TX3 Series

TX3 Vision Manual

TX3 Vision Manual Version 3

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

Contents

1 Introduction

TX3 Vision is a cloud-based configuration tool designed for managing all controllers within a TX3 network. It utilizes the TX3 Cloud Gateway box to establish a connection between on-site TX3 controllers and TX3 Vision.

This manual provides information about the configuration of TX3 Vision, and must be read in its entirety before beginning any configuration work.

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

For warranty and special notices see the Warranty and Special Notices chapter on page 73.

1.1 TX3 Vision Features

TX3 Vision offers all the features of the TX3 PC Configurator, along with additional features such as maps and charts.

1.2 Administrator’s Responsibilities

Warning! In order to keep the TX3 system secure, follow these precautions:

Perform a virus scan on all picture and video files before importing them into TX3 Vision.

Secure the TCP/IP network to prevent unauthorized access to TX3 Vision.

1.3 Additional Documentation

These documents are available on **http://www.mircom.com**.

- LT-995 TX3 System Configuration and Administration Manual
- LT-1194 TX3 Nano Configuration Manual
- LT-6638 TX3 MiEntry Manual
- LT-969 TX3 Telephone Access System Installation and Operation Manual
- LT-6082 Unified Building Solution Administration Guide

2 TX3 Vision

This chapter provides an overview of TX3 Vision.

2.1 Requirements

TX3 Vision works with all browsers but the following browsers are recommended:

- Microsoft Edge on Windows
- Google Chrome on Windows

See Section 6 for a list of compatible TX3 products.

2.2 Log into TX3 Vision

1. Open a Web browser on your computer.
2. Type **tx3vision.mircom.com** and then press Enter.

   The Login page appears.

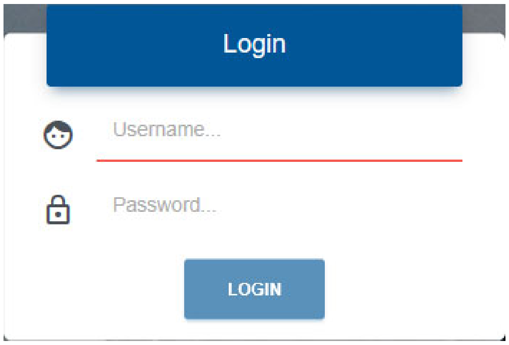


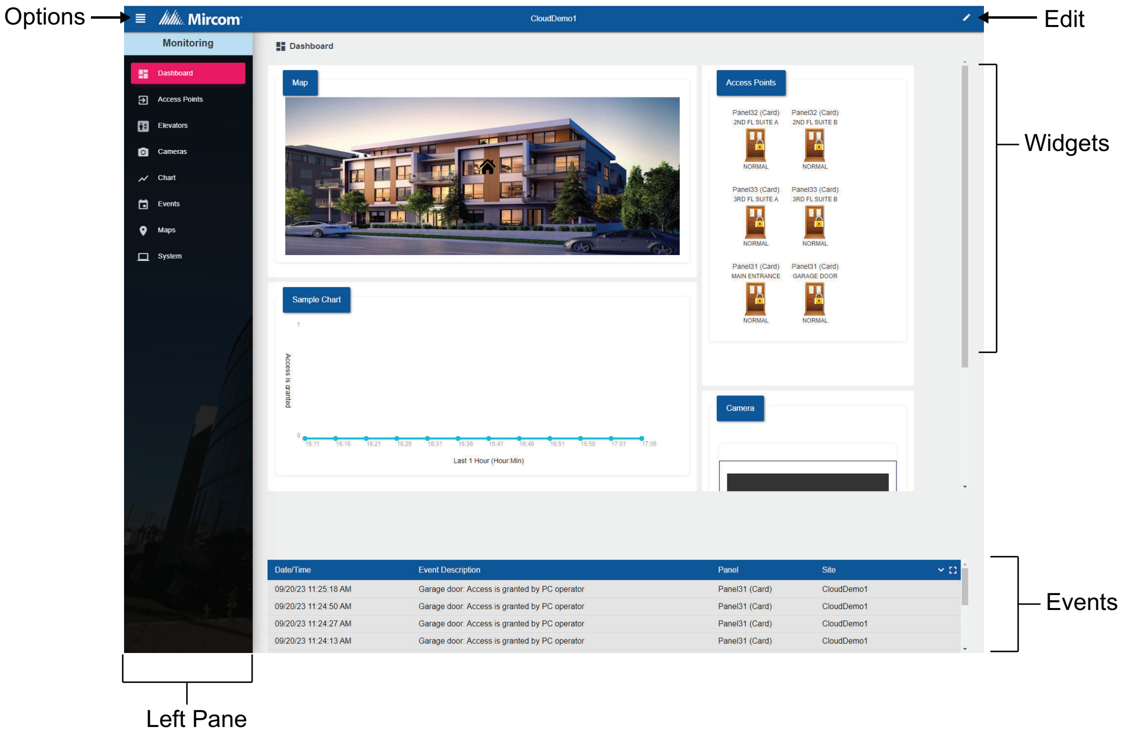
Figure 1. Login page

3. Enter the username and password for TX3 Vision.

   The list of sites appears. A site corresponds to a job in the TX3 PC Configurator.

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

The TX3 Vision Dashboard appears.



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 2. TX3 Vision Dashboard

By default it shows the Monitoring section. Click the Options menu in the upper left corner to access these options:

- Sites
- Monitoring - page 14
- Configuration - page 30
- Reports - page 60
- Tools
- Language
- Help
- Log Out

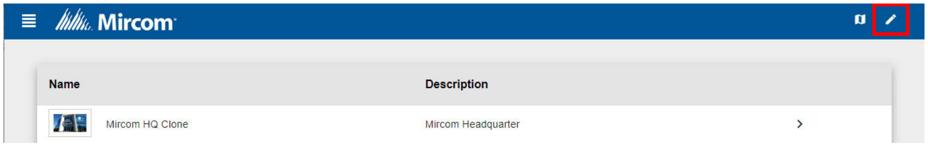
Monitoring, Configuration and Reports are explained in the following chapters. The other options are explained below.

2.3 Sites

Sites is a list of configured sites. A site corresponds to a job in the TX3 PC Configurator.

2.3.1 Edit Sites

1. To edit your sites in the Sites window, click the pencil icon in the upper right.

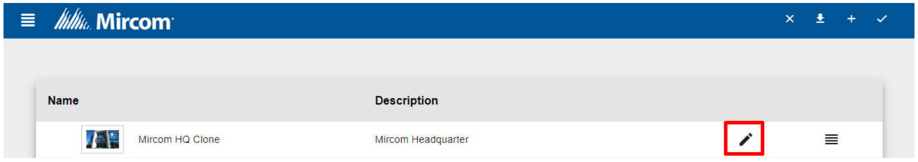


Name	Description
Mircom HQ Clone	Mircom Headquarter

Figure 3. Edit Sites button

A pencil icon appears beside each site.

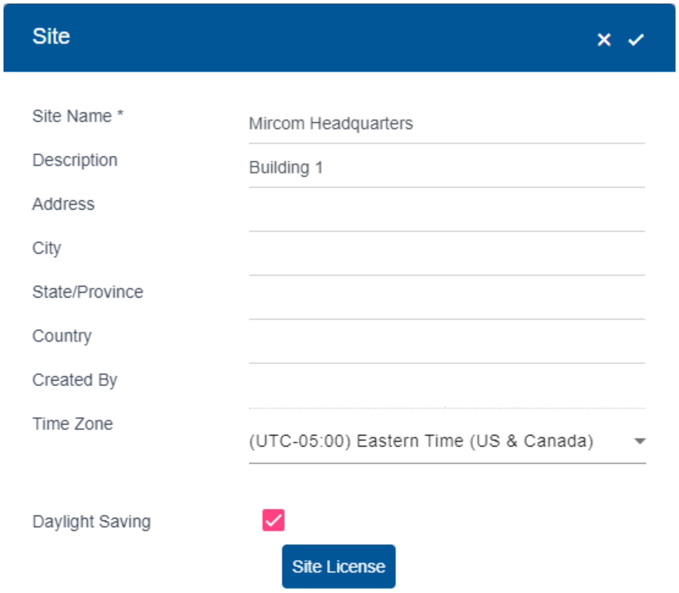
2. Click the pencil icon for the site that you want to edit.



Name	Description
Mircom HQ Clone	Mircom Headquarter

Figure 4. Edit Sites icon

A window for the site appears.



Site

Site Name * Mircom Headquarters

Description Building 1

Address

City

State/Province

Country

Created By

Time Zone (UTC-05:00) Eastern Time (US & Canada)

Daylight Saving ☑

Figure 5. Site window

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

Description. Enter a description of the site.

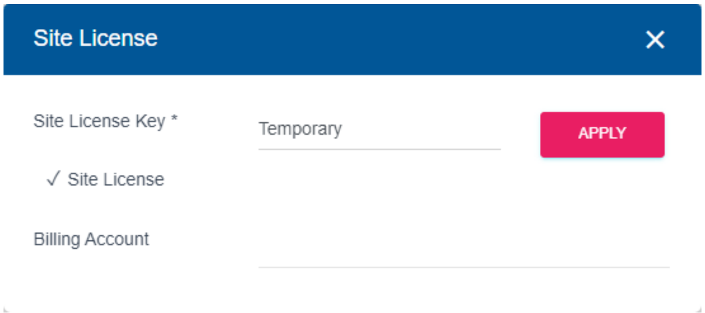
Address. Enter the site's address.

Time Zone. Specify the site's time zone.

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

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

Note: Each site requires a license key in order for TX3 Vision to communicate with the site.



Site License ✕

Site License Key * Temporary APPLY

✓ Site License

Billing Account

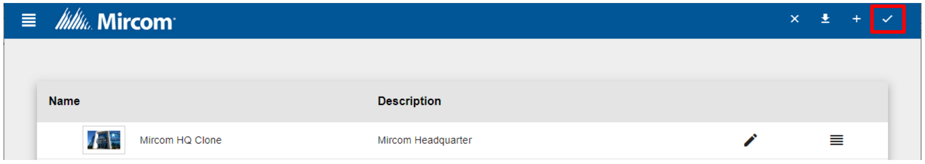
Figure 6. Site License

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

Billing Account. This field is read-only.

