site in MiVision. Sections 3 to 13 describe how to add control panels to a site, and how to configure them.

1.5.1 Edit Site Description, Address, Time Zone, and License

1. To edit your sites in the **Sites** window, click the Edit button in the upper right.

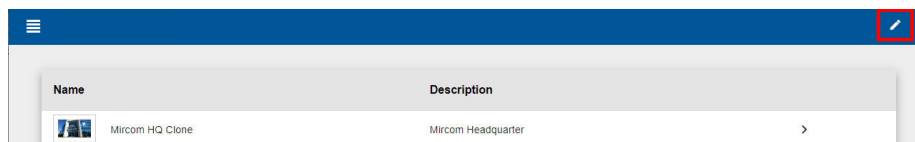


Figure 6. Edit Sites button

An **Edit** button appears beside each site.

2. Click the **Edit** button  for the site that you want to edit.

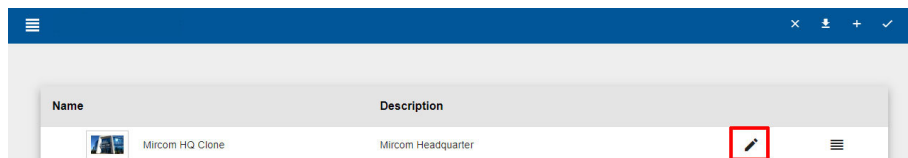


Figure 7. Edit Sites icon

A window for the site appears.

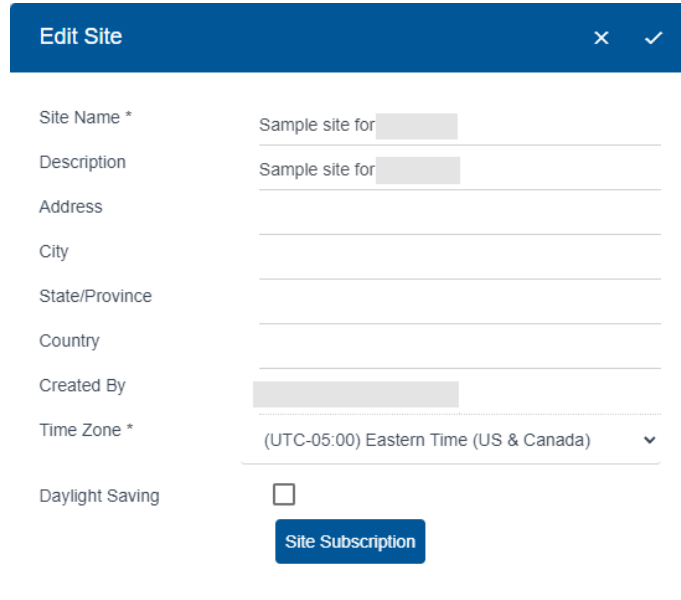


Figure 8. Edit Site window

3. **Site Name.** Enter a name. This is the name that appears in the list of sites.

Description. Enter a description of the site.

Address. Enter the site's address.

Time Zone. Specify the site's time zone.

Daylight Saving. Select this box if the selected time zone uses daylight savings time.

Site Subscription. Select and enter the license key for this site.

Note: Each site requires a license key in order for MiVision to communicate with the site. The building manager receives the license key from the MiConnect portal when they enable the MiVision subscription.

Site Subscription

Site :

Sample site

Subscription Key *

APPLY

Site not Subscribed



Billing Account

1

Figure 9. Site Subscription

Subscription Key. The format is XXXX-XXXX-XXXX-XXXX and consists of letters and numbers. You do not need to enter the dashes; they are automatically filled in.

Billing Account. This field is read-only.

- Click the **Done** button  in the upper right corner to save your changes, or **Cancel** button  to cancel changes.

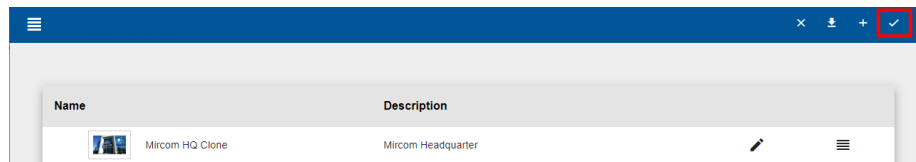


Figure 10. Done button in the Edit Sites window

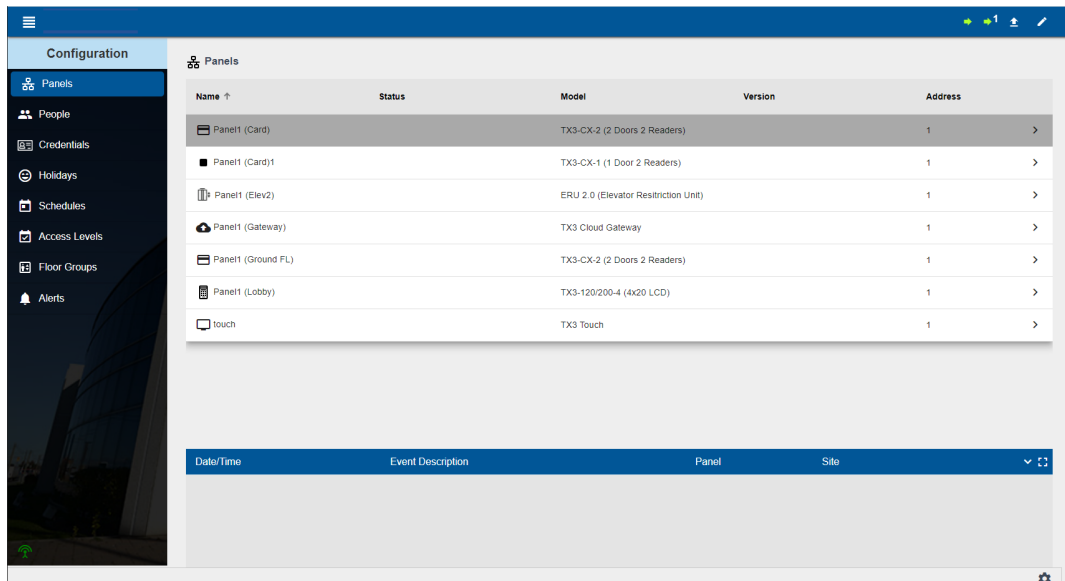
1.5.2 Add a Main Node to a Site

Note: If you are having problems adding nodes to your Job, there may be another program using the TCP/IP ports that the TX3 system communicates on. See section 15.1.1 for information on what ports the TX3 system uses.

Note: If you cannot find the panel, then it might have a static IP and be on a different subnet. Follow the instructions in section 1.13.

1. Click the **Options** menu, then click **Configuration**.
2. Click **Panels** in the left pane.

The Panels window appears.



Name	Status	Model	Version	Address
Panel1 (Card)		TX3-CX-2 (2 Doors 2 Readers)		1
Panel1 (Card)1		TX3-CX-1 (1 Door 2 Readers)		1
Panel1 (Elev2)		ERU 2.0 (Elevator Restriction Unit)		1
Panel1 (Gateway)		TX3 Cloud Gateway		1
Panel1 (Ground FL)		TX3-CX-2 (2 Doors 2 Readers)		1
Panel1 (Lobby)		TX3-120/200-4 (4x20 LCD)		1
touch		TX3 Touch		1

Figure 11. Panels

The panels are grouped by main node.

The view has the following columns:



Panel Name. The panel name.

Status. Normal, alarm, or trouble.

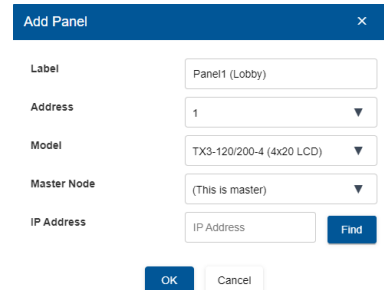
Model. The panel model.

Version. The firmware version.

Address. The RS-485 address.

3. Click the **Edit** button  in the upper right, then click the **Add** button .

The Add Panel window appears.



The screenshot shows the 'Add Panel' dialog box. It has a title bar with 'Add Panel' and a close button. Inside, there are five fields: 'Label' with 'Panel1 (Lobby)', 'Address' with '1', 'Model' with 'TX3-120/200-4 (4x20 LCD)', 'Master Node' with '(This is master)', and 'IP Address' with 'IP Address'. There is a 'Find' button next to the IP Address field. At the bottom, there are 'OK' and 'Cancel' buttons.

Figure 12. Add Panel

Label. Enter a name for the panel.

Address. Specify the RS-485 address of the panel.

Model. Select a panel model.

Master Node. Select **(This is a Master)**.

Note: In MiVision, the terms **Master** and **Main** are equivalent.



IP Address. Enter the IP address of the panel, or click **Find** to see a list of panels on the network.

4. Click **OK**.
5. Repeat these steps for every main node in your network.

1.5.3 Add a Secondary Node to a Site

Notes: Before you can add a secondary node to a site, you must do the following:

- Add the secondary node's main node to the job.
- Record the RS-485 address and model of the secondary node.

1. In the **Configuration** screen, click the **Edit** button  in the upper right, then click the **Add** button .

The Add Panel window appears (Figure 12).

2. Provide the following information:




Label. Provide a name for the panel.

Address. Specify the RS-485 address of the panel.



Model. Select a panel model.

Master Node. Select the panel that is the main node of the panel you want to add.
3. Click **OK**.
4. Repeat these steps for every secondary node in your network.

1.5.4 Delete a Panel

1. In the **Panels** window, click the edit button  in the upper right.
2. Click the delete button  beside the panel that you want to delete.
3. Click the Done button  in the upper right corner of the Sites window.

1.5.5 Edit a Panel's Network Information

1. In the **Panels** window, click the edit button  in the upper right.
2. Click the edit button  beside the panel that you want to edit.

The Edit Panel window appears.

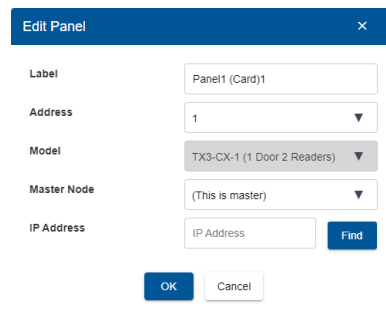


Figure 13. Edit Panel


Label. Enter a name for the panel.

Address. Specify the RS-485 address of the panel.

Model. Select a panel model.

Master Node. Select **(This is a Master)** if the panel is a main node, otherwise select the panel's main node.

IP Address. Enter the IP address of the panel, or click **Find** to see a list of panels on the network.

3. Click the Done button  in the upper right corner of the Sites window.

1.6 Tools

The Tools option has the following features, depending on your role.

- Backup and Restore
- Change Password
- User Management

1.6.1 Backup and Restore

The Backup feature backs up one site or all the sites to an online repository.

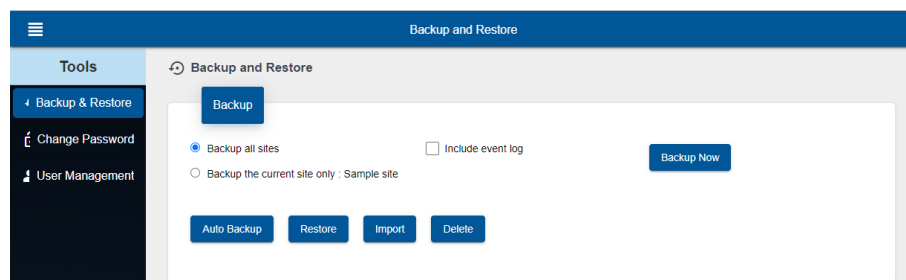



Figure 14. Backup and Restore

1. Click the Options menu button  in the upper left corner.
2. Select **Tools**.
3. Click **Backup & Restore**.

Backup all sites. Select to back up either all sites or the current site.

Include event log. Select this to include the event log in the backup.

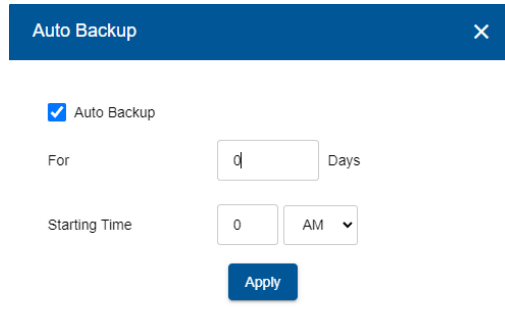
Backup Now. Click this button to start the backup.

Restore. Click this button to select a backup to restore from.

Import. This feature lets you import a job file that was created by the TX3 desktop Configurator. Click this button to select a TX3 Configurator job file to import into MiVision.

Delete. Click this button to delete a backup.

Auto Backup. Click this button to schedule an automatic backup.



The image shows a dialog box titled "Auto Backup" with a close button (X) in the top right corner. Inside the dialog, there is a checked checkbox labeled "Auto Backup". Below this, there is a "For" label followed by a text input field containing the number "0" and a "Days" label. Underneath, there is a "Starting Time" label followed by a time selection interface consisting of a text input field containing "0" and a dropdown menu currently showing "AM". At the bottom center of the dialog is a blue button labeled "Apply".

Figure 15. Auto Backup

Auto Backup. Select this checkbox to make MiVision perform automatic daily backups.


For. This is the retention period of the backup. Enter the number of days that MiVision will keep the backups for.

For example, if **For** is **5 Days**, then MiVision will keep the backups for the previous 5 days. If today is October 9, you can restore a backup from the previous 5 days, so the earliest backup that you can restore is from October 5. On October 10, the earliest backup that you can restore is from October 6.

Starting Time. Enter the time when the daily backup should start.

1.6.2 Change Password

This option changes the password for the currently logged in account.

1. Click the Options menu button  in the upper left corner.
2. Select **Tools**.
3. Click **Change Password**.

1.6.3 User Management

The User Management section lets you add and modify users. You can assign different permissions to users.

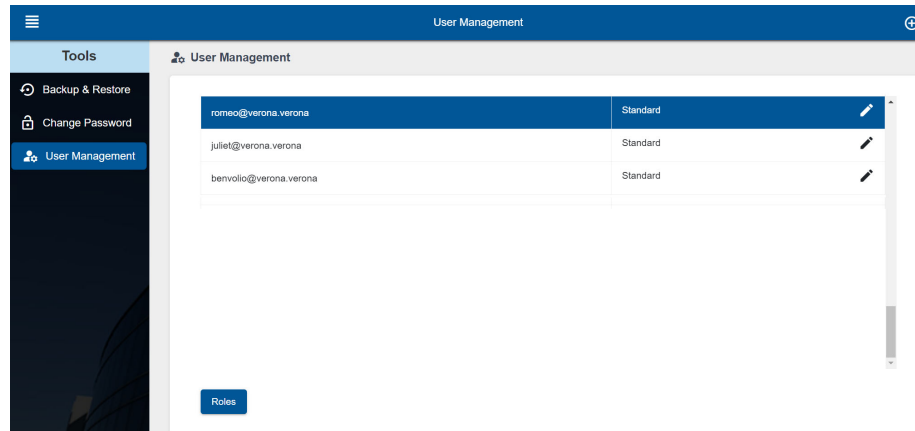





Figure 16. User Management

Note: When you create a new user, MiVision creates a temporary password, and forces the user to change the password the first time they log in.

1. Click the Options menu button  in the upper left corner.
2. Select **Tools**.
3. Click **User Management**.

4. Click the Add button  to add a new user, or click the Edit button  to modify a user.

Add User
✓ ✕

Email (User Name)

First Name

Last Name

☐ Enable Two-Factor Authentication

☐ Use Text message (SMS)
☐ Use Authenticator App

☒ Active

Sites Access

Site	Role
Mircom HQ	None ▼
CloudDemo1	None ▼
Mircom HQ Clone	None ▼

Figure 17. Add User

User Name. The User Name is the user's email address.

First Name, Last Name. Enter the user's name.

Enable Two-Factor Authentication. Select this option to enable two-factor authentication for this user. You can use either text messages or an authenticator app such as Google Authenticator or Microsoft Authenticator, which are available on the Apple App Store and Google Play Store. When a user logs in and two-factor authentication is enabled, MiVision will request a code that the user receives to verify their identity. See section 1.6.4.

Active. Select this option if the user is active. If this is deselected, then the user cannot log in.

Sites Access. Select the role that this user should have for each of the sites. See section 1.6.5.

Delete User. Delete this user.

Change Password. Change the password for this user.

1.6.4 Two-Factor Authentication

Two-factor authentication offers two options:

- **Text Message (SMS).** If the user has registered a mobile number, they will receive an SMS with a six-digit code. (Note: This option is available only for Canadian numbers.)

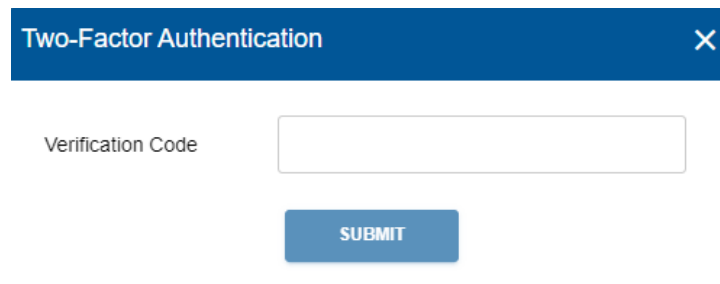


Figure 18. Two-Factor Authentication: text message

- **Authenticator App.** Upon login attempt, a pop-up will guide the user to open their authenticator app, such as Google Authenticator which is available on the Apple App Store and Google Play Store, or Microsoft Authenticator which is available on the Apple App Store.

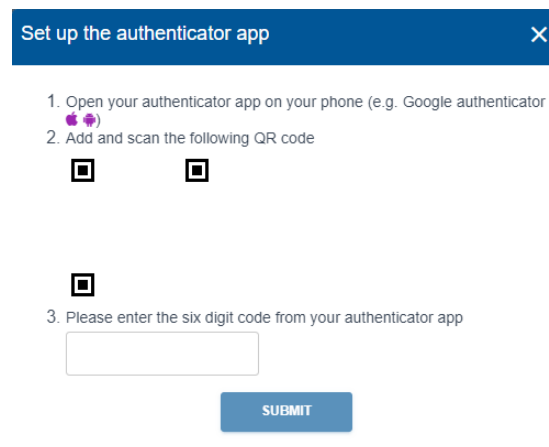


Figure 19. Two-Factor Authentication: Authenticator app

The user will then scan a QR code displayed on the screen, generating a six-digit code within the app.

1.6.5 User Roles

Roles define what permissions the user has on a site. A user can have different roles on different sites.

None. The user has no access to this site.

Operator. The user has read access only, and can monitor and send real time commands to access points and elevators.


User. The same as Operator.

Advanced user. The same as User but with advanced site administration permissions including: edit dashboard, edit charts, edit buildings, edit floors, send job, upgrade firmware, edit people, edit credentials, edit holidays, edit schedules, edit access levels, and edit floor groups.

Manager. The same as Advanced User but with permission to create reports and alerts.

Administrator. The user has complete access to the site.

1.7 Language

1. Click the Options menu button  in the upper left corner.
2. Select **Language**.
3. Select the language that you want to view the site in, and then click **OK**. You can choose between English and French.

1.8 Help

Contact information for Mircom technical support is provided here.

1.9 Log Out

Select this option to log out, and it will take you to the login page. If other people are using the computer, you should log out when you are finished using MiVision.

1.10 Send the Job

After you have configured the site, you must send the configuration data to the TX3 panels. Sending the data to the panels is called **sending a job**.

1. Click the **Options** menu, then click **Configuration**.
2. Click **Panels** in the left pane.

The Panels window appears.

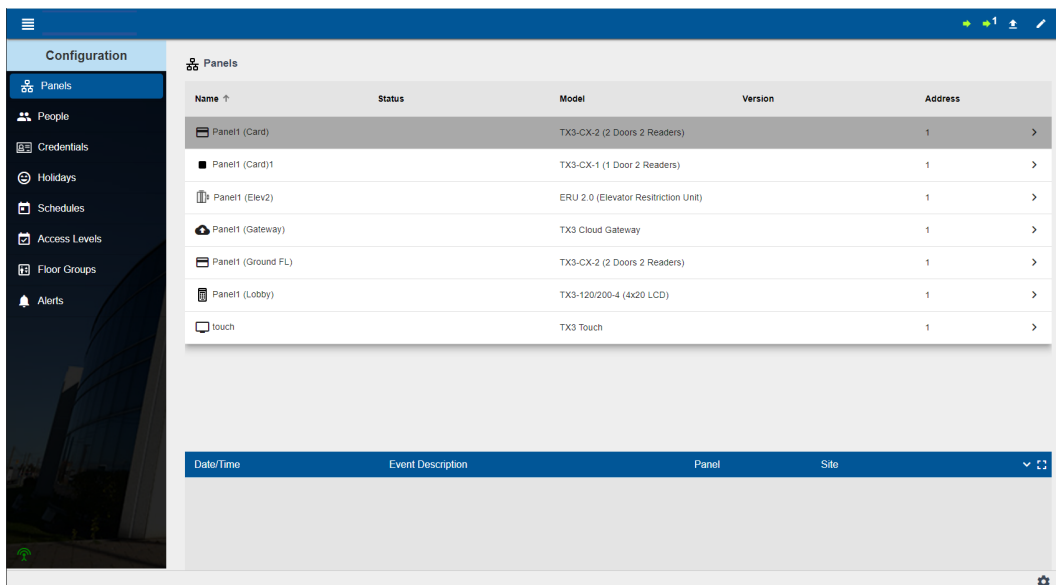



Figure 20. Panels

1.10.1 Send the Job to all Panels

This is the recommend option for sending jobs. This option sends only the changed information and is usually fast.

1. Click the green arrow in the upper right corner. 

The job is sent right away.

2. The **Send Job Status** window appears.

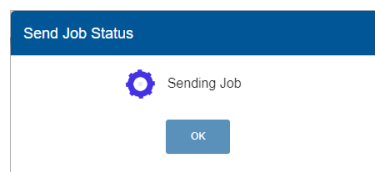


Figure 21. Send Job Status

The process takes several minutes to complete.

1.10.2 Send the Job to a Single Panel

This option sends all information, not just the changed information, to a single panel. This can take a long time.

1. Select the panel that you want to send the job to.

2. Click the green arrow with the letter 1 beside it in the upper right corner.



Figure 22. Send to Single Panel

3. The **Send Job Status** window appears.

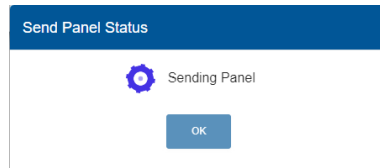



Figure 23. Send Panel Status

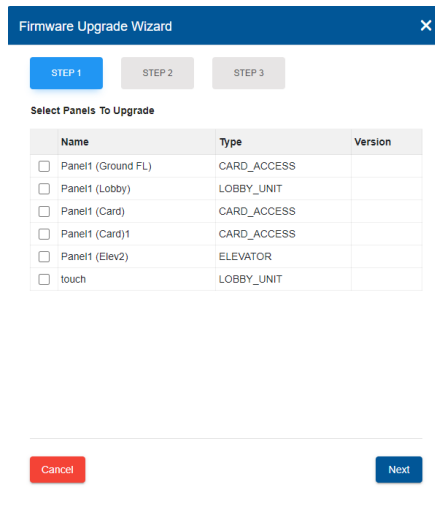
The process takes several minutes to complete.

1.11 Firmware Upgrade

The Firmware Upgrade Wizard allows you to upgrade the firmware on many panels simultaneously.

1. Ensure that all of the panels to be updated in the network are powered on.
2. Click the **Options** menu, then click **Configuration**.
3. Click **Panels** in the left pane.
4. Click the Firmware Upgrade icon in the upper right corner. 

The Firmware Upgrade Wizard appears.



Name	Type	Version
<input type="checkbox"/> Panel1 (Ground FL)	CARD_ACCESS	
<input type="checkbox"/> Panel1 (Lobby)	LOBBY_UNIT	
<input type="checkbox"/> Panel1 (Card)	CARD_ACCESS	
<input type="checkbox"/> Panel1 (Card)1	CARD_ACCESS	
<input type="checkbox"/> Panel1 (Elev2)	ELEVATOR	
<input type="checkbox"/> touch	LOBBY_UNIT	

Figure 24. Firmware Upgrade Wizard Step 1

5. Select the panels on the network to upgrade with new firmware by selecting the corresponding checkboxes on the left.
6. Click **Next**.

The Step 2 window appears.

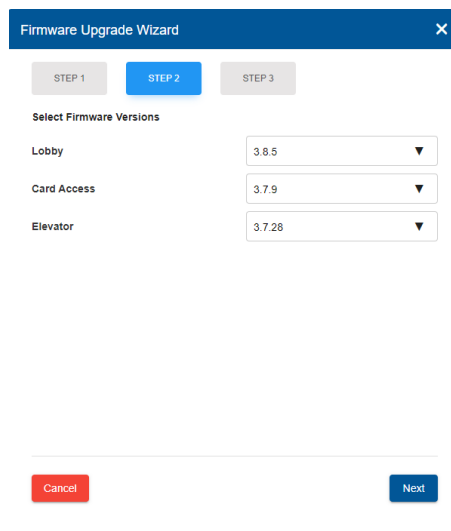


Figure 25. Firmware Upgrade Wizard Step 2

Each type of panel on the network uses a different firmware file.

Note: TX3 **-256** products have firmware files ending in **-256K**.

You cannot upgrade -256 products and non-256 products at the same time. If you have a mix of -256 products and non-256 products in the job, do this procedure twice: once for the -256 products and once for the non-256 products.

7. For each panel, select the firmware version to use.
8. Click **Next**.

The Step 3 window appears.

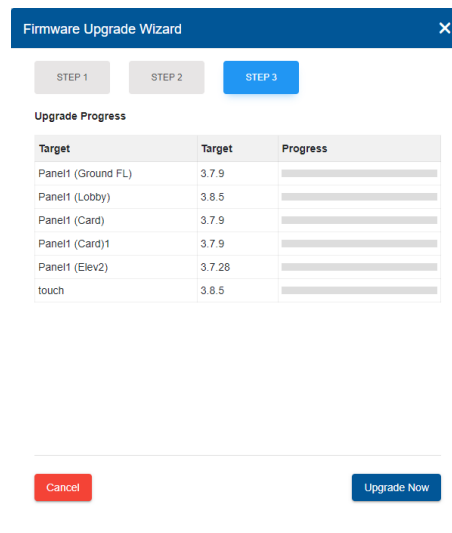


Figure 26. Firmware Upgrade Wizard Step 3


9. Click **Upgrade Now**.

The firmware upgrade process takes several minutes to complete. A progress of each upgrade is shown next to each panel. Once the firmware has been upgraded, the panel automatically restarts. Wait for all panels to finish restarting.

1.12 Commands

You can send commands to a panel.

1. Click the **Options** menu, then click **Configuration**.
2. Click **Panels** in the left pane.

3. Click the arrow  on the right to see details of a panel.

The Panels Configuration screen appears.

4. Click the **Commands** button.

A menu appears listing the commands that you can send to the panel. The available commands depend on the type of panel.

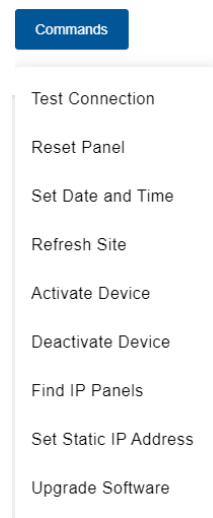


Figure 27. Commands menu

Test Connection. This option tests the connection between MiVision and a main node. If the connection is working, the message **Test Connection successful** appears.

Reset Panel. This command restarts the panel.

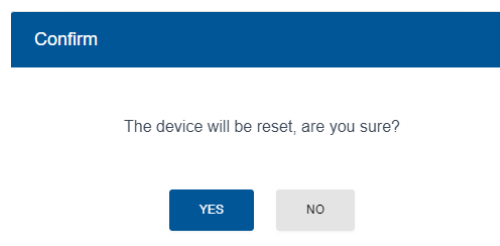
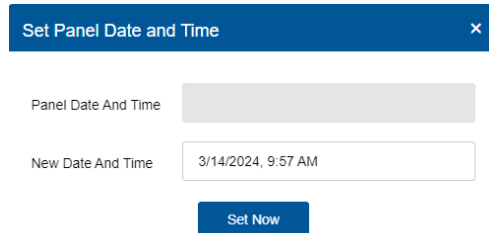


Figure 28. Reset Panel

Set Date and Time. (TX3 card access, voice access, elevator and touch screen) This option lets you set the panel clock to a time other than the PC clock. Every time you access the **Set Date and Time** window the current PC time is shown.



The window titled "Set Panel Date and Time" contains two input fields. The first field, labeled "Panel Date And Time", is currently empty. The second field, labeled "New Date And Time", contains the text "3/14/2024, 9:57 AM". Below these fields is a blue button labeled "Set Now".

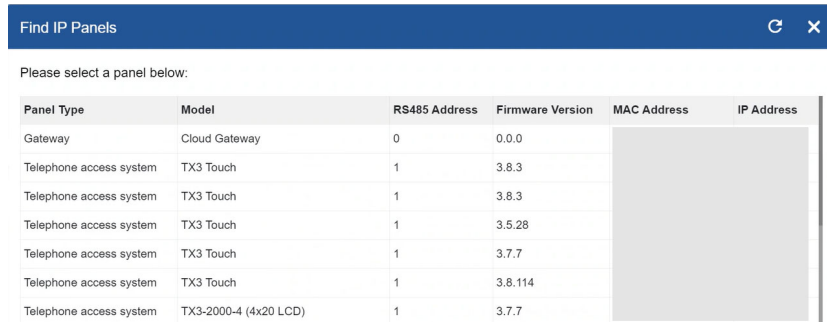
Figure 29. Set Date and Time

Refresh Site. (TX3 Cloud Gateway and touch screen) MiVision connects to the panels again. This option is useful if you change the IP address of a panel.

Activate Device. (TX3 Cloud Gateway and touch screen) This option activates the TX3 Cloud Gateway. See LT-6773 TX3 Cloud Gateway Quick Start Guide for more information.

Deactivate Device. (TX3 Cloud Gateway and touch screen) This option deactivates the TX3 Cloud Gateway.

Find IP Panels. (TX3 Cloud Gateway and touch screen) This option shows all the main nodes on the TCP/IP network.



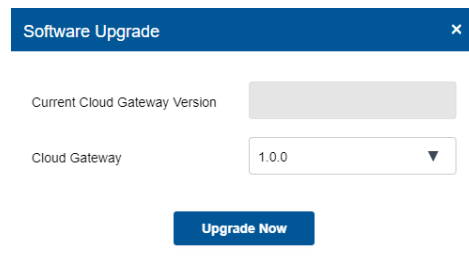
The window titled "Find IP Panels" displays a table of networked panels. The table has six columns: Panel Type, Model, RS485 Address, Firmware Version, MAC Address, and IP Address. The first row shows a Gateway with RS485 Address 0 and Firmware Version 0.0.0. Subsequent rows list various Telephone access systems with different models and firmware versions. The MAC Address and IP Address columns for these systems are currently obscured by a greyed-out area.

Panel Type	Model	RS485 Address	Firmware Version	MAC Address	IP Address
Gateway	Cloud Gateway	0	0.0.0		
Telephone access system	TX3 Touch	1	3.8.3		
Telephone access system	TX3 Touch	1	3.8.3		
Telephone access system	TX3 Touch	1	3.5.28		
Telephone access system	TX3 Touch	1	3.7.7		
Telephone access system	TX3 Touch	1	3.8.114		
Telephone access system	TX3-2000-4 (4x20 LCD)	1	3.7.7		

Figure 30. Find IP Panels

Set Static IP Address. (TX3 Cloud Gateway and touch screen) This option lets you change the static IP address of a non-Touch Screen panel. See section 1.13.

Upgrade Software. (TX3 Cloud Gateway and touch screen) Use this option to upgrade the software on the TX3 Cloud Gateway.



Software Upgrade [X]

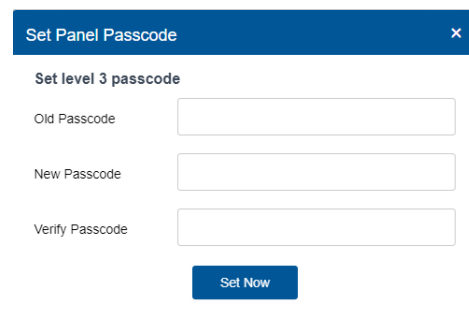
Current Cloud Gateway Version

Cloud Gateway

Upgrade Now

Figure 31. TX3 Cloud Gateway Software Upgrade

Set Passcode. Use this option to set the level 3 passcode. In order to connect to the panel, this passcode must match the level 3 passcode on the panel.



Set Panel Passcode [X]

Set level 3 passcode

Old Passcode

New Passcode

Verify Passcode

Set Now

Figure 32. Set Panel Passcode

Note: The level 3 passcode is initially set at the panel. The default is 3333.

Note: For Touch Screen panels, this only sets the passcode for the lobby controller panel inside the Touch Screen. It does not change the administrator password used to log in to the Touch Screen.

Event Log. (TX3 voice access) This option lets you read the user and system logs, and save them to an online repository. You may also erase the logs from the panel or from an online repository.

1.13 Change a Main Node's IP Address

You might need to change a non-Touch Screen main node's IP address when you are adding the panel to a new network, or when the panel was turned on for the first time with DIP switch 8 on.

-
- Notes:** Before you change a main node's IP address:
- If you are having problems changing IP addresses, there may be another program using the TCP/IP ports that the TX3 system communicates on. See section 15.1.1 for information on what ports the TX3 system uses.
 - You **cannot** change the IP address for a Touch Screen panel using MiVision. Touch Screens are configured to use DHCP to get their IP addresses.
-


1.13.1 Static or Dynamic IP Address

For non-Touch Screen units with an IP Module installed, DIP switch 8 determines how the IP address is assigned. (See LT-969 TX3 Telephone Access System Installation and Operation Manual for details.)

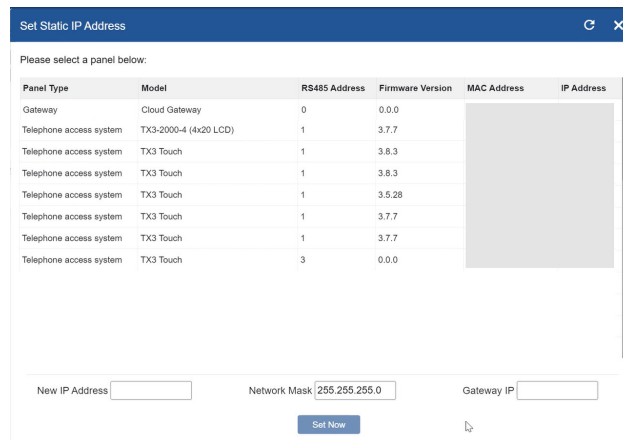
- **DIP switch 8 OFF:** The IP address is assigned using a DHCP server. This is the default factory setting.
- **DIP switch 8 ON when it was previously OFF:** The IP address is static and is set to the last IP address that was assigned to the panel.
- **DIP switch 8 ON when the panel is turned on for the first time:** The IP address is static and is set to 192.168.1.74.

If the panel is turned on for the first time with DIP switch 8 on, then follow the instructions below to change the IP address.

1.13.2 Change the Panel's IP Address

1. Click the **Options** menu, then click **Configuration**.
2. Click **Panels** in the left pane.
3. Click the arrow  on the right to see details of the panel.
4. Click **Commands**, then click **Set Static IP Address**.

The Set Static IP Address window appears.



The 'Set Static IP Address' window displays a table of panels and fields for configuration.



Panel Type	Model	RS485 Address	Firmware Version	MAC Address	IP Address
Gateway	Cloud Gateway	0	0.0.0		
Telephone access system	TX3-2000-4 (4x20 LCD)	1	3.7.7		
Telephone access system	TX3 Touch	1	3.8.3		
Telephone access system	TX3 Touch	1	3.8.3		
Telephone access system	TX3 Touch	1	3.5.28		
Telephone access system	TX3 Touch	1	3.7.7		
Telephone access system	TX3 Touch	1	3.7.7		
Telephone access system	TX3 Touch	3	0.0.0		

Below the table, there are input fields for 'New IP Address', 'Network Mask' (set to 255.255.255.0), and 'Gateway IP'. A 'Set Now' button is located at the bottom center.

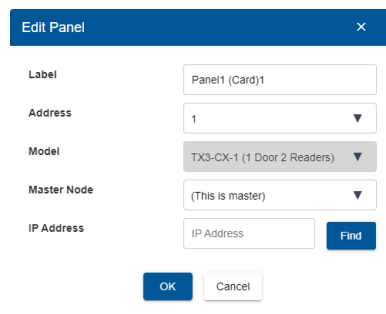
Figure 33. Set Static IP Address

5. Select the panel that you want to change the IP address for.
6. Enter the new IP address in the **New IP Address** field.
7. Enter the gateway IP address in the **Gateway IP** field. Consult the network administrator.
8. Click **Set Now**.

1.13.3 Change the IP Address in the Job File

1. In the **Panels** window, click the edit button  in the upper right.
2. Click the edit button  beside the panel that you want to edit.

The **Edit Panel** window appears.




The 'Edit Panel' window contains the following fields and controls:

- Label:** Panel1 (Card)1
- Address:** 1 (dropdown menu)
- Model:** TX3-CX-1 (1 Door 2 Readers) (dropdown menu)
- Master Node:** (This is master) (dropdown menu)
- IP Address:** IP Address (text field) with a **Find** button next to it.
- Buttons:** **OK** and **Cancel** at the bottom.

Figure 34. Edit Panel

IP Address. Enter the IP address of the panel.

3. Click the Done button  in the upper right corner of the Sites window.

2



Monitoring

The Monitoring section provides tools to monitor access points and events, to view maps and charts, and to send elevator commands.

2.1 Dashboard




The dashboard displays a summary of the system. It consists of widgets and the events list (see Figure 2). Each widget represents a view of one of the monitoring components. You can add and remove widgets. Widgets include system status, maps, charts, and access points.

2.1.1 Add a Widget




1. On the Dashboard, click the Edit button  in the upper right corner.
2. From the **Widgets** on the left, click and drag widgets on to the grid, and rearrange and resize widgets as desired.
3. Click the Done button  in the upper right corner to save your changes.

Or click the Cancel button  to go back to the dashboard without saving.



2.1.2 Remove a Widget

1. On the Dashboard, click the Edit button  in the upper right corner.
2. To remove a widget from your dashboard, hover on the name of the widget, and it will show two options, Delete and Edit. 
3. Click the Delete button  to remove the widget. This action cannot be reverted even if you click Cancel.

2.1.3 Edit a Widget

1. On the Dashboard, click the Edit button  in the upper right corner.
2. To edit a widget from your dashboard, hover on the name of the widget, and it will show two options, Delete and Edit. 
3. Click the Edit button  to edit the widget.

Only Maps and Charts can be edited. The edit option in Maps will let you select a map that you want to keep on display. The edit option in charts will let you edit parameters of the chart that is displayed.

4. Click the Done button  in the upper right corner to save your changes.
5. Or click the Cancel button  to go back to the dashboard without saving.

2.2 Access Points

The Access Points section displays the current status of all the card reader access points on the network and shows their status as 'normal', 'trouble', 'alarm', or 'offline', as well as their lock/unlock and high security on/off status.

Access Point Status also lets you grant access, and turn the unlock and high security functions on or off in real time.

1. Click **Access Points** in the left pane.

The Access Points window appears.

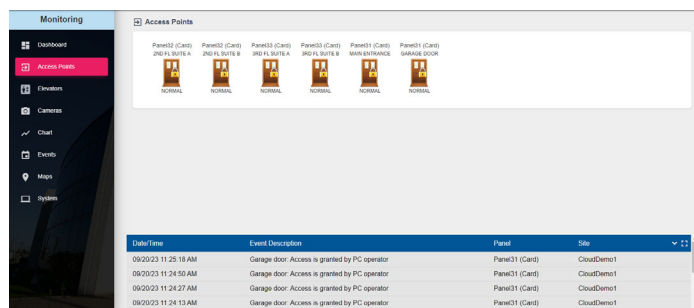


Figure 35. Access points

2. Click an access point. The following selections appear:

Grant Access. Use Grant Access to admit access point entry. Typically this unlocks the door.

Unlock Mode ON. Turns on the unlock mode until the next scheduled event or the panel is reset. When the access point is in unlock mode, the door is unlocked.

Unlock Mode OFF. Turns off the unlock mode until the next scheduled event or the panel is reset.

High Sec Mode ON. Turns on the high security mode until the next scheduled event or the panel is reset. When high security mode is enabled, only access cards with high security privilege can unlock the door.

High Sec Mode OFF. Turns off the high security mode until the next scheduled event or the panel is reset.

Map. Shows the access point on the floor map.

3. If you want to send a command to the access point (for example, **Unlock mode ON**), click the command.

2.3 Elevators

The Elevators screen lets you activate elevator relays and see the activation status of all relays if the job has a TX3-ER-8-B Elevator Restriction Unit (ERU 2.0).

2.3.1 Send Elevator Commands

1. Click **Elevators** in the left pane.

The status window shows all TX3-ER-8-B Elevator Restriction Units (ERU 2.0) in the job.

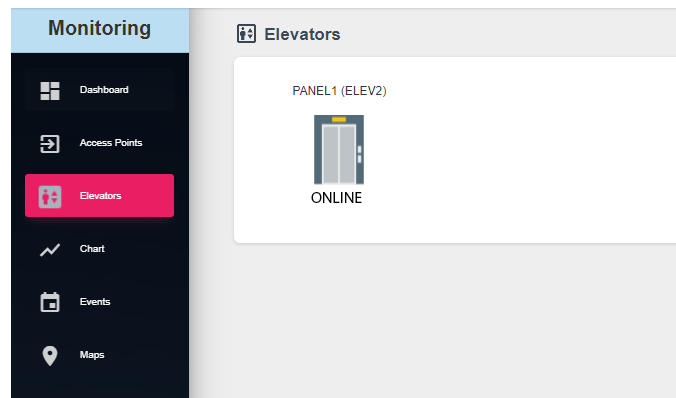
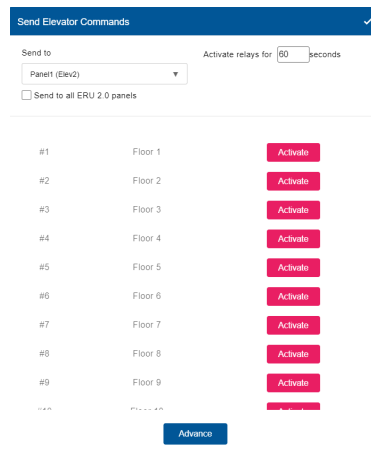


Figure 36. Elevator Status

2. Click the icon for a TX3-ER-8-B Elevator Restriction Unit (ERU 2.0).

The Send Elevator Commands window appears.

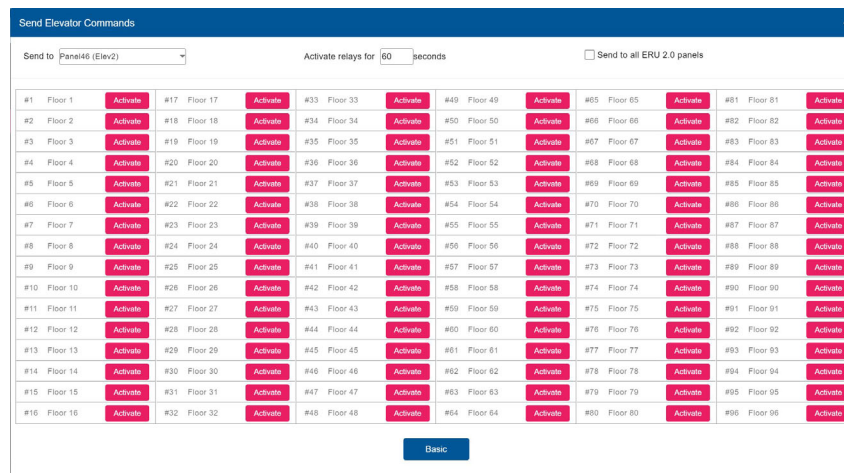


The window is titled "Send Elevator Commands" with a checkmark icon. It features a "Send to" dropdown menu set to "Panel1 (Elev2)", an "Activate relays for" input field set to "60" seconds, and a checkbox for "Send to all ERU 2.0 panels" which is unchecked. Below this, there is a list of floors from #1 to #9, each with a corresponding "Activate" button. At the bottom right, there is an "Advance" button.

Figure 37. Send Elevator Commands Window

3. Click the **Advanced** button to expand the window.

The window expands to show all the elevator relays.



The expanded window shows a grid of 96 "Activate" buttons, arranged in 8 rows and 12 columns. Each button is labeled with a relay number and a floor number (e.g., #1 Floor 1, #2 Floor 2, ..., #96 Floor 96). The "Send to" dropdown is now set to "Panel46 (Elev2)", and the "Activate relays for" field remains at "60" seconds. The "Send to all ERU 2.0 panels" checkbox is still unchecked. At the bottom center, there is a "Basic" button.

Figure 38. Expanded Send Elevator Commands Window

Note: Active relays are highlighted in green.


4. Click the menu beside **Send to** and select which ERU2.0 panel to send the activation command to.
5. Select a time in the **Activate relays for** menu. This is the period of time during which the elevator relays will remain active.

6. Select **Send to all ERU 2.0 panels** if you want to send the activation command to all ERU 2.0 panels instead of just the panel selected in the **Send to** menu. If you select this option, then the activation command is sent to the same relay on all the ERU 2.0 panels.
7. Click the **Activate** button beside the relays that you want to activate.
The active relays are highlighted in green.

2.4 Chart

The Charts screen shows a live chart that is regularly updated. The chart shows the total number of events over a period of time. For example, the chart can plot the total number of grant access events of a particular door over the last 24 hours. The horizontal axis (X axis) shows time, and the vertical axis (Y axis) shows the number of events.

2.4.1 Edit a Chart

1. Click the Edit button  in the upper right corner.
2. Enter the following information.

Title. The title of the chart.

Select Site. The job site.

When. Select an event that you want to plot on the chart. For a description of the events, see section 13.2.1.

On panel. Select one panel in the system, or select **All**.

Duration. Select one of:

- **Last 10 minutes.**
- **Last 1 hour.**
- **Last 24 hours.**
- **Yesterday.**
- **Custom**, and then select the beginning and end date and time.

Note: If you select **Last 10 minutes**, **Last 1 hour**, or **Last 24 hours**, then the chart will be regularly updated to show activity for only that time period. For example, if you select **Last 1 hour**, the chart will change regularly to show activity for only the last hour.

Interval. Select how often the points are calculated.

Chart type. Currently only a line charts is available.

3. Click the Save button at the bottom to save your changes.

2.4.2 Example Chart

Figure 39 shows a chart that plots the **Input is active** event in the last 1 hour. The horizontal axis shows the time in intervals of 5 minutes. The vertical axis shows the number of events from 0 to 3. From 16:34 to 16:39 there were no events, and from 16:39 to 16:44 there were 3 events.

The chart is regularly updated to show data from one hour ago to the present. This means that the times on the horizontal axis change as time passes.

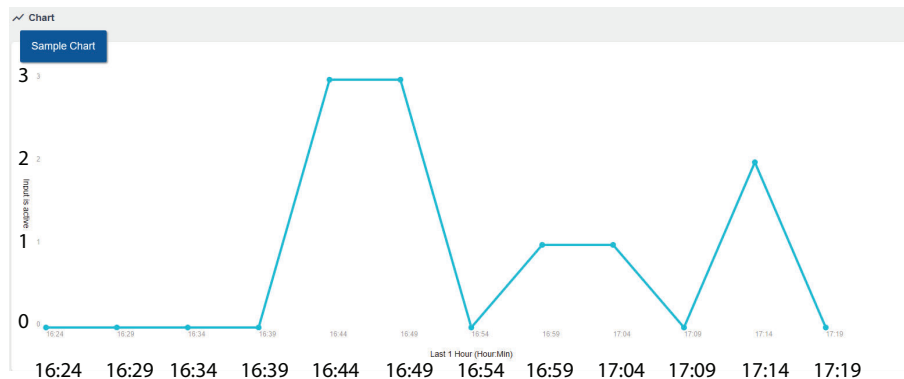



Figure 39. Example chart

2.4.3 Export a Chart

1. Click the Export button  in the upper right corner.
2. Select either XLS, CSV, or PDF as the format to save the chart in.

2.5 Events

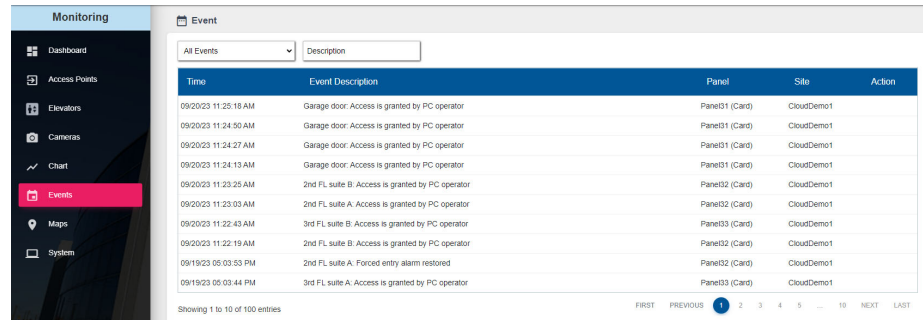
The Events section displays all events received by the TX3 system.

Events may be initiated by the panels or by the software. Only user activity is logged to the event log.

2.5.1 View Events

- Click **Events** in the left pane.

The Event window appears.



Time	Event Description	Panel	Site	Action
09/20/23 11:25:18 AM	Garage door: Access is granted by PC operator	Panel01 (Card)	CloudDemo1	
09/20/23 11:24:50 AM	Garage door: Access is granted by PC operator	Panel01 (Card)	CloudDemo1	
09/20/23 11:24:27 AM	Garage door: Access is granted by PC operator	Panel01 (Card)	CloudDemo1	
09/20/23 11:24:13 AM	Garage door: Access is granted by PC operator	Panel01 (Card)	CloudDemo1	
09/20/23 11:23:25 AM	2nd FL suite A: Access is granted by PC operator	Panel02 (Card)	CloudDemo1	
09/20/23 11:23:03 AM	2nd FL suite B: Access is granted by PC operator	Panel02 (Card)	CloudDemo1	
09/20/23 11:22:43 AM	3rd FL suite B: Access is granted by PC operator	Panel03 (Card)	CloudDemo1	
09/20/23 11:22:19 AM	2nd FL suite B: Access is granted by PC operator	Panel02 (Card)	CloudDemo1	
09/19/23 05:03:53 PM	2nd FL suite A: Forced entry alarm restored	Panel02 (Card)	CloudDemo1	
09/19/23 05:03:44 PM	3rd FL suite A: Access is granted by PC operator	Panel03 (Card)	CloudDemo1	

Figure 40. Event

The view has the following columns:

Time. Time stamp of the event according to the job's time zone.

Event Description. Description of the event.

Panel. The panel that the event come from.

Site. The site that the event comes from.

Action. If the access point or input has been placed on a map, a map icon appears here. Click the icon to show the floor map.

2.5.2 Filter Events

- Use the two filters at the top of the window that you can use to search for:
 - Event types (All Events, Alarms Only, Warnings Only, or Alarms and Warnings)
 - Description

2.6 Maps

The maps section lets you configure the maps for the site, buildings, and floors. You can place icons on the maps to represent buildings, access points, and inputs.

MiVision supports maps in JPEG and PNG format.

2.6.1 View Maps

- Click **Maps** in the left pane.

The site map appears.

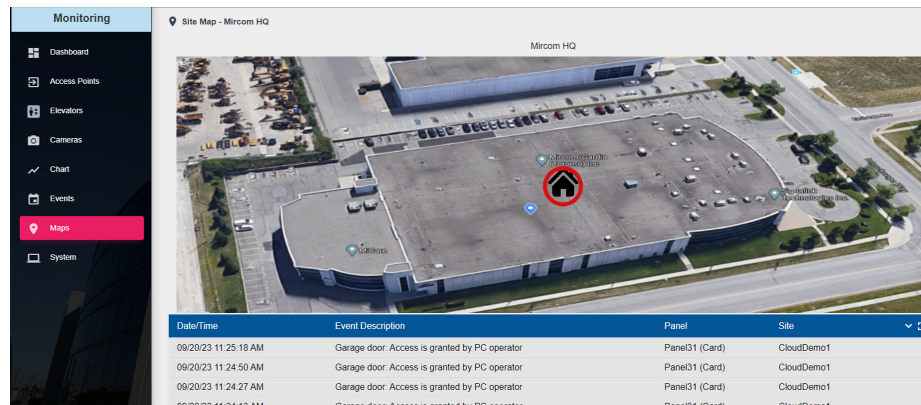




Figure 41. Maps

2.6.2 View an Event on a Map

Each building is represented on the site map with the building icon. 

If there is an event in a building, concentric circles appear around the icon.

View an event

1. Click the building icon  that has the event.
2. In the notification window that appears, click **GO TO**.

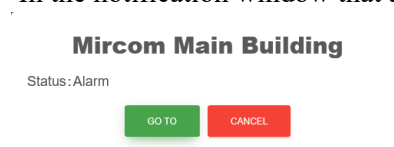


Figure 42. Alarm notification

The building view appears. Concentric circles appear next to the floor that has the event.

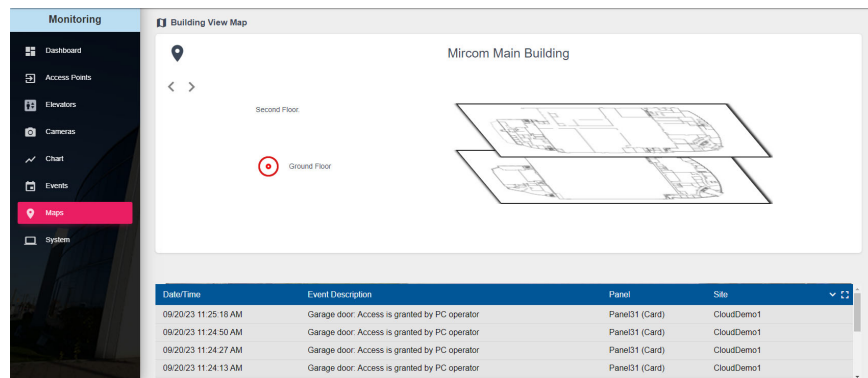


Figure 43. Building view

- Click the circles to see more detail about the event.

The floor map appears.

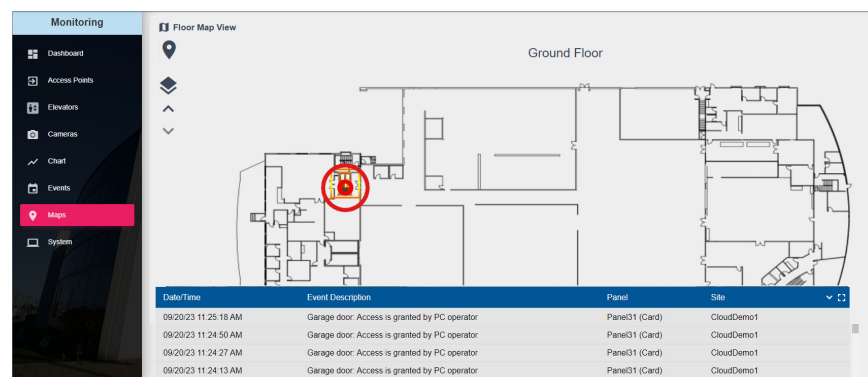


Figure 44. Floor map


The concentric circles appear around the input or access point that has the event.

- Click any input or access point to see information about the device.

To add an access point to a floor, see section 2.6.11.

2.6.3 Navigate Buildings and Floors

Navigate the building view

- On the site map, click the building icon  to view a building.

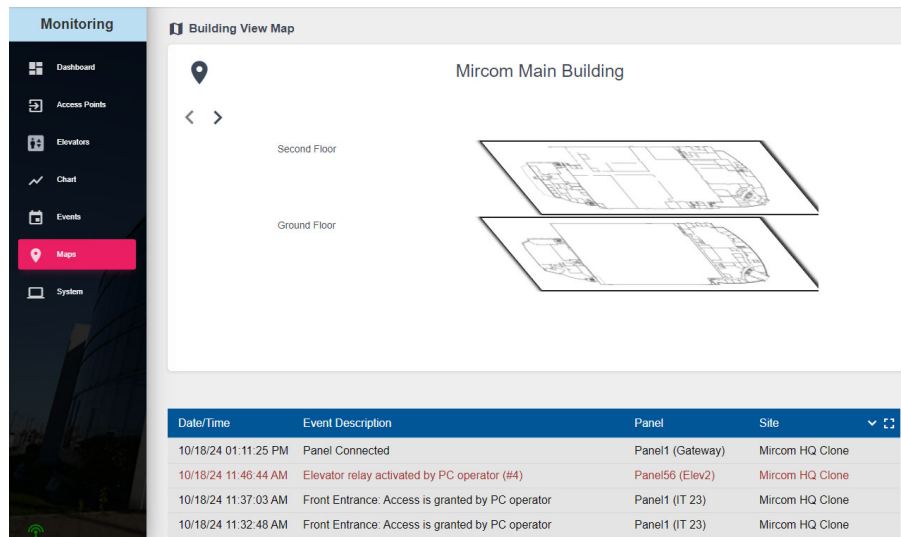





Figure 45. Building view

- On the building view:
 - Click the Site icon  to go back to the site map.
 - Or click the arrows   to see the other buildings on the site.
 - Click the name of a floor to see the floor view.

Navigate the floor view

- On the building view, click a floor to see the floor view.

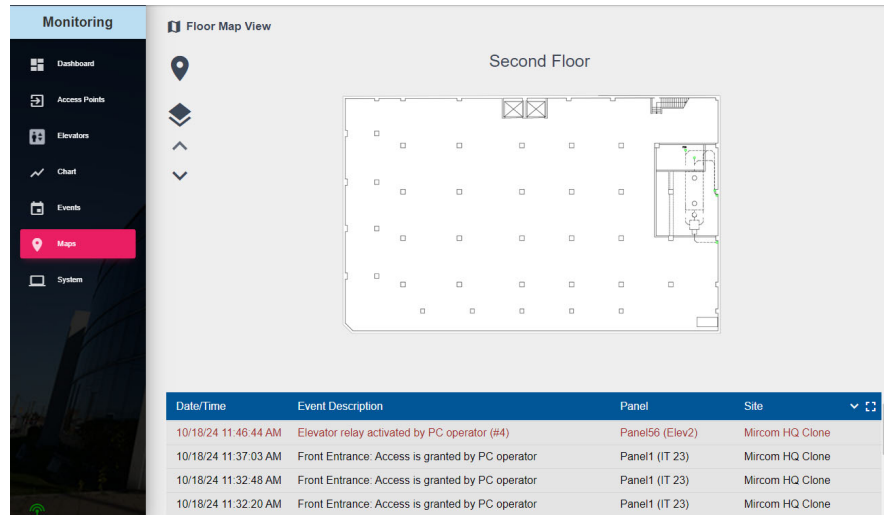








Figure 46. Floor view

- On the floor view:
 - Click the Site icon  to go back to the site map.
 - Click the Building icon  to go back to the building view.
 - Click the arrows  to see the other floors in the building.

2.6.4 Edit the Site, Buildings and Floors

You can place a building icon  showing where a building is located on the site map. You can place access point icons  showing where access points are located on the floor map. Locating buildings and access points on maps makes it easier to see where alarms are happening.

Enter the Edit window

- On the site map, click the Edit button  in the upper right corner.

The Edit window appears.

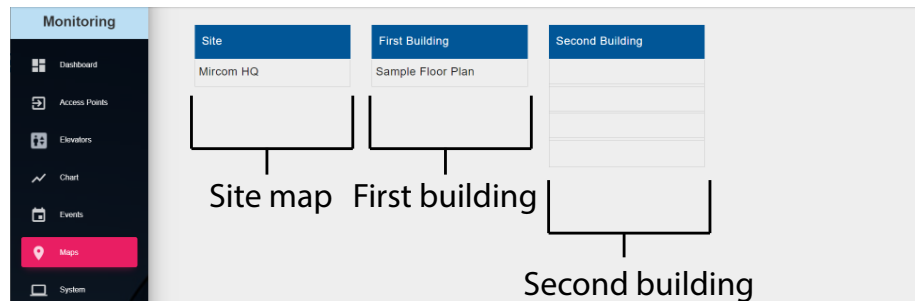






Figure 47. Edit window


The Edit window shows the site map on the left, and the buildings on the right.

2. Edit the map and buildings as described in sections 2.6.5 to 2.6.12 below.
3. When you are finished editing the site map, buildings, and floors, click the Done button  in the upper right corner to save your changes.

Or click the Cancel button  to go back to the site map without saving.

2.6.5 Edit a site map

1. In the Edit window, click the name of the site map, and then click the red Edit button  that appears.
2. Edit the site's description and showcase picture (see section 2.6.12), and then click **Submit**.
3. Click the Done button  in the upper right corner to save your changes.

Or click the Cancel button  to go back to the site map without saving.

2.6.6 Upload a Map for the Site

1. In the Edit window, click the name of the site map, then click Edit.

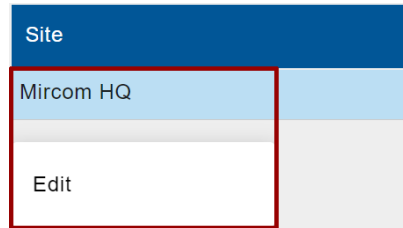


Figure 48. Edit Site Map

The Edit Map window appears.

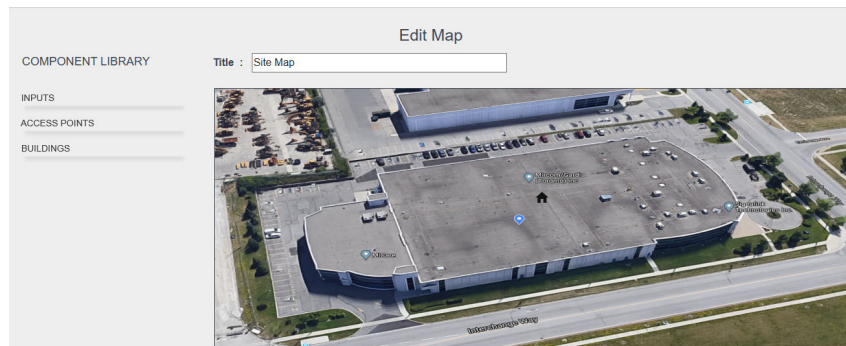





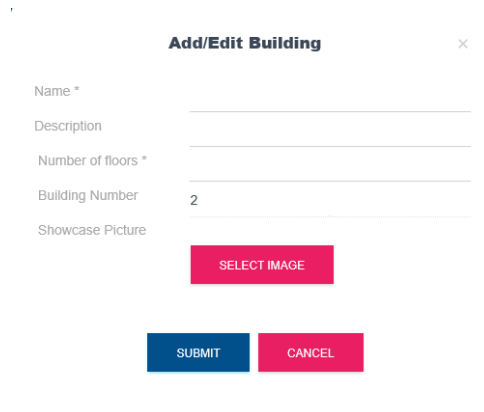
Figure 49. Edit Site Map window

2. Click the Upload button  in the upper right corner.
3. Click **Select Image**, choose a map to upload, and then click **Submit**.
4. Click the Done button  in the upper right corner to save your changes.

2.6.7 Add a Building

1. In the Edit window, click the plus sign  in the upper right corner.



The Add/Edit Building window appears.



The image shows a web form titled "Add/Edit Building" with a close button (X) in the top right corner. The form contains the following fields and buttons:

- Name ***: A text input field.
- Description**: A text input field.
- Number of floors ***: A text input field.
- Building Number**: A text input field containing the value "2".
- Showcase Picture**: A section with a pink "SELECT IMAGE" button.
- At the bottom, there are two buttons: a blue "SUBMIT" button and a pink "CANCEL" button.

Figure 50. Add/Edit Building

2. Enter the building's name, description, and number of floors.
3. Click **Select Image** to upload a showcase picture of the building (see section 2.6.12).
4. Click **Submit**.
5. Click the Done button  in the upper right corner to save your changes.
Or click the Cancel button  to go back to the site map without saving.

2.6.8 Place your Buildings on the Site Map

1. In the **Edit** window, click the name of the site map, then click **Edit**.

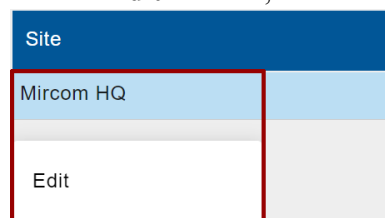




Figure 51. Site Map Edit menu

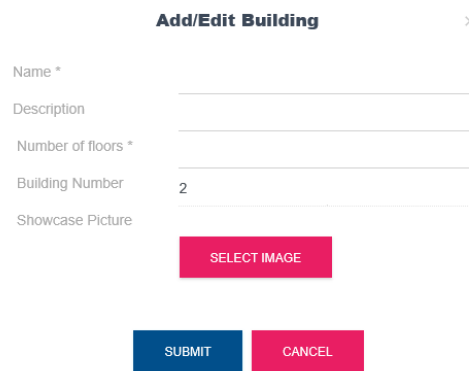
The Edit Map window appears (Figure 49).

2. From the **Component Library** on the left, click **Buildings**, and then click and drag the name of the building on to the map.
3. Click the Done button  in the upper right corner to save your changes.

2.6.9 Edit the Buildings

1. In the Edit window, click the name of a building, and then click the red Edit button  that appears.



The Add/Edit Building window appears.







The Add/Edit Building window is a modal dialog with a title bar "Add/Edit Building" and a close button (X). It contains the following fields and buttons:

- Name *: Text input field
- Description: Text input field
- Number of floors *: Text input field
- Building Number: Text input field with the value "2"
- Showcase Picture: Text input field with a "SELECT IMAGE" button below it
- SUBMIT: Blue button
- CANCEL: Red button

Figure 52. Add/Edit Building

2. Edit the building's name, description, and number of floors, and showcase picture (see section 2.6.12), and then click **Submit**.
3. Click the Done button  in the upper right corner to save your changes.
Or click the Cancel button  to go back to the site map without saving.

2.6.10 Remove a Building

1. In the Edit window, click the building that you want to remove so that the red Edit button  appears.
2. Click the minus sign  in the upper right corner.
3. Click **Yes, delete it**.
4. Click the Done button  in the upper right corner to save your changes.
Or click the Cancel button  to go back to the site map without saving.

2.6.11 Edit the Floors

Each building consists of one or more floors. You can place inputs and access points on the floor maps. Locating access points on the floor map makes it easier to see where alarms are happening.

Edit a floor and upload a floor map

1. In the Edit window, click a floor of a building, then click **Edit**.

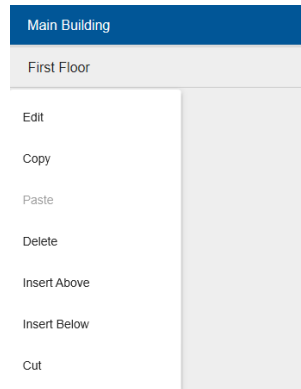




Figure 53. Floor Edit menu

The Edit Map window appears (Figure 49).


2. On the Edit Map window, enter a title for the floor.
3. Click the Upload button  in the upper right corner.
4. Click **Select Image**, choose a map to upload, and then click **Submit**.
5. From the **Component Library** on the left, click and drag a component (for example an access point) to the map.

Note: Place access points on the floor map in order to make it easier to see where alarms are happening. When an access point is in alarm, it will be surrounded by red concentric circles on the floor map.

If you place an input on the floor map, then the input will show whether it is open or closed.

6. Click the Done button  in the upper right corner to save your changes.

2.6.12 View the Showcase Pictures

The showcase picture button () in the upper right corner of the Maps window shows a slideshow of the site and buildings. You can add these pictures in the Edit window (section 2.6.4). Showcase pictures are not maps, but are photographs of the site and buildings.

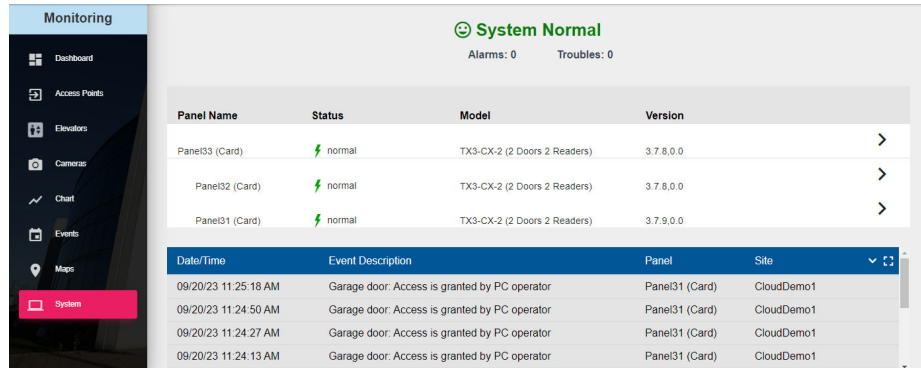
2.7 System

The System window shows the system status and all the panels in the network.

2.7.1 View the System

- Click **System** in the left pane.

The System window appears.



Panel Name	Status	Model	Version
Panel33 (Card)	normal	TX3-CX-2 (2 Doors 2 Readers)	3.7.8.0.0
Panel32 (Card)	normal	TX3-CX-2 (2 Doors 2 Readers)	3.7.8.0.0
Panel31 (Card)	normal	TX3-CX-2 (2 Doors 2 Readers)	3.7.9.0.0

Date/Time	Event Description	Panel	Site
09/20/23 11:25:18 AM	Garage door: Access is granted by PC operator	Panel31 (Card)	CloudDemo1
09/20/23 11:24:50 AM	Garage door: Access is granted by PC operator	Panel31 (Card)	CloudDemo1
09/20/23 11:24:27 AM	Garage door: Access is granted by PC operator	Panel31 (Card)	CloudDemo1
09/20/23 11:24:13 AM	Garage door: Access is granted by PC operator	Panel31 (Card)	CloudDemo1

Figure 54. System

The panels are grouped by main node.

The view has the following columns:

Panel Name. The name is assigned in MiVision.

Status. Normal, alarm, or trouble.

Model. The panel model.

Version. The firmware version.