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

4. When you are finished editing sites, click the Done button ✓ in the upper right corner of the Sites window.



≡ Mircom × ⭳ + ✓

Name	Description
Mircom HQ Clone	Mircom Headquarter

Figure 7. Done button in the Edit Sites window

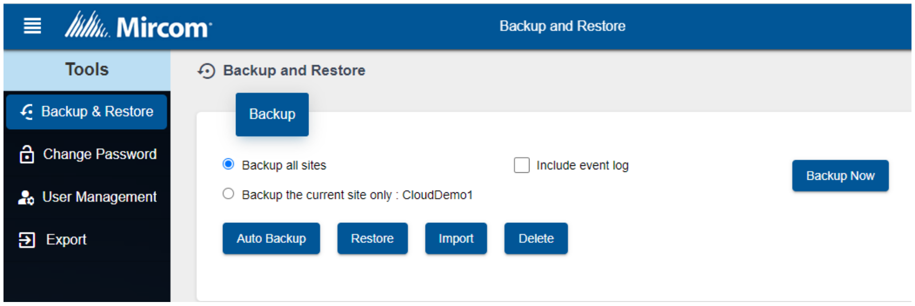
2.4 Tools

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

- Backup & Restore
- Change Password
- User Management
- Export

2.4.1 Backup & Restore

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



● Backup all sites
○ Backup the current site only : CloudDemo1
□ Include event log

Figure 8. Backup and Restore

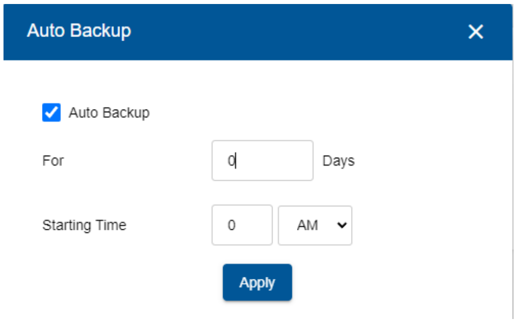
1. Click the menu in the upper left corner.
2. Select **Tools**.
3. Click **Backup & Restore**.

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.

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



☑ Auto Backup
For 0 Days
Starting Time 0 AM

Figure 9. Auto Backup

For. Enter the number of days that the backup should be performed for. For example, **For 5 Days** means that TX3 Vision will conduct a backup every day for 5 days, and then stop.

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

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 TX3 Vision.

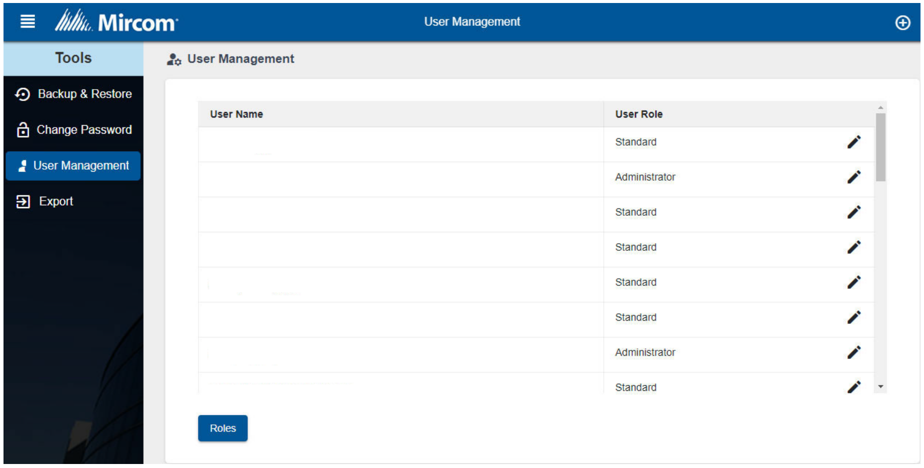
Delete. Click this button to delete a backup.

2.4.2 Change Password

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

2.4.3 User Management

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



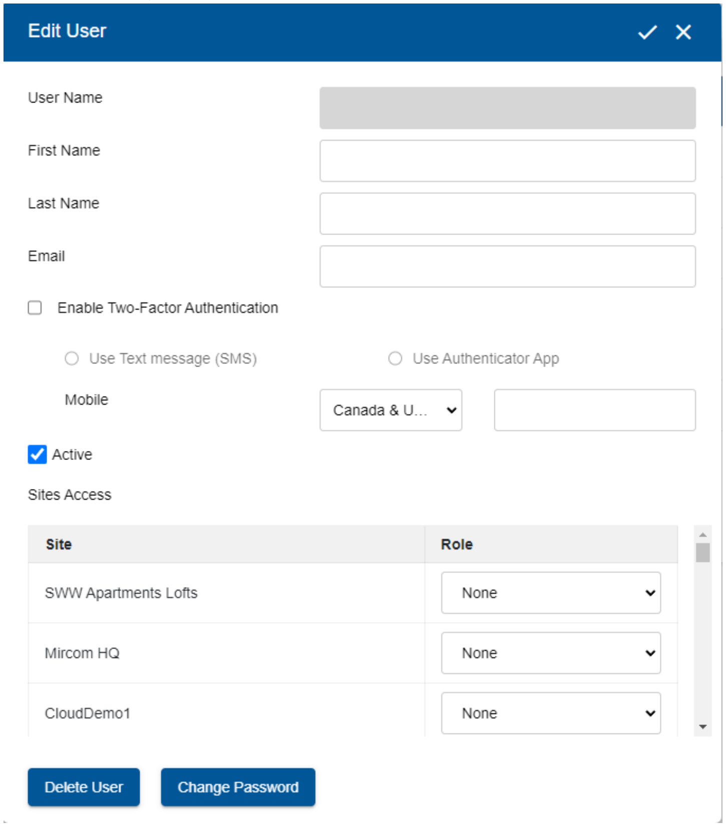
User Name	User Role
	Standard
	Administrator
	Standard
	Standard
	Standard
	Standard
	Administrator
	Standard

Figure 10. User Management

Note: When you create a new user, TX3 Vision creates a temporary password, and forces the user to change the password the first time they log in.

1. Click the menu 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.



Edit User ✓ ✕

User Name

First Name

Last Name

Email

□ Enable Two-Factor Authentication

○ Use Text message (SMS) ○ Use Authenticator App

Mobile Canada & U...

☑ Active

Sites Access

Site	Role
SWW Apartments Lofts	None
Mircom HQ	None
CloudDemo1	None

Figure 11. Edit User

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

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

Email. The user’s email address.

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.When a user logs in and two-factor authentication is enabled, TX3 Vision will request a code that the user receives to verify their identity.

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.)

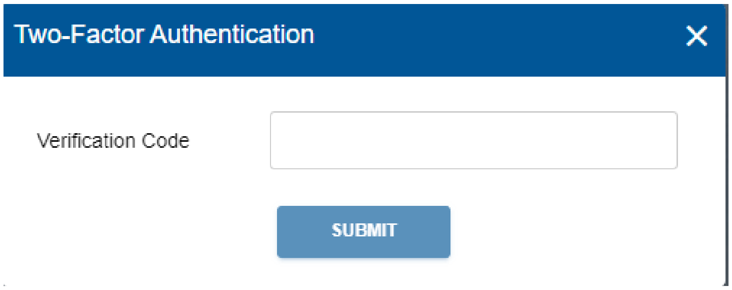
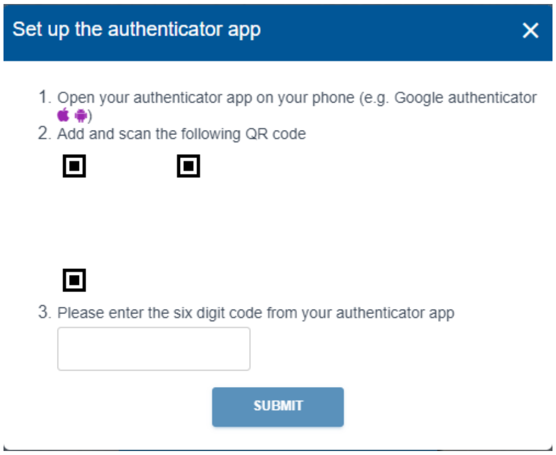


Figure 12. Two-Factor Authentication: text message

- 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.



1. Open your authenticator app on your phone (e.g. Google authenticator)
2. Add and scan the following QR code
3. Please enter the six digit code from your authenticator app

Figure 13. 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.

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 2.4.4.

Delete User. Delete this user.

Change Password. Change the password for this user.

2.4.4 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 but with basic site administration permissions.

Advanced user. The same as User but with advanced site administration permissions.

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

Administrator. The user has complete access to the site.

2.4.5 Export

This option exports the current job in a format for use by OpenGN.

2.5 Language

1. Click the 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.

2.6 Help

Contact information for Mircom technical support is provided here.

2.7 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 TX3 Vision.

3 Monitoring

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

3.1 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.

3.1.1 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.

3.1.2 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. ✎ —

   Click the Delete button — to remove the widget. This action cannot be reverted even if you click Cancel.

3.1.3 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.

   Not all options are editable, 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.

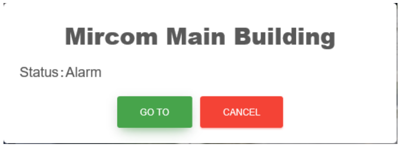
4. Click the Done button ✓ in the upper right corner to save your changes.
5. Or click the Cancel button ☒ to go back to the dashboard without saving.

3.1.4 View an Event on a Map Widget

Each building is represented on the site map with the 🏠 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**.

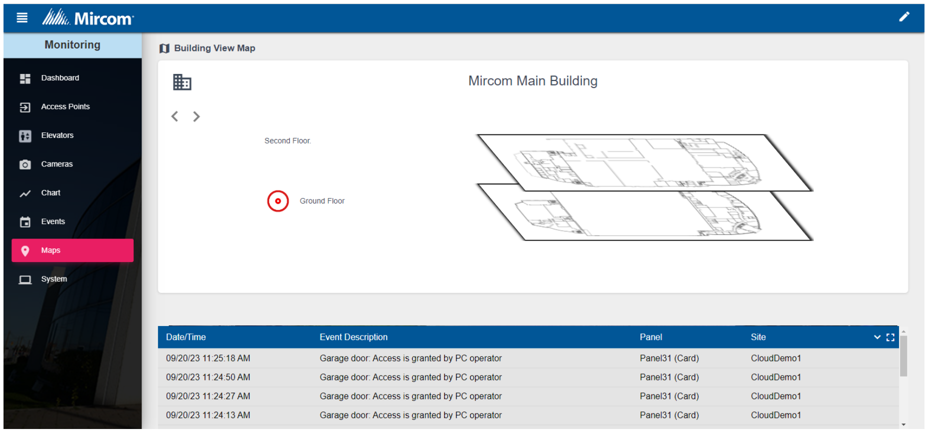


Mircom Main Building

Status : Alarm

Figure 14. Alarm notification

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

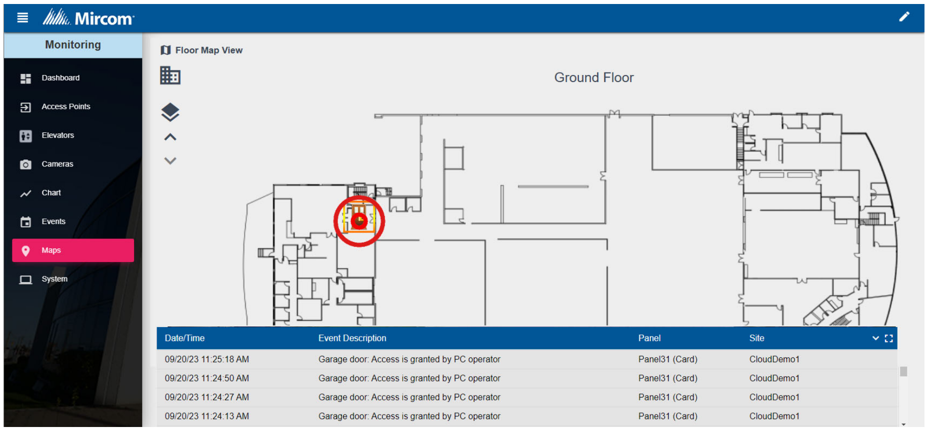


Date/Time	Event Description	Panel	Site
09/20/23 11:25:18 AM	Garage door: Access is granted by PC operator	Panel31 (Card)	CloudDemo1
09/20/23 11:24:50 AM	Garage door: Access is granted by PC operator	Panel31 (Card)	CloudDemo1
09/20/23 11:24:27 AM	Garage door: Access is granted by PC operator	Panel31 (Card)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

Figure 15. Building view

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

The floor map appears.