2.7.2 See Panel Details

1. Click the arrow ➤ on the right to see details of the panel.

Panel Details shows the following information:

- Panel Name
- Type
- Model
- Firmware version
- Hardware version - for telephone entry controller boards, this line provides information about the model of board.
 - 0.17.127: MD-1245
 - 0.0.127: MD-1086
- RS-485 address
- IP address
- Serial number
- The date of the last change
- For Touch screens, the window also shows the following:
 - Touch software version
 - Touch hardware version
 - Touch database version
 - Touch GUID
 - WAN IP address

Panel Details

×

Panel Name	Panel33 (Card)
Type	2
Model	TX3-CX-2 (2 Doors 2 Readers)
Firmware	3.7.8
Hardware	0.1.0
RS485 address	33
IP address	10.10.8.49
Serial number	-858029984
Last changed	2024-09-24T11:09:24
Touch software	0.0
Touch hardware	0.0
Touch database	0.0
Touch GUID	261d386f-6cb4-41f3-892f-faa2ef9468a7
WAN IP Address	0.0.0.0

OK

Figure 55. Panel Details

3

Touch Screen, Telephone Entry, and Emergency Phone Configuration

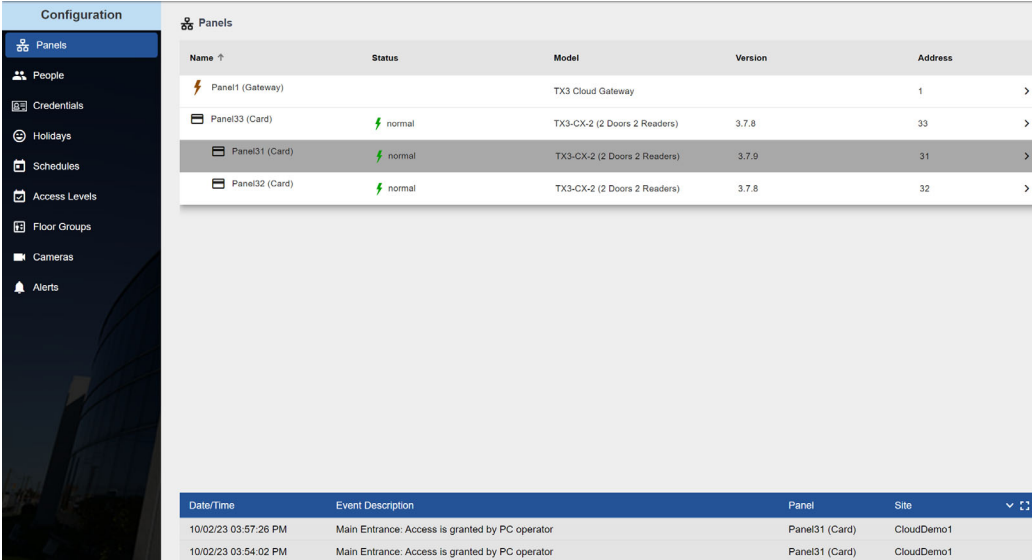
MiVision lets you access, add, and modify Touch Screens, telephone entry system panels, and emergency phones.

Note: After you configure the site for the first time, and after any time you make changes, you must send the job. See section 1.10.

3.1 Configure a Panel

1. Click the **Options** menu, then click **Configuration**.
2. Click **Panels** in the left pane.

The Panels window appears.



Name ↑	Status	Model	Version	Address
Panel1 (Gateway)		TX3 Cloud Gateway		1
Panel33 (Card)	normal	TX3-CX-2 (2 Doors 2 Readers)	3.7.8	33
Panel31 (Card)	normal	TX3-CX-2 (2 Doors 2 Readers)	3.7.9	31
Panel32 (Card)	normal	TX3-CX-2 (2 Doors 2 Readers)	3.7.8	32

Date/Time	Event Description	Panel	Site
10/02/23 03:57:26 PM	Main Entrance: Access is granted by PC operator	Panel31 (Card)	CloudDemo1
10/02/23 03:54:02 PM	Main Entrance: Access is granted by PC operator	Panel31 (Card)	CloudDemo1

Figure 56. Panels

3. Click the arrow  on the right to see details of the panel.

The Panels Configuration screen appears. It is divided into several sections. To see a specific section, click the section in the left pane.

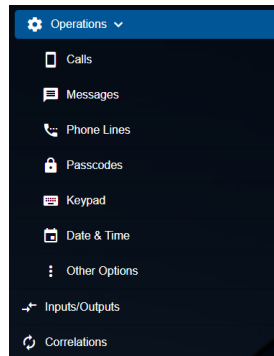


Figure 57. Telephone Entry Configuration left pane

3.1.1 Operations - General

Panel label. Provide a name for the panel.

The other fields in this section are read-only. To edit them see section 1.5.5.

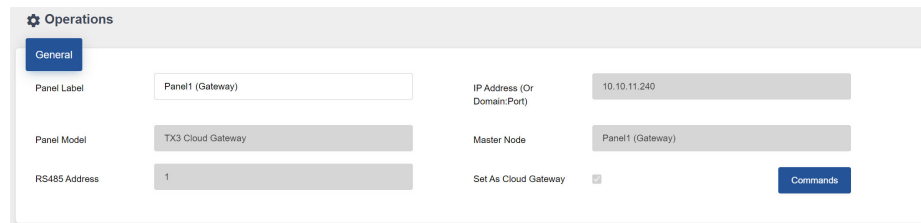


Figure 58. Panel Configuration - General

3.1.2 Operations - Calls

Configuring calls lets you specify the call duration, number of rings and call scheduling.

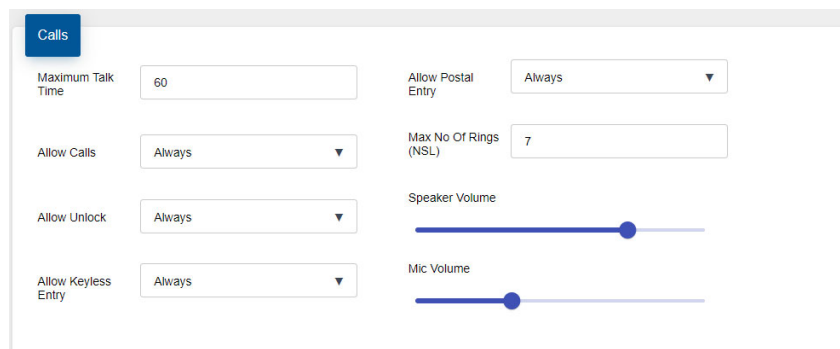


Figure 59. Panel Configuration - Calls

4. Provide information for each of the following:

Maximum Talk Time. Specify the maximum time in seconds the visitor may communicate with the resident on a single call. After this time, the panel disconnects.

Allow Calls. Use this selection to allow calls to the residents based on the selected schedule.

Allow Unlock. Use this selection to allow the resident to use their phone to unlock doors during a set schedule.

Allow Keyless Entry. Use this selection to allow keyless entries during selected schedule.

Allow Postal Entry. Use this selection to enable the postal lock during a set schedule.

Maximum No of Rings (NSL). For NSL lines, specify the number of rings of each call before the panel reports no answer and hangs up. For ADC lines, this setting is not used and ring duration is determined by the maximum talk time.

Speaker Volume. Specify the panel speaker call volume.

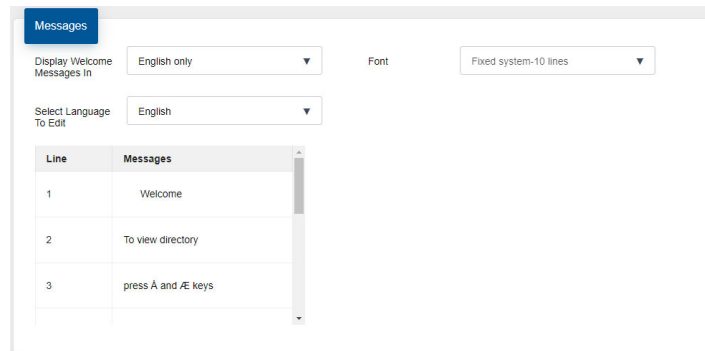
Mic Volume. Specify the microphone call sensitivity.

Note: On Touch Screens with telephone entry controller board model MD-1086, use the speaker and microphone volumes only for telephone calls (not VOIP calls). Use the **Touch Screen More Options** (section 4.7) to set the volume for notifications, event prompts and VOIP calls.

On Touch Screens with telephone entry controller board model MD-1245, use the **Touch Screen More Options** (section 4.7) to set the volume for notifications, event prompts, VOIP calls, and telephone calls.

3.1.3 Operations - Messages

Messages is a feature that determines how messages and settings associated with a lobby panel appear on the LCD. This feature is not used by Touch Screen.



Line	Messages
1	Welcome
2	To view directory
3	press Å and Æ keys

Figure 60. Panel Configuration - Messages

Display Welcome Message In. Select the language to use for welcome messages. A multiple language selection scrolls sequentially through each message.

Select Language To Edit. Select the welcome message to edit based on language.

Font. Select the type of font to use when displaying welcome messages. This option is only available for the 8-line lobby unit model. This feature is not used by Touch Screen.

Welcome message lines. Welcome messages shows the instructions in the specified language. Use this area to make changes to the text. This feature is not used by Touch Screen.

The up arrow and down arrow symbols are represented in MiVision with the following ASCII characters:

- **Up arrow:** Å (hold down the Alt key and type 0197 on the numeric keypad)
- **Down arrow:** Æ (hold down the Alt key and type 0198 on the numeric keypad)

These two characters will appear on the TX3 screen as the correct up and down arrow symbols.

3.1.4 Operation - VOIP (Touch Screen Only)

You can configure the TX3 Touch Screen to make VOIP (voice over IP) calls to residents using SIP (Session Initiation Protocol). SIP is a protocol for controlling phone or video messaging on an IP network. The TX3 Touch Screen is a SIP client and can communicate with other SIP clients through a SIP server.

3.1.4.1 Requirements

The TX3 Touch supports the following codecs for SIP calls. The SIP server and other SIP clients must support one or more of these codecs to work with the TX3 Touch system:

- Audio codecs: G.722-64k, G.722.2, G.722.1-32K, G.722.1-24K, G.711-ALaw-64k
- Video codecs: H.263, H.263plus

SIP on the TX3 Touch is compatible with Mircom's Unified Building Solution, and the MiEntry mobile app.

3.1.4.2 Configure SIP

To configure SIP, you need:

- The IP address or URL of the SIP server.
- The proxy IP address or URL of the SIP server (also called outbound proxy). This is required by Mircom SIP Service. Other SIP services may not require it.
- The SIP username, SIP password, and authorization ID (also called authorization username) of the Touch Screen. These are configured in the SIP server. Not all SIP servers require an authorization ID.
- The SIP username of each resident.

The building manager or reseller configures this information in MiConnect (<https://miconnect.mircom.com>).

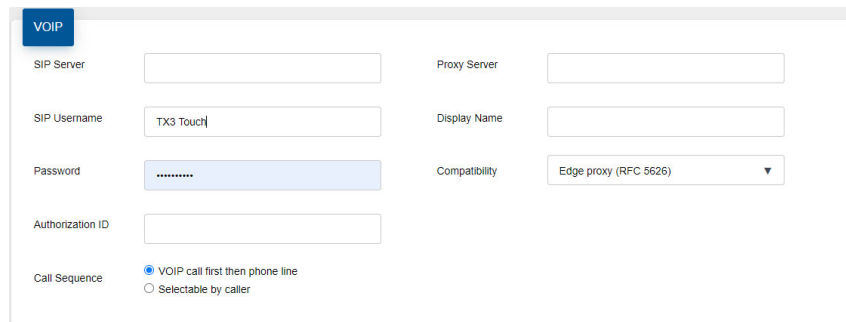


Figure 61. VOIP

SIP Server. The URL of the SIP server.

SIP Username. The SIP username of the Touch Screen.

Password. The SIP password for the Touch Screen.

Authorization ID. The authorization ID (also called authorization username) for the Touch Screen. Not all SIP servers require this.

Proxy Server. The proxy server (also called outbound proxy) required by the SIP server. Not all SIP servers require this.

Display Name. This name appears on the resident's SIP phone when the Touch Screen calls the resident.

Compatibility. Leave this option at the default (**Edge proxy**) if you are using the MiConnect VOIP service.

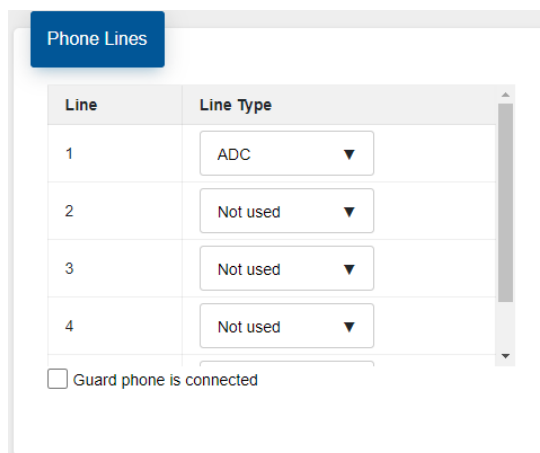
Call sequence. If you select **VOIP call first then phone line**, the Touch Screen will try to call the resident's VOIP number first when a visitor makes a call. If you select **Selectable by caller**, the Touch Screen will prompt the visitor to select either VOIP or PSTN when the visitor makes a call.

Note: The **VOIP call first then phone line** option works only if both a VOIP account and phone line are configured for the resident.

3.1.5 Operation - Phone Lines

The Phone Lines window lets you select the resident's telephone line type as either ADC or NSL. Up to five lines may be configured.

If a guard phone is installed with the system, in order to use it you must first activate the guard phone using this window. For a description on how to install and use the guard phone, see LT-969 TX3 Telephone Access System Installation and Operation Manual.



Line	Line Type
1	ADC
2	Not used
3	Not used
4	Not used

☐ Guard phone is connected

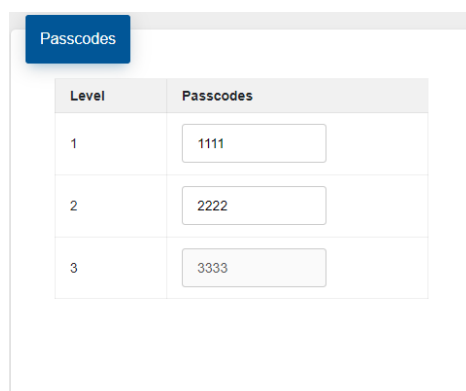
Figure 62. Panel Configuration - Phone Lines

Phone Lines. Select either **not used**, **ADC** or **NSL**.

Guard phone is connected. Select this check box if the TX3-GPM Guard Phone Module is installed on this panel

3.1.6 Operation - Passcodes

Passcodes let you define and set the code to permit panel access. There are three levels of access. Panel passcode levels 1 and 2 are set by Touch Screen. Passcode level 3 is read only and is initially set at the panel. All passcodes are 10 digits long.



Level	Passcodes
1	1111
2	2222
3	3333

Figure 63. Panel Configuration - Passcodes

Level 1. Future use.

Level 2. Level 2 provides access to operations without configuration privileges.

Level 3. Level 3 grants full panel access and is read only. It is initially set at the panel, but can be changed afterwards using the **Commands** menu (section 1.12). The level 3 passcode is also the network passcode.

Note: At any time if you lose or forget the passcode, call Technical Support to receive a temporary passcode. This temporary passcode is only valid for the day it is issued.

3.1.7 Operation - Keypad

Configuring the Keypad lets you set permissions for the resident for opening doors, using call waiting and using the panel during calls.

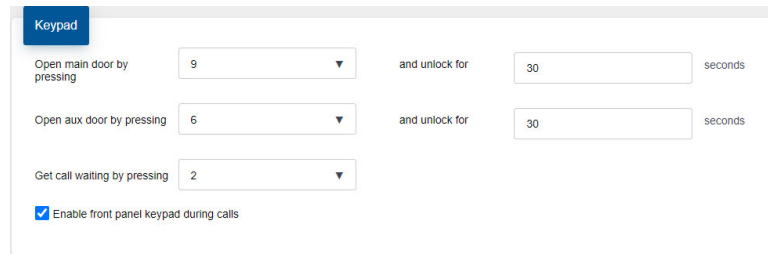


Figure 64. Panel Configuration - Keypad

5. Provide information for each the following:

Open Main door by pressing. Specifies which key on the resident's phone unlocks the main door.

Note: Do not select 4 (this is used to refuse entry or disconnect).

Do not use the same number for the main door, auxiliary door, and call waiting (call waiting works on NSL systems only).

and unlock for. Specifies the number of seconds to unlock the main door.

Open Aux door by pressing. Specifies on telephone entry systems the key to press on the residence phone to unlock the auxiliary door.

Note: Do not select 4 (this is used to refuse entry or disconnect).

Do not use the same number for the main door, auxiliary door, and call waiting (call waiting works on NSL systems only).

Note: If the telephone entry system panel has controller board model MD-1245, do not select 1, 7, or * for **Open Main Door by Pressing** and **Open Aux Door by Pressing**.

and unlock for. Specifies the number of seconds to unlock the auxiliary door.

Get call waiting by pressing. Specifies the key to press on the residence phone to connect to the lobby phone while on an outside call. Do not select 4. This is used to refuse entry or disconnect.

Note: **Get call waiting by pressing** works only on NSL systems.

Enable front panel keypad during calls. Selecting this check box allows the panel keypad to be used during a call.

3.1.8 Operation - Date and Time

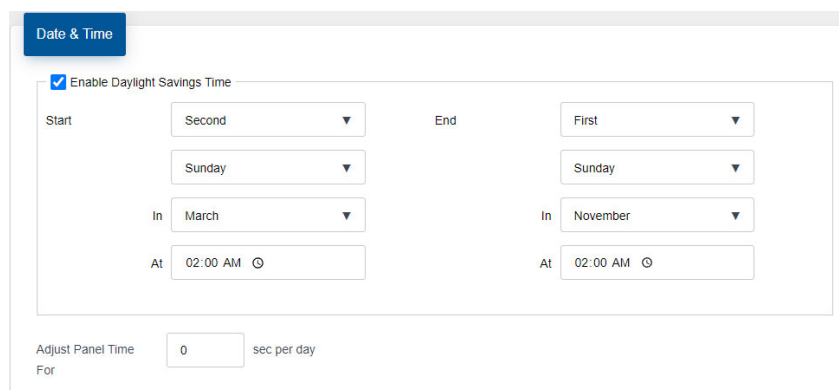


Figure 65. Date and Time Options

Enable Daylight Savings Time. Select this check box to enable daylight saving time. When enabled provide the daylight savings start and end time for the local area.

Adjust Panel Time For. Provide a value to compensate for the daily drift away from the true time.

3.1.9 Operation - Other Options

Other Options lets you specify the main door unlock schedule, elevator restriction time, postal lock use, phone line type and display scroll speed.

The elevator restriction feature limits building accessibility by granting visitor access only to the destination floor. This prevents the visitor from accessing non-designated floors.

If installed the postal lock provides mail carriers access to the building. The building administrator arranges for the installation of this lock with the post office and defines its usage on a daily or indefinite basis. The “Postal Usage” function lets you define the maximum usage for the postal lock.

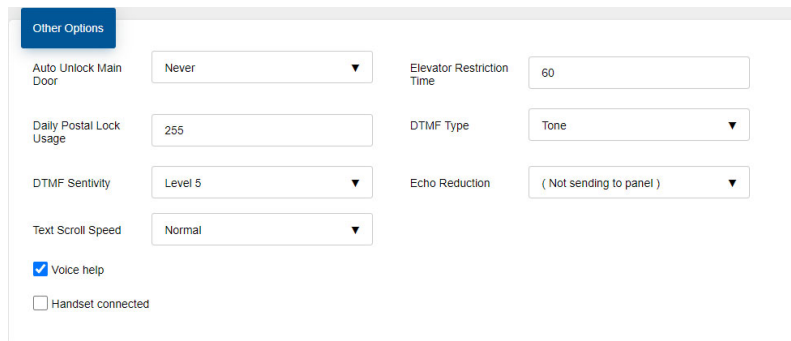


Figure 66. Panel Configuration - Other Options

Auto Unlock Main Door. Use this selection to unlock the main door based on the selected schedule.

Elevator Restriction Time. Specifies the amount of time an elevator is accessible for a visitor after the resident grants access.

Daily Postal Lock Usage. Specifies the daily limit for postal access. The range is 1 to 254 and the default is 4. For unlimited usage set the value to 255.

DTMF Type. This is set to **Tone** and is not configurable.

DTMF Sensitivity. Set the sensitivity to a level between 1 to 8. The default is 5. Lower sensitivity levels reduce interference from nearby cell phones

Echo Reduction. Select a setting to enhance call clarity by reducing the echo in the room.

Text Scroll Speed. Specifies the scroll speed for the resident record directory display on telephone entry system panels. This option is not available on Touch Screen.

Voice help. Select this check box to enable voice help for the telephone entry system. This is not available on Touch screens.

Handset connected. Select this if a handset is connected to the Lobby Control Unit.

3.2 Touch Screen

The Touch Screen options are described in section 4.

3.3 Inputs

1. Click **Inputs/Outputs** in the left pane.

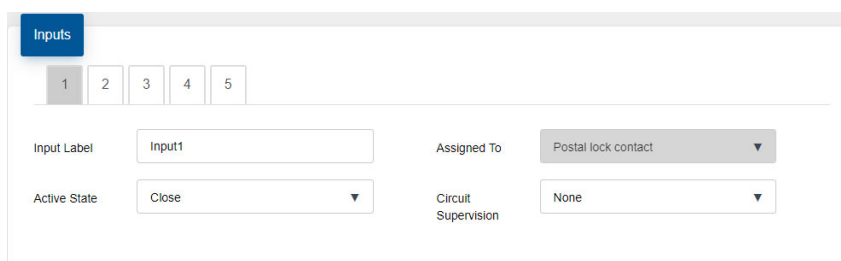


Figure 67. Inputs

Inputs 1 to 5 are assigned specific functions. Inputs 1 to 3 have pre-defined functions and connect to specific devices. Inputs 4 and 5 are general purpose inputs that can be manually assigned (correlated) to activate a general purpose output.

The application automatically senses the on/off status of connected components. In order to accurately monitor the functional state of the panel inputs, you must first define the electrical circuit characteristics of the input.

3.3.1 Inputs 1 to 5

Inputs 1 to 5 are designated as follows:

Input 1. Input 1 connects to the Postal Lock. Activation of this input unlocks the main door and starts the main door timer. The door locks when the timer expires or when the door sense input is activated. Daily usage is limited according to a pre-defined amount. Any attempt to use the postal lock beyond this point causes a warning message to appear and the system to return to normal operation. Input 1 can also, when configured, activate a general purpose output to perform any required function.

Input 2. Input 2 connects to the fire alarm panel and receives fire notification. Activation of this input unlocks the main and auxiliary doors. These outputs are active as long as the fire panel input is active. Input 2 can also, when configured, activate a general purpose output to perform any required function.

Input 3. Input 3 connects to the door sense switch. Unlocking the main door activates the main door open timer. Activation of the Main Door Sense locks the main door and resets the main door open timer. This function is typically used to prevent ‘tailgating’. Input 3 can also, when configured, activate a general purpose output to perform any required function.

Input 4. Input 4 is a general purpose input that, when configured, activates a general purpose output to perform any required function.

Input 5. Input 5 is a general purpose input that, when configured, activates a general purpose output to perform any required function.

1. Click an input number to configure that input.

Input Label. Use this text box to provide a label name for this panel input. This information is not stored in the panel and reverts to the state when a Job is retrieved from the panel.

Assigned To. Contains a drop-down list of all assigned inputs. This option is read only on telephone entry system panels.

Active State. Specifies the state by which it is considered active. Two selections are presented. Select one of the following:

Open

Close

Circuit Supervision. Specifies the circuit type and indicates whether the input is supervised. Select one of the following:

None

Open circuit

Short circuit

Open and short circuit

3.4 Outputs

1. Click **Inputs/Outputs** in the left pane.

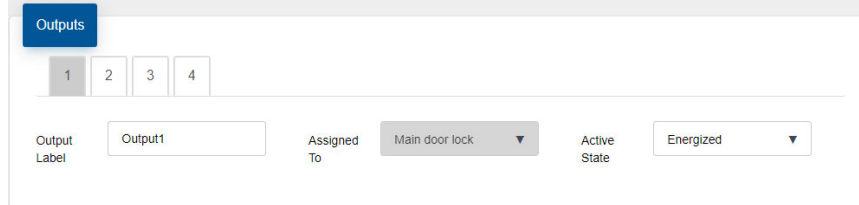


Figure 68. Outputs

Outputs are programmed for specific functionality, such as specific delay and on/off times.

The telephone entry system has the following four panel outputs:

Output 1. Output 1 is a dedicated output that controls the relays for the AC and DC main door lock strikes.

Output 2. Output 2 is a dedicated output that controls the relay for the auxiliary door lock strike.

Output 3. Output 3 is a general purpose output that performs any required function.

Output 4. Output 4 is a general purpose output that performs any required function.

2. Click an output number to configure that output.

Label. Use this text box to provide a label name for this panel output. This information is not stored in the panel and reverts to the default state when a Job is retrieved from the panel.

Assigned To. Designates the panel output to the device. From the list select a device. This option is read only on telephone entry system panels.

Active State. Specifies the state by which it is considered active. Two selections are presented. Select one of the following:

Energized. When the device is energized it is considered to be active.

De-energized. When the device is de-energized it is considered to be active.

3.5 Correlations

Correlations let you establish specific relationships between panel inputs (events) and outputs (actions). Use Correlations to specify the relationships between events, actions and schedules.

Note: All inputs, outputs and schedules must be defined before applying correlations.

1. Click **Correlations** in the left pane.

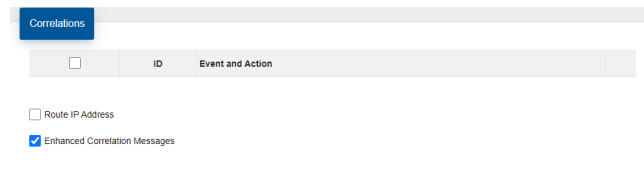




Figure 69. Correlations

Route IP Address. (Touch Screen only) If the Touch Screen is a main node connecting two RS-485 networks, it does not route correlations from one network to the other by default. Select this checkbox to make the Touch Screen share correlations between RS-485 networks.

You can have more than one Touch Screen main node on the same RS-485 network, but only one Touch Screen main node can have this option selected.

Enhanced Correlation Messages. (Touch Screen only) If the firmware in the job is 3.5 or above, select this option. If the firmware is lower than version 3.5, unselect this option.

3.5.1 Add or Edit a correlation

1. Click the **Add** button  add a correlation, or click on the **Edit** button  next to a correlation to edit it.

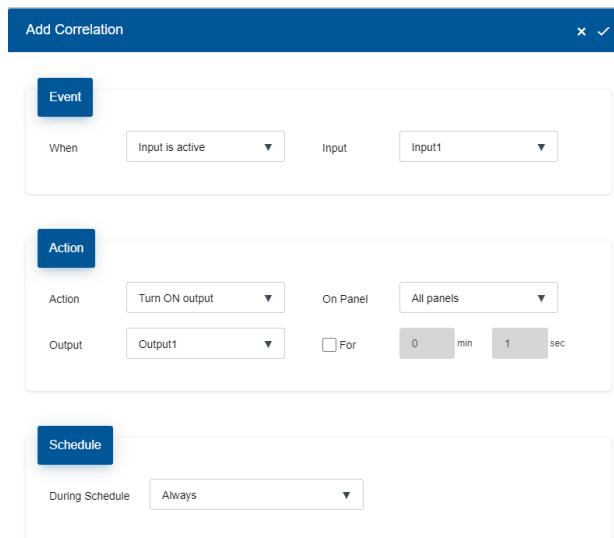


Figure 70. Add/Edit a Correlation

When. This parameter defines the input event that activates an output action. Select one of the following:

Input is active. Select a panel input from the **Input** menu.

Input is normal. The general purpose input becomes inactive.

Call Started. A call to a resident is placed from the lobby.

Call finished. A call to a resident ends.

Call is connected. A call is established.

Access is granted. Resident grants access using their telephone keypad.

Access is denied. Resident denies access.

Action. Specifies the type of action to occur for a specific input. Select one of the following:

Turn ON output.

Turn OFF output.

Call dial code. Call the dial code 9991 or 9992. This is used for the emergency phone. See LT-6113 TX3 Emergency Phone Installation and Operation Manual on <http://www.mircom.com>.

On panel. Applies the action either to one of the panels on your system or to a group of panels on your system. If, for example, you have two panels (Panel 1 and Panel 2) in your TX3 system, you could select from the following options:

Panel 1. Apply the correlation to Panel 1 only.

Panel 2. Apply the correlation to Panel 2 only.

All panels. Apply the correlation to all telephone entry, card access, and Touch Screen panels on the network.

Custom. Apply the correlation to a custom target. This option is only available for TCP/IP network connections. When you select this option, you can click on the **Custom** button to select from the following custom targets:



- **Nano IP Address.** Apply the correlation to a TX3 Nano. This option is only available for TCP/IP network connections.
- **All panels On The RS485 Network Of The Master Node.** (Select a main node from the list.)
- **All Master Nodes Only.**
- **All Panels With RS485 Address.** (Select the address from the list.)

Note: Correlation signals are not transmitted by Touch Screen main nodes by default. If you plan on using the **All** or **Custom** correlation options, select the **Route IP Address** checkbox on one of the main nodes.


Output. Applies the action to a specific output on the panel.

For. Represents the duration of the action in minutes and seconds up to a maximum of 600 minutes. Uncheck the box if you want the action to continue indefinitely.

During schedule. This parameter lets you apply this correlation to a schedule, which means that the correlation will be active only while the schedule is active. The two default selections (Always and Never) and any previously defined schedules are presented.

Click the **Done** button  in the upper right corner to save your changes, or **Cancel** button  next to it to cancel changes.

3.5.2 Remove a correlation

1. Click the **Remove** button  next to the correlation you want to remove.
2. Click **YES**.



Delete

Are you sure you want to delete this correlation?

YES

NO

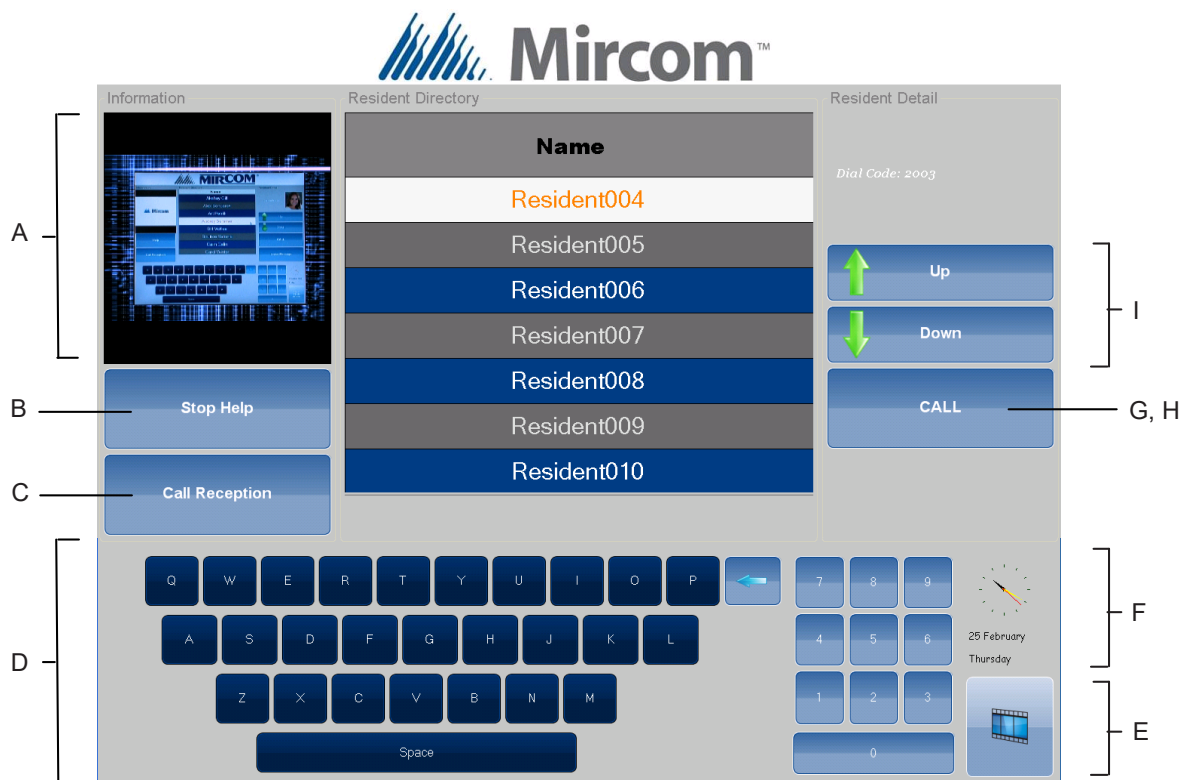
Figure 71. Remove Correlation

4 Touch Screen Appearance Configuration

MiVision lets you easily change the layout, theme, videos and banners of a Touch Screen.

The appearance of all Touch Screen screen elements are configurable and may be saved and re-applied. Figure 72 shows the user interface configurable screen elements.

Note: If your network connection type is TCP/IP, you can configure the appearance of main node Touch Screens in your job, but not secondary node Touch Screens. The appearance of a secondary node Touch Screen can only be changed at the Touch Screen or by connecting to it using Remote Desktop. See LT-995 for details.



A. Main Video B. Help Button C. Call Reception D. Keyboard E. Bottom Banner F. Clock/Language Selection G. Call Resident H. Disconnect I. Resident Scroll Buttons

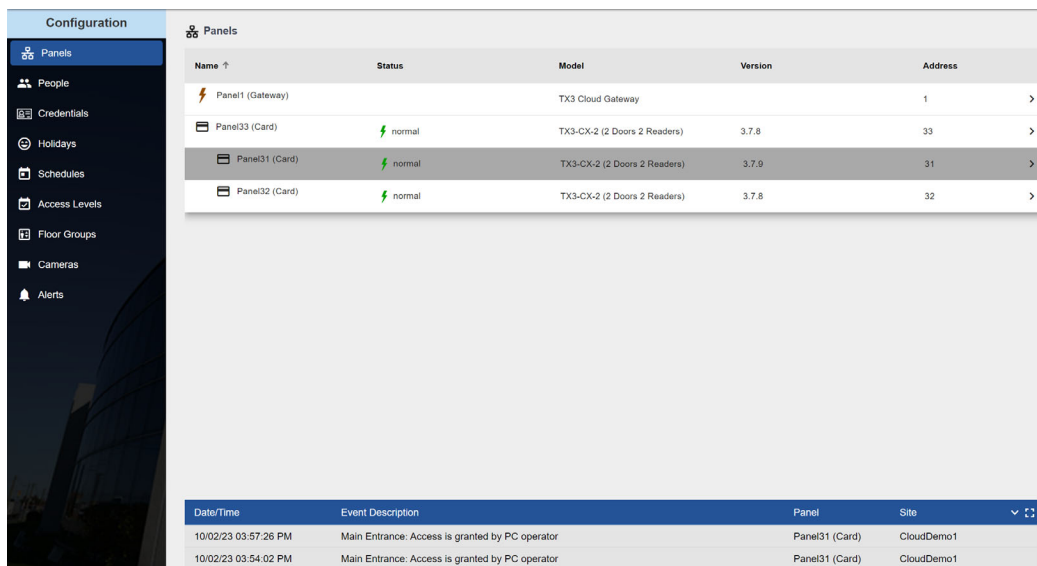
Figure 72. User Interface Screen Elements

Note: After you configure the site for the first time, and after any time you make changes, you must send the job. See section 1.10.

4.1 Panels

1. Click the **Options** menu, then click **Configuration**.
2. Click **Panels** in the left pane.


The Panels window appears.



Name	Status	Model	Version	Address
Panel1 (Gateway)		TX3 Cloud Gateway		1
Panel33 (Card)	normal	TX3-CX-2 (2 Doors 2 Readers)	3.7.8	33
Panel31 (Card)	normal	TX3-CX-2 (2 Doors 2 Readers)	3.7.9	31
Panel32 (Card)	normal	TX3-CX-2 (2 Doors 2 Readers)	3.7.8	32

Date/Time	Event Description	Panel	Site
10/02/23 03:57:26 PM	Main Entrance: Access is granted by PC operator	Panel31 (Card)	CloudDemo1
10/02/23 03:54:02 PM	Main Entrance: Access is granted by PC operator	Panel31 (Card)	CloudDemo1

Figure 73. Panels

3. Click the arrow  on the right to see details of the Touch Screen panel.

The Panels Configuration screen appears. It is divided into several sections. Click the **Touch Screen** section.

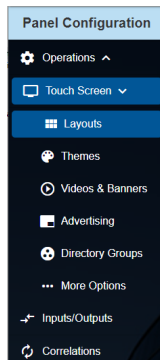


Figure 74. Touch Screen Configuration left pane

4.2 Layouts

Layouts determines how each of the major screen areas are arranged and portrayed, and may be selected from existing templates or customized.

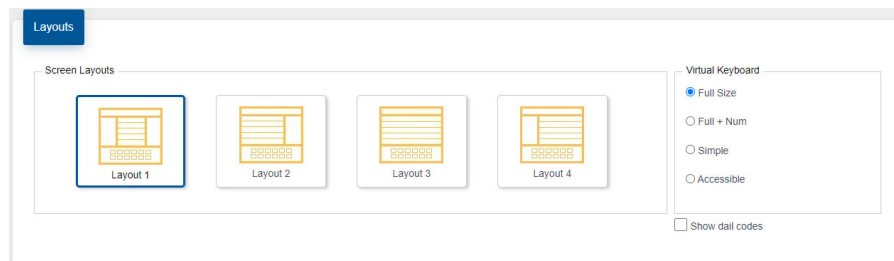


Figure 75. Touch Screen Layouts

1. From the **Screen Layouts** select one of the four available layouts.
2. From the **Virtual Keyboards** select from one of the following options:
 - Full size.** Displays the keyboard in full size.
 - Full + Num.** Displays the keyboard in full size with numbers.
 - Simple.** Displays the keyboard in basic formatted lettering.
 - Accessible.** Displays a keyboard, selection button, and resident scroll buttons at the bottom of the screen.
3. To show the dial codes on the residential directory select **Show dial codes**.

4.3 Themes

Themes lets you set the screen font size, color and element attributes. Selections may be saved as **.thm** files and existing themes may be imported. You can accept an existing customized theme or modify it as necessary. Preset themes are fixed and cannot be modified.

See section 17 for a detailed description of the user interface elements.

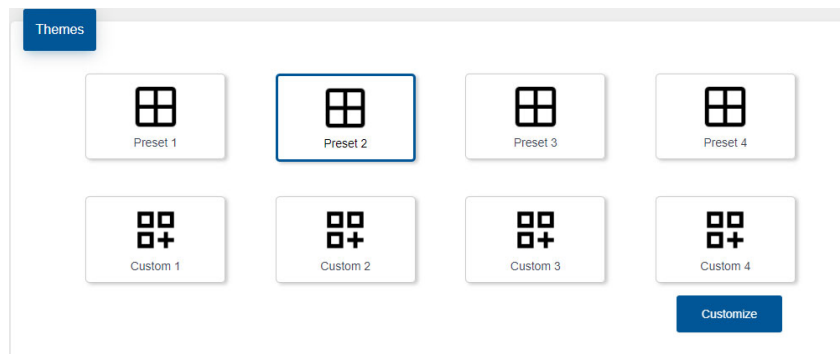


Figure 76. Touch Screen Themes

Note: Preset themes can not be modified, only exported.

4. Select a custom theme and click **Customize**. The Customize Theme window appears showing the font and color selections.

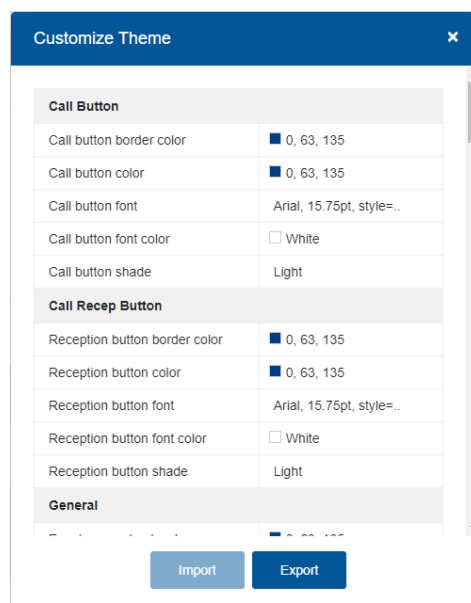
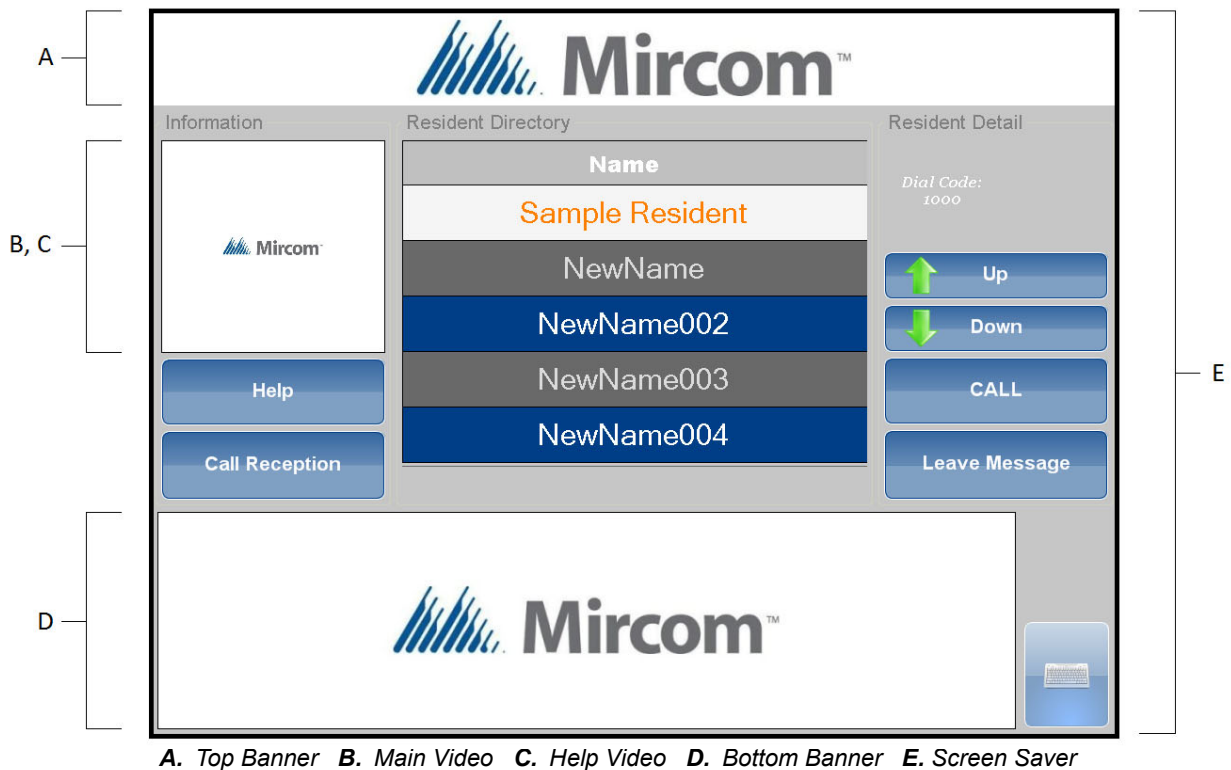


Figure 77. Touch Screen Customize Theme

5. Select the font size and color for the user interface elements. For a complete list of all the configurable user interface elements see section 17.
6. Click **Import** to retrieve an existing theme or click **Export** to save the theme to a file.

4.4 Videos and Banners

Videos and Banners lets you define and select the multi media options for the Touch Screen user interface. There are four different locations where media can be displayed. Figure 78 shows the customizable Touch Screen user interface areas. Table 1 gives the dimensions for these areas. Media can be in any of the following video or still image formats: **.avi**, **.wmv**, **.swf**, **.jpg**, **.jpeg**, **.bmp**, or **.png**.

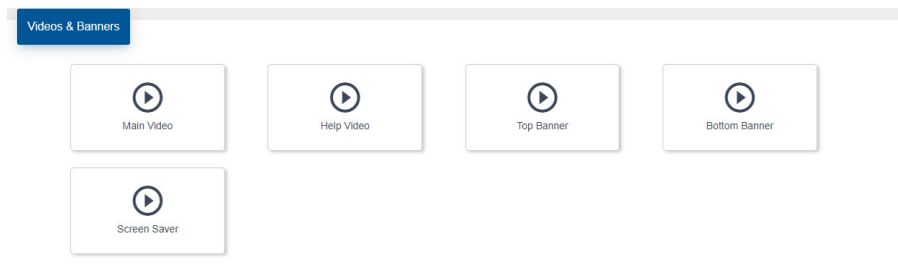


A. Top Banner B. Main Video C. Help Video D. Bottom Banner E. Screen Saver

Figure 78. Touch Screen Videos and Banners

Table 1: Banner Dimensions

Banner	Banner Dimensions in Pixels (Width x Height)	
	15" Touch Screen Models	22" Touch Screen Models
A. Top Banner	1024 x 100	1080 x 100
B. Main Video	238 x 230	250 x 227
C. Help Video	238 x 230	250 x 227
D. Bottom Banner	911 x 230	960 x 374
E. Screen Saver	1024 x 768	1080 x 1920


Figure 79. Touch Screen Videos and Banners

Configure the Main Video, Help Video, Top Banner, Bottom Banner and Screen Saver as described in the following sections.

4.4.1 Set the Main Video

1. Select **Main Video**. The Media Selection window appears.

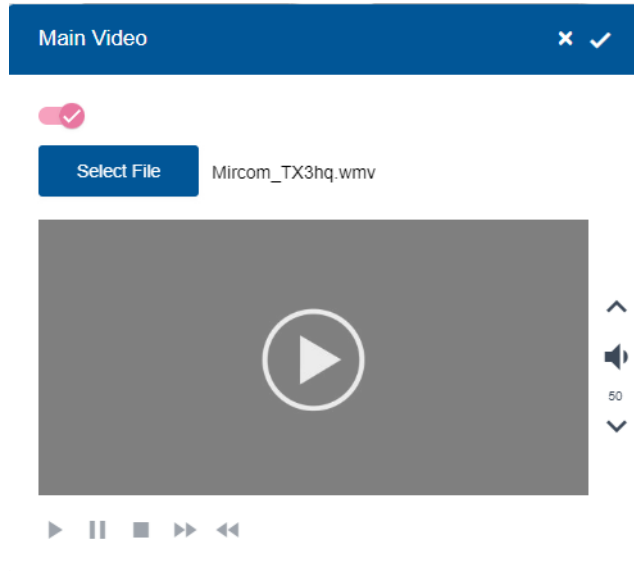


Figure 80. Touch Screen Main Video

Disable. To disable the main video click the check mark. The check mark changes to a minus sign when the main video is disabled.

Select File. Press **Select File** to select a media file from a directory.

2. To adjust the volume use the volume control buttons to the right of the media preview window.

4.4.2 Set the Help Video

1. Select **Help Video**. The Media Selection window appears.

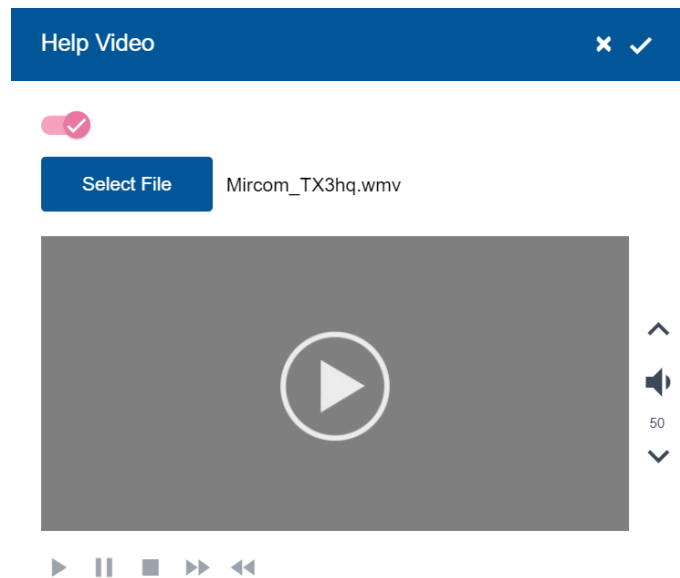


Figure 81. Touch Screen Help Video

Disable. To disable the help video click the check mark. The check mark changes to a minus sign when the help video is disabled.

Select File. Click **Select File** to select a media file from a directory.

2. To adjust the volume use the volume control buttons to the right of the media preview window.

4.4.3 Set the Top Banner

1. Select **Top Banner**. The Media Selection window appears.

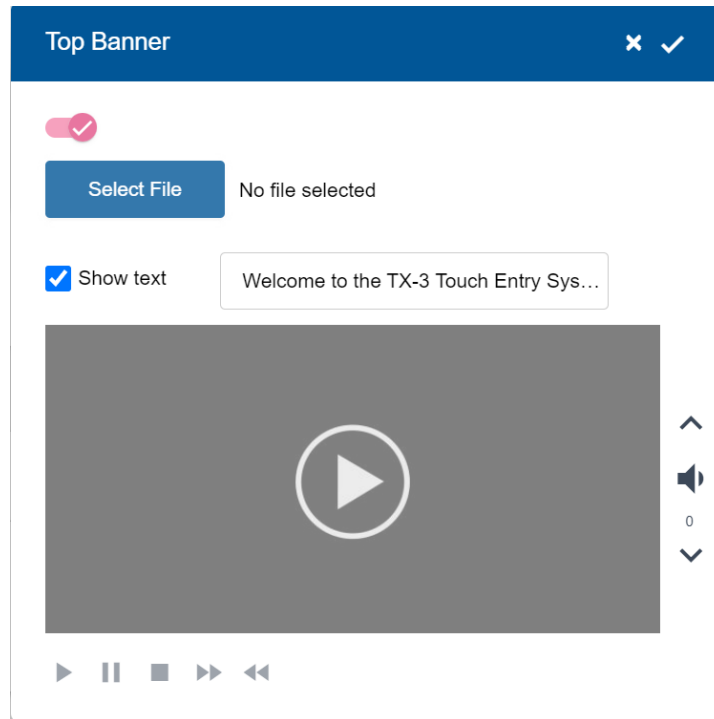


Figure 82. Touch Screen Top Banner

Disable. To disable the top banner click the check mark. The check mark changes to a minus sign when the top banner is disabled.

Select File. Press **Select File** to select a media file from a directory.

Show Text. To display customized text select this option and enter the desired text into the text field on the right. When this option is selected only text appearing in the text field will be displayed and any previously selected media files will not be displayed in the top banner. The text format can be edited as described in section 4.3.

4.4.4 Set the Bottom Banner

1. Select **Bottom Banner**. The Media Selection window appears.

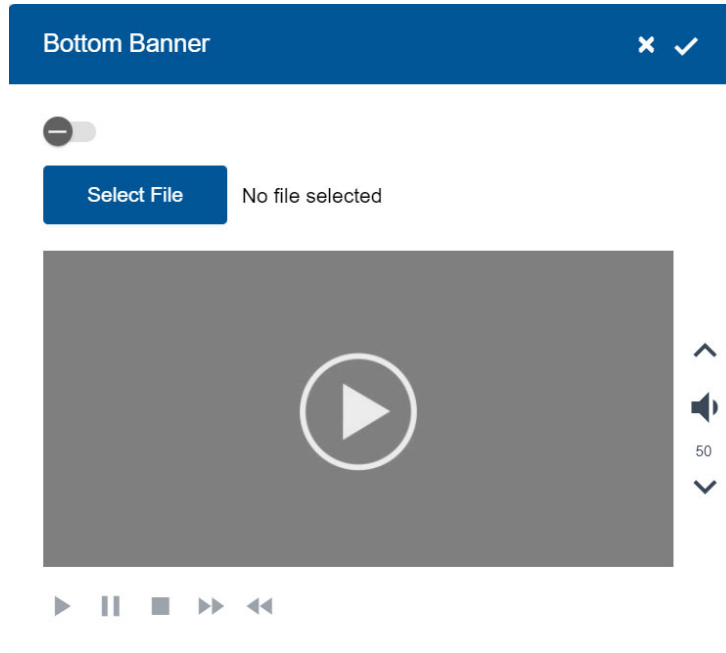


Figure 83. Touch Screen Bottom Banner

Disable. To disable the bottom banner click the check mark. The check mark changes to a minus sign when the bottom banner is disabled.

Select File. Click **Select File** to select a media file from a directory.

4.4.5 Set the Screen Saver

1. Select **Screen Saver**. The Media Selection window appears.

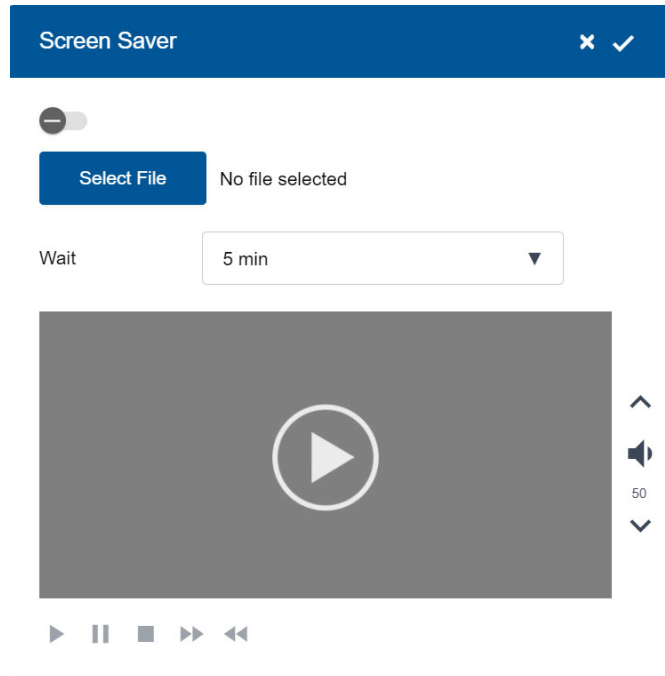


Figure 84. Screen Saver Options

Disable. To disable the screen saver click the check mark. The check mark changes to a minus sign when the screen saver is disabled.

Select File. Press **Select File** to select a media file from a directory.

Wait. Specify the amount of time before the screen saver begins playing.

2. To adjust the volume use the volume control buttons to the right of the media preview window.

4.5 Advertising

Note: In order to enable the advertising module, you must log into the Touch Screen terminal (see LT-995). To configure the advertising module, use MiVision.

The advertising module is an optional addition to the TX3 Touch. It allows advertisements in the form of videos, images or animations to be displayed on the touch screen. Advertising media can play on the Main Video display, the Bottom Banner display and as a Screen Saver over the entire display.

The advertising module allows property managers to recoup the costs of their telephone entry and card access security system by selling advertising time on their Touch Screens in high traffic lobbies and entrance ways.

4.5.1 Add an Advertisement

1. Click either **Main Video**, **Bottom Banner**, or **Screen Saver**.

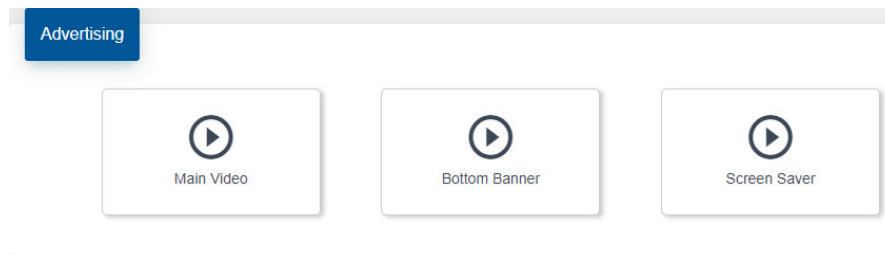


Figure 85. Advertising


2. In the list of media files that appears, click the **Add** button  to add a video.



Figure 86. Media Files

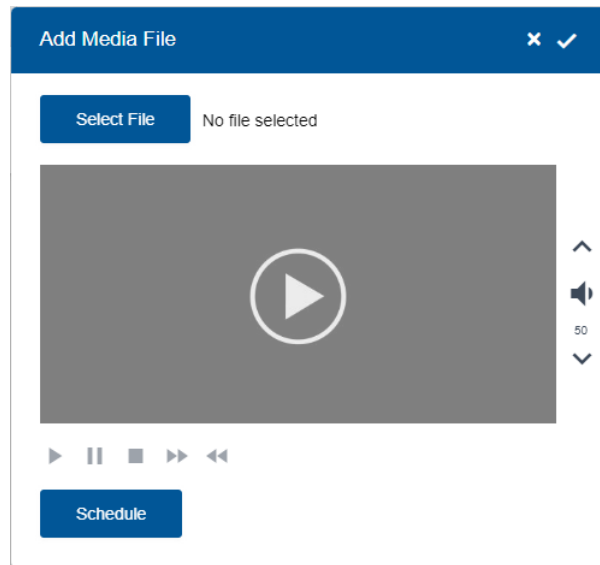


Figure 87. Add Media File

3. Click **Select File** to select a media file from the directory.

Note: In addition to the other file formats, audio file formats **.wav** and **.mp3** are enabled for screensaver media file selection.

Note: If the dimensions for your image or flash file are not the same as the dimensions for the Main Video banner, the Bottom Banner or the Screen Saver, there may be some distortion when the image or flash file are displayed. See Table 1 for the dimensions of these areas.

4. To adjust the volume use the volume control buttons to the right of the preview file window.

5. Click **Schedule**.

Media File Play Schedule

Scheme
All

Start Date
3/6/2024
End Date
3/6/2025

Preview


Time	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
12:00 AM	✓	✓	✓	✓	✓	✓	✓
03:00 AM	✓	✓	✓	✓	✓	✓	✓
06:00 AM	✓	✓	✓	✓	✓	✓	✓
09:00 AM	✓	✓	✓	✓	✓	✓	✓
12:00 PM	✓	✓	✓	✓	✓	✓	✓
03:00 PM	✓	✓	✓	✓	✓	✓	✓
06:00 PM	✓	✓	✓	✓	✓	✓	✓
09:00 PM	✓	✓	✓	✓	✓	✓	✓

Figure 88. Media File Play Schedule

- The schedule for the advertisement can be set to one of several preset times by using the **Scheme** drop down menu. The **Start Date** and **End Date** indicate when the advertisement will be added to and removed from the schedule rotation. Select the corresponding drop down menus to set them. The default setting will keep the file in the rotation for 5 years.
- Click the checkbox ☒ to save the schedule, then click the checkbox ☒ in the **Add Media File** window to save video, then click the checkbox ☒ in the **Media Files** list.

4.5.2 Edit an Advertisement

Editing video file entries allows changes and updates to existing entries without having to create new entries. All the settings selected for the initial addition of the media file are saved including the associated scheduling settings. This is useful for quickly replacing an old advertisement with an updated version.

- In the **Media Files** list, click the arrow  to the right of the video you want to edit.

The **Edit Media File** window appears.

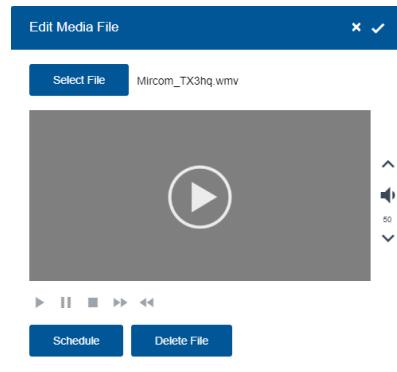



Figure 89. Edit Media File

2. Click **Select File** to replace the current media file with another file from the directory.
3. To adjust the volume use the volume control buttons to the right of the preview file window.
4. Click **Schedule** to change the schedule for the media. See step 5 on page 80.
5. Click the checkbox ☒ to save the schedule, then click the checkbox ☒ in the **Add Media File** window to save video, then click the checkbox ☒ in the **Media Files** list.

4.5.3 Delete an Advertisement

1. To remove a media file from the video file rotation, click the arrow  to the right of the media file, then click **Delete File**.

4.6 Directory Groups

You may configure residents into specific groups by their dial codes using designated text and logos. This feature allows visitors to easily make a selection using the Group Buttons at the top of the user interface. Up to five groups may be created.

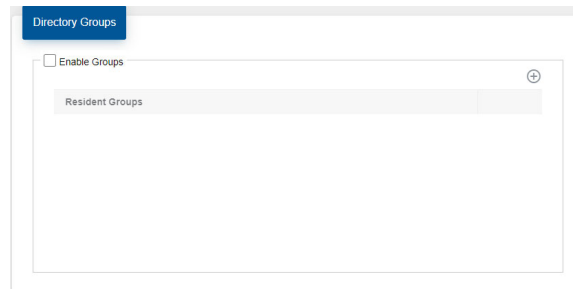



Figure 90. Directory Groups

1. Select **Enable Groups**.
2. Click the add  button to create a new group.

Group Details
✕ ✓


Group Name


Dial Code Range Start


Dial Code Range End

☒
Set as default group

Button Mode


 Text Only


 Logo Only

 **Mircom**
 Logo & Text

Group Logo

Select

No file selected

Figure 91. Group Details

Group name. Provide a group name.

Dial Code Range Start. Enter the start value for the group dial code.

Dial Code Range End. Enter the end value for the group dial code.

Set as default group. The default group is the group that is displayed by default on the Touch Screen.

Text Only. Select to display only the Group Name.

Logo Only. Select to display only the Logo.

Logo and Text. Select to display both the Logo and Text.

Group Logo. Select a logo for the group from a file.

4.7 More Options

More Options lets you specify more specific screen characteristics such as screen contrast, volume and other various user options.

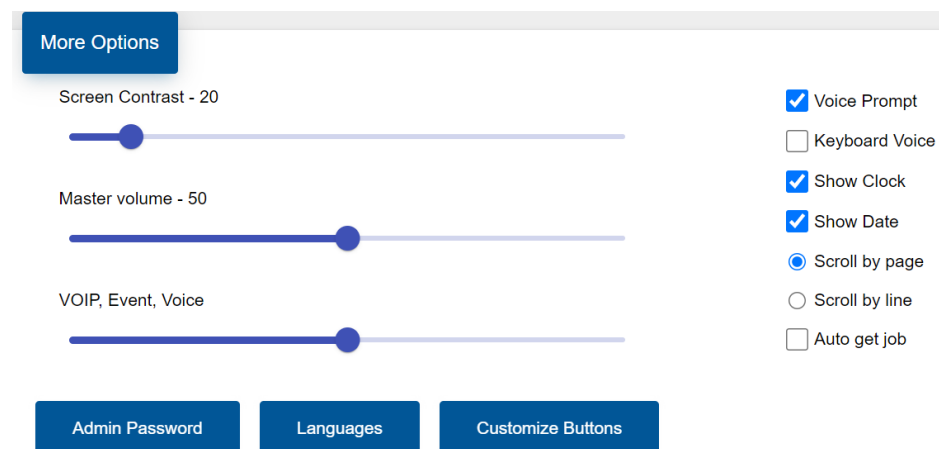


Figure 92. Touch Screen More Options

Screen Contrast. Defines the brightness ratio of the lightest to the darkest part of the Touch Screen interface.

Master Volume. Defines the volume of the speakers for videos, event prompts, and VOIP calls.

VOIP, Event, Voice. Defines the volume of all notifications and VOIP calls as a percentage of the master volume. Select the play button to preview the volume level.

Note: If the Touch Screen has telephone entry controller board model MD-1086, use these two volume controls only for notifications and VOIP calls (not telephone calls). Telephone call volume is controlled from **Panel Configuration** (section 3.1.2).

If the Touch Screen has telephone entry controller board model MD-1245, use these two volume controls for notifications, VOIP calls, and telephone calls.

Voice prompt. Enables voice prompting for every selection.

Keyboard voice. Enables the audible keystrokes.

Show clock. Enables the clock display.

Show date. Enables date display.

Scroll by page. Enables page scrolling.

Scroll by line. Enables line scrolling.

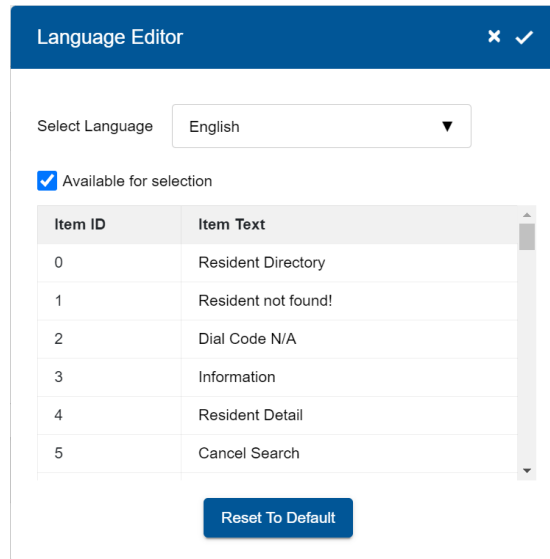
Auto Get Job. This option applies to Touch Screens that are either Secondary Nodes or nodes on an RS-485 network and ensures that the Touch Screen database is up-to-date. When you select this option, the Touch Screen monitors its internal lobby board for any changes. When a change is made to the internal lobby board database, the Touch Screen automatically updates its own database. This option can only be enabled at the Touch Screen unit or by connecting to the Touch Screen by Remote Desktop (see LT-995).

4.7.1 Admin Password

The value stored in **Admin Password** is used by MiVision to connect to a Touch Screen main node. This value must match the Touch Screen administrator password. Specifically, whenever you change the administrator password on a Touch Screen main node (see LT-995), you must make the same change to **Admin Password** for that Touch Screen main node in MiVision.

4.7.2 Languages

1. On the **More Options** tab, click **Languages**. The Language Editor window appears.



Item ID	Item Text
0	Resident Directory
1	Resident not found!
2	Dial Code N/A
3	Information
4	Resident Detail
5	Cancel Search

Figure 93. Language Editor

2. Select the language to edit using the menu.
3. Once a language has been chosen it can be set as **Available for selection** using the check box. At least one language must always be set as **Available for selection** and by default this is English. If more than one language is set as **Available for selection** an option appears on the main Touch Screen display to choose between languages.
4. Click a message to edit it.

Note: If you erase the message, then the associated element on the user interface screen is hidden.

5. Click **Reset to default** to restore all messages to their original content.



Figure 94. Language Selection

If multiple languages are enabled, the main Touch Screen display will have a button to select between languages. This will replace the clock as shown in Figure 94. Press the language button and buttons appear for each language enabled then press the button corresponding to the language you wish to select.

Note: With multiple languages enabled the Touch Screen will prompt for a language choice each time the screen saver clears.

4.7.3 Customize Buttons

The functions of the **Call Reception** and **Leave Message** buttons on the Touch Screen main interface are customizable. By default, the **Call Reception** button calls the guard phone. By default, the **Leave Message** button opens a window where the visitor can enter a message that is sent to the resident if email messages are configured (See LT-995 TX3 System Configuration and Administration Manual).

You can configure these buttons to call a specific dial code instead.

Note: To change the text on these buttons, see section 4.7.2.

1. In the **More Options** section, click **Customize Buttons**.

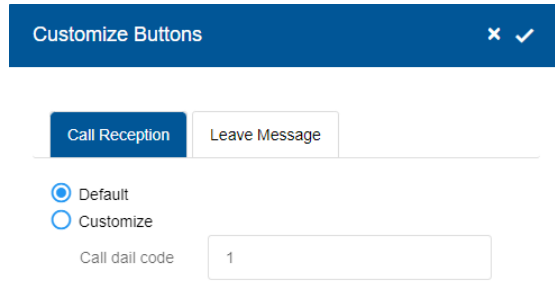


Figure 95. Customize Buttons

2. On the **Call Reception** tab, click **Customize**, then enter the dial code to call when a visitor presses the **Call Reception** button.

Click **Default** to set the **Call Reception** button to call the guard phone.

3. Click the **Leave Message** tab, then click **Customize**, then enter the dial code to call when a visitor presses the **Leave Message** button.

Click **Default** to set the **Leave Message** button to leave an email message. Email messages are configured on the Touch Screen itself. See LT-995 TX3 System Configuration and Administration Manual.

4. Click **OK**.

5

Card Access System Panel Configuration

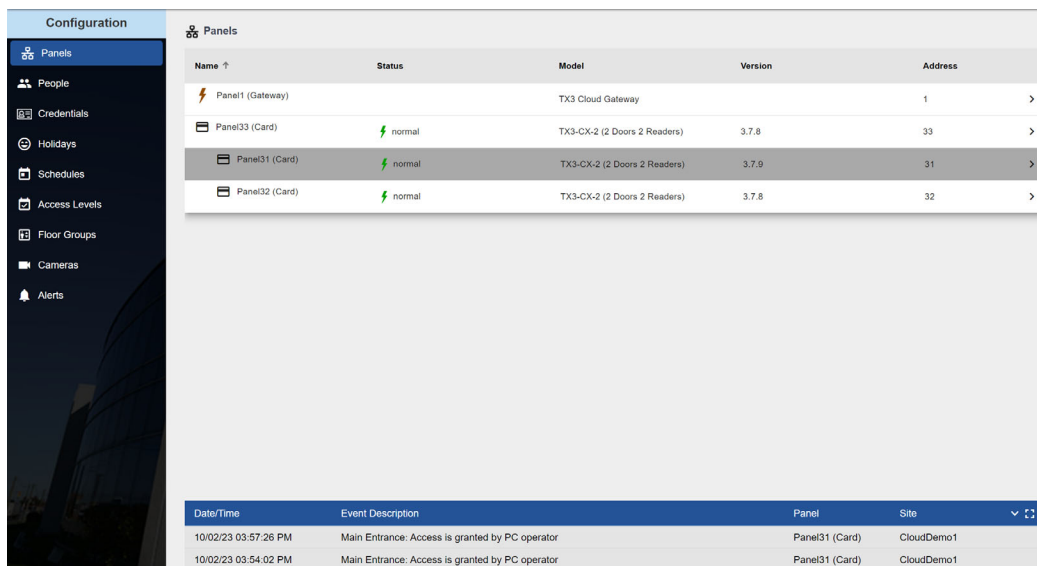
MiVision lets you access, add and modify two door controller and single door controller card access system panels.

Note: After you configure the site for the first time, and after any time you make changes, you must send the job. See section 1.10.

5.1 Configure a Panel

1. Click the **Options** menu, then click **Configuration**.
2. Click **Panels** in the left pane.


The Panels window appears.



Name	Status	Model	Version	Address
Panel1 (Gateway)		TX3 Cloud Gateway		1
Panel33 (Card)	normal	TX3-CX-2 (2 Doors 2 Readers)	3.7.8	33
Panel31 (Card)	normal	TX3-CX-2 (2 Doors 2 Readers)	3.7.9	31
Panel32 (Card)	normal	TX3-CX-2 (2 Doors 2 Readers)	3.7.8	32

Date/Time	Event Description	Panel	Site
10/02/23 03:57:26 PM	Main Entrance: Access is granted by PC operator	Panel31 (Card)	CloudDemo1
10/02/23 03:54:02 PM	Main Entrance: Access is granted by PC operator	Panel31 (Card)	CloudDemo1

Figure 96. Panels

3. Click the arrow  on the right to see details of the panel.

The Panels Configuration screen appears. It is divided into several sections. To see a specific section, click the section in the left pane.

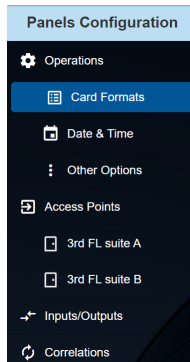


Figure 97. Card Access Configuration left pane

5.2 Operations

5.2.1 Operations - General

Panel label. Provide a name for the panel.

The other fields in this section are read-only. To edit them see section 1.5.5.

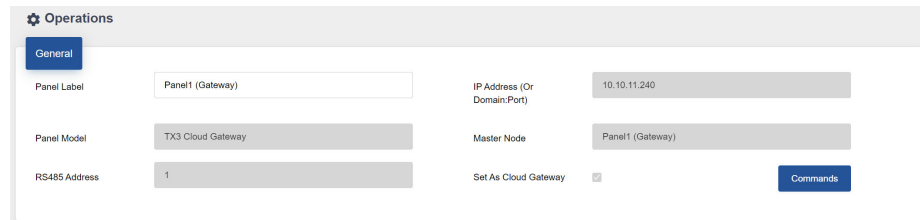


Figure 98. Panel Configuration - General

5.2.2 Operations - Card Formats

Card formats. Select the card reader format for each access point. Select only the formats that are being used. In addition, do not select more than one format with the same bit length. For example, select either 36-bit HID Simplex or 36-bit Keyscan, but do not select both.

Card discovery mode. Enable this option, then send the Job to the panel to put the panel into card discovery mode. While the panel is in card discovery mode and you present a card to the reader, the panel will display the card's raw data in the Online Events pane. To disable the feature, uncheck Card discovery mode, then send the job to the panel again.