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 16. Floor map

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

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

To add an access point to a floor, see section 3.6.10 on page 26.

3.2 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 on or off the unlock and high security functions in real time.

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

The Access Points window appears.

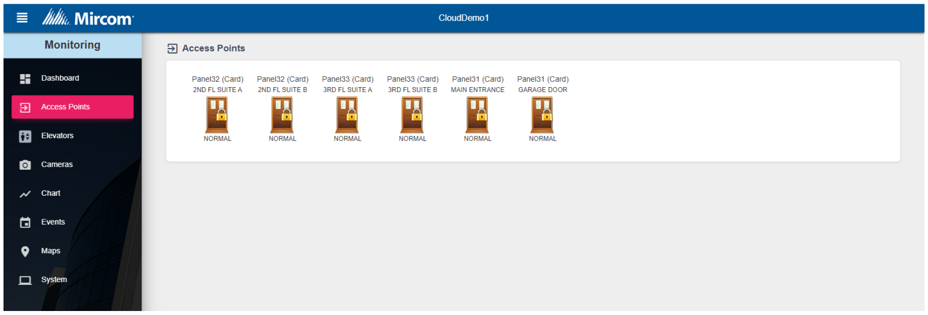


Figure 17. Access points

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.

3.3 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).

3.3.1 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. They are labelled **Elev2**.

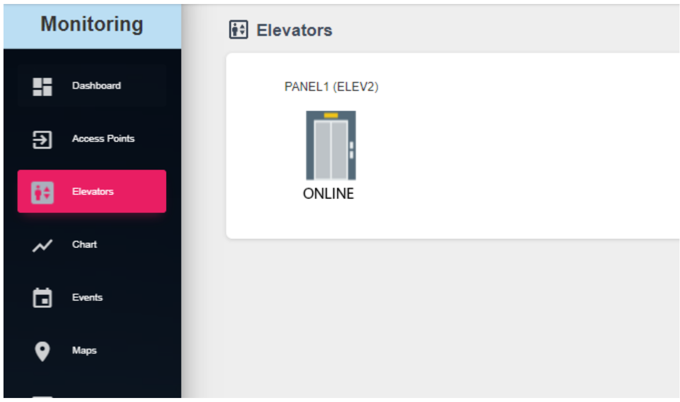
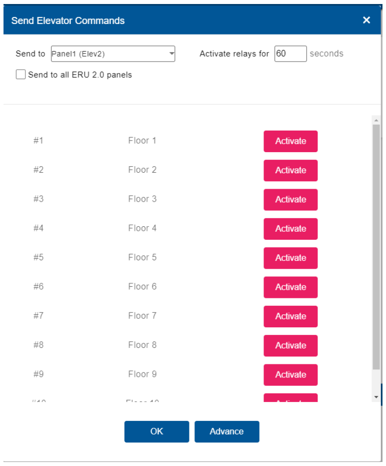


Figure 18. Elevator Status

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

   The Send Elevator Commands window appears.



Send Elevator Commands ✕

Send to Panel1 (Elev2) Activate relays for 60 seconds

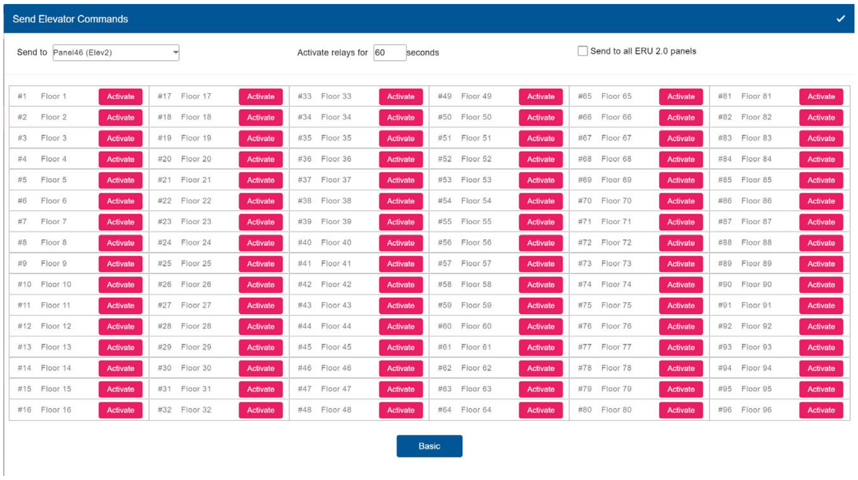
□ Send to all ERU 2.0 panels

#1	Floor 1	Activate
#2	Floor 2	Activate
#3	Floor 3	Activate
#4	Floor 4	Activate
#5	Floor 5	Activate
#6	Floor 6	Activate
#7	Floor 7	Activate
#8	Floor 8	Activate
#9	Floor 9	Activate

Figure 19. Send Elevator Commands Window

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

   The window expands to show all the elevator relays.



Send Elevator Commands ✓

Send to Panel46 (Elev2) Activate relays for 60 seconds □ Send to all ERU 2.0 panels

#1	Floor 1	Activate	#17	Floor 17	Activate	#33	Floor 33	Activate	#49	Floor 49	Activate	#65	Floor 65	Activate	#81	Floor 81	Activate
#2	Floor 2	Activate	#18	Floor 18	Activate	#34	Floor 34	Activate	#50	Floor 50	Activate	#66	Floor 66	Activate	#82	Floor 82	Activate
#3	Floor 3	Activate	#19	Floor 19	Activate	#35	Floor 35	Activate	#51	Floor 51	Activate	#67	Floor 67	Activate	#83	Floor 83	Activate
#4	Floor 4	Activate	#20	Floor 20	Activate	#36	Floor 36	Activate	#52	Floor 52	Activate	#68	Floor 68	Activate	#84	Floor 84	Activate
#5	Floor 5	Activate	#21	Floor 21	Activate	#37	Floor 37	Activate	#53	Floor 53	Activate	#69	Floor 69	Activate	#85	Floor 85	Activate
#6	Floor 6	Activate	#22	Floor 22	Activate	#38	Floor 38	Activate	#54	Floor 54	Activate	#70	Floor 70	Activate	#86	Floor 86	Activate
#7	Floor 7	Activate	#23	Floor 23	Activate	#39	Floor 39	Activate	#55	Floor 55	Activate	#71	Floor 71	Activate	#87	Floor 87	Activate
#8	Floor 8	Activate	#24	Floor 24	Activate	#40	Floor 40	Activate	#56	Floor 56	Activate	#72	Floor 72	Activate	#88	Floor 88	Activate
#9	Floor 9	Activate	#25	Floor 25	Activate	#41	Floor 41	Activate	#57	Floor 57	Activate	#73	Floor 73	Activate	#89	Floor 89	Activate
#10	Floor 10	Activate	#26	Floor 26	Activate	#42	Floor 42	Activate	#58	Floor 58	Activate	#74	Floor 74	Activate	#90	Floor 90	Activate
#11	Floor 11	Activate	#27	Floor 27	Activate	#43	Floor 43	Activate	#59	Floor 59	Activate	#75	Floor 75	Activate	#91	Floor 91	Activate
#12	Floor 12	Activate	#28	Floor 28	Activate	#44	Floor 44	Activate	#60	Floor 60	Activate	#76	Floor 76	Activate	#92	Floor 92	Activate
#13	Floor 13	Activate	#29	Floor 29	Activate	#45	Floor 45	Activate	#61	Floor 61	Activate	#77	Floor 77	Activate	#93	Floor 93	Activate
#14	Floor 14	Activate	#30	Floor 30	Activate	#46	Floor 46	Activate	#62	Floor 62	Activate	#78	Floor 78	Activate	#94	Floor 94	Activate
#15	Floor 15	Activate	#31	Floor 31	Activate	#47	Floor 47	Activate	#63	Floor 63	Activate	#79	Floor 79	Activate	#95	Floor 95	Activate
#16	Floor 16	Activate	#32	Floor 32	Activate	#48	Floor 48	Activate	#64	Floor 64	Activate	#80	Floor 80	Activate	#96	Floor 96	Activate

Figure 20. 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 ERU2.0 panels** if you want to send the activation command to all ERU2.0 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.

3.4 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.

3.4.1 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 the Event List in LT-995 TX3 System Configuration and Administration Manual.

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.

3.4.2 Example Chart

Figure 21 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 access change as time passes.

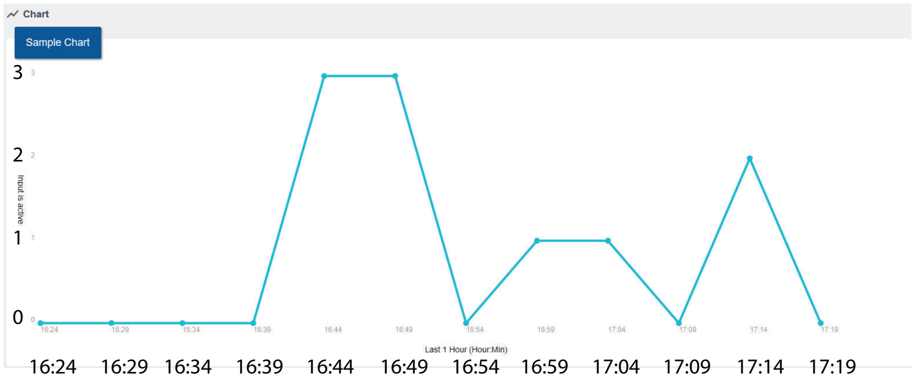


Figure 21. Example chart

3.4.3 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.