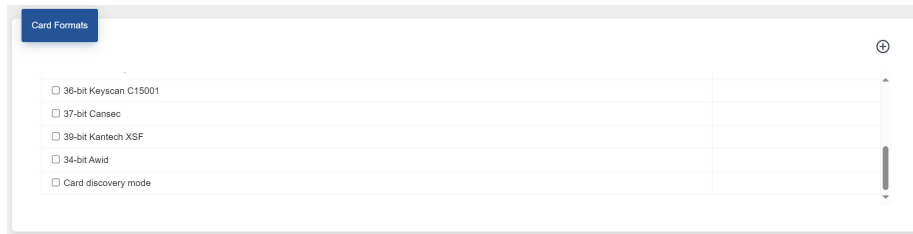


Figure 99. Panel Configuration - Card Formats

5.2.3 Operations - Date and Time

Enable Daylight Savings Time. Select this check box to enable daylight saving time. When enabled provide the daylight savings start and end time for the local area.

Adjust panel time for. Provide a value to compensate for the daily drift away from the true time.

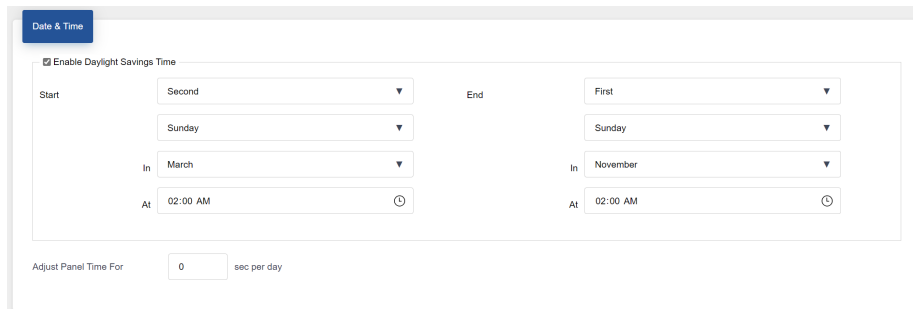


Figure 100. Panel Configuration - Date and Time

5.2.4 Operations - Other Options

Report real time events to PC. Enable or disable real time event sending to MiVision. If enabled, only the real time logs are sent to MiVision.

Facility code. Enter the building's facility code with a value from 0 to 2147483647. Enabling the facility code mode lets you grant access to cards based on facility code.

Interlock. If enabled door B cannot be unlocked until door A is locked and closed. Door A cannot be unlocked until door B is locked and closed.

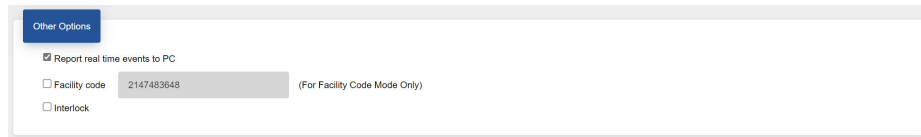


Figure 101. Panel Configuration - Other Options

5.3 Access Points

1. Click an **Access Point** in the left pane.

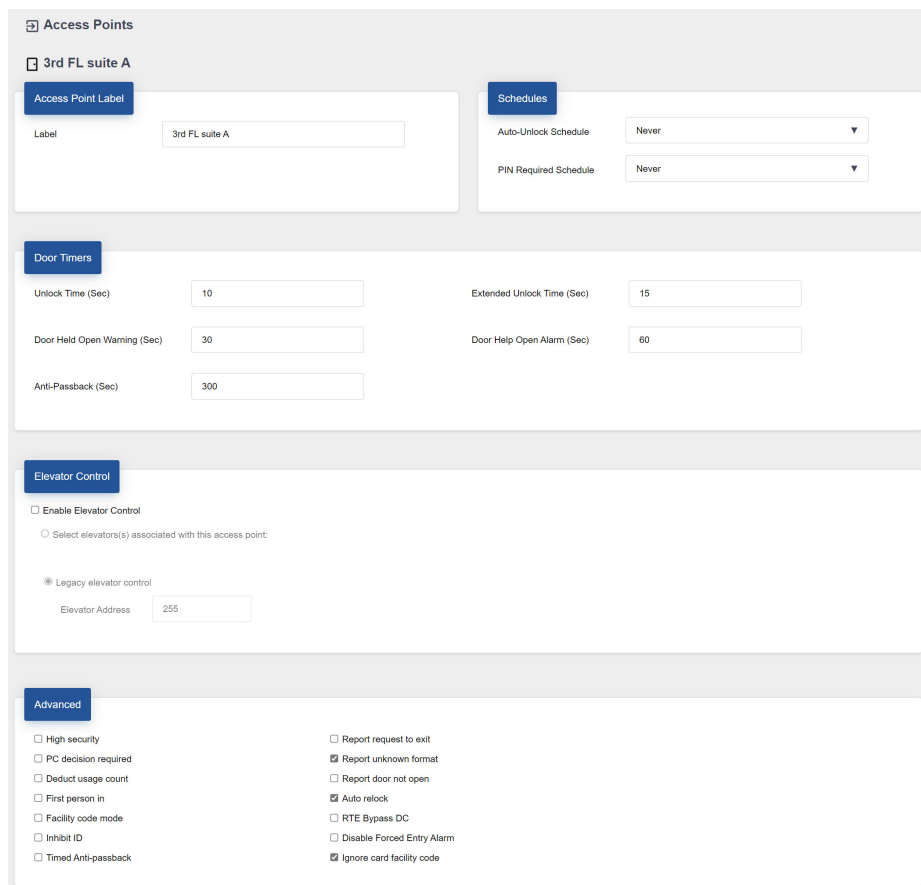


Figure 102. Access Points

2. In the **Access point label** provide a name for the access point.
3. Provide information for each the following:

Auto-unlock schedule. The auto-unlock schedule lets you specify when the door will be unlocked. From the list select an auto-unlock schedule.

PIN required schedule. If a card is assigned a PIN, this schedule lets you specify when to grant access to a card with a PIN. From the list select the schedule.

Unlock time. Specify the amount of time the door remains unlocked after granting access.

Extended unlock time. Specify the amount of time the door remains unlocked for a card assigned with the extended unlock time privilege.

Door held open warning. Specify the amount of time for the door to stay open until a warning is issued.

Door held open alarm. Specify the amount of time for the door to stay open until an alarm is issued.

Anti-passback. Specify the time period in which the same card cannot be used twice at this reader.

Elevator Control. Select **Enable Elevator Control** to let this access point control the elevators, then select the elevator restriction units that this access point controls.

High security. Selecting **High security** grants access only to cards assigned with the high security privilege.

PC decision required. When enabled the PC decision to grant access is transferred from the controller to the PC with an attendant. For this option to work the PC needs to be on all the time. Use this option when the building has a security desk or a concierge.

Deduct usage count. Selecting this option enables a counter to deduct by one every time a card is used at this access point. When it reaches zero, the card is deactivated.

First person in. When enabled the door becomes unlocked by the first valid card presented during the unlock schedule, causing the door to remain unlocked for the duration of the unlock schedule. The 'First person in' option must also be set on the card.

Facility code mode. Enabling the Facility code mode grants access to cards based on only their facility code. Card holders with the same facility code are granted access, regardless of their card numbers.

Note: If you are enabling the facility code mode ensure that the facility code is set on the panel.

Inhibit ID. When enabled the card code is not sent to the PC. This feature prevents the logging and reporting of cards at this access point.

Timed anti-passback. Selecting this option enables the anti-passback feature in which the same card cannot be used twice at the same reader until the anti-pass back time period expires.

Report request to exit. Selecting this option enables the panel to report 'request to exit events' to the PC.

Report unknown format. Selecting this option enables the panel to report 'unknown card format' events to the PC.

Report door not open. Selecting this option enables the panel to log and report 'door not open' events to the PC when access is granted but the door remains closed.

Auto relock. Selecting this option locks the door as soon as the door closes before the door open timer or extended door timer expire. Disabling this option locks the door, but only after the expiration of door open timer or extended door open timer.

RTE bypass DC. Enable this option if there is a mechanical egress device installed on the door. In this situation, the door is unlocked manually, and the TX3 system does not unlock the door. If the door is opened, the system updates the door status and the LED on the reader turns green. The door contact is bypassed and so there is no forced entry alarm.

Disable forced entry alarm. Selecting this option disables the forced entry alarm.

Ignore card facility code. Selecting this option grants access to card holders on the basis of their card numbers and not the card facility code.

5.4 Inputs

1. Click **Inputs/Outputs** in the left pane.

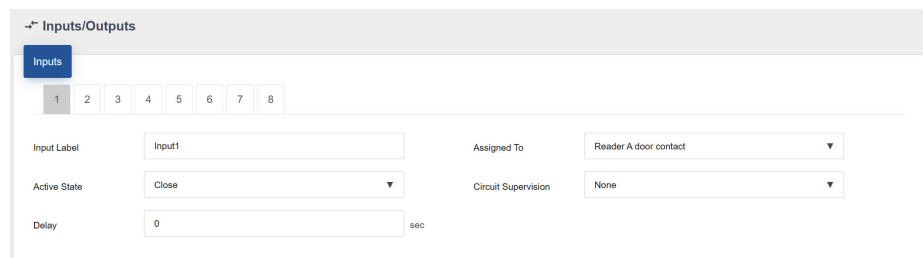


Figure 103. Inputs/Outputs

Each two door controller has eight inputs that can be configured to accommodate specific events for the following controller functions:

Door contact for reader A or B. An input assigned this function senses if a door is opened or closed.

Request to exit for reader A or B. An input assigned this function sends a signal to the controller that a request to exit has been made.

General purpose function. An input assigned this function can activate a general purpose output to perform any required function or turn on or off the high security mode.

General door status. An input assigned this function monitors a door for open or closed status. This door appears in the Access Point Status.

Each single door controller has 4 programmable inputs that can be configured to accommodate specific events for the following controller functions:

Door contact. An input assigned this function senses if a door is opened or closed.

Request to exit. An input assigned this function sends a signal to the controller that a request to exit has been made.

General purpose. An input assigned this function activates a general purpose output to perform any required function or turn on or off the high security mode.

General door status. An input assigned this function monitors a door for open or closed status. This door appears in the Access Point Status.

2. Click an input number to configure that input.

Input Label. Use this text box to provide a name for the input.

Assigned to. Select an input from the menu. Select **General door status** to make the input monitor a door for open or closed status. This door appears in the Access Point Status.

Active state. This option specifies the state by which it is considered active. Two selections are presented. Select one of the following:

Open

Close

Circuit supervision. This option specifies the circuit type and indicates whether the input is supervised. Select one of the following:

None

Open circuit

Short circuit

Open and short circuit

Delay. MiVision shows the panel as being in an alarm state when the input becomes active. The delay specifies the amount of time to wait before raising the alarm condition.

5.5 Outputs

By default output 1 is assigned to Reader A lock with an energized active state. When access is granted this output unlocks the main door.

Whenever you configure an output, the active state of the output must be defined as a function of the device it attaches. When the device is energized it is considered to be active. When the device is de-energized it is considered to be inactive.

The outputs can be configured to accommodate specific actions for the following controller functions:

Lock for reader A or B. This output is assigned to either reader A or B to unlock the main door. When access is granted at the designated reader, this output unlocks the door.

Handicap lock for reader A or B. This output is assigned to either reader A or B to unlock the accessible door. When access is granted at the designated reader, this output unlocks the door. Access is granted to cards with designated handicap privileges.

General purpose output. An output assigned this function can perform any required function, such as turning on a light.

Outputs 1 to 8 have the following default settings:

- **Output 1.** Lock for reader A
- **Output 2.** Reader A handicap
- **Output 3.** General Purpose
- **Output 4.** General Purpose
- **Output 5.** Lock for reader B
- **Output 6.** Reader B handicap
- **Output 7.** General Purpose
- **Output 8.** General Purpose

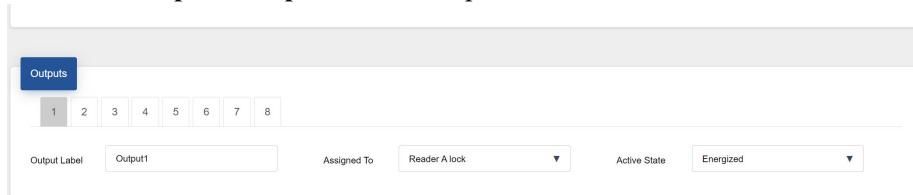
On a single door controller, outputs 1, 2 and 3 are configured as follows:

Output 1: Lock. Connect this output to a door strike. By default output 1 has an energized active state. When access is granted, this output unlocks the door.

Output 2: General purpose. An output assigned this function can perform any required function, such as turning on a light.

Output 3: General purpose. This output can power a door strike or a maglock.

1. Click **Inputs/Outputs** in the left pane.



Output Label	Assigned To	Active State
Output1	Reader A lock	Energized

Figure 104. Outputs

Label. Use this text box to provide a label name for this panel output.

Assigned to. Select a function from the menu.

Reader A lock

Reader B lock

Reader A handicap

Reader B handicap

General Purpose

Note: On a single door controller, for output 3, select **Lock** if you want output 3 to power a door strike or a maglock.

Active state. This option specifies the state by which it is considered active. Two selections are presented. Select one of the following:

Energized. When the device is energized it is considered to be active.

De-energized. When the device is de-energized it is considered to be active.

Note: On a single door controller, for output 3, select **Energized** for a door strike or **De-energized** for a maglock.

5.6 Correlations

Correlations let you establish specific relationships between panel inputs (events) and outputs (actions). Use Correlations to specify the relationships between events, actions and schedules.



Note: All inputs, outputs and schedules must be defined before applying correlations.

5.6.1 Add or Edit a correlation

1. Click **Correlations** in the left pane.



Figure 105. Correlations

2. Click the **Add** button  add a correlation, or click on the Edit button  next to a correlation to edit it.

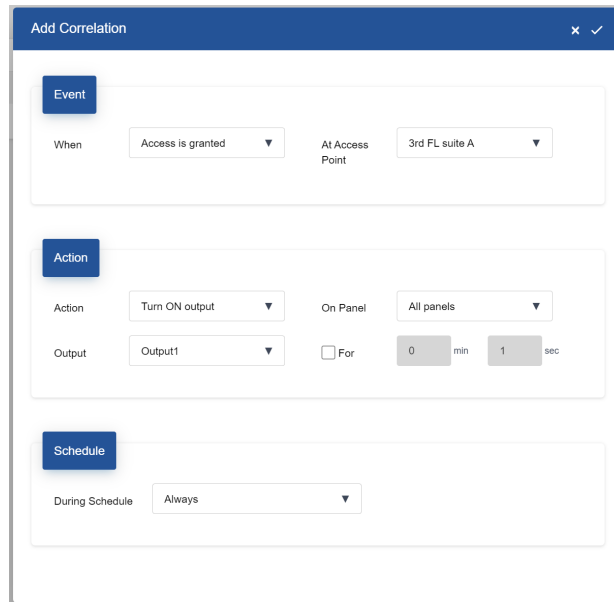


Figure 106. Add/Edit a Correlation

3. Enter the following parameters:

When. This parameter defines the input event. Select one of the following (the parameters available depend on the kind of panel):

Access is granted. Access is granted.

Access is denied. Access is denied.

Forced entry alarm. A door is forced open.

Forced entry alarm restored. The forced entry alarm is restored.

Door held open alarm. A door did not close and the door held open alarm was issued.

Door held open alarm restored. The door held open alarm is restored.

Door held open warning. A door did not close and the door held open warning was issued.

Door held open warning restored. The door held open warning was restored.

Door not open. Access granted but the door remains closed.

Request to Exit. A request to exit has been made.

Input is active. Select a panel input.

Input is normal. The general purpose input becomes inactive.

Unlock mode is on. When in unlock mode the door is unlocked.

Unlock mode is off. When in lock mode the door is locked.

High security is on. When enabled only access cards with this privilege are able to open the door.

High security is off. When disabled all access cards are able to open the door.

Tamper detected. (single door controller) The tamper alarm is on.

Tamper restored. (single door controller) The tamper alarm is off.

Call Started. A call to a resident is placed from the lobby.

Call finished. A call to a resident ends.

Call is connected. A call is established.

Access is granted. (lobby and Touch Screen) Resident grants access using their telephone keypad.

Access is denied. (lobby and Touch Screen) Resident denies access.

At access point/Input label. This parameter defines the access point or input.

Action. This option specifies the type of action to occur for a specific input. Select one of the following:

Turn ON output. When enabled the output assigned a specific function performs the required action.

Turn OFF output. When disabled the output assigned this specific function does not perform the designated action.

Turn ON high security. When enabled only access cards with this privilege are able to open the door.

Turn OFF high security. When disabled all access cards are able to open the door.

On panel. This option applies the action either to one of the panels on your system or to a group of panels on your system. If, for example, you have two panels (Panel 1 and Panel 2) in your TX3 system, you could select from the following options:

Panel 1. Apply the correlation to Panel 1 only.

Panel 2. Apply the correlation to Panel 2 only.

All. Apply the correlation to all telephone entry, card access, and Touch Screen panels on the network.

Custom. Apply the correlation to a custom target. This option is only available for TCP/IP network connections. When you select this option, you can click on the **Custom** button to select from the following custom targets:

- **Nano IP Address.** Apply the correlation to a TX3 Nano. This option is only available for TCP/IP network connections.
- **All panels on the RS485 network of the Master Node.** (select a main node from the list)
- **All Master Nodes Only.**



- **All Panels With RS485 Address.** (select the address from the list)

Note: Correlation signals are not transmitted by Touch Screen main nodes by default. If you plan on using the **All** or **Custom** correlation options, select the **Route IP Address** checkbox on one of the Touch Screen main nodes.

Output. This parameter applies the action to a specific output or access point on the panel. For an output to appear on this list it must be designated as a general purpose output. For a reader to appear on this list the output must be assigned to a reader.


For. This option represents the duration of the action in minutes and seconds up to a maximum of 600 minutes. Uncheck the box if you want the action to continue indefinitely.

During schedule. This parameter lets you apply this correlation to a pre-defined schedule.

Click the **Done** button  in the upper right corner to save your changes, or **Cancel** button  next to it to cancel changes.

5.6.2

Remove a correlation

1. Click the **Remove** button  next to the correlation you want to remove.
2. Click **YES**.

Delete

Are you sure you want to delete this correlation?

YES NO

Figure 107. Remove Correlation

6

Elevator Restriction Panel Configuration

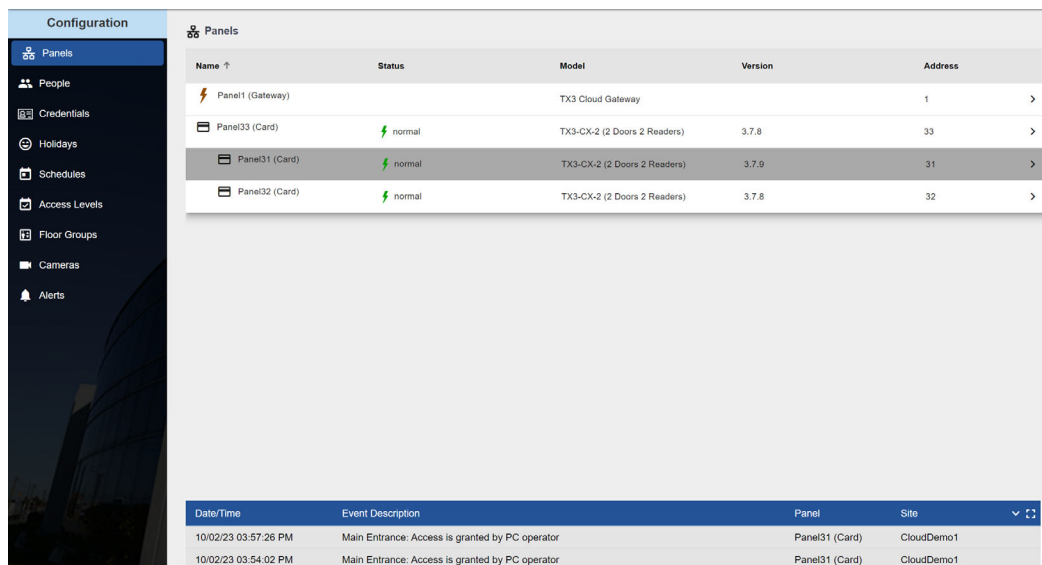
This chapter describes how to set up card access and residents with elevator restriction in MiVision.

Note: After you configure the site for the first time, and after any time you make changes, you must send the job. See section 1.10.

6.1 Add an Elevator Restriction Unit

1. Click the **Options** menu, then click **Configuration**.
2. Click **Panels** in the left pane.



The Panels window appears.



Name ↑	Status	Model	Version	Address
Panel1 (Gateway)		TX3 Cloud Gateway		1
Panel33 (Card)	normal	TX3-CX-2 (2 Doors 2 Readers)	3.7.8	33
Panel31 (Card)	normal	TX3-CX-2 (2 Doors 2 Readers)	3.7.9	31
Panel32 (Card)	normal	TX3-CX-2 (2 Doors 2 Readers)	3.7.8	32

Date/Time	Event Description	Panel	Site
10/02/23 03:57:26 PM	Main Entrance: Access is granted by PC operator	Panel31 (Card)	CloudDemo1
10/02/23 03:54:02 PM	Main Entrance: Access is granted by PC operator	Panel31 (Card)	CloudDemo1

Figure 108. Panels

3. Click the edit button  in the upper right, then click the add button .

The Add Panel window appears.

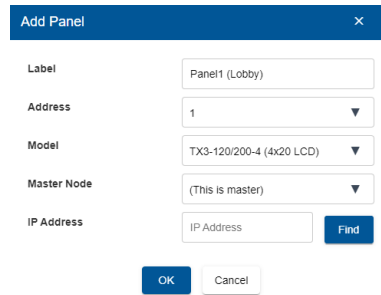


Figure 109. Add Panel

Label. Enter a name for the elevator restriction unit.

Address. Specify the RS-485 address of the elevator restriction unit.

Model.

ERU (Elevator Restriction Unit) for TX3-ER-8-A

ERU 2.0 (Elevator Restriction Unit) for TX3-ER-8-B

Master Node. Select **(This is a Master)** if the panel is a main node, otherwise select the panel's main node.

4. Click **OK**.
5. Repeat these steps for every elevator restriction unit in the job.

Note: You can add up to 6 TX3-ER-8-A Elevator Restriction Units (ERU) to a site, and up to 16 TX3-ER-8-B Elevator Restriction Units (ERU 2.0) to a site. The maximum number of Elevator Restriction Units in a site is 16.

6.2 Operations

6.2.1 Operations - General

Panel label. Provide a name for the panel.

The other fields in this section are read-only. To edit them see section 1.5.5.

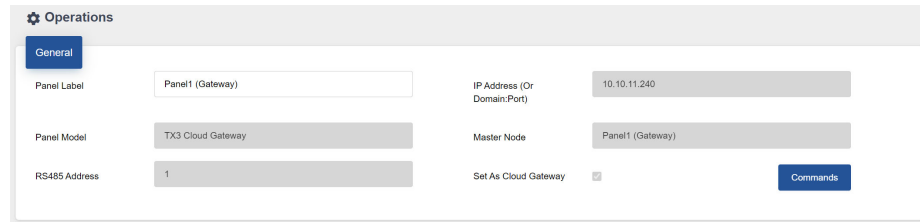


Figure 110. Panel Configuration - General

6.3 Configure Card Access with Elevator Restriction

Follow the steps below to configure card access with elevator restriction.

6.3.1 Configure an Access Point to Control an Elevator Restriction Unit

1. In the **Panels** window, select the card access panel that contains the access point that you want to control the elevator.
2. Click an **Access Point** in the left pane.

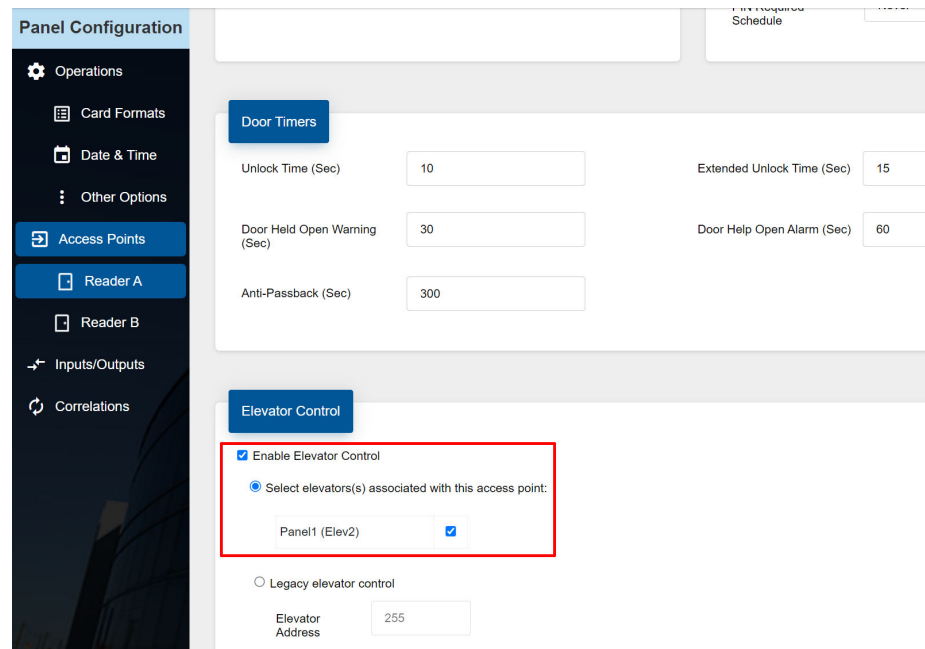


Figure 111. Access Points

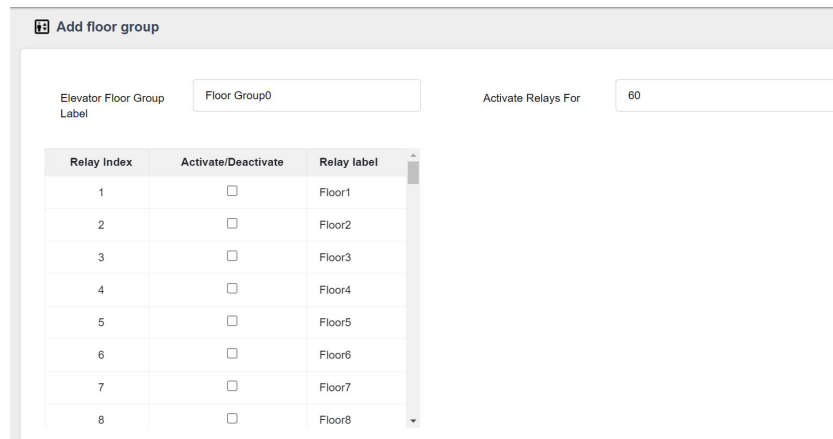
3. Select **Enable Elevator Control**, then select **Select elevator(s) associated with this access point**.
4. Select the elevator restriction units that this access point controls.

6.3.2 Create a Floor Group

Floor groups are groups of floors that are assigned to access levels.

1. Select **Floor Groups** in the Configuration pane.
2. Click the **Add** button .

The **Add floor group** window appears.



Relay Index	Activate/Deactivate	Relay label
1	<input type="checkbox"/>	Floor1
2	<input type="checkbox"/>	Floor2
3	<input type="checkbox"/>	Floor3
4	<input type="checkbox"/>	Floor4
5	<input type="checkbox"/>	Floor5
6	<input type="checkbox"/>	Floor6
7	<input type="checkbox"/>	Floor7
8	<input type="checkbox"/>	Floor8

Figure 112. Add floor group


3. Select the floors that you want in this floor group.

Note: With TX3-ER-8-A (ERU), a maximum of 24 relays can be assigned to a floor group. With TX3-ER-8-B (ERU 2.0), a maximum of 96 relays can be assigned to a floor group.

4. Provide the following information.

Activate relays for. Specify the amount of time that the ERU relays are active. This timer starts when the access point reads the card.

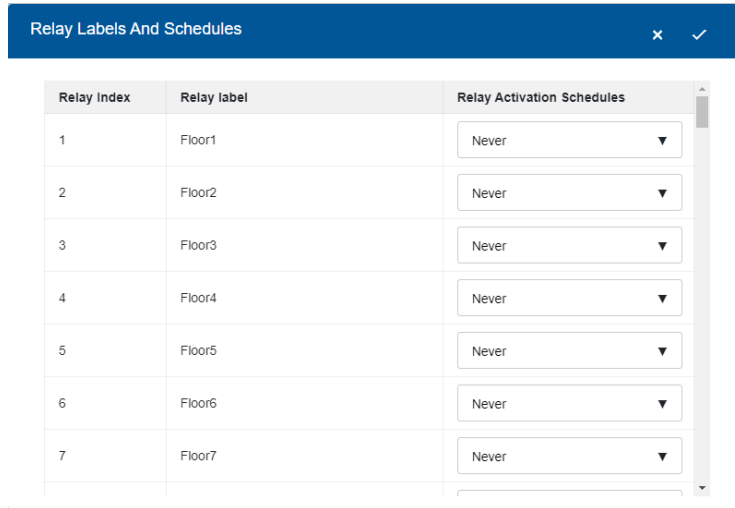
Note: The minimum is 5 seconds and the maximum is 600 seconds.

5. Click the checkbox ☒ to save the floor group, then click add button  to create another floor group.

6.3.3 Edit Relays and Schedules

1. Click **Floor Groups** in the Configuration pane.
2. Click **Relay Labels and Schedules**.

The Edit Relay Labels and Schedules window appears.



Relay Index	Relay label	Relay Activation Schedules
1	Floor1	Never
2	Floor2	Never
3	Floor3	Never
4	Floor4	Never
5	Floor5	Never
6	Floor6	Never
7	Floor7	Never

Figure 113. Edit Relay Labels and Schedules

Note: Relay labels are the same for all elevator restriction units in the job.

3. Under **Relay Activation Schedule**, select when this relay should be active. You can select **Always**, **Never**, or another user-defined schedule. See section 10 for instructions on creating schedules.

Note: Relay schedules work only with TX3-ER-8-B (ERU 2.0).

4. Click the **Done** button  in the upper right corner to save your changes, or **Cancel** button  next to it to cancel changes.

6.3.4 Create an Access Level


1. Click **Access Levels** in the Configuration pane.

The **Access Levels** screen appears.



Figure 114. Access Levels

Note: The Admin level includes all access points. This cannot be changed.

2. Click the **Add** button  in the upper right to add an access level.

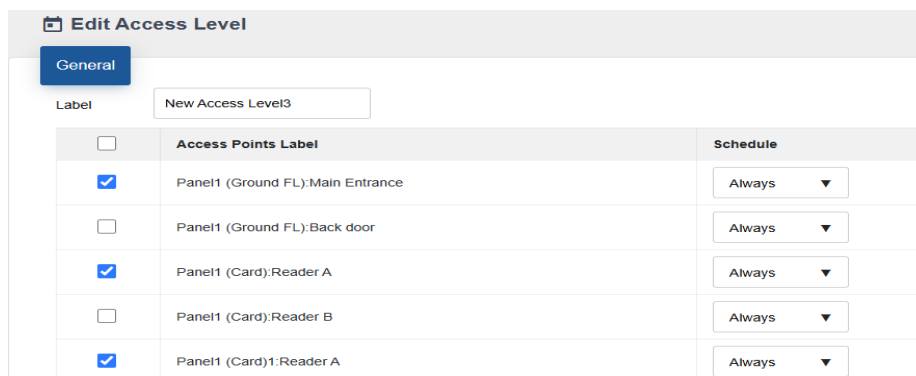


Figure 115. Add Access Level

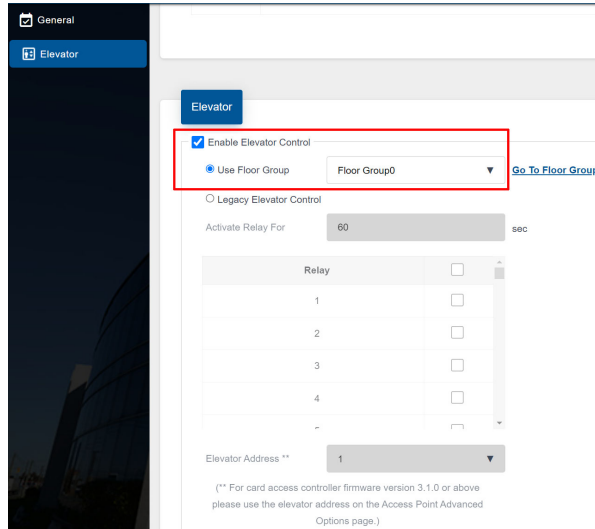
3. Supply the following information:

Label. Provide a name for this access level.

Access Points. Select the checkbox for an access point to enable or disable access. If an access point is unchecked, it will not allow access to credentials with this access level.

Schedule. From the schedule, list select when access is granted. You can select from **Always**, **Never** or any other user-defined schedule.

Elevator. Click **Enable Elevator Control** to enable elevator access control for this access level, then select **Use Floor Group** and select a floor group.



Elevator

☒ Enable Elevator Control

☒ Use Floor Group Floor Group0 ▼ [Go To Floor Group](#)

☐ Legacy Elevator Control



Activate Relay For 60 sec

Relay	
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
...	<input type="checkbox"/>


Elevator Address ** 1 ▼

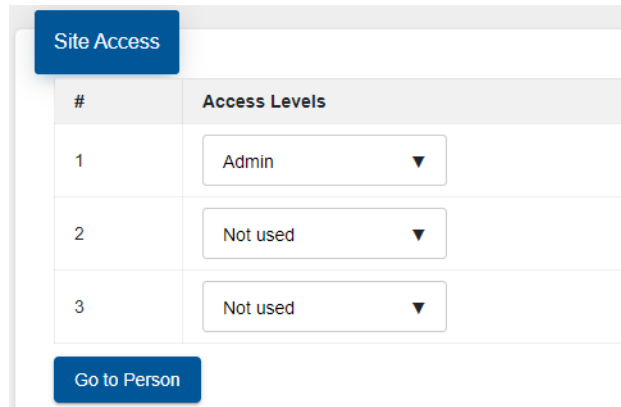
(** For card access controller firmware version 3.1.0 or above please use the elevator address on the Access Point Advanced Options page.)

Figure 116. Access Level - Elevator

Click the **Done** button  in the upper right corner to save your changes, or **Cancel** button  next to it to cancel changes.

6.3.5 Assign Credentials to the Access Level

1. Select **Credentials** in the Configuration pane.
2. Click the arrow to the right of an existing credential  to see its details.





#	Access Levels
1	Admin ▼
2	Not used ▼
3	Not used ▼

Go to Person

Figure 117. Credentials - Site Access

Note: You can edit multiple credentials at the same time by selecting the button to the left of the credential.

3. In the **Site Access** section, select up to three access levels for the card. Access privileges to designated areas are defined by the administrator.
4. Click the **Done** button  in the upper right corner to save your changes, or **Cancel** button  next to it to cancel changes.


6.4 Configure Residents with Elevator Restriction

The elevator restriction feature limits building accessibility by granting the visitor access only to the destination floor. This prevents the visitor from accessing non-designated floors.

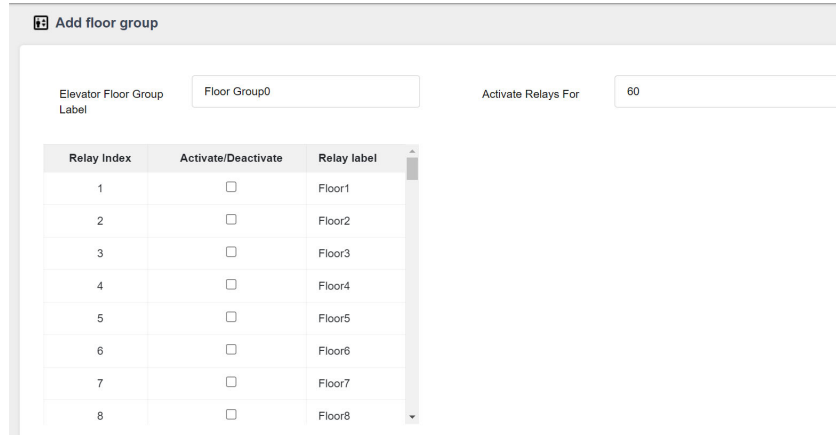
Follow the steps below to configure card access with elevator restriction.

6.4.1 Create a Floor Group

Floor groups are groups of floors that are assigned to access levels.

1. Select **Floor Groups** in the Configuration pane.
2. Click the **Add** button .

The **Add floor group** window appears.



Relay Index	Activate/Deactivate	Relay label
1	<input type="checkbox"/>	Floor1
2	<input type="checkbox"/>	Floor2
3	<input type="checkbox"/>	Floor3
4	<input type="checkbox"/>	Floor4
5	<input type="checkbox"/>	Floor5
6	<input type="checkbox"/>	Floor6
7	<input type="checkbox"/>	Floor7
8	<input type="checkbox"/>	Floor8

Figure 118. Add floor group



3. Select the floors that you want in this floor group.

Note: With TX3-ER-8-A (ERU), a maximum of 24 relays can be assigned to a floor group. With TX3-ER-8-B (ERU 2.0), a maximum of 96 relays can be assigned to a floor group.

4. Provide the following information.

Activate relays for. Specify the amount of time that the ERU relays are active. This timer starts when the access point reads the card.

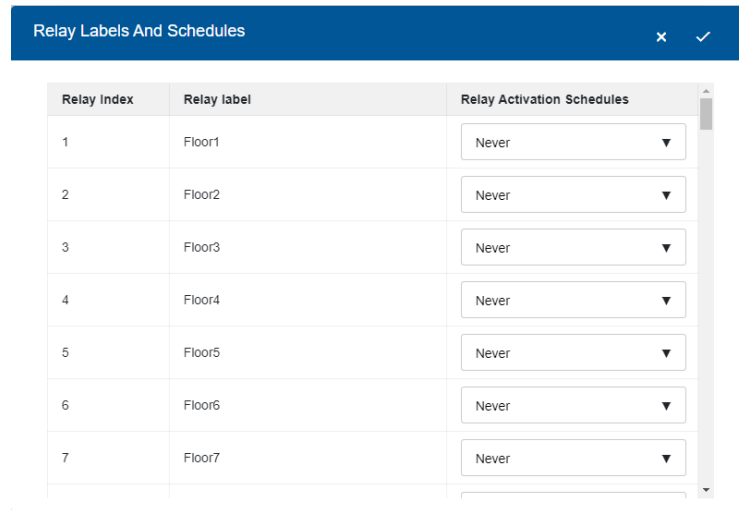
Note: The minimum is 5 seconds and the maximum is 600 seconds.

5. Click the checkbox  to save the floor group, then click add button  to create another floor group.

6.4.2 Edit Relays and Schedules

1. Click **Floor Groups** in the Configuration pane.
2. Click **Relay Labels and Schedules**.

The Relay Labels and Schedules window appears.



Relay Index	Relay label	Relay Activation Schedules
1	Floor1	Never
2	Floor2	Never
3	Floor3	Never
4	Floor4	Never
5	Floor5	Never
6	Floor6	Never
7	Floor7	Never

Figure 119. Relay Labels and Schedules

Note: Relay labels are the same for all elevator restriction units in the job.

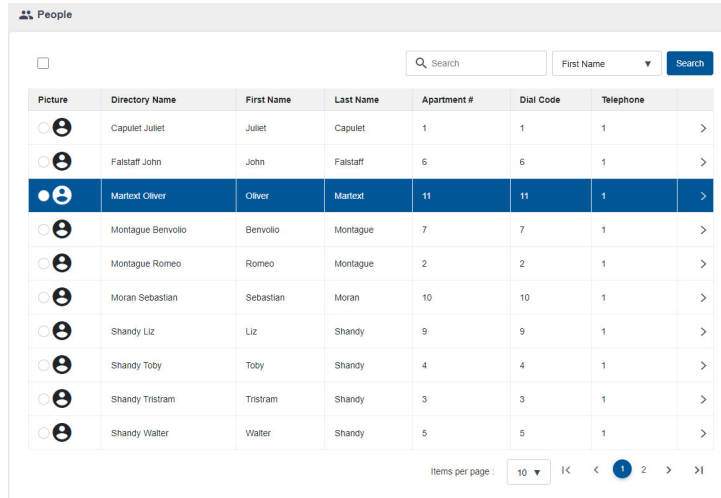
- Under **Relay Activation Schedule**, select when this relay should be active. You can select **Always**, **Never**, or another user-defined schedule. See section 10 for instructions on creating schedules.

Note: Relay schedules work only with TX3-ER-8-B (ERU 2.0).

- Click the **Done** button  in the upper right corner to save your changes, or **Cancel** button  next to it to cancel changes.


6.4.3 Configure Residents for Elevator Restriction

1. Click **People** in the Configuration pane.



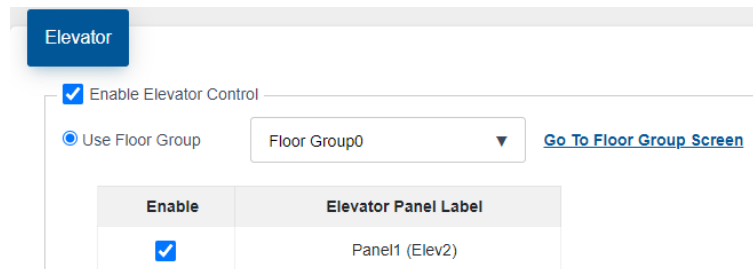
Picture	Directory Name	First Name	Last Name	Apartment #	Dial Code	Telephone	
	Capulet Juliet	Juliet	Capulet	1	1	1	>
	Falstaff John	John	Falstaff	6	6	1	>
	Markos Oliver	Oliver	Markos	11	11	1	>
	Montague Benvolio	Benvolio	Montague	7	7	1	>
	Montague Romeo	Romeo	Montague	2	2	1	>
	Moran Sebastian	Sebastian	Moran	10	10	1	>
	Shandy Liz	Liz	Shandy	9	9	1	>
	Shandy Toby	Toby	Shandy	4	4	1	>
	Shandy Tristram	Tristram	Shandy	3	3	1	>
	Shandy Walter	Walter	Shandy	5	5	1	>

Figure 120. People

2. Click the arrow on the right  to see details of a person.
3. Click **Elevator** in the left pane.

Enable Elevator Control. Select this to allow this person access to the elevators.

Use Floor Group. Select a floor group for this person. If no floor groups are defined, click **Go to Floor Group screen** to define them.



Elevator

☒ Enable Elevator Control



☒ Use Floor Group

Floor Group0

[Go To Floor Group Screen](#)

Enable	Elevator Panel Label
<input checked="" type="checkbox"/>	Panel1 (Elev2)

Figure 121. Elevators

4. Select the Elevator Restriction Units that are allowed for this resident.
5. Click the **Done** button  in the upper right corner to save your changes, or **Cancel** button  next to it to cancel changes.

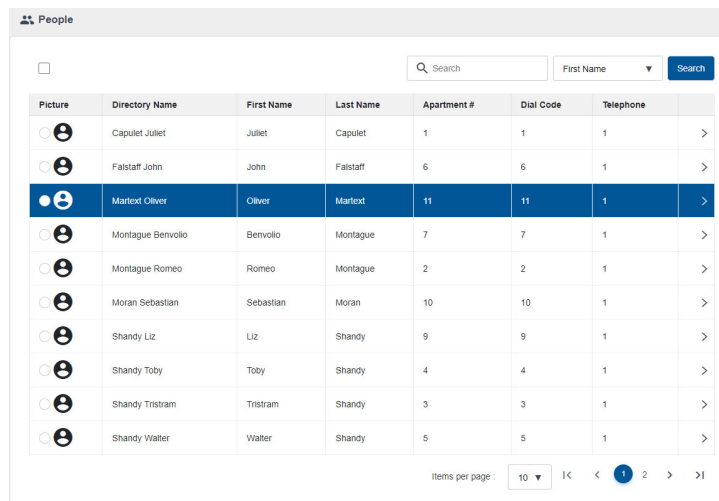
7 People

People are residents, occupants of suites, and other individuals who have credentials that allow them access through the card access system. They are listed in the directory for voice and video access for visitors.

Note: After you configure the site for the first time, and after any time you make changes, you must send the job. See section 1.10.

7.1 View People

1. Click **People** in the Configuration pane.



The screenshot shows the 'People' configuration page. At the top, there is a search bar with a magnifying glass icon and a dropdown menu for 'First Name' with a 'Search' button. Below this is a table with columns: Picture, Directory Name, First Name, Last Name, Apartment #, Dial Code, and Telephone. The table contains 10 rows of data. The third row, 'Marlex Oliver', is highlighted in blue. At the bottom right, there is a pagination control showing 'Items per page: 10' and navigation arrows.

Picture	Directory Name	First Name	Last Name	Apartment #	Dial Code	Telephone
	Capulet Juliet	Juliet	Capulet	1	1	1
	Falstaff John	John	Falstaff	6	6	1
	Marlex Oliver	Oliver	Marlex	11	11	1
	Montague Benvolio	Benvolio	Montague	7	7	1
	Montague Romeo	Romeo	Montague	2	2	1
	Moran Sebastian	Sebastian	Moran	10	10	1
	Shandy Liz	Liz	Shandy	9	9	1
	Shandy Toby	Toby	Shandy	4	4	1
	Shandy Tristram	Tristram	Shandy	3	3	1
	Shandy Walter	Walter	Shandy	5	5	1

Figure 122. People

Clicking the column header sorts the list by that column in either ascending or descending order.

7.2 Add People

1. Click the **Add** button  in the upper right to add a person.

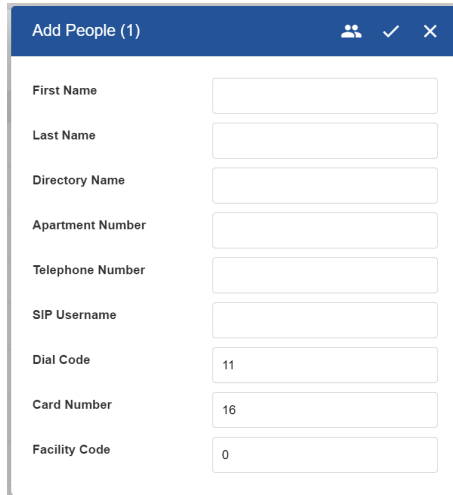


Figure 123. Add People

2. Provide information for the following parameters:

First Name, Last Name, Directory Name, Apartment Number.

Provide the person's name and apartment number. The directory name is the name that will appear in the list of residents on the telephone entry panel display or the Touch Screen directory.


Telephone Number. Provide the resident's phone number. This selection is available for ADC lines only. Type a comma (,) for a 1 second pause, and type a semi-colon (;) for a 3 second pause.

SIP username. The SIP username of the resident.

Card number. Provide a unique card number. If more than one card is added at a time, a number will be attached to the cards to make them unique.

Facility code. Enter a facility code for the card with a value from 0 to 2147483647. Access is granted when this facility code matches the value set for the card access panel.

7.3 Remove People

1. Select the person or people you want to remove by clicking the button  beside each name.

2. Click the **Remove** button  in the upper right corner.
3. Click **YES**.

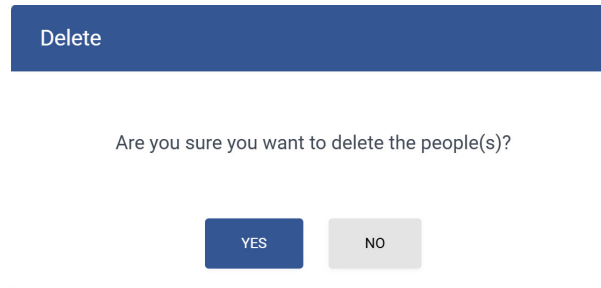



Figure 124. Remove People

7.4 View a Person's Profile

1. From the **People** window, click the arrow on the right  to see details of a person.

The Person Configuration screen appears. It is divided into several sections. To see a specific section, click it in the left pane.

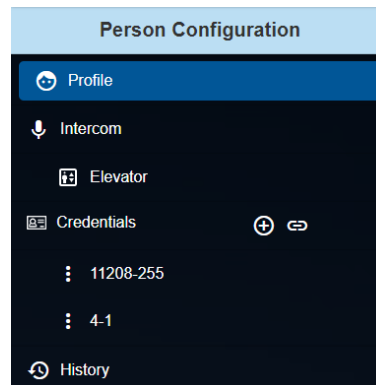
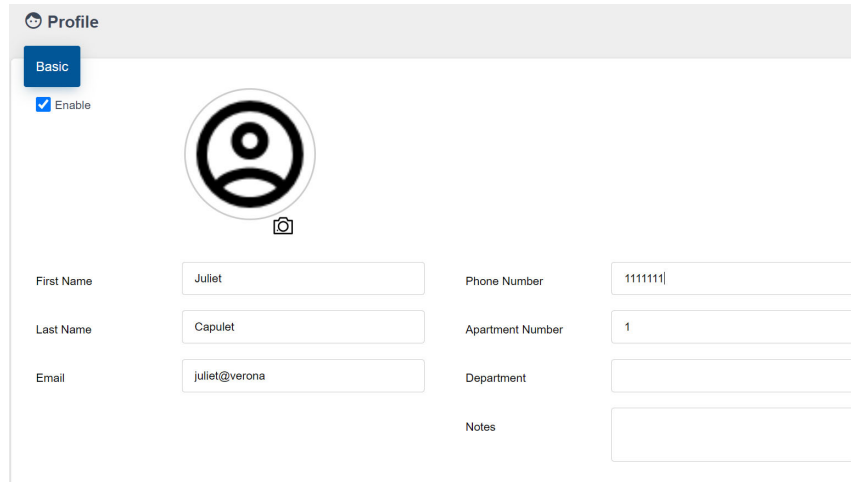


Figure 125. Person Configuration (left pane)

7.4.1 Basic

1. Provide information for the following parameters:

Basic and Address. Provide the person's details like their name, email address, phone number, and address.



Profile

Basic

☒ Enable

First Name: Juliet

Last Name: Capulet

Email: juliet@verona

Phone Number: 11111111

Apartment Number: 1

Department:

Notes:

Figure 126. Profile

7.4.2 Intercom

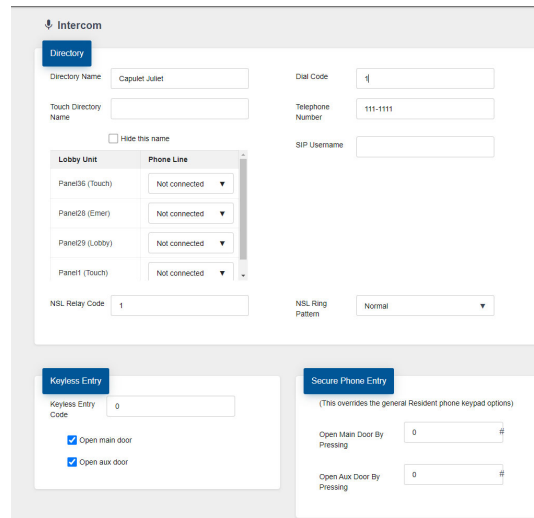


Figure 127. Intercom

1. Provide information for the following parameters:

Directory Name. Provide the person's directory name. The maximum length of this field is 15 characters. This is the name that will appear in the list of residents on the telephone entry panel display or the Touch Screen directory.

Touch Directory Name. This field is optional. The Touch Directory Name appears in the list of residents on the Touch Screen directory. The maximum length of this field is 50 characters. If this field is blank, then the Directory Name is used instead.

Hide this name. Check this box to hide the Touch Directory Name from the panel directory.

Dial code. Enter the resident's dial code (maximum 4 digits).

Telephone Number. Provide the resident's phone number. This selection is available for ADC lines only. Type a comma (,) for a 1 second pause, and type a semi-colon (;) for a 3 second pause.

SIP username. The resident's SIP username.

NSL Relay code. The NSL relay code is set automatically for each resident based on the initial starting value.

NSL Ring pattern. Select the resident's phone ring pattern from the list. Each panel may have its own unique ring.

Keyless entry code. Enter the resident keyless entry code using a number from 0 to 999999.

Open Main door. Selecting this box opens the main door when the resident enters their keyless entry code.

Open Aux door. Selecting this box opens the auxiliary door when the resident enters their keyless entry code.

Open main door by pressing. Enter a series of up to 4 digits from 0 to 9 followed by pound (#). This code will replace the general resident phone keypad options. This applies to the specific resident.

Note: Do not select 4 (this is used to refuse entry or disconnect).

Do not use the same number for the main door, auxiliary door, and call waiting (call waiting works on NSL systems only).

Open aux door by pressing. Enter a series of up to 4 digits from 0 to 9 followed by pound (#). This code will replace the general resident phone keypad options. This applies to the specific resident.

Note: Do not select 4 (this is used to refuse entry or disconnect).

Do not use the same number for the main door, auxiliary door, and call waiting (call waiting works on NSL systems only).

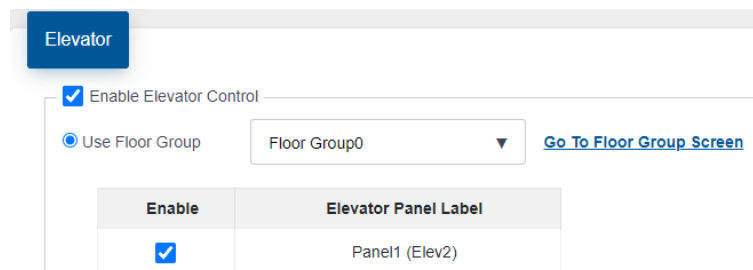
Note: Do not select 1, 7, or * for **Open Main Door by Pressing** and **Open Aux Door by Pressing**.

7.4.3 Elevator

1. Provide information for the following parameters:

Enable Elevator Control. Select this to allow this person access to the elevators.

Use Floor Group. Select a floor group for this person. If no floor groups are defined, click **Go to Floor Group screen** to define them.



Enable	Elevator Panel Label
<input checked="" type="checkbox"/>	Panel1 (Elev2)

Figure 128. Elevators

7.4.4 Credentials

The left pane lists the credentials associated with this person.

Figure 48 shows a Person with one linked credential. The numbers are the card number and the facility code. In this example, the card number is 52430 and the facility code is 0.

Click the credential to view its details.

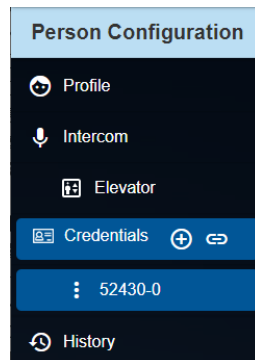



Figure 129. Person Configuration (left pane)

7.4.5 Link a Credential

1. Click the link icon  on the left to link an existing credential to this person.

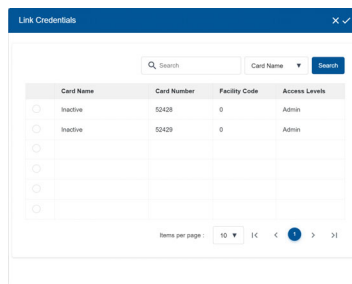



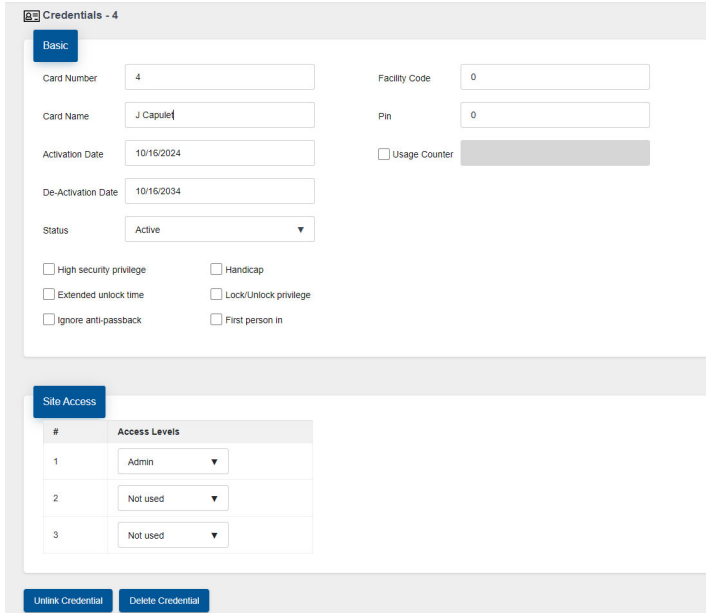


Figure 130. Link Credentials

2. In the **Link Credentials** window, select the existing credentials that you want to link to this person.
3. Click the **Done** button  in the upper right corner to save your changes, or **Cancel** button  next to it to cancel changes.

7.4.6 Add or Edit a Credential

1. In the left pane, click the **Add** button  to add a credential, or click a credential to edit it.



Basic

Card Number: 4 Facility Code: 0

Card Name: J Capule Pin: 0

Activation Date: 10/16/2024 Usage Counter: ☐

De-Activation Date: 10/16/2034

Status: Active

☐ High security privilege ☐ Handicap
☐ Extended unlock time ☐ Lock/Unlock privilege
☐ Ignore anti-passback ☐ First person in

Site Access

#	Access Levels
1	Admin
2	Not used
3	Not used

Unlink Credential Delete Credential

Figure 131. Credentials

2. Provide information for the following parameters:

Card number. Provide a unique card number. If more than one card is added at a time, a number will be attached to the cards to make them unique.

Card name. Specify a name for the card. The maximum number of characters is 30.

Activation date. Specify the activation date for the card.

De-activation date. Specify the de-activation date.

Status. **Status** shows the current status of this card. Select **Inactive** to de-activate or **Active** to activate the card.

Facility Code. Provide the facility code.

PIN. Enter a Personal Identification Number. The PIN is 1 to 4 digits long and is programmed for each card. 0 is not accepted. This is required if the 'PIN required schedule' feature is enabled on the card reader.

Usage counter. This feature uses a counter to specify a card usage limit at a reader. Each time the card is used this value decreases by one in the database. When it reaches zero, the card is de-activated. Select the check box and specify the maximum usage count for this card. When deselected the card has an unlimited use.

High security privilege. Assigns the card access rights to areas designated as high security. A card with this privilege can toggle the high security mode to either on or off by swiping the card four times in succession.

Extended unlock time. Enables the card to be used during the extended unlock time period. During this time the door remains unlocked. This option is commonly given to seniors and persons with limited mobility.

Ignore anti-passback. When this option is specified the card holder is not restricted, if set, by the timed anti-passback mode of the reader. Selecting this option allows the same card unlimited use at the same reader.

Handicap. Enables the card to access points designated as accessible as well as the regular lock. The access point must be designated as a handicap lock.



Lock/Unlock privilege. Enabling the lock/unlock privilege overrides any scheduled card access restrictions. An access card with lock/unlock privileges, if swiped twice in succession, toggles between lock and unlock mode.

First person in. When enabled the door becomes unlocked by the first valid card presented during the unlock schedule, causing the door to

remain unlocked for the duration of the unlock schedule. This option must also be set when configuring the Access Point.

Unlink Credential. Click this button to unlink the credential from the resident so that it can be used for another resident.

Delete Credential. Click this button to delete the credential.

Click the **Done** button  in the upper right corner to save your changes, or **Cancel** button  next to it to cancel changes.


7.4.7 History

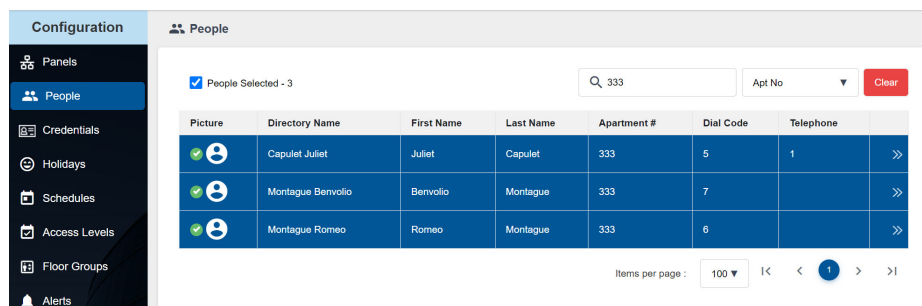
The History window shows the past events associated with this person.



Figure 132. History

7.5 Edit Multiple People

1. Select the button to the left of each person that you want to edit.
2. Click the double arrow icon  to the right of one of the selected people to edit details.









Picture	Directory Name	First Name	Last Name	Apartment #	Dial Code	Telephone	
	Capulet Juliet	Juliet	Capulet	333	5	1	
	Montague Benvolio	Benvolio	Montague	333	7		
	Montague Romeo	Romeo	Montague	333	6		

Figure 133. Edit Multiple People

3. Click the **Done** button  in the upper right corner to save your changes, or **Cancel** button  next to it to cancel changes.

8

Credentials

Residents use credentials to gain access to a building. Credentials can be physical cards, or digital tokens.


Note: After you configure the site for the first time, and after any time you make changes, you must send the job. See section 1.10.

8.1

View Credentials

Click **Credentials** in the Configuration pane to display all currently configured credentials and their corresponding details.

Click on an item in the column header to sort the list in either ascending or descending order.

Click the link icon  on the left to see the resident that the credential is linked to.












Credentials							
<input type="checkbox"/>	<input type="text" value="Search"/>		Card Name <input type="text"/>		<input type="button" value="Search"/>		
	Card Name	First Name	Last Name	Card Number	Facility Code	Access Levels	
<input type="radio"/>	 997840	Juliet	Capulet	52431	0	Admin	>
<input type="radio"/>	 997850	Romeo	Montague	52432	0	Admin	>
<input type="radio"/>	 997860	Tristram	Shandy	52433	0	Admin	>
<input type="radio"/>	 997870	Toby	Shandy	52434	0	Admin	>
<input type="radio"/>	 997880	Walter	Shandy	52435	0	Admin	>
<input type="radio"/>	 997890	John	Falstaff	52436	0	Admin	>
<input type="radio"/>	 997900	Benvolio	Montague	52437	0	Admin	>
<input type="radio"/>	 997910	John	Watson	52438	0	Admin	>
<input type="radio"/>	 997920	Liz	Shandy	52439	0	Admin	>
<input type="radio"/>	 997930	Sebastian	Moran	52440	0	Admin	>

Figure 134. Credentials

Note: An unlinked credential is not associated with a resident, but it will still grant access. To disable a credential, change the Status to Inactive in the Credential Details.

8.2 Add a Credential

1. Click the Add button  in the upper right to add a credential.

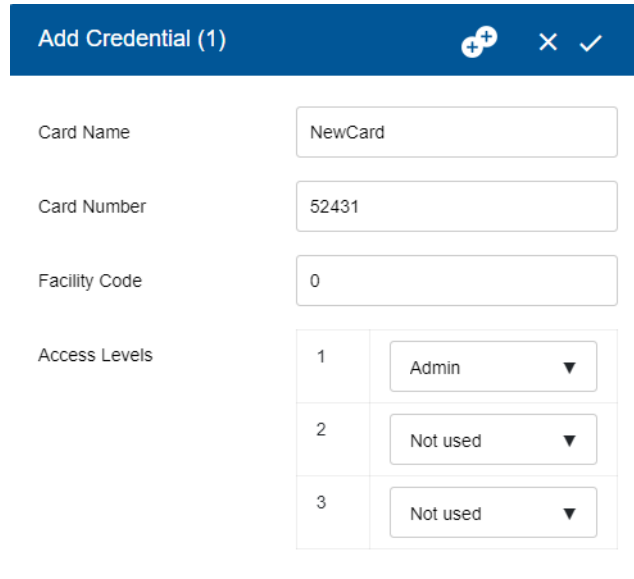


Figure 135. Add Credential

Card name. Specify a name for the card. The maximum number of characters is 30.


Card number. Provide a unique card number.

Facility Code. Provide the facility code.


Access Levels. Select the access levels that apply to this credential.

2. Click the **Done** button  in the upper right corner to save your changes, or **Cancel** button  next to it to cancel changes.



8.2.1 Add Multiple Credentials

1. In the **Add Credential** window, click the Add Multiple Credentials icon. 
2. Enter the number of credentials to add, then click **OK**.

The **Add Credentials** window shows a number in the title bar indicating how many credentials will be added. The name of each card will be the **Card Name** followed by a number, and the **Card Number** will be increased by one for each card added.

3. Click the Done button  in the upper right corner to add the cards.

8.3 Remove a Credential

1. Select the credential(s) you want to remove by clicking the button  beside it.
2. Click the **Remove** button  in the upper right corner.
3. Click **YES**.

Delete


Are you sure you want to delete the credential(s)


YES

NO

Figure 136. Remove Credential

8.4 Edit a Credential

1. Click the arrow to the right of an existing credential  to see its details.

 Credentials - 4

Basic

Card Number

Card Name

Activation Date

De-Activation Date

Status Active ▼

☐ High security privilege
☐ Extended unlock time
☐ Ignore anti-passback

☐ Handicap
☐ Lock/Unlock privilege
☐ First person in

Facility Code

Pin

☐ Usage Counter

Site Access

#	Access Levels
1	Admin ▼
2	Not used ▼
3	Not used ▼

Go to Person

Figure 137. Credentials Details

Card number. Provide a unique card number.

Card name. Specify a name for the card. The maximum number of characters is 30.

Activation date. Specify the activation date for the card.

De-activation date. Specify the de-activation date.

Status. This option shows the current status of this card. Select **Inactive** to de-activate or **Active** to activate the card.

Facility Code. Provide the facility code.

PIN. Enter a Personal Identification Number. The PIN is 1 to 4 digits long and is programmed for each card. 0 is not accepted. This is required if the 'PIN required schedule' feature is enabled on the card reader.

Usage counter. This feature uses a counter to specify a card usage limit at a reader. Each time the card is used this value decreases by one in the database. When it reaches zero, the card is de-activated. Select the check box and specify the maximum usage count for this card. When deselected the card has an unlimited use.

High security privilege. Assigns the card access rights to areas designated as high security. A card with this privilege can toggle the high security mode to either on or off by swiping the card four times in succession.

Extended unlock time. Enables the card to be used during the extended unlock time period. During this time the door remains unlocked. This option is commonly given to seniors and persons with limited mobility.


Ignore anti-passback. When this option is specified the card holder is not restricted, if set, by the timed anti-passback mode of the reader. Selecting this option allows the same card unlimited use at the same reader.

Handicap. Enables the card to access points designated as accessible as well as the regular lock. The access point must be designated as a handicap lock.


Lock/Unlock privilege. Enabling the lock/unlock privilege overrides any scheduled card access restrictions. An access card with lock/unlock privileges, if swiped twice in succession, toggles between lock and unlock mode.

First person in. When enabled the door becomes unlocked by the first valid card presented during the unlock schedule, causing the door to remain unlocked for the duration of the unlock schedule. This option must also be set when configuring the Access Point.

Site Access. Select the access levels that apply to this credential.

2. Click the Done button  in the upper right corner to save your changes.

8.4.1 Edit Multiple Credentials

1. Select the button to the left of each credential that you want to edit.
2. Click the double arrow icon  to the right of one of the selected credentials to edit details.

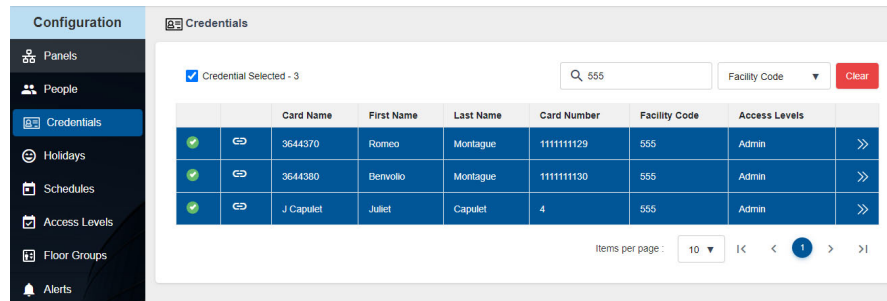


Figure 138. Edit Multiple Credentials

3. Click the **Done** button  in the upper right corner to save your changes, or **Cancel** button  next to it to cancel changes.

9

Holidays

Holidays allow you to define a calendar of holiday periods for determining when certain panel functions, such door access permission, are allowed.

Holidays consist of start date and time, end date and time, and may include holidays that re-occur on the same date every year.

Note: After you configure the site for the first time, and after any time you make changes, you must send the job. See section 1.10.

9.1 View Holidays

1. Click **Holidays** in the Configuration pane. The Holiday Configuration window appears listing the available holidays.

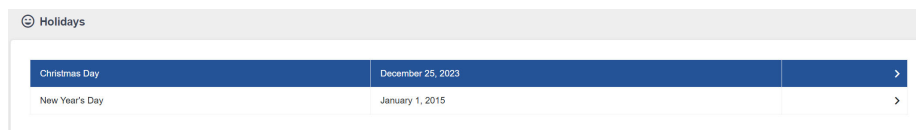




Figure 139. Holidays

9.2 Add or Edit a Holiday

1. Click the Add button  in the upper right to add a holiday, or click the arrow to the right of an existing holiday  to view or edit its details.

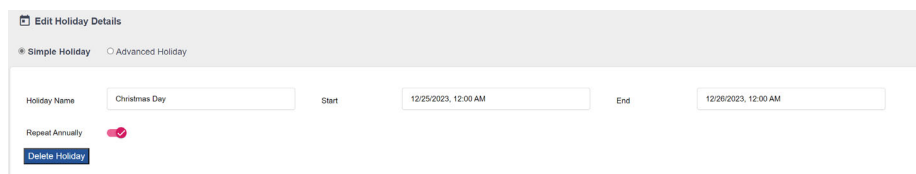




Figure 140. Edit Holiday



2. Provide information for the following parameters:
Holiday Name. Provide a name for the holiday.
Start. Specify a start day and time.

End. Specify an end day and time.

Repeat annually. Check this box if the same start, end date and time re-occur every year.

Click the **Done** button  in the upper right corner to save your changes, or **Cancel** button  next to it to cancel changes.

9.3 Remove a Holiday

1. Click the arrow to the right of an existing holiday  to edit its details.
2. Click **Delete Holiday** button  to remove the holiday.
3. Click **YES**.

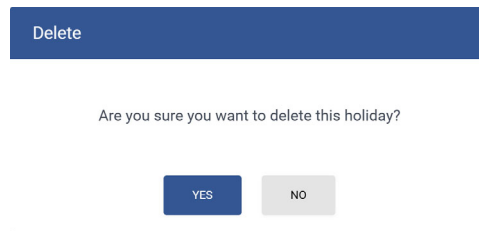


Figure 141. Delete Holiday

10 Schedules

Schedules let you define a timetable to establish when certain panel functions are permitted to occur, such as when calls to residents are allowed, when residents can grant access to a visitor or when the postal lock can be used. These schedules are designated and listed by name, and are available for selection wherever it is necessary to invoke access permission.

Multiple periods may be used if the schedule is not continuous or does not span to the next day.

Note: After you configure the site for the first time, and after any time you make changes, you must send the job. See section 1.10.

10.1 View Schedules

1. Click **Schedules** in the Configuration pane.

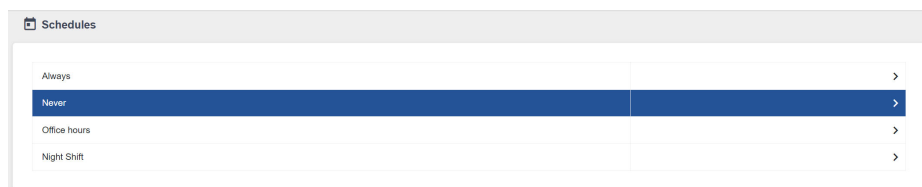




Figure 142. Schedules

10.2 Add or Edit a Schedule

1. Click the Add button  in the upper right to add a schedule, or click the arrow to the right of an existing schedule  to view or edit its details.