3.5 Events

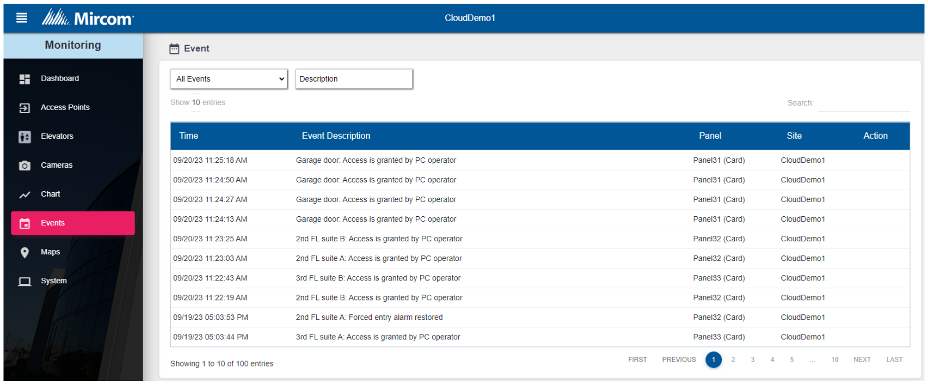
The Events section displays all events received by the TX3 system.

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

3.5.1 View Events

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

The Event window appears.



All Events

Description

Show 10 entries

Time	Event Description	Panel	Site	Action
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	
09/20/23 11:23:25 AM	2nd FL suite B: Access is granted by PC operator	Panel32 (Card)	CloudDemo1	
09/20/23 11:23:03 AM	2nd FL suite A: Access is granted by PC operator	Panel32 (Card)	CloudDemo1	
09/20/23 11:22:43 AM	3rd FL suite B: Access is granted by PC operator	Panel33 (Card)	CloudDemo1	
09/20/23 11:22:19 AM	2nd FL suite B: Access is granted by PC operator	Panel32 (Card)	CloudDemo1	
09/19/23 05:03:53 PM	2nd FL suite A: Forced entry alarm restored	Panel32 (Card)	CloudDemo1	
09/19/23 05:03:44 PM	3rd FL suite A: Access is granted by PC operator	Panel33 (Card)	CloudDemo1	

Showing 1 to 10 of 100 entries

Figure 22. 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.

3.5.2 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

3.6 Maps

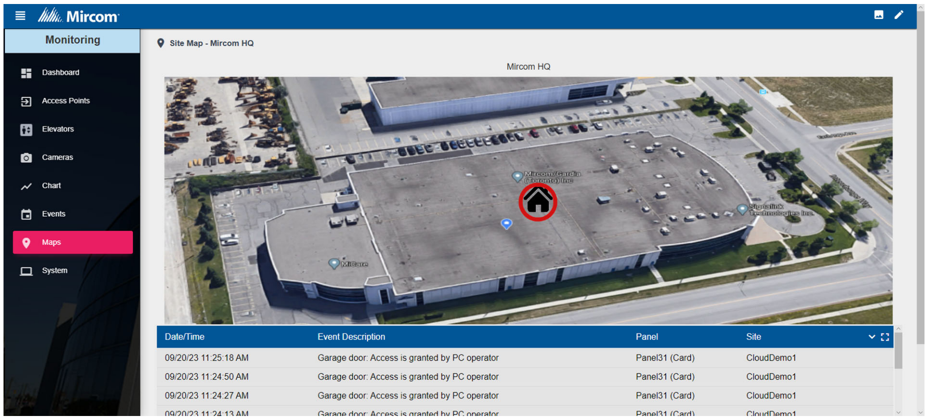
The maps section lets you configure the maps for the site, buildings, and floors. You can place icons on the maps to represent buildings, access points, and inputs.

TX3 Vision supports maps in JPEG and PNG format.

3.6.1 View Maps

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

The site map appears.



Site Map - Mircom HQ

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 23. Maps

3.6.2 Navigate Buildings and Floors

Navigate the 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.

Navigate the 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.

3.6.3 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

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

The Edit window appears.

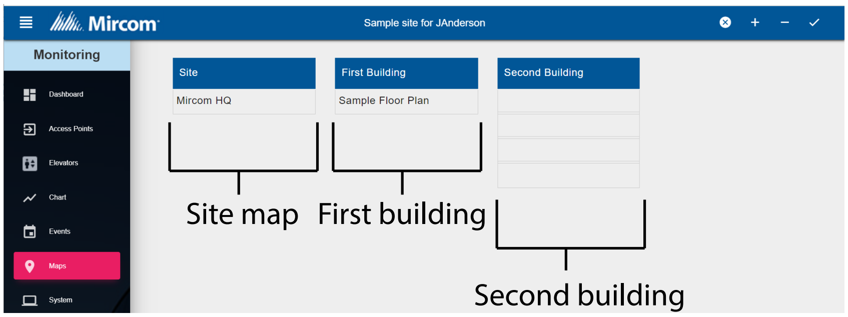


Figure 24. Edit window

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 3.6.4 to 3.6.11 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.

3.6.4 Edit a site map

1. In the Edit window, click the name of the site map, and then click the red pencil icon ✎ that appears.

2. Edit the site's description and showcase picture (see section 3.6.11), 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.

3.6.5 Upload a map for the site

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

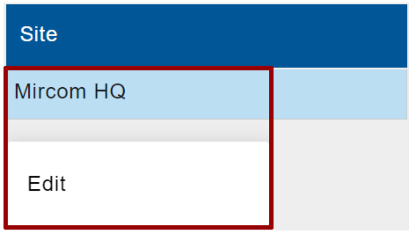
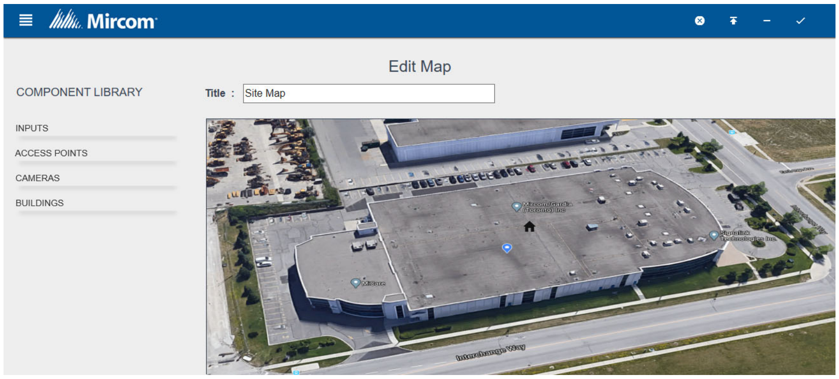


Figure 25. Edit Site Map

The Edit Map window appears.



Title : Site Map

Figure 26. Edit Site Map window

2. Click the Upload button ⤒ in the upper right corner.

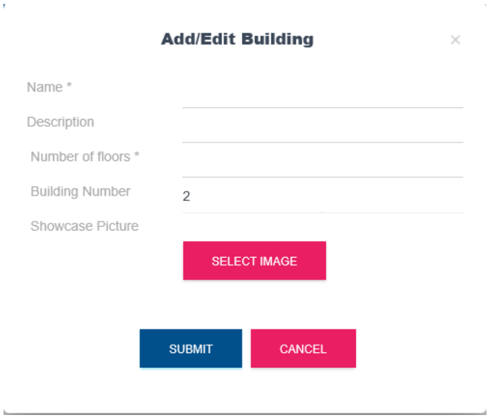
3. Click **Select Image**, choose a map to upload, and then click **Submit**.

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

3.6.6 Add a building

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

The Add/Edit Building window appears.



Building Number 2

Figure 27. 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 3.6.11).

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.

3.6.7 Place your buildings on the site map

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

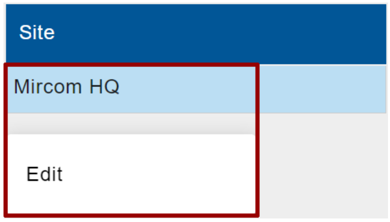


Figure 28. Site Map Edit menu

   The Edit Map window appears (Figure 26).

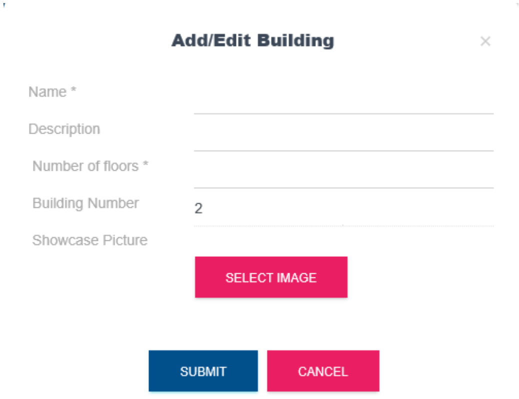
2. From the **Component Library** on the left, click **Buildings**, and then click and drag the name of the building on to the map.

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

3.6.8 Edit the Buildings

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

   The Add/Edit Building window appears.



Add/Edit Building ×

Name *

Description

Number of floors *

Building Number 2

Showcase Picture

Figure 29. Add/Edit Building

2. Edit the building's name, description, and number of floors, and showcase picture (see section 3.6.11), 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.

3.6.9 Remove a building

1. In the Edit window, click the building that you want to remove so that the red pencil icon ✎ 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.

3.6.10 Edit the Floors

Each building consists of one or more floors. You can place inputs, access points, and cameras 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**.

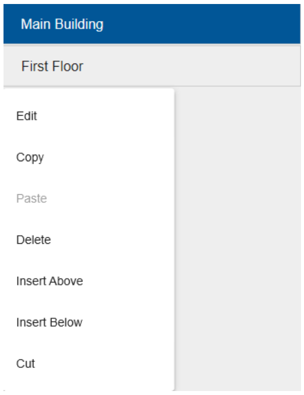


Figure 30. Floor Edit menu

   The Edit Map window appears (Figure 26).

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.

3.6.11 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 3.6.3). Showcase pictures are not maps, but are photographs of the site and buildings.

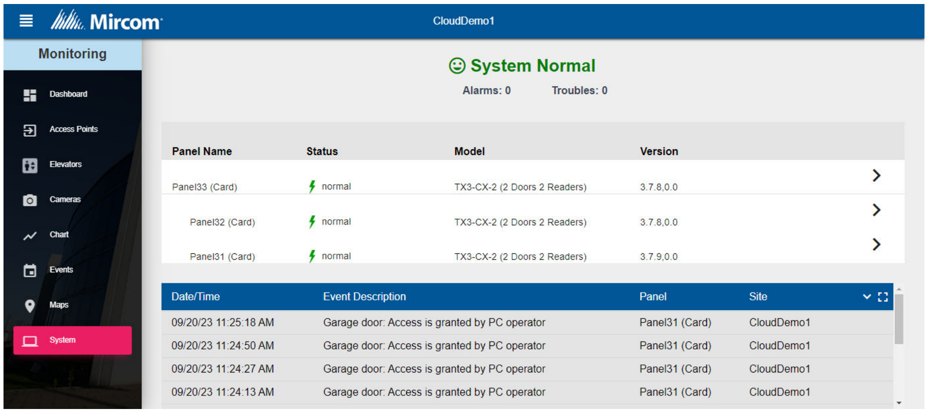
3.7 System

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

3.7.1 View the System

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

  The System window appears.



CloudDemo1

System Normal

Alarms: 0 Troubles: 0

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 31. System

The panels are grouped by Master Node.

The view has the following columns:

Panel Name. The name is assigned in the PC Configurator.

Status. Normal, alarm, or trouble.

Model. The panel model.

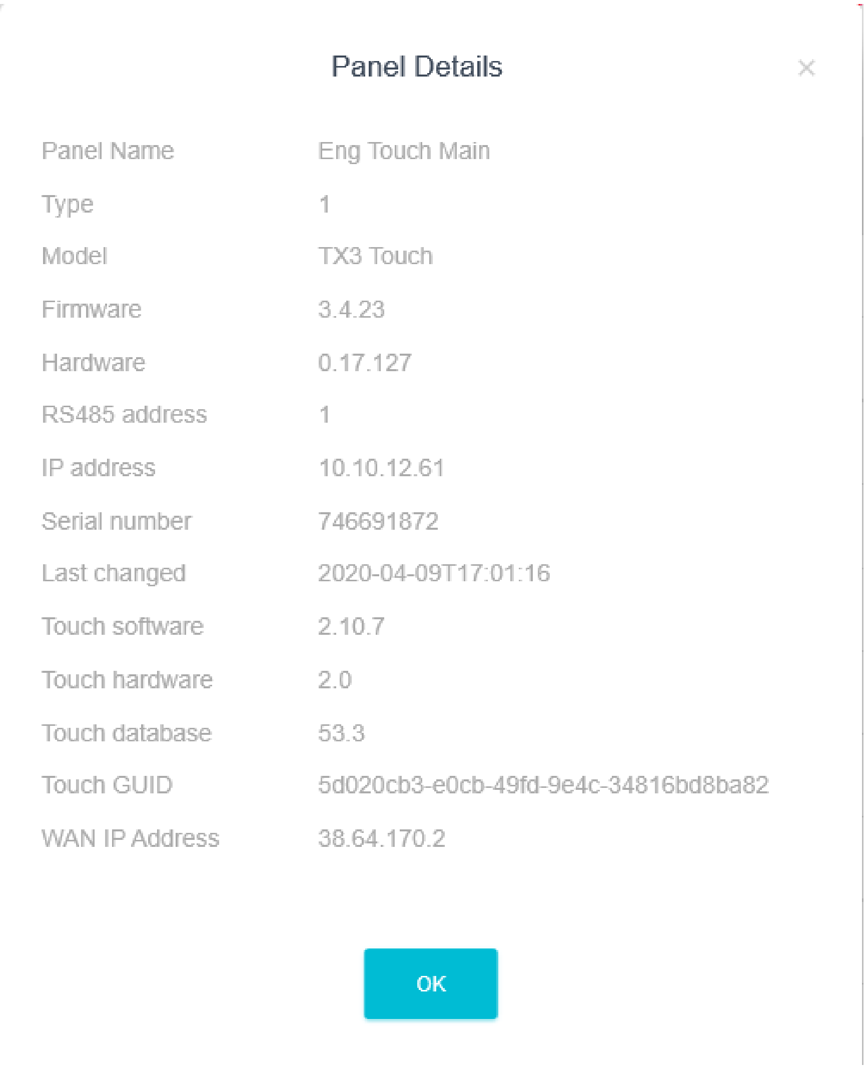
Version. The firmware version.

3.7.2 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
- 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 Name	Eng Touch Main
Type	1
Model	TX3 Touch
Firmware	3.4.23
Hardware	0.17.127
RS485 address	1
IP address	10.10.12.61
Serial number	746691872
Last changed	2020-04-09T17:01:16
Touch software	2.10.7
Touch hardware	2.0
Touch database	53.3
Touch GUID	5d020cb3-e0cb-49fd-9e4c-34816bd8ba82
WAN IP Address	38.64.170.2

Figure 32. Panel Details

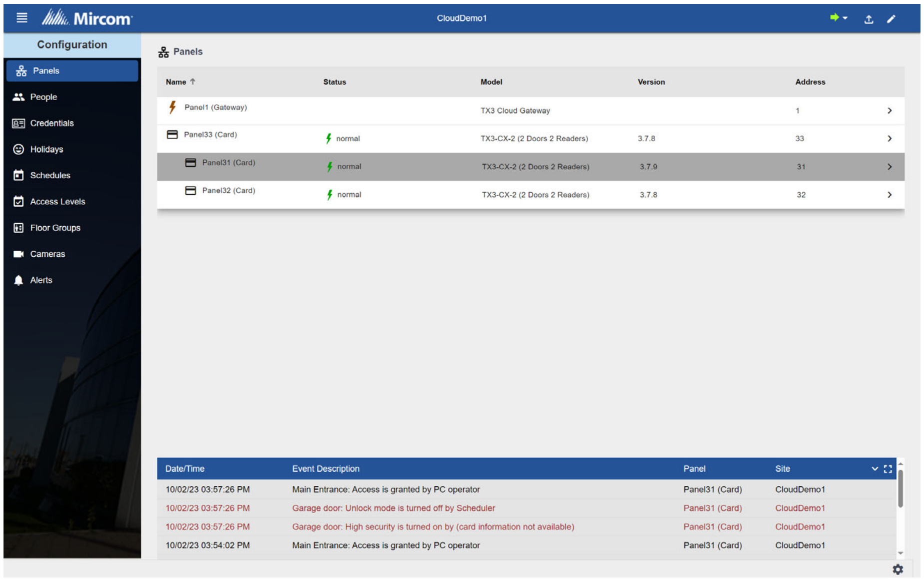
4 Configuration

The Configuration section lets you modify panels, add people and credentials, and create schedules.

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 03:57:26 PM	Garage door: Unlock mode is turned off by Scheduler	Panel31 (Card)	CloudDemo1
10/02/23 03:57:26 PM	Garage door: High security is turned on by (card information not available)	Panel31 (Card)	CloudDemo1
10/02/23 03:54:02 PM	Main Entrance: Access is granted by PC operator	Panel31 (Card)	CloudDemo1

Figure 33. Panels

The panels are grouped by Master Node.
The view has the following columns:

Panel Name. The name is assigned in the PC Configurator.

Status. Normal, alarm, or trouble.

Model. The panel model.

Version. The firmware version.

Address. The RS-485 address.

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.

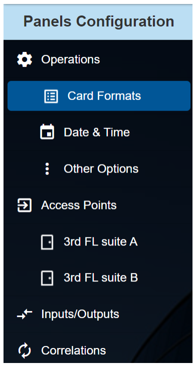


Figure 34. Configuration left pane

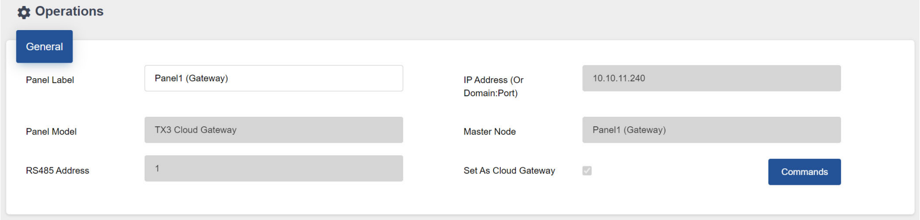
4.1.1 Operations - General

Panel label. Provide a name for the Panel.

Panel model. The application automatically retrieves the selected panel model information. This field is read only.

RS485 Address. This field is read only.

Master Node. The panel's main node. This field is read only.



Panel Label: Panel1 (Gateway)

IP Address (Or Domain:Port): 10.10.11.240

Panel Model: TX3 Cloud Gateway

Master Node: Panel1 (Gateway)

RS485 Address: 1

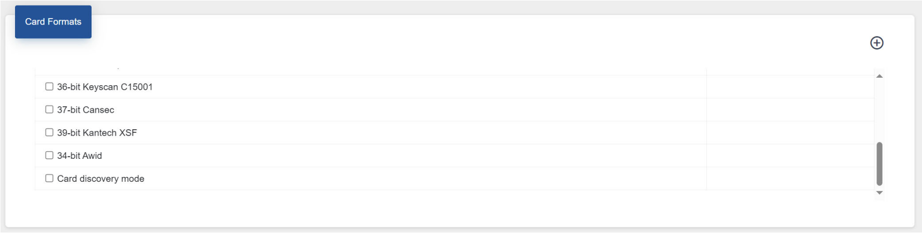
Set As Cloud Gateway: ☑

Figure 35. Panel Configuration - General

Other options below are not available for the TX3 Cloud Gateway.

4.1.2 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 Formats

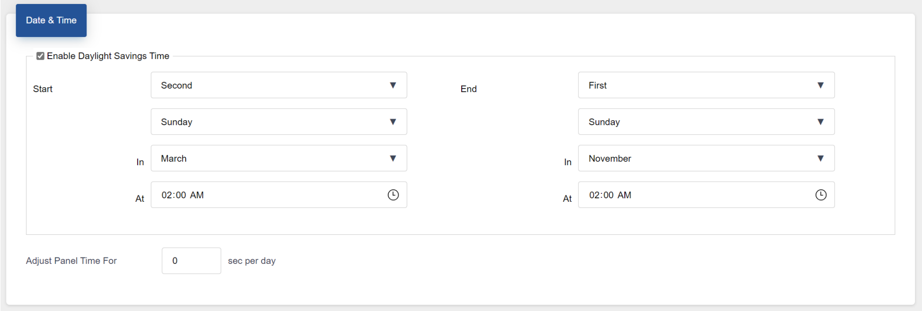
- ☐ 36-bit Keyscan C15001
- ☐ 37-bit Cansec
- ☐ 39-bit Kantech XSF
- ☐ 34-bit Awid
- ☐ Card discovery mode

Figure 36. Panel Configuration - Card Formats

4.1.3 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.



Date & Time

☑ Enable Daylight Savings Time

Start	Second	End	First
	Sunday		Sunday
In	March	In	November
At	02:00 AM	At	02:00 AM

Adjust Panel Time For 0 sec per day

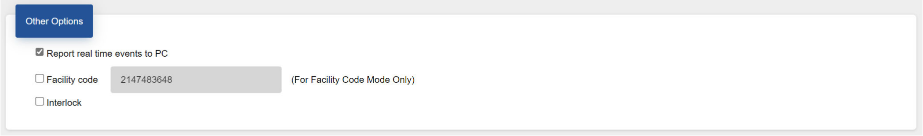
Figure 37. Panel Configuration - Date and Time

4.1.4 Operations - Other Options

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

Facility code. Enter the building's facility code with a value from 0 to 4294967294. 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.