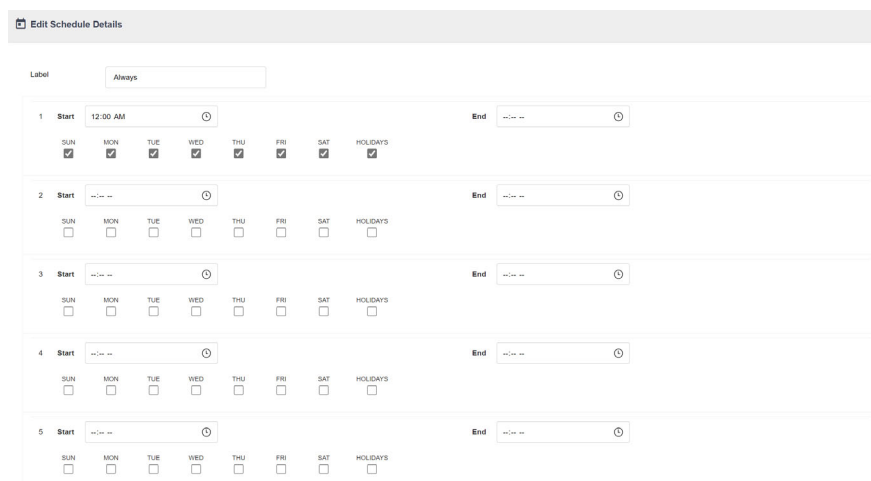


Figure 143. Schedule

2. Provide information for the following parameters:

Label. Provide a name for the schedule.

Start. Specify a start time.

End. Specify an end time.


Sun to Sat. Select the day or days of the week for the schedule to take effect.

Holidays. Select whether this schedule includes holidays.


Note: If your schedule starts before midnight on one day and ends the next day, you must define **two** periods (one for each day). For example, if you have a schedule that goes from 10:00PM on Tuesday to 2:00AM on Wednesday, you need one period for Tuesday and a second period for Wednesday. The Tuesday period starts at 10:00PM and ends at 11:59PM; the Wednesday period starts at 12:00AM and ends at 2:00AM.

3. Click the **Done** button  in the upper right corner to save your changes, or **Cancel** button  next to it to cancel changes.

10.3 Delete a Schedule

1. Click the arrow to the right of an existing schedule  to see its details.

Note: You cannot view details for the **Always** and **Never** schedules. Only schedules created by the user can be deleted.

2. Click **Delete Schedule** button  to remove the schedule.
3. Click **YES**.

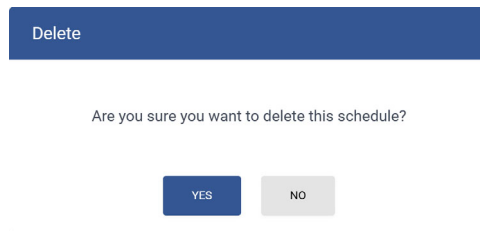


Figure 144. Delete Schedule

11

Access Levels

Note: After you configure the site for the first time, and after any time you make changes, you must send the job. See section 1.10.

Creating an access level lets you define where and when to use a credential, and how to set elevator usage if elevator restriction units are used. Access levels are assigned to credentials to help the administrator keep track of access privileges.

You can create a maximum of 128 access levels for each controller and a recommended maximum of 2000 access levels for the job. For each access level, you can select a schedule for all of the access points in your job.

For example, if your job has a card access system panel called Panel 1 with two access points (Reader A and Reader B) and a card access system panel called Panel 2 with two access points (Reader C and Reader D), you could define the following access levels.

Access Level 1

- Panel 1: Reader A schedule = Always
- Panel 1: Reader B schedule = Never
- Panel 2: Reader C schedule = Never
- Panel 2: Reader D schedule = Never

Access Level 2

- Panel 1: Reader A schedule = Office hours
- Panel 1: Reader B schedule = Always
- Panel 2: Reader C schedule = Always
- Panel 2: Reader D schedule = Always

If a credential is assigned to Access Level 1, the user has access to Reader A on Panel 1 at all times but will not have access to any other access point.

If a credential is assigned to Access Level 2, the user has access to Reader A during the Office Hours schedule only and will have access to all of the other access points all of the time.

11.1 View Access Levels

1. Select **Access Levels** on the left pane.

The Access Levels screen appears.

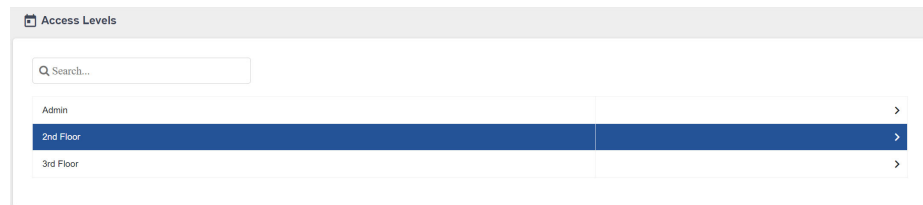


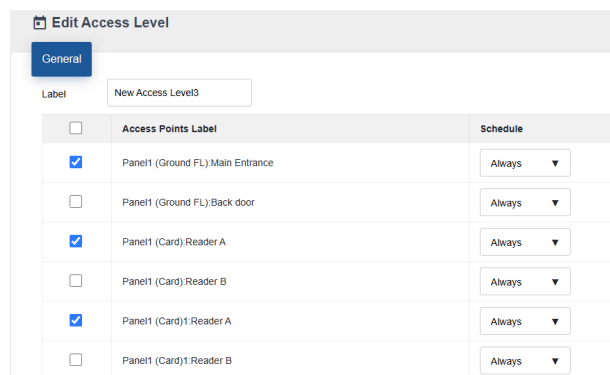


Figure 145. Access Levels

Note: By default the **Admin** level has access to all access points at all times and it is not configurable.

11.2 Add or Edit an Access Level

1. Click the Add button  in the upper right to add an access level, or click the arrow to the right of an existing access level  to view or edit its details.



Access Points Label	Schedule
<input checked="" type="checkbox"/> Panel1 (Ground FL) Main Entrance	Always ▼
<input type="checkbox"/> Panel1 (Ground FL) Back door	Always ▼
<input checked="" type="checkbox"/> Panel1 (Card) Reader A	Always ▼
<input type="checkbox"/> Panel1 (Card) Reader B	Always ▼
<input checked="" type="checkbox"/> Panel1 (Card) Reader A	Always ▼
<input type="checkbox"/> Panel1 (Card) Reader B	Always ▼

Figure 146. Add or Edit Access Level

2. Supply the following information:

Label. Provide a name for this access level.



Access Points. Select the checkbox for an access point to enable or disable access. If an access point is unchecked, it will not allow access to cards with this access level.

Schedule. From the schedule, list select when access is granted. You can select from **Always**, **Never** or any other user-defined schedule.

Elevator. Click **Enable Elevator Control** to enable elevator access control for this access level, then select **Use Floor Group** and choose a floor group.

3. Click the **Done** button  in the upper right corner to save your changes, or **Cancel** button  next to it to cancel changes.

11.3 Delete an Access Level

1. Click the arrow to the right of an existing access level  to see its details.
2. Click **Delete Access Level** button  to remove the access level.
3. Click **YES**.

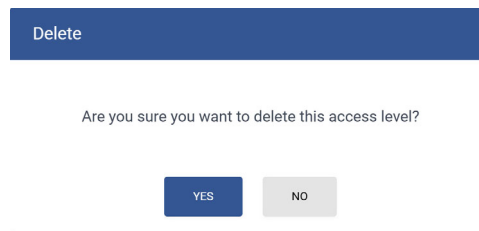


Figure 147. Delete Access level

12 Floor Groups



Floor groups are groups of floors that are assigned to access levels for elevator control.

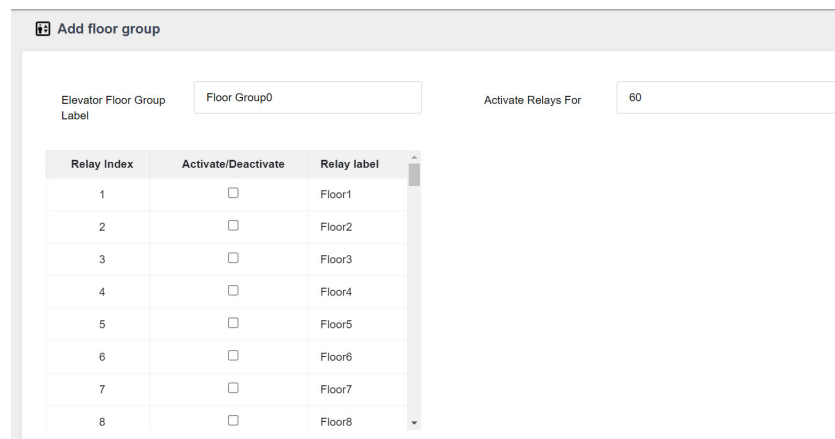
Note: After you configure the site for the first time, and after any time you make changes, you must send the job. See section 1.10.

12.1 View Floor Groups

1. Select **Floor Groups** from Configuration pane.

12.2 Add or Edit a Floor Group

1. Click the Add button  in the upper right to add a floor group, or click the arrow to the right of an existing floor group  to view or edit its details.



Relay Index	Activate/Deactivate	Relay label
1	<input type="checkbox"/>	Floor1
2	<input type="checkbox"/>	Floor2
3	<input type="checkbox"/>	Floor3
4	<input type="checkbox"/>	Floor4
5	<input type="checkbox"/>	Floor5
6	<input type="checkbox"/>	Floor6
7	<input type="checkbox"/>	Floor7
8	<input type="checkbox"/>	Floor8

Figure 148. Add floor group

2. Click the **Activate/Deactivate** checkbox to select the floors that you want in this floor group.



3. Provide the following information:

Activate relays for. Specify the amount of time that the ERU relays are active. This timer starts when the access point reads the card.

Note: The minimum is 5 seconds and the maximum is 600 seconds.

4. Click the **Done** button  in the upper right corner to save your changes, or **Cancel** button  next to it to cancel changes.

12.3 Delete Floor Group

1. Click the arrow to the right of an existing access level  to see its details.
2. Click **Delete Floor Group** button  to remove the access level.
3. Click **YES**.



Delete

Are you sure you want to delete this floor group?



YES



NO

Figure 149. Delete Access level

13 Alerts

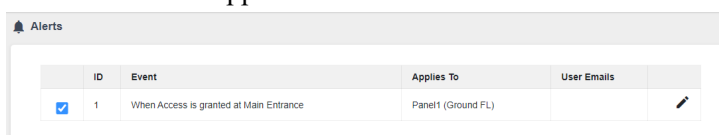
The system can send an email message when a specific event happens.

Note: After you configure the site for the first time, and after any time you make changes, you must send the job. See section 1.10.

13.1 View Alerts

1. Click **Alerts** in the Configuration pane.

The Alerts screen appears.






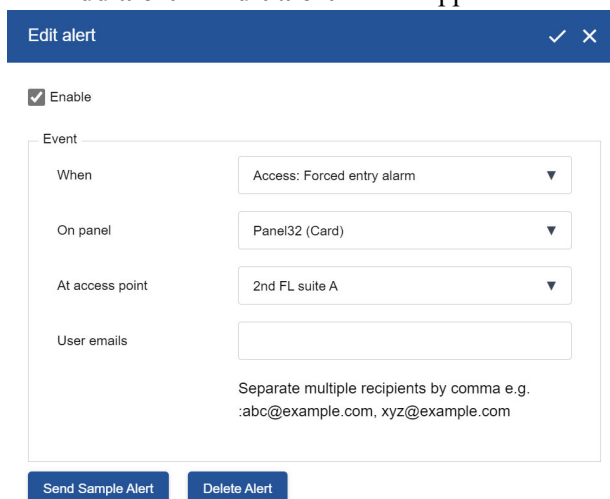
	ID	Event	Applies To	User Emails	
<input checked="" type="checkbox"/>	1	When Access is granted at Main Entrance	Panel1 (Ground FL)		

Figure 150. Alerts

13.2 Add or Edit an Alert

1. Click the **Edit** icon  on the right to edit the alert, or click the **Add** button  to create a new alert.

The **Add alert** or **Edit alert** screen appears.



Edit alert ✓ ✕

☒ Enable

Event

When

Access: Forced entry alarm ▼

On panel

Panel32 (Card) ▼

At access point

2nd FL suite A ▼

User emails

Separate multiple recipients by comma e.g.
 :abc@example.com, xyz@example.com

Send Sample Alert

Delete Alert

Figure 151. Edit alert

When. Choose an event that will activate an alert. For a description of the events, see section 13.2.1.

On panel. This option applies the action either to one of the panels on your system or to a group of panels on your system. If, for example, you have two panels (Panel 1 and Panel 2) in your TX3 system, you could select from the following options:

Panel 1 - Apply the correlation to Panel 1 only.

Panel 2 - Apply the correlation to Panel 2 only.

All panels - Apply the correlation to all telephone entry, card access, and Touch Screen panels on the network.

At access point. If the panel is a card access panel, select the access point.

User emails. Enter the email addresses that the alert should be sent to. If you enter more than one email address, separate the addresses with commas.

2. Click the **Done** button  in the upper right corner to save your changes, or **Cancel** button  next to it to cancel changes.

13.2.1 Event List

Access: Access is granted.

Access: Access is denied.

Access: Forced entry alarm. A door is forced open.

Access: Unknown card format.

Access: Forced entry alarm restored. The forced entry alarm is restored.

Access: Door held open alarm. A door did not close.

Access: Door held open alarm restored. The door held open alarm is restored.

Access: Door held open warning. A door did not close and the door held open warning is issued.

Access: Door held open warning restored. The door held open warning is restored.

Access: Door not open. Access is granted but the door remains closed.

Access: Request to Exit. A request to exit is made.

Access: Input is active. The general purpose input becomes active.

Access: Input is normal. The general purpose input becomes inactive.

Access: Unlock mode is on. Unlock mode is activated, either by the Auto unlock schedule, or manually, or by a card with the lock/unlock privilege.

Access: Unlock mode is off. Unlock mode is deactivated, either by the Auto unlock schedule, or manually, or by a card with the lock/unlock privilege.

Access: High security is on. High security mode is activated, either by a card with high security privilege, or manually, or by a correlation.

Access: High security is off. High security mode is deactivated, either by a card with high security privilege, or manually, or by a correlation.

Access: Tamper detected. The controller's tamper alarm is on.

Access: Tamper restored. The controller's tamper alarm is off.

Access: Battery OK. Not used.

Access: Battery Low. Not used.

Access: Battery flat. Not used.

Access: Lockset offline. Not used.

Access: Lockset online. Not used.

Access: Door is locked. Not used.

Access: Door is unlocked. Not used.

Access: FC not matching. Access denied. When Facility code mode is enabled, access is denied because the facility code is invalid. See section 5.3.

Access: PIN not matching. Access denied. During the PIN required schedule, access is denied because the PIN is invalid. See section 5.3.

Access: PIN timed out. Access denied. During the PIN required schedule, access is denied because no PIN was entered during the PIN Timeout time. See section 5.3.

Access: Card number not found. Access denied. Access is denied because the card number is invalid.

Access: Temp card usage exceeded. Access denied. Access is denied because the card's usage counter has reached zero. See section 8.4.

Access: Card not active. Access denied. Access is denied because the card's Status is Inactive. See section 8.4.

Access: Card expired. Access denied. Access is denied because the card's Deactivation date has passed. See section 8.4.

Access: Schedule not matching. Access denied. The card is valid but the schedule for the card's access level is not active. See section 11.

Access: High security right not set. Access denied. The access point is set to high security but the card does not have high security privilege. See section 5.3.

Access: Anti passback. Access denied. Access is denied because the card is used for a second time while the anti-passback timer is running. See section 5.3.

Access: Anti PB list full. Access denied. The first time a card is used, it is added to the anti-passback list. When the anti-passback timer for that card expires, the card is removed from the list. On a card access system, the list holds 100 cards. While the list is full, access is denied.

Access: Hub is online. Not used.

Access Hub is offline. Not used.

Access: All HISEC mode on. A correlation turns on high security on all the access points of one panel.

Access: All HISEC mode off. A correlation turns off high security on all the access points of one panel.

Access: Door is jammed. Not used.

Access: Card discovery mode. Not used.

Access: Elevator Relay Activated by PC Operator.

Lobby: Input is active. The general purpose input becomes active.

Lobby: Input is normal. The general purpose input becomes inactive.

Lobby: Call Started. The lobby unit calls a resident.

Lobby: Call finished. A call to a resident ends.

Lobby: Call is connected. A call is established.

Lobby: Access is granted (lobby). The resident grants access using a telephone keypad.

Lobby: Access denied (lobby). The resident denies access.

Lobby: Unlock mode is turned on (lobby). The Auto unlock Main door schedule becomes active. See section 3.1.9.

Lobby: Unlock mode is turned off (lobby). The Auto unlock Main door schedule becomes inactive. See section 3.1.9.

Lobby: Dial code not found. The dial code is invalid.

Lobby: Call and access schedule inactive. A visitor tries to call a resident but access is denied because the Allow calls schedule is inactive. See section 3.1.2.

Lobby: Line not connected. The phone line is not connected.

Lobby: Line is in use. The phone line is in use.

Lobby: Guard phone connected. A successful call is made to the guard phone.

Lobby: Calling guard phone. A resident or visitor is calling the guard phone.

Lobby: Disconnecting call. The resident or visitor is disconnecting the call.

Lobby: Keyless code schedule is inactive. The resident tries to enter a keyless code but access is denied because the Allow keyless entry schedule is not active. See section 3.1.2.

Lobby: Keyless code not found. The resident's keyless entry code is invalid. See section 7.4.2.

Lobby: Main and Aux door are open. The resident opens both the main and auxiliary door with keyless entry. See section 7.4.2.

Lobby: main door is open. The resident opens the main door from the keypad. See section 7.4.2.

Lobby: Auxiliary door is open. The resident opens the auxiliary door from the keypad. See section 7.4.2.

Lobby: Called party is busy. The phone line is busy.

Lobby: Call in process. The lobby unit has placed a call and the phone is ringing.

Lobby: Guard phone not connected or disabled. A resident or visitor tries to call the guard phone, but the guard phone is not connected or not enabled.

Lobby: No dial tone. The phone line is connected but there is no dial tone.

Lobby: Guard phone calling. The guard phone is calling the panel or a resident.

Lobby: Postal lock usage exceeded the limit. The daily postal lock usage is exceeded. See section 3.1.9.



Lobby: Unlock schedule inactive. The resident tries to grant access by pressing the DTMF digit, but access is denied because the Allow unlock schedule is inactive. See section 3.1.2.

Lobby: Postal lock usage not allowed at this time. The postal lock is used outside of the postal lock schedule, or the postal lock usage has exceeded its limit.

Config: Panel offline. The Configurator is disconnected from a panel.

Config: Panel connected. The Configurator is connected to a panel.

13.3 Send Sample Alert

1. Click the **Edit** button  on the right to edit the alert.
2. Click **Send Sample Alert** button  to send the alert.

13.4 Delete an Alert

1. Click the **Edit** button  on the right to edit the alert.
2. Click **Delete Alert** button  to remove the alert.
3. Click **YES**.

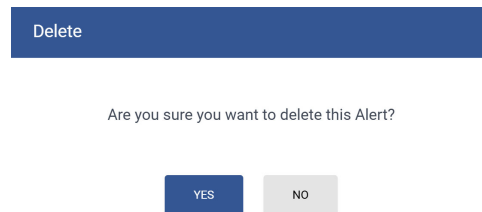


Figure 152. Delete Alert

14 Reports

The **Reports** option lets you generate reports on events, residents and access cards, and lets you print a paper directory.

Note: After you configure the site for the first time, and after any time you make changes, you must send the job. See section 1.10.

To see the Reports pane, click the **Options** menu, then click **Reports**.

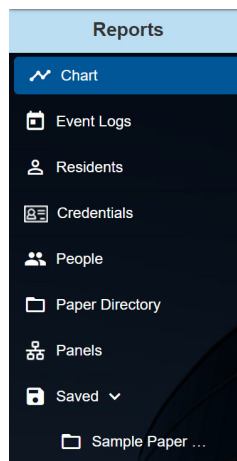




Figure 153. The Reports Pane

14.1 Save and Export Reports

After you have configured a report to display only the information you want, click the Save button  in the upper right corner.

Saved reports appear at the bottom of the Reports pane.

Click the Export button  in the upper right to save the report as a PDF, XSLX, or CSV file. Exported reports are saved in the Downloads folder of the computer or laptop.

14.2 Show and Hide Columns

You can show and hide columns in the reports for residents, credentials, people, and panels.

1. Click the menu at the top of the report.
2. Select the columns that you want to show.

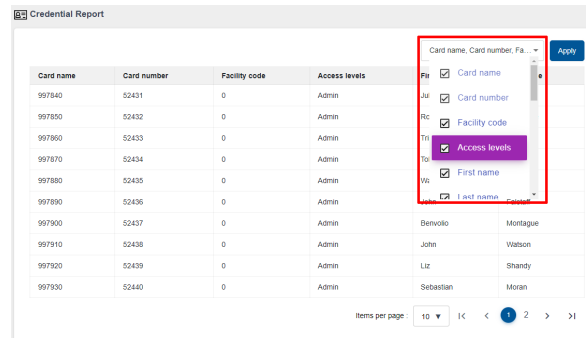


Figure 154. Showing and Hiding Columns

3. Click **Apply**.

14.3 Chart

This chart is the same as the chart described in section 2.4.

14.4 Event Logs

You can generate a report of some or all of the event log report.

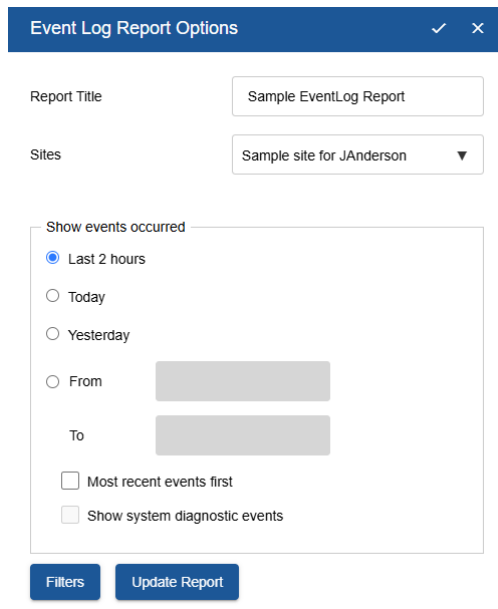
1. Click **Event Logs** in the Reports pane.

The Event Log Report window appears.



Figure 155. Event Log Report

2. Click the Edit button  to edit the event log.



The dialog box is titled "Event Log Report Options" with a blue header bar containing a checkmark and a close button. It contains the following fields and controls:

- Report Title:** A text input field with the value "Sample EventLog Report".
- Sites:** A dropdown menu showing "Sample site for JAnderson" with a downward arrow.
- Show events occurred:** A section with radio buttons for "Last 2 hours" (selected), "Today", and "Yesterday". Below these are two input fields labeled "From" and "To" for date range selection.
- Most recent events first:** A checkbox that is currently unchecked.
- Show system diagnostic events:** A checkbox that is currently unchecked.
- Buttons:** At the bottom are two buttons: "Filters" and "Update Report".

Figure 156. Event Log Report Options

3. Provide information for the following:

Report Title. This will appear at the top of the report.

Sites. Select the site that should be included in the report.

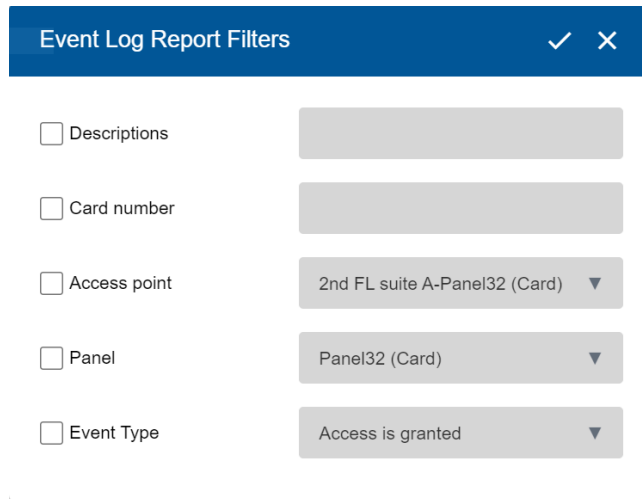
Show events occurred. Select During last 2 hours, Today or Yesterday, or select a range of dates.

Most recent events first. Select this option to display the most recent events at the top of the report.

Show system diagnostic events. Technicians can select this option to get diagnostic information for troubleshooting.

4. Click **Update Report** to retrieve all the events from all panels on the network. This could take a few minutes.
5. Click **Filters**.

The Event Log Report Filters window appears.



The image shows a window titled "Event Log Report Filters" with a blue header bar containing a checkmark and a close button. Below the header, there are five filter options, each with a checkbox and a corresponding input field:

- ☐ Descriptions: A text input field.
- ☐ Card number: A text input field.
- ☐ Access point: A dropdown menu showing "2nd FL suite A-Panel32 (Card)".
- ☐ Panel: A dropdown menu showing "Panel32 (Card)".
- ☐ Event Type: A dropdown menu showing "Access is granted".

Figure 157. Event Log Report Filters

6. Provide the following information if you want to narrow down the report results.

Descriptions. Type the text to search for in the event description. The report shows only events that contain this text in the event description.

Card number. Type a card number to search for. The report shows only events that contain this card number.

Access point. The report shows only events for this access point.

Panel. The report shows only events for this panel.

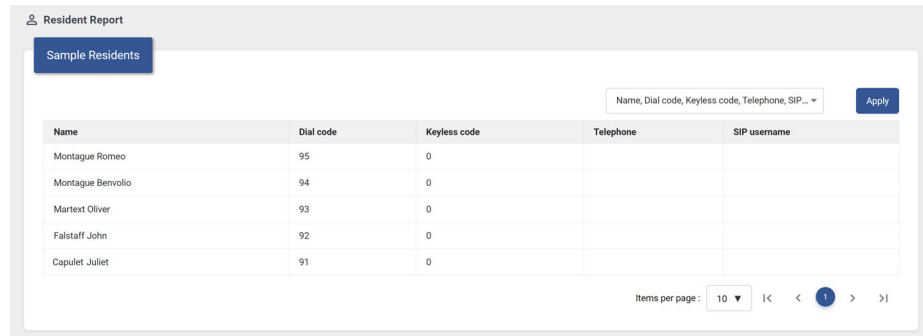
Event Type. The report shows only events for this event type.

14.5 Residents

You can generate a report of some or all of the residents.

1. Click **Residents** in the **Reports** pane.

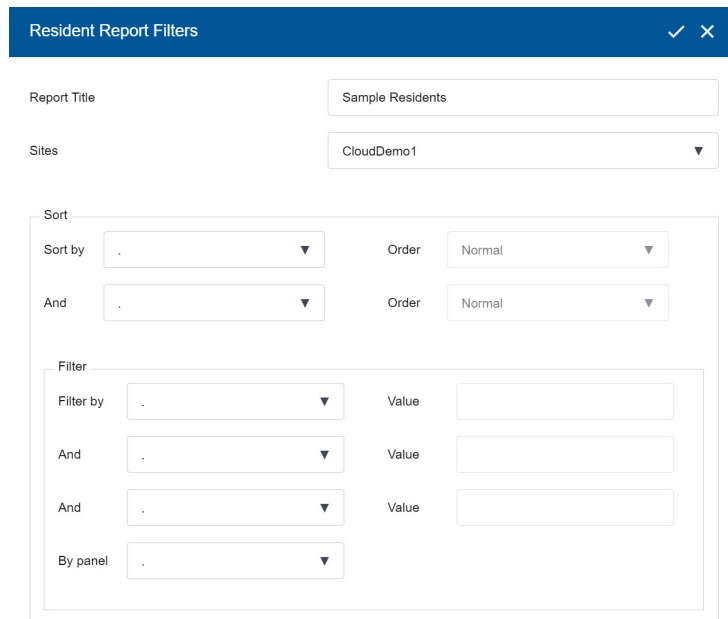
The **Resident Report** window appears.



Name	Dial code	Keyless code	Telephone	SIP username
Montague Romeo	95	0		
Montague Benvolio	94	0		
Martext Oliver	93	0		
Falstaff John	92	0		
Capulet Juliet	91	0		

Figure 158. Resident Report

- Click the **Edit** button  to edit the resident report.



Resident Report Filters

Report Title: Sample Residents

Sites: CloudDemo1

Sort

Sort by: Name Order: Normal

And: Name Order: Normal

Filter

Filter by: Name Value:

And: Name Value:

And: Name Value:

By panel: Name Value:

Figure 159. Resident Report Filters

- Provide information for the following:

Report Title. This will appear at the top of the report.

Sites. Select the site that should be included in the report.

Sort. Select up to 2 criteria to sort the report by.

For example, if you select **Apt No.** in the **Sort by** menu and **Name** in the **And** menu, then the report is sorted by apartment number, and for each apartment, the residents are sorted by name.

In the **Order** menu, select **Reverse** to sort the residents in the opposite direction.

Name	Apt #	Dial Code	Keyless Code	Telephone	Relay
Achilles	1	2348	0		1
Chiron	1	17	0		1
Hera	1	7349	0		1
Cronos	2	7643	0		1
Hades	2	9278	0		1
Persephone	2	792	0		1

Figure 160. Resident Report sorted by Apt# first and Name second

Filter. Select up to 4 criteria to filter by. The report shows only entries that begin with the criteria that you select.

For example, to show only residents whose names begin with **S** on panel 1, select **Name** in the **Filter by** menu, select **Panel 1** in the **By panel** menu, then type **S** in the **Value** field.

To show residents who have **S** anywhere in their names and who have **5** anywhere in their dial codes:

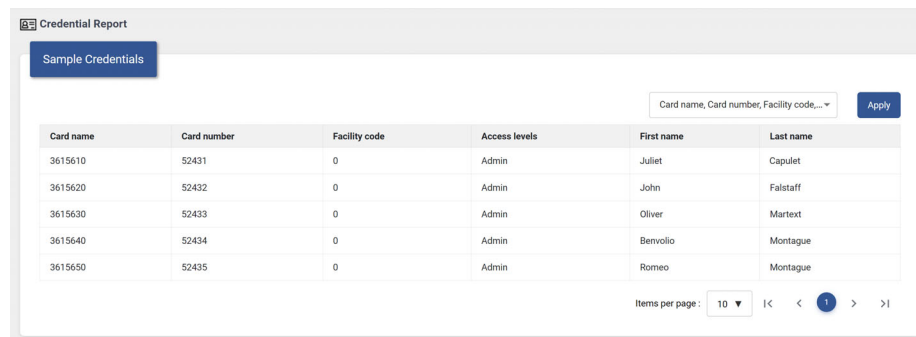
- Select **Name** in the **Filter by** menu, then type **S** in the **Value** field.
- Select **Dial Code** in the **And** menu, then type **5** in the **Value** field.

14.6 Credentials

You can generate a report of some or all of the credentials.

- Click **Credentials** in the **Reports** pane.

The Credential Report window appears.



Card name	Card number	Facility code	Access levels	First name	Last name
3615610	52431	0	Admin	Juliet	Capulet
3615620	52432	0	Admin	John	Falstaff
3615630	52433	0	Admin	Oliver	Martext
3615640	52434	0	Admin	Benvolio	Montague
3615650	52435	0	Admin	Romeo	Montague

Figure 161. Credential Report

2. Click the **Edit** button  to edit the credential report.

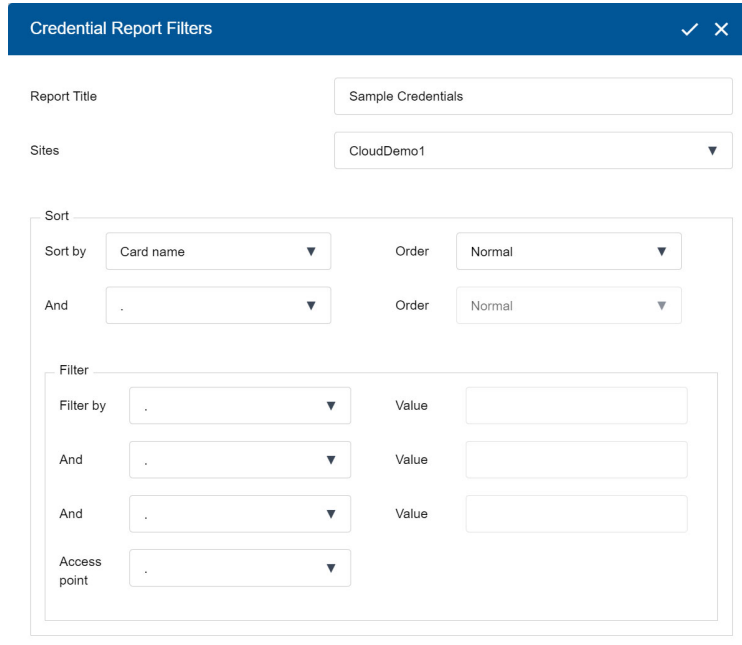


Figure 162. Credential Report Filters

3. Provide information for the following:

Report Title. This will appear at the top of the report.

Sites. Select the site that should be included in the report.

Sort. Select up to 2 criteria to sort the report by.

For example, if you select **Facility Code** in the **Sort by** menu and **Card Number** in the **And** menu, then the report is sorted by facility code, and for each facility code, the credentials are sorted by card number.

In the **Order** menu, select **Reverse** to sort the cards in the opposite direction.

Filter. Select up to 4 criteria to filter by. The report shows only entries that begin with the criteria that you select.

For example, to show only the cards whose facility codes begin with **1** on Reader A, select **Facility Code** in the **Filter by** menu, select **Reader A** in the **Access point** menu, and then type **1** in the **Value** field.

To show cards that have **1** anywhere in their facility codes and that have **2** anywhere in their card numbers:

- a. Select **Facility Code** in the **Filter by** menu, then type **1** in the **Value** field.

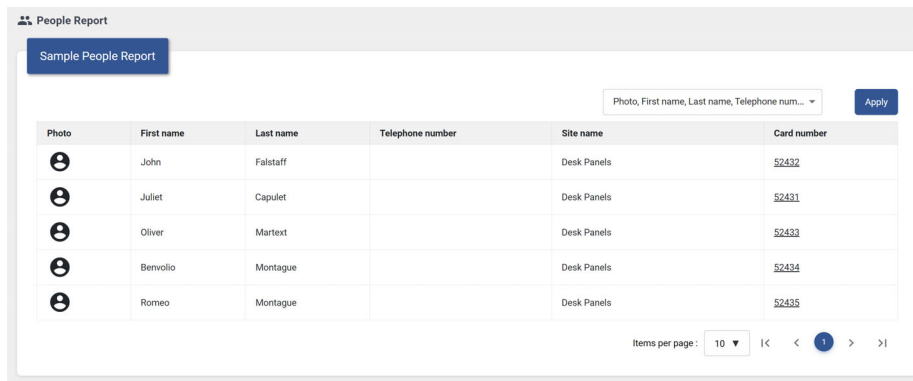
- b. Select **Card Number** in the **And** menu, then type **2** in the **Value** field.

14.7 People

You can generate a report of some or all of the people.

1. Click **People** in the Reports pane.






The **People Report** window appears.