Other Options

☑ Report real time events to PC

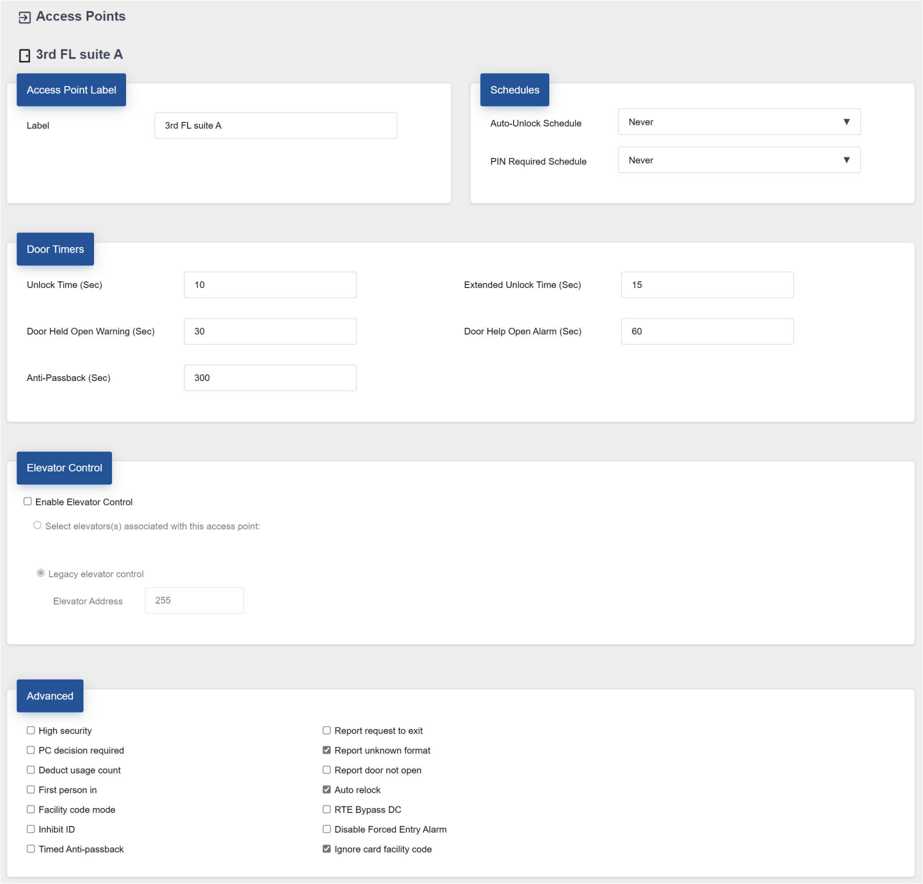
☐ Facility code 2147483648 (For Facility Code Mode Only)

☐ Interlock

Figure 38. Panel Configuration - Other Options

4.1.5 Access Points

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



Access Points

3rd FL suite A

Access Point Label

Label: 3rd FL suite A

Schedules

Auto-Unlock Schedule: Never ▼

PIN Required Schedule: Never ▼

Door Timers

Unlock Time (Sec): 10

Extended Unlock Time (Sec): 15

Door Held Open Warning (Sec): 30

Door Help Open Alarm (Sec): 60

Anti-Passback (Sec): 300

Elevator Control

☐ Enable Elevator Control

○ Select elevators(s) associated with this access point:

● Legacy elevator control

Elevator Address: 255

Advanced

☐ High security

☐ PC decision required

☐ Deduct usage count

☐ First person in

☐ Facility code mode

☐ Inhibit ID

☐ Timed Anti-passback

☐ Report request to exit

☑ Report unknown format

☐ Report door not open

☑ Auto relock

☐ RTE Bypass DC

☐ Disable Forced Entry Alarm

☑ Ignore card facility code

Figure 39. 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.

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.

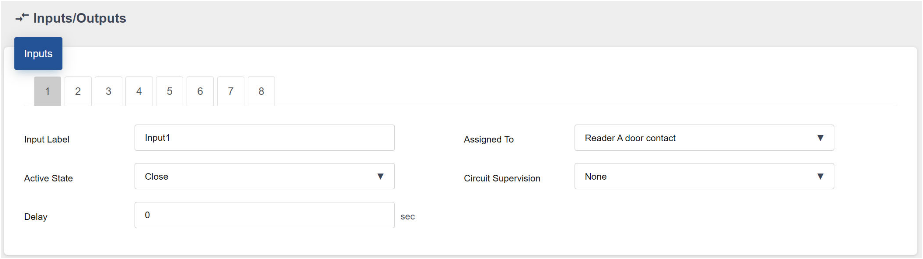
RTE bypass DC. Enable this option if there is a mechanical egress device installed on the door. In this situation, the door is unlocked manually, and the TX3 system does not unlock the door. If the door is opened, the system updates the door status and the LED on the reader turns green. The door contact 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.

4.1.6 Inputs

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



Input Label: Input1

Assigned To: Reader A door contact

Active State: Close

Circuit Supervision: None

Delay: 0 sec

Figure 40. 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. The Configurator 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.

4.1.7 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

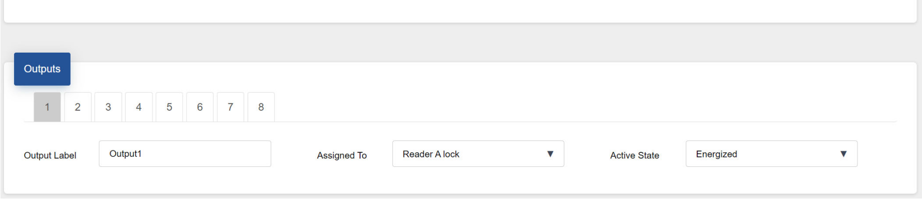
On a single door controller, outputs 1, 2 and 3 are configured as follows:

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.



Outputs

Output Label: Output1

Assigned To: Reader A lock

Active State: Energized

Figure 41. 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.

4.1.8 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.

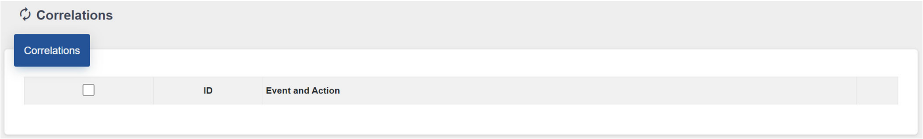


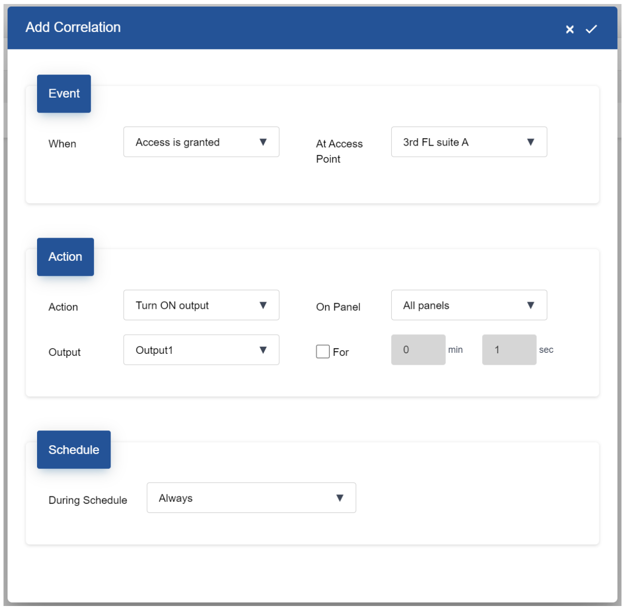
Figure 42. Correlations

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.

2. Click the **Add** button ⊕.



Add Correlation ✕ ✓

Event

When: Access is granted ▼

At Access Point: 3rd FL suite A ▼

Action

Action: Turn ON output ▼

On Panel: All panels ▼

Output: Output1 ▼

□ For 0 min 1 sec

Schedule

During Schedule: Always ▼

Figure 43. Add 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.

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. 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 (Panel1 and Panel2) in your TX3 system, you could select from the following options:

Panel1 - Apply the correlation to Panel1 only.

Panel2 - Apply the correlation to Panel2 only.

All - Apply the correlation to all Telephone Access, 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. 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.

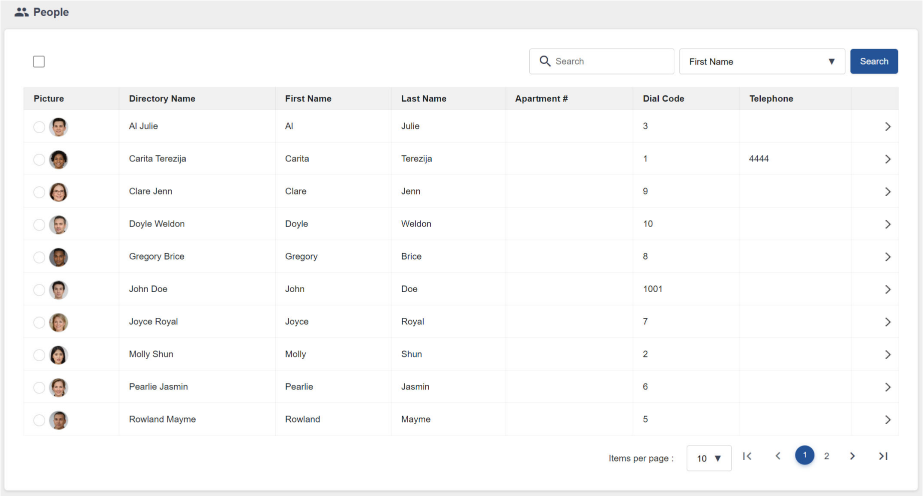
4.2 People

People refers to residents associated with credentials, occupants of the suite, and individuals who have credentials that allow them access through the card access system. They are listed in the directory for voice/video access for visitors.

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

4.2.1 Add a Person

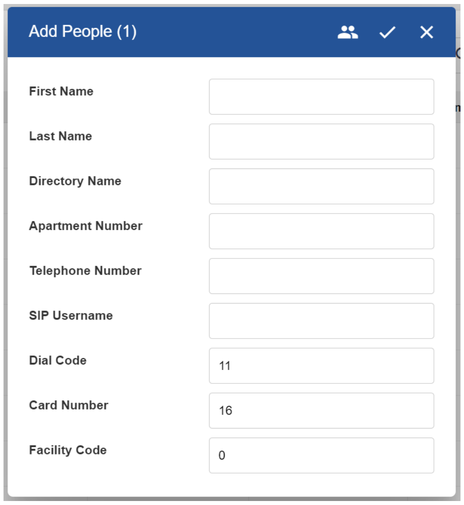
1. Click **People** in the Configuration pane.



Picture	Directory Name	First Name	Last Name	Apartment #	Dial Code	Telephone
○	Al Julie	Al	Julie		3	
○	Carita Terezija	Carita	Terezija		1	4444
○	Clare Jenn	Clare	Jenn		9	
○	Doyle Weldon	Doyle	Weldon		10	
○	Gregory Brice	Gregory	Brice		8	
○	John Doe	John	Doe		1001	
○	Joyce Royal	Joyce	Royal		7	
○	Molly Shun	Molly	Shun		2	
○	Pearlie Jasmin	Pearlie	Jasmin		6	
○	Rowland Mayme	Rowland	Mayme		5	

Figure 44. People

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



First Name	
Last Name	
Directory Name	
Apartment Number	
Telephone Number	
SIP Username	
Dial Code	11
Card Number	16
Facility Code	0

Figure 45. Add People

3. 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 access 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 4294967294. Access is granted when this facility code matches the value set for the Card Access Panel.