People Report

Sample People Report

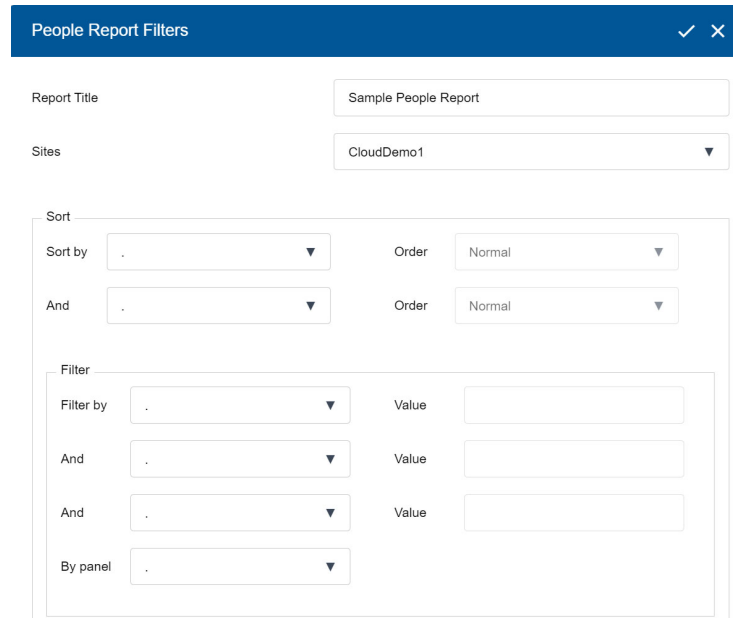
Photo, First name, Last name, Telephone num... Apply

Photo	First name	Last name	Telephone number	Site name	Card number
	John	Falstaff		Desk Panels	52432
	Juliet	Capulet		Desk Panels	52431
	Oliver	Martext		Desk Panels	52433
	Benvolio	Montague		Desk Panels	52434
	Romeo	Montague		Desk Panels	52435

Items per page: 10 < 1 > >|

Figure 163. People Report

2. Click the **Edit** button  to edit the People Report.



People Report Filters ✓ ✕

Report Title: Sample People Report

Sites: CloudDemo1 ▼

Sort

Sort by: . ▼ Order: Normal ▼

And: . ▼ Order: Normal ▼

Filter

Filter by: . ▼ Value:

And: . ▼ Value:

And: . ▼ Value:

By panel: . ▼

Figure 164. People Report Filters

3. Provide information for the following:

Report Title. This text will appear at the top of the report.

Sites. Select the site that should be included in the report.

Sort. Select up to 2 criteria to sort the report by.

For example, if you select **Apartment** in the **Sort by** menu and **First Name** in the **And** menu, then the report is sorted by apartment number, and for each apartment, the residents are sorted by name.

In the **Order** menu, select **Reverse** to sort the residents in the opposite direction.

Filter. Select up to 4 criteria to filter by. The report shows only entries that begin with the criteria that you select.

For example, to show only residents whose last names begin with **S** on panel 1, select **Last Name** in the **Filter by** menu, select **Panel 1** in the **By panel** menu, then type **S** in the **Value** field.

To show residents who have **S** anywhere in their names and who have **5** anywhere in their dial codes:

- a. Select **Name** in the **Filter by** menu, then type **S** in the **Value** field.
- b. Select **Dial Code** in the **And** menu, then type **5** in the **Value** field.

14.8 Paper Directory

You can a paper directory that you can display on a panel (for instance TX3-120C-A). The paper directory displays two pieces of information: the resident's name and the dial code. It can have 1, 2, or 3 columns per page.

1. Click **Paper Directory** on the left pane.

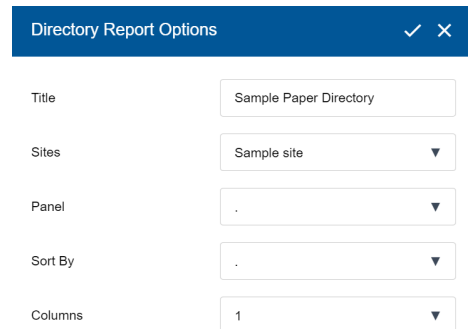
The Paper Directory Report window appears.



Figure 165. Paper Directory Report

2. Click the **Edit** button .

The **Directory Report Options** window appears.



Directory Report Options	
Title	Sample Paper Directory
Sites	Sample site ▼
Panel	. ▼
Sort By	. ▼
Columns	1 ▼

Figure 166. Directory Report Options

3. Provide information for the following:

Report Title. This will appear at the top of the report.

Sites. Select the site that should be included in the report.

Panel. Select the panel that will display this paper directory.

Sort By. Select the column, either **Resident Name** or **Dial Code**, to sort the directory by.

Columns. Select the number of columns. The report can have 1, 2, or 3 columns per page.

Olympus Towers					
NAME	DIAL	NAME	DIAL	NAME	DIAL
Achilles	2348	John Watson	3463	Tyndareus	784
Aeacus	4567	Juliet Capulet	6445	Uranus	793
Aegisthus	36	Julius Caesar	7456	Walter Shandy	234
Aerope	346	Junius Brutus	456	William Lucy	6464
Agamemnon	744	Laertes	556	Zeus	6742
Alcibiades	7654	Liz Shandy	2354		
Anne Bullen	463	Megapenthes	9		
Anthony Denny	5646	Menelaus	5664		
Antiolea	4363	Miltiades	76		
Aphrodite	73	Nicholas Vaux	4764		
Apollo	4562	Nicostratus	6		
Ares	742	Octavius Caesar	564		
Artemis	634	Odysseus	465		
Athena	2894	Oeneus	4		
Atreus	65	Oliver Martext	5644		
Bobby Shandy	4365	Patroclus	54		
Caius Cassius	364	Penelope	3465		
Caius Lucius	5353	Periboea	7		
Chiron	17	Persephone	792		
Cimon	67	Peter Quince	3454		
Clytaemnestra	56	Phorcys	5654		
Cronos	7643	Pleisthenes	657		
Decius Brutus	5634	Polyphides	47		
Deiphobus	57	Popilius Lena	5665		
Dionysus	7650	Proteus	49		
George Seacoal	3664	Rhea	745		
Hades	9278	Romeo Montague	3654		
Hephaestus	493	Sebastian Moran	6745		
Hera	7349	Telemachus	365		
Heracles	5976	Teucer	75		
Hermes	734	Thomas Vaughan	4564		
Jack Cade	643	Thucydides	765		
James Blunt	2543	Thyestes	48		
James Gurney	5645	Tobias Gregson	46		
James Soundpost	4654	Toby Shandy	2345		
James Tyrrell	646	Tristram Shandy	2342		
Jaques DeBoys	9569	Tullus Aufidius	2533		
John Falstaff	3564				

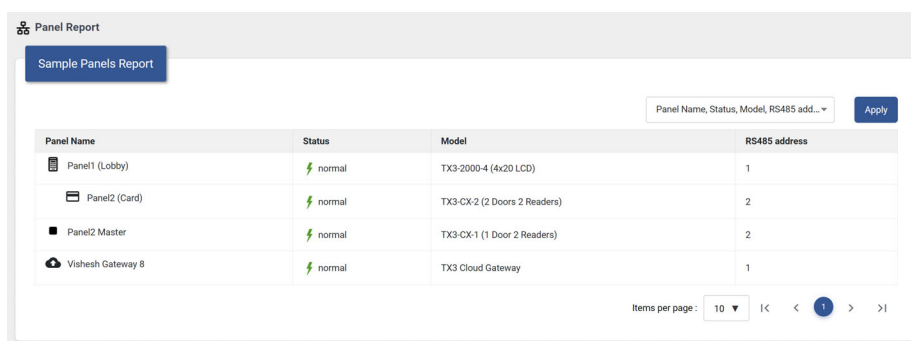
Figure 167. Paper Directory in a 3-column layout

14.9 Panels

You can generate a report of some or all of the panels.

1. Click **Panels** in the **Reports** pane.

The **Panel Report** window appears.



Panel Report

Sample Panels Report

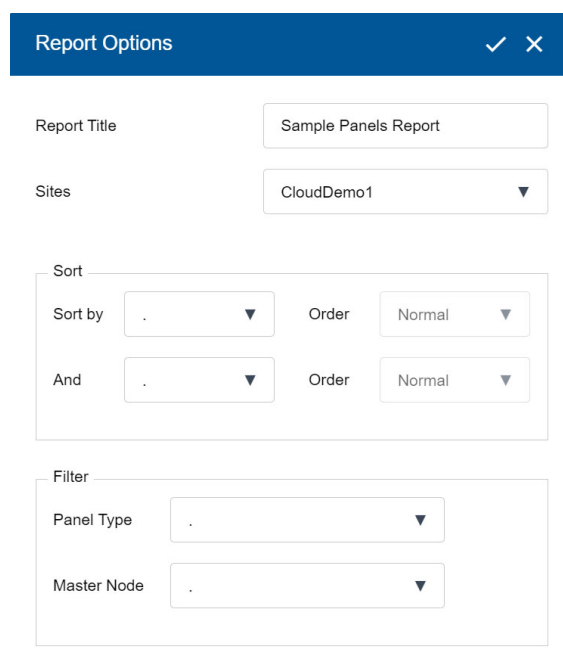
Panel Name, Status, Model, RS485 address... Apply

Panel Name	Status	Model	RS485 address
Panel1 (Lobby)	normal	TX3-2000-4 (4x20 LCD)	1
Panel2 (Card)	normal	TX3-CX-2 (2 Doors 2 Readers)	2
Panel2 Master	normal	TX3-CX-1 (1 Door 2 Readers)	2
Vishesh Gateway 8	normal	TX3 Cloud Gateway	1

Items per page: 10 < 1 >

Figure 168. Panel Report

2. Click the Edit button  to edit the panel report.



Report Options ✓ ✕

Report Title: Sample Panels Report

Sites: CloudDemo1 ▼

Sort

Sort by: . ▼ Order: Normal ▼

And: . ▼ Order: Normal ▼

Filter

Panel Type: . ▼

Master Node: . ▼

Figure 169. Panel Report Filters

3. Provide information for the following:

Report Title. This will appear at the top of the report.

Sites. Select the site that should be included in the report.

Sort. Select up to 2 criteria to sort the report by.

For example, if you select **Model** in the **Sort by** menu and **Panel Name** in the **And** menu, then the report is sorted by model, and for each model, the panels are sorted by name.

In the **Order** menu, select **Reverse** to sort the panels in the opposite direction.

Filter. Select up to 2 criteria to filter by. The report shows only entries that begin with the criteria that you select.

15 TX3 Networks with MiVision

15.1 Overview

The TX3 product suite consists of access control panels (telephone entry, card access and Touch Screen), the TX3 Cloud Gateway, and MiVision. The telephone and card access systems are the traditional keypad and card access type of entry systems.

Mircom devices such as the card access controller, the telephone entry unit, and the Touch Screen can be networked with the TX3 system through an Ethernet TCP/IP network, or a combination of Ethernet and RS-485 networks.

MiVision can connect to both of these network configurations.

Figure 170 shows a configuration with TX3 devices connected to an Ethernet TCP/IP network. The devices connected to an Ethernet TCP/IP network are called **main nodes**.

Note: In MiVision, the terms **Master** and **Main** are equivalent.

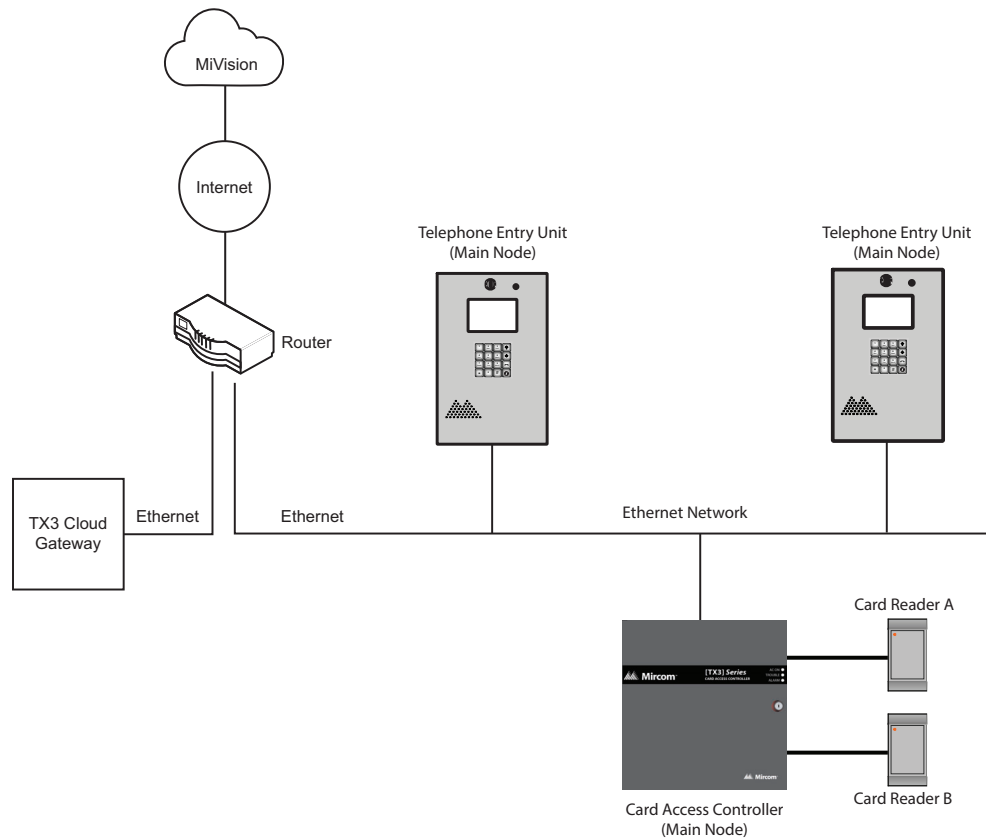


Figure 170. TX3 devices connected to an Ethernet TCP/IP network

Note: In order to connect MiVision to a TX3 network, the TX3 Cloud Gateway must be installed and activated as described in LT-6773 TX3 Cloud Gateway Installation Manual, available on <http://www.mircom.com>.

In order for a panel that is not a Touch Screen to be a main node, it must have a TX3-IP IP Module installed.

Figure 171 shows a configuration with TX3 devices connected on both an Ethernet TCP/IP network and on RS-485 subnetworks. Devices connected to a main node's RS-485 subnetwork are **secondary nodes** to the main node. Each RS-485 subnetwork can have up to 63 devices connected to it.

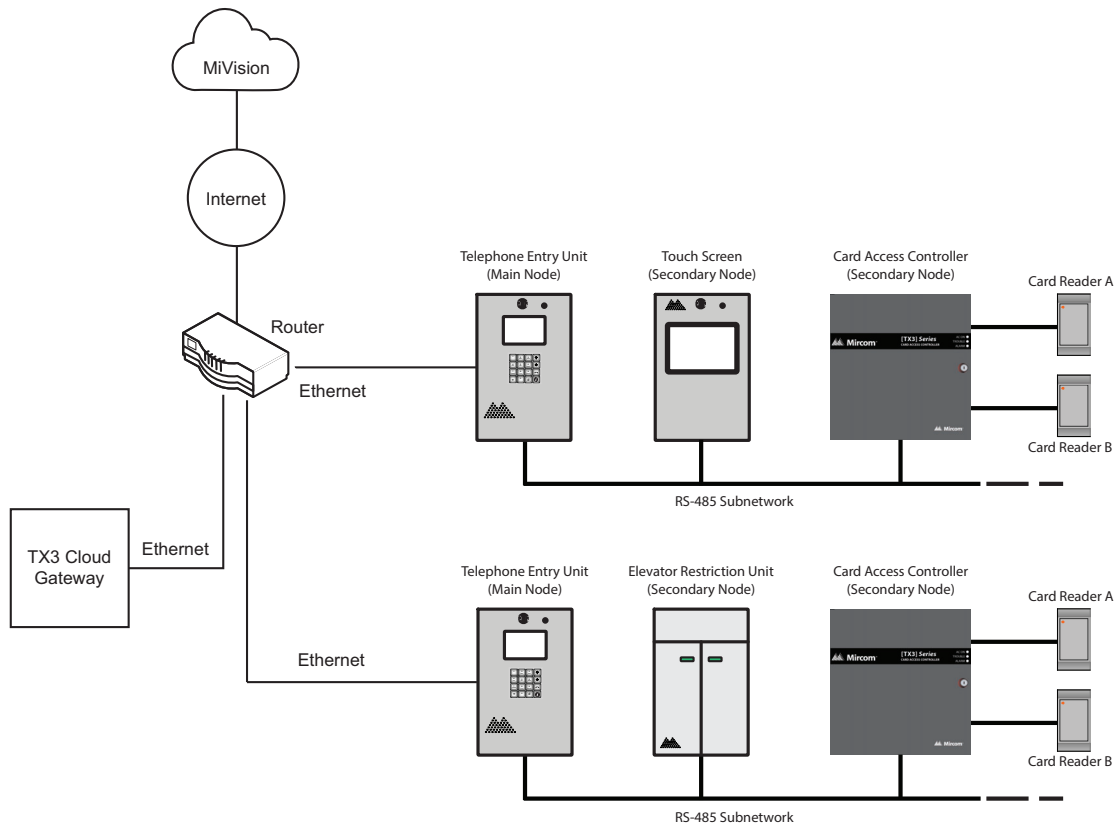


Figure 171. TX3 devices connected to a combination Ethernet TCP/IP network with RS-485 subnetworks

Note: In order to connect MiVision to a TX3 network, the TX3 Cloud Gateway must be installed and activated as described in LT-6773 TX3 Cloud Gateway Installation Manual, available on <http://www.mircom.com>.

There can only be **one** main node on an RS-485 subnetwork. That is, you cannot connect one RS-485 subnetwork to another RS-485 subnetwork. However, if you want to connect to a Touch Screen panel remotely over the Internet (for instance, to enable the advertising module), the Touch Screen panel must be set as a main node even if there is no secondary panel connected to it.

15.1.1 TCP/IP Ports

In order for your TX3 system to communicate over a TCP/IP network, the following ports **must** be available for the TX3 system.

Touch Screens: 8080

Non-Touch Screens:

- 14000
- 14001
- 14002
- 14003

If you are using a TCP/IP network and your TX3 system is not communicating properly, there may be another program on the network using ports 8080 or 14000-14003. In this case, configure the other program to use a different range of ports.

15.1.2 ADC and NSL Capability

Touch Screen and the telephone entry system support full ADC and NSL telephone connectivity for a single panel or a networked system of panels. A single panel supports up to five ADC and/or NSL telephone lines.

An ADC connection requires a dedicated subscriber telephone line service connected to an outside telephone line. This connection lets the visitor call the tenant and access their voice mail.

An NSL type connection uses the existing building telephone lines for communication and does not require an outside telephone line. The NSL units intercept all telephone lines into the building's suites and communicate directly to the resident phone. This connection lets the visitor call the tenant and access their voice mail and call waiting.

15.1.3 Card Formats Supported by the Card Access System

- 26-bit Wiegand SIA
- 32-bit CSN
- 34-bit Awid
- 35-bit HID corporate 1000
- 35-bit Indala
- 36-bit HID Simplex
- 36-bit Keyscan C15001
- 37-bit Cansec

- 37-bit HID 10304
- 37-bit Mircom
- 39-bit Kantech XSF
- 50-bit RBH

15.2 MiVision and the Touch Screen

Use MiVision to perform all configurations on the TX3 system, except for the features listed below. In order to access the features below, you must log into the Touch Screen itself.

- Set the Touch Screen administrator password
- Save Touch Screen log files
- Change the appearance of a Touch Screen Secondary Node (a Touch Screen Secondary Node is a Touch Screen connected by RS-485). You can only change the appearance of a Touch Screen Secondary Node by logging in to the Touch Screen either at the terminal or by using Remote Desktop.
- Test themes
- Enable the Advertising Module
- Print an advertising report
- Calibrate the Touch Screen

To access one of these features, log into the Touch Screen as described in LT-995 available on <http://www.mircom.com>.

For all other configurations, use MiVision.

15.3 Administrator's Responsibilities



Warning! In order to keep the TX3 system secure, follow these precautions:

Change the default password on the Touch Screen to prevent strangers from accessing the configuration. See LT-995.

Perform a virus scan on all picture and video files before importing them into MiVision.

Secure the TCP/IP network to prevent unauthorized access to the Touch Screen.

Do not forward the Remote Desktop port of the Touch Screen to the Internet.

15.4 Additional Documentation

These documents are available on <http://www.mircom.com>.

- LT-6773 TX3 Cloud Gateway Installation Manual
- LT-995 TX3 System Configuration and Administration Manual
- LT-969 TX3 Telephone Access System Installation and Operation Manual
- LT-980 TX3 CX Card Access System Manual
- LT-996 TX3 Touch Screen Installation Manual
- LT-6638 TX3 MiEntry Manual
- LT-6082 Unified Building Solution Administration Guide

16

Compatible Products

MiVision is compatible with the following products.

TX3 Product	Firmware and Software Version
TX3-ER-8-A TX3-ER-8-B	SO-468 3.7.128 or higher SO-254 3.7.x or higher
TX3-120U-C TX3-200-8U-C TX3-1000-8U-C TX3-2000-8U-C TX3-2000-8UR-C TX3-200-4U-C TX3-1000-4U-C TX3-2000-4U-C TX3-2000-4UR-C TX3-120C-C TX3-200-8C-C TX3-1000-8C-C TX3-2000-8C-C TX3-2000-8CR-C TX3-EMER-1S-C TX3-EMER-200KS-C	SO-466 3.8.112 or higher SO-253 3.7.x or higher
TX3-CX-2K-A TX3-CX-4K-A TX3-CX-6K-A TX3-CX-8K-A TX3-CX-2-A TX3-CX-1 TX3-CX-1NP	SO-465 3.7.112 or higher SO-252 3.7.x or higher
TX3-TOUCH-S15-D TX3-TOUCH-F15-D	SO-440 V3.x.x or higher MSW-026 Touch Screen software 3.1 or higher
TX3-TOUCH-S15-E TX3-TOUCH-F15-E	SO-470 V3.x.x or higher MSW-026 Touch Screen software 3.1 or higher
TX3-TOUCH-S22-D TX3-TOUCH-F22-D TX3-TOUCH-S22-E TX3-TOUCH-F22-E	SO-441 V3.x.x or higher MSW-026 Touch Screen software 3.1 or higher
TX3-TOUCH-S22-F TX3-TOUCH-F22-F	SO-472 V3.x.x or higher MSW-026 Touch Screen software 3.1 or higher
TX3-TOUCH-S15B-WR TX3-TOUCH-S15S-WR	SO-411 V3.x.x or higher MSW-026 Touch Screen software 3.1 or higher
TX3-TOUCH-S15B-WR-A TX3-TOUCH-S15S-WR-A	SO-478 V3.x.x or higher MSW-026 Touch Screen software 3.1 or higher

17

Configurable Touch Screen User Interface Elements

The following tables describe the Touch Screen user interface elements that can be customized (section 4).

Table 2: Call Button

Element	Description
Call button border color	Call button border color
Call button color	Call button color
Call button font	Font used for call button
Call button font color	Font color used for call button
Call button shade	Call button shade

Table 3: Call Reception

Element	Description
Reception button border color	Call reception button border color
Reception button color	Call reception button color
Reception button font color	Font color used for call reception button
Reception button font	Font used for call reception button
Reception button shade	Call reception button shade

Table 4: General

Element	Description
Event screen back color	Background color of the event screen that appears when calling a resident
Event screen button color	Color of the button on the event screen that appears when calling a resident

Table 4: General (Continued)

Element	Description
Event screen font color	Color of the font that is used in the event screen that appears when calling a resident
Event screen font	Font that is used in the event screen that appears when calling a resident
Invalid name/dial code back color	Background color of the box that appears when an invalid resident name or dial code is entered
Invalid name/dial code font color	Color of the font used for the box that appears when an invalid resident name or dial code is entered
Invalid name/dial code font	Font used for the box that appears when an invalid resident name or dial code is entered
Keyboard back color	Background color of the keyboard
Main screen back color	Background color of the main screen

Table 5: Help Button

Element	Description
Help button border color	Help / Information button border color
Help button color	Help / Information button color
Help button font color	Font color used for help / information button
Help button font	Font used for help / information button
Help button shade	Help / Information button shade

Table 6: Keyboard Buttons

Element	Description
Letter button border color	Border color of all keyboard letter (alphabetic) buttons
Letter button color	Color of all keyboard letter (alphabetic) buttons
Letter button font	Font used for all keyboard letter (alphabetic) buttons
Letter button shade	Button shade of all keyboard letter (alphabetic) buttons
Num button border color	Border color of all keyboard numeric buttons
Num button color	Color of all keyboard numeric buttons
Num button font color	Font color used for all keyboard numeric buttons
Num button font	Font used for all keyboard numeric buttons
Num button shade	Button shade of all keyboard numeric buttons
Letter button font color	Font color used for all keyboard letter (alphabetic) buttons

Table 7: Leave Message Button

Element	Description
Msg. button border color	Leave message button border color
Msg. button color	Leave message button color
Msg. button font color	Font color used for leave message button
Msg. button font	Font used for leave message button
Msg. button shade	Leave message button shade

Table 8: Miscellaneous

Element	Description
Clock hour color	Color of the hour hand for the analogue clock
Clock minute color	Color of the minute hand for the analogue clock
Clock sec. color	Color of the second hand for the analogue clock
Clock ticks color	Color of the ticks for the analogue clock
Date font color	Color of the date font
Date font	Font used for the date label
Dial code font color	Font color used for dial code label found in the resident detail box
Dial code font	Font used for dial code label found in the resident detail box
Info box border color	Border color used for the title of the information box
Info box font color	Font color used for the title of the information box
Info box font	Font used for the title of the information box
Res. box border color	Border color used for the resident directory box,
Res. box font color	Font color used for the title of the resident directory box
Res. detail box font	Font used for the title of the resident detail box
Res. detail box border color	Border color used for the resident detail box
Res. detail box color	Font color used for the title of the resident detail box
Search box color	Search text box background color
Search box font color	Search text box font color
Search box font	Search text box font

Table 9: Resident Group

Element	Description
Group button border color	Border color of the group button
Group button color	Color of the group button
Group button font	Font used in the group button
Group button font color	Color of font used in the group button
Group button selected color	Color of button when selected

Table 10: Residents

Element	Description
Alternate highlight color	Color of alternate rows when selected
Back color	Background color (Recommended: Use same as Main Screen background color)
Column size	Size of dial code column (The resident name column is adjusted automatically)
Column title back color	Background color of the column title
Column title font color	Color of the font used in column title
Column title font	Font used for the column title
Column title text align	Text alignment of the column title
Font color	Color of font used for resident names and dial codes
Font	Font used for resident names and dial codes
Grid color	Color of grid lines separating rows and columns
Highlight color	Color of row when selected
Highlight font color	Color of font used for resident name and dial code when selected

Table 10: Residents (Continued)

Element	Description
Row size	Size of rows that hold resident names and dial codes
Text alignment	Text alignment for resident names and dial codes
Alternate highlight color	Color of alternate rows when selected

Table 11: Scroll Up Down Buttons

Element	Description
Scroll border color	Border color for scroll up and down buttons
Scroll button color	Button color for scroll up and down buttons
Scroll button shade	Button shade for scroll up and down buttons

Table 12: Show Flash Button

Element	Description
Flash button border color	Show flash banner button border color
Flash button color	Show flash banner button color
Flash button font color	Font color used for show flash banner button
Flash button font	Font used for show flash banner button
Flash button shade	Show flash banner button shade

18

Warranty and Warning Information

WARNING!

Please read this document **CAREFULLY**, as it contains important warnings, life-safety, and practical information about all products manufactured by the Mircom Group of Companies, including Mircom and Secutron branded products, which shall include without limitation all fire alarm, nurse call, building automation and access control and card access products (hereinafter individually or collectively, as applicable, referred to as “**Mircom System**”).

NOTE TO ALL READERS:

1. **Nature of Warnings.** The within warnings are communicated to the reader out of an abundance of caution and create no legal obligation for Mircom Group of Companies, whatsoever. Without limiting the generality of the foregoing, this document shall NOT be construed as in any way altering the rights and obligations of the parties, governed by the legal documents that apply in any given circumstance.
2. **Application.** The warnings contained in this document apply to all Mircom System and shall be read in conjunction with:
 - a. the product manual for the specific Mircom System that applies in given circumstances;
 - b. legal documents that apply to the purchase and sale of a Mircom System, which may include the company’s standard terms and conditions and warranty statements;
 - c. other information about the Mircom System or the parties’ rights and obligations as may be application to a given circumstance.
3. **Security and Insurance.** Regardless of its capabilities, no Mircom System is a substitute for property or life insurance. Nor is the system a substitute for property owners, renters, or other occupants to act prudently to prevent or minimize the harmful effects of an emergency situation. Building automation systems produced by the Mircom Group of Companies are not to be used as a fire, alarm, or life-safety system.

NOTE TO INSTALLERS:

All Mircom Systems have been carefully designed to be as effective as possible. However, there are circumstances where they may not provide protection. Some reasons for system failure include the following. As the only individual in contact with system users, please bring each item in this warning to the attention of the users of this Mircom System. Failure to properly inform system end-users of the circumstances in which the system might fail may result in over-reliance upon the system. As a result, it is imperative that you properly inform each customer for whom you install the system of the possible forms of failure:

4. **Inadequate Installation.** All Mircom Systems must be installed in accordance with all the applicable codes and standards in order to provide adequate protection. National standards require an inspection and approval to be conducted by the local authority having jurisdiction following the initial installation of the system and following any changes to the system. Such inspections ensure installation has been carried out properly.
5. **Inadequate Testing.** Most issues and/or problems that would prevent a Mircom System alarm from operating as intended, can be identified through regular testing and maintenance. The complete system should be tested by the local authority having jurisdiction immediately after a fire, storm, earthquake, accident, or any kind of construction activity inside or outside the premises. The testing should include all sensing devices, keypads, consoles, alarm indicating devices and any other operational devices that are part of the system.

NOTE TO USERS:

All Mircom Systems have been carefully designed to be as effective as possible. However, there are circumstances where they may not provide protection. Some reasons for system failure include the following. The end user can minimize the occurrence of any of the following by proper training, testing and maintenance of the Mircom Systems:

6. **Inadequate Testing and Maintenance.** It is imperative that the systems be periodically tested and subjected to preventative maintenance. Best practices, local codes, applicable laws and industry regulations, and any local authority having jurisdiction to do so, determine the frequency and type of testing that is required at a minimum. Mircom System may not function properly, and the occurrence of other system failures identified below may not be minimized, if the periodic testing and maintenance of Mircom Systems is not completed with diligence and as required.
7. **Improper Operation.** It is important that all system users be trained in the correct operation of the alarm system and that they know how to respond when the system indicates an alarm. A Mircom System may not function as intended during an emergency situation where the user is unable to operate

a panic or emergency switch by reason of permanent or temporary physical disability, inability to reach the device in time, unfamiliarity with the correct operation, or related circumstances.

8. **Insufficient Time.** There may be circumstances when a Mircom System will operate as intended, yet the occupants will not be protected from the emergency due to their inability to respond to the warnings in a timely manner. If the system is monitored, the response may not occur in time enough to protect the occupants or their belongings.
9. **Carelessness or Safety Hazards.** Moreover, smoke detectors may not provide timely warning of fires caused by carelessness or safety hazards such as smoking in bed, violent explosions, escaping gas, improper storage of flammable materials, overloaded electrical circuits or children playing with matches or arson.
10. **Power Failure.** Some Mircom System components require adequate electrical power supply to operate. Examples include: smoke detectors, beacons, HVAC, and lighting controllers. If a device operates only by AC power, any interruption, however brief, will render that device inoperative while it does not have power. Power interruptions of any length are often accompanied by voltage fluctuations which may damage Mircom Systems or other electronic equipment. After a power interruption has occurred, immediately conduct a complete system test to ensure that the system operates as intended.
11. **Battery Failure.** If the Mircom System or any device connected to the system operates from batteries it is possible for the batteries to fail. Even if the batteries have not failed, they must be fully charged, in good condition, and installed correctly. Some Mircom Systems use replaceable batteries, which have a limited life-span. The expected battery life is variable and in part dependent on the device environment, usage and type. Ambient conditions such as high humidity, high or low temperatures, or large temperature fluctuations may reduce the expected battery life. Moreover, some Mircom Systems do not have a battery monitor that would alert the user in the event that the battery is nearing its end of life. Regular testing and replacements are vital for ensuring that the batteries function as expected, whether or not a device has a low-battery monitor.
12. **Physical Obstructions.** Motion sensors that are part of a Mircom System must be kept clear of any obstacles which impede the sensors' ability to detect movement. Signals being communicated by a Mircom System may not reach the receiver if an item (such as metal, water, or concrete) is placed on or near the radio path. Deliberate jamming or other inadvertent radio signal interference can also negatively affect system operation.
13. **Wireless Devices Placement Proximity.** Moreover all wireless devices must be a minimum and maximum distance away from large metal objects, such as refrigerators. As the end user, you are required to consult the specific Mircom System manual and application guide for any maximum distances required between devices and suggested placement of wireless devices for optimal functioning.

14. **Failure to Trigger Sensors.** Moreover, Mircom Systems may fail to operate as intended if, motion, heat, carbon monoxide (CO) and/or smoke sensors, are not triggered.
 - a. Sensors in a fire system may fail to be triggered when the fire is in a chimney, walls, roof, or on the other side of closed doors. Smoke and heat detectors may not detect smoke or heat from fires on another level of the residence or building. In this situation the control panel may not alert occupants of a fire.
 - b. Sensors in a nurse call system may fail to be triggered when movement is occurring outside of the motion sensors' range. For example, if movement is occurring on the other side of closed doors or on another level of the residence or building the motion detector may not be triggered. In this situation the central controller may not register an alarm signal.
15. **Interference with Audible Notification Appliances.** Audible notification appliances may be interfered with by other noise sources such as stereos, radios, televisions, air conditioners, appliances, or passing traffic. Audible notification appliances, however loud, may not be heard by a hearing-impaired person.
16. **Other Impairments.** Alarm notification appliances such as sirens, bells, horns, or strobes may not warn or waken a sleeping occupant if there is an intervening wall or door. It is less likely that the occupants will be alerted or awakened when notification appliances are located on a different level of the residence or premise.
17. **Software Malfunction.** Most Mircom Systems contain software. No warranties are provided as to the software components of any products or stand-alone software products within a Mircom System. For a full statement of the warranties and exclusions and limitations of liability please refer to the company's standard Terms and Conditions and Warranties.
18. **Telephone Line/Network Malfunction.** Telephone service can cause system failure where telephone lines/networks are relied upon by a Mircom System. Alarms and information coming from a Mircom System may not be transmitted if a phone line/network is out of service or busy for a certain period of time. Alarms and information may not be transmitted where telephone lines/networks have been compromised by criminal tampering, local construction, storms or earthquakes.
19. **Component Failure.** Although every effort has been made to make this Mircom System as reliable as possible, the system may fail to function as intended due to the failure of a component.

20. **Integrated Products.** Mircom System might not function as intended if it is connected to a non-Mircom product or to a Mircom product that is deemed non-compatible with a particular Mircom System. A list of compatible products can be requested and obtained.
21. A Mircom System's Auto Configuration feature is intended to assign the Alarm process type to all inputs and to provide an initial set up by detecting connected devices and generates a basic job configuration upon the initial installation of the Mircom System. Mircom makes no representations, warranties or guarantees regarding the accuracy or suitability of the basic job configuration generated upon installation, for any specific site requirements.
The end user shall be solely and exclusively responsible to thoroughly review the basic job generated by the auto configuration feature upon initial installation and to implement necessary adjustments and modifications to customize the job configuration in accordance with the functional and/or technical requirements of the site. Mircom expressly disclaims any responsibility or liability for any failure, malfunction or defective operation of a Mircom System and any associated components, resulting from the end user's failure to customize or adjust the job configuration accordingly.
By installing and utilizing the Mircom System, the user acknowledges and agrees that Mircom shall not be liable for any claims, losses, damages, or defects arising from the failure of the user or installer and those for whom it is responsible at law, to customize the basic job configuration generated on the initial set-up in accordance with the requirements of the site.

Warranty

Purchase of all Mircom products is governed by:

<https://www.mircom.com/product-warranty>

<https://www.mircom.com/purchase-terms-and-conditions>

<https://www.mircom.com/software-license-terms-and-conditions>