4.2.2 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.

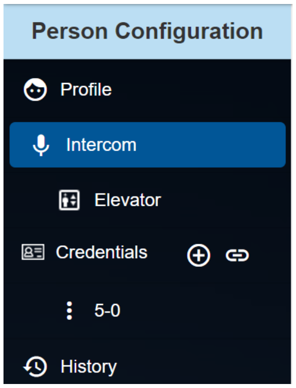
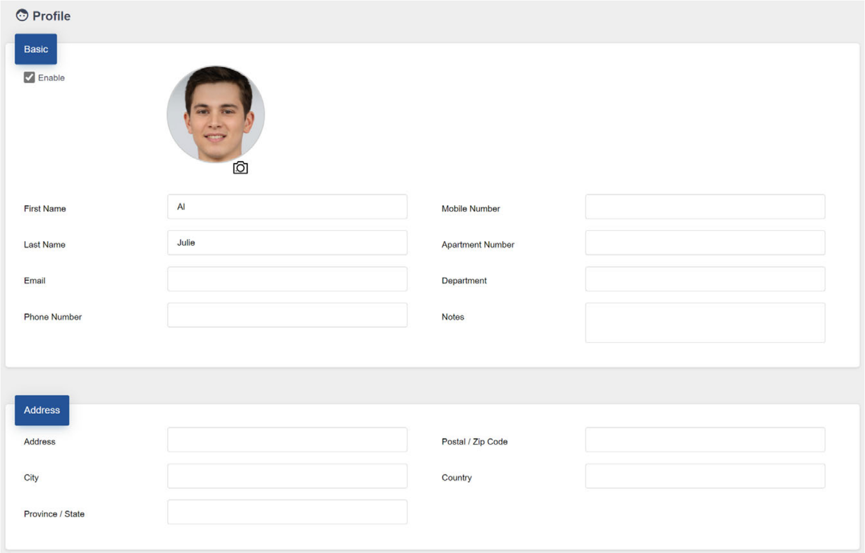


Figure 46. Person Configuration (left pane)

4.2.3 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

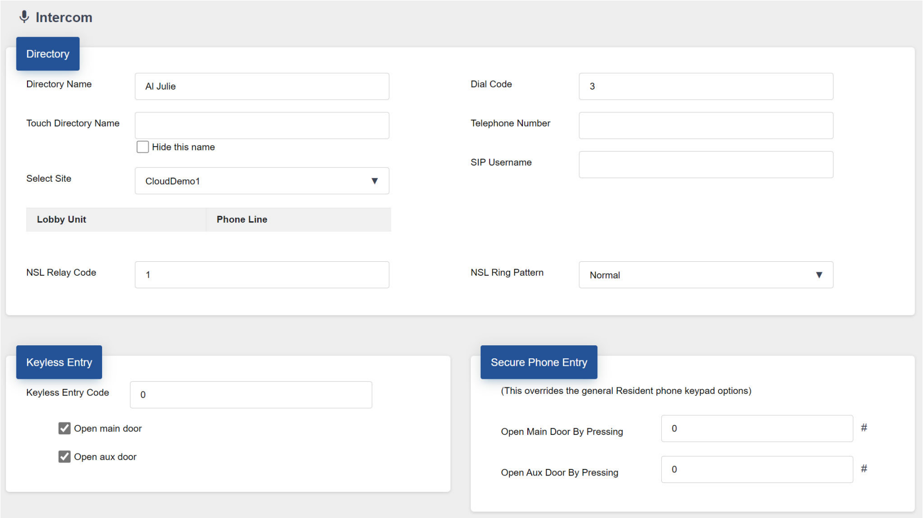
First Name	Al	Mobile Number	
Last Name	Julie	Apartment Number	
Email		Department	
Phone Number		Notes	

Address

Address		Postal / Zip Code	
City		Country	
Province / State			

Figure 47. Profile

4.2.4 Intercom



Intercom

Directory

Directory Name	Al Julie	Dial Code	3
Touch Directory Name		Telephone Number	
	□ Hide this name	SIP Username	
Select Site	CloudDemo1 ▼		

Lobby Unit	Phone Line

NSL Relay Code	1	NSL Ring Pattern	Normal ▼

Keyless Entry

Keyless Entry Code: 0

☑ Open main door

☑ Open aux door

Secure Phone Entry

(This overrides the general Resident phone keypad options)

Open Main Door By Pressing: 0 #

Open Aux Door By Pressing: 0 #

Figure 48. 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 access 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.

Select Site. Select the site that this person belongs to.

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 1 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).

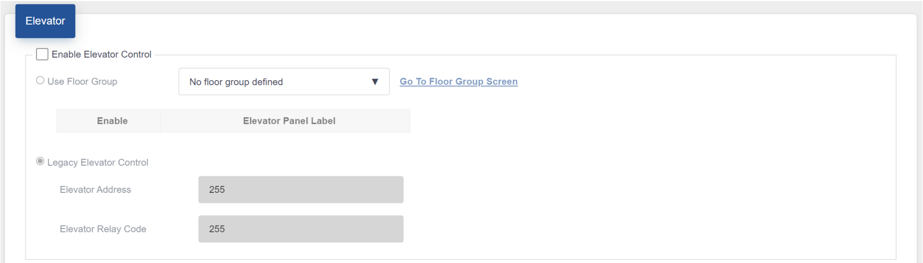
Note: Do not select 1, 7, or * for **Open Main Door by Pressing** and **Open Aux Door by Pressing**.

4.2.5 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.



Elevator

□ Enable Elevator Control

○ Use Floor Group: No floor group defined ▼ Go To Floor Group Screen

Enable	Elevator Panel Label

● Legacy Elevator Control

Elevator Address: 255

Elevator Relay Code: 255

Figure 49. Elevators

4.2.6 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.

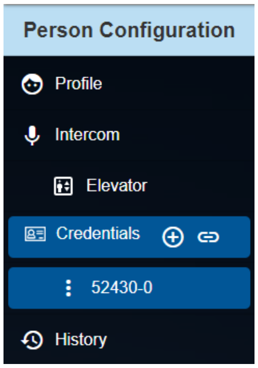
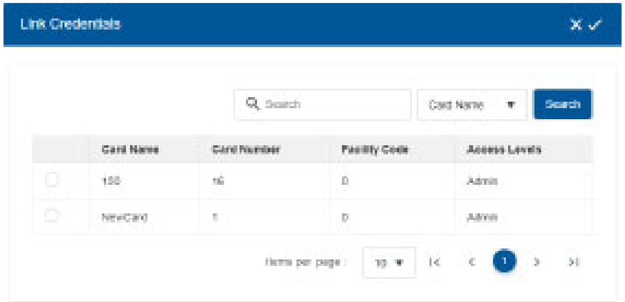


Figure 50. Person Configuration (left pane)

4.2.7 Link a Credential

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



Link Credentials

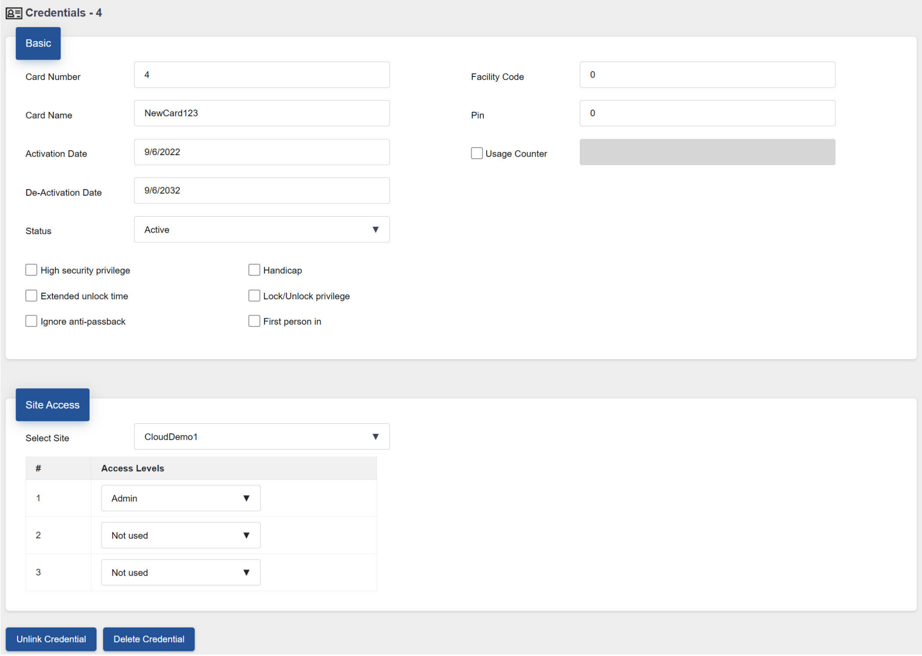
	Card Name	Card Number	Facility Code	Access Levels
○	150	16	0	Admin
○	NewCard	1	0	Admin

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.

4.2.8 Add a Credential

1. In the left pane, click the **Add** button ⊕ to add a credential.



Credentials - 4

Card Number	4	Facility Code	0
Card Name	NewCard123	Pin	0
Activation Date	9/6/2022	□ Usage Counter	
De-Activation Date	9/6/2032		
Status	Active ▾		

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

Select Site: CloudDemo1 ▾

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

Figure 51. 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.

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

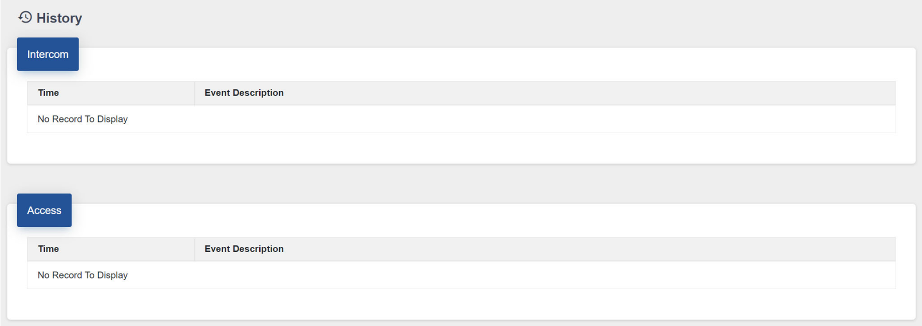
Unlink Credential. Click this button to unlink the credential from the resident so that it can be used for another resident.

Delete Credential. Click this button to delete the credential.

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

4.2.9 History

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



History

Intercom

Time	Event Description
No Record To Display	

Access

Time	Event Description
No Record To Display	

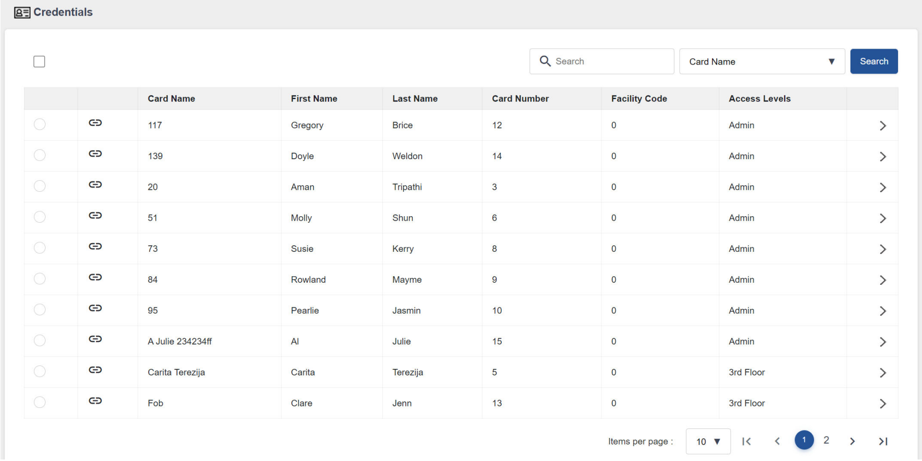
Figure 52. History

4.3 Credentials

Select 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

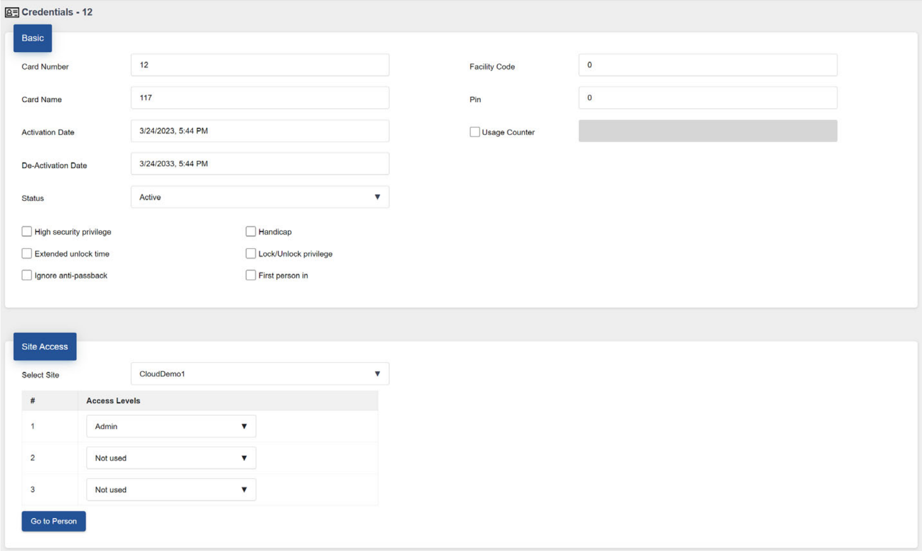
		Card Name	First Name	Last Name	Card Number	Facility Code	Access Levels	
○	⊖	117	Gregory	Brice	12	0	Admin	>
○	⊖	139	Doyle	Weldon	14	0	Admin	>
○	⊖	20	Aman	Tripathi	3	0	Admin	>
○	⊖	51	Molly	Shun	6	0	Admin	>
○	⊖	73	Susie	Kerry	8	0	Admin	>
○	⊖	84	Rowland	Mayme	9	0	Admin	>
○	⊖	95	Pearlie	Jasmin	10	0	Admin	>
○	⊖	A Julie 234234ff	Al	Julie	15	0	Admin	>
○	⊖	Carita Terezija	Carita	Terezija	5	0	3rd Floor	>
○	⊖	Fob	Clare	Jenn	13	0	3rd Floor	>

Items per page : 10 ▼

Figure 53. 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.

Click the Add button ⊕ in the upper right to add a credential, or click the arrow to the right of an existing credential > to see its details.



Credentials - 12

Basic

Card Number	12	Facility Code	0
Card Name	117	Pin	0
Activation Date	3/24/2023, 5:44 PM	□ Usage Counter	
De-Activation Date	3/24/2033, 5:44 PM		
Status	Active ▾		

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

Site Access

Select Site: CloudDemo1 ▾

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

Figure 54. 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 site and access levels that apply to this credential.

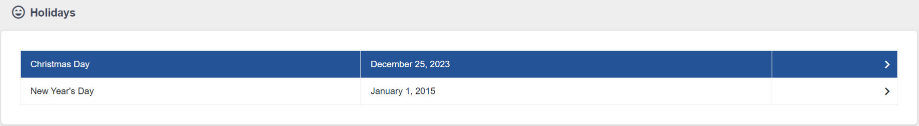
Click the Done button ✓ in the upper right corner to save your changes.

4.4 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.

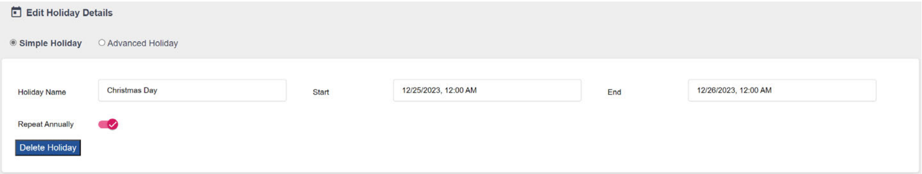
1. Click **Holidays** in the Configuration pane. The Holiday Configuration window appears listing the available holidays.



Christmas Day	December 25, 2023	>
New Year's Day	January 1, 2015	>

Figure 55. Holidays

2. Click the Add button ⊕ in the upper right to add a holiday, or click the arrow to the right of an existing holiday > to see its details.



Edit Holiday Details

● Simple Holiday ○ Advanced Holiday

Holiday Name: Christmas Day
Start: 12/25/2023, 12:00 AM
End: 12/26/2023, 12:00 AM
Repeat Annually ✓

Figure 56. Holiday

3. 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.

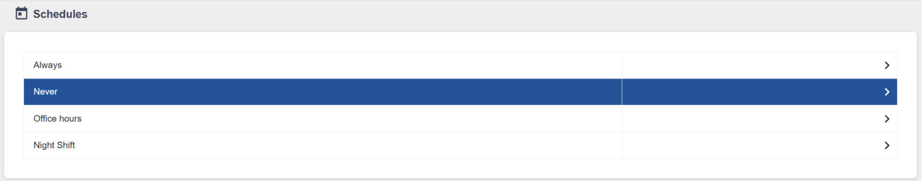
Repeat annually. Check this box if the same start, end date and time re-occur every year.

4.5 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.

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

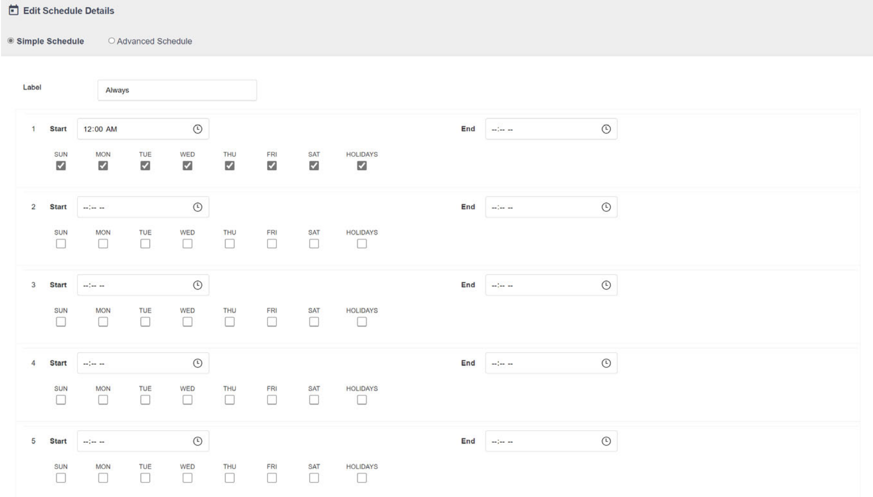


Schedules

- Always >
- Never >
- Office hours >
- Night Shift >

Figure 57. Schedules

2. Click the Add button ⊕ in the upper right to add a schedule, or click the arrow to the right of an existing schedule > to see its details.



Edit Schedule Details

● Simple Schedule ○ Advanced Schedule

Label: Always

1 Start 12:00 AM End --:-- --

SUN	MON	TUE	WED	THU	FRI	SAT	HOLIDAYS
☑	☑	☑	☑	☑	☑	☑	☑

2 Start --:-- -- End --:-- --

SUN	MON	TUE	WED	THU	FRI	SAT	HOLIDAYS
□	□	□	□	□	□	□	□

3 Start --:-- -- End --:-- --

SUN	MON	TUE	WED	THU	FRI	SAT	HOLIDAYS
□	□	□	□	□	□	□	□

4 Start --:-- -- End --:-- --

SUN	MON	TUE	WED	THU	FRI	SAT	HOLIDAYS
□	□	□	□	□	□	□	□

5 Start --:-- -- End --:-- --

SUN	MON	TUE	WED	THU	FRI	SAT	HOLIDAYS
□	□	□	□	□	□	□	□

Figure 58. Simple Schedule

3. Provide information for the following parameters:

Label. Provide a name for the schedule.

Start. Specify a start time.

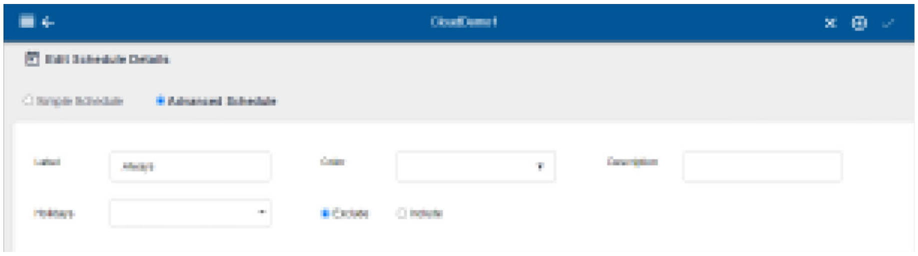
End. Specify an end time.

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.

4. Click **Advanced Schedule** to add more detail to the schedule.



Edit Schedule Details

○ Simple Schedule ● Advanced Schedule

Label: Always

Color:

Description:

Holidays:

● Exclude ○ Include

Figure 59. Advanced Schedule

5. Provide information for the following parameters:

   Label. Provide a name for the schedule.

   Holidays. Select whether this schedule includes holidays.

   Exclude. If **Exclude** is selected, then the schedule is not active during the selected holidays.

   Include. If **Include** is selected, then the schedule is active during the selected holidays.

   Color. Select a color for the schedule.

   Description. Enter a description of the schedule.

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

4.6 Access Levels

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 Panel1 with two access points (Reader A and Reader B) and a Card Access System panel called Panel2 with two access points (Reader C and Reader D), you could define the following access levels.

Access Level ID = 1

- Panel1: Reader A schedule = Always
- Panel1: Reader B schedule = Never

- Panel2: Reader C schedule = Never
- Panel2: Reader D schedule = Never

Access Level ID = 2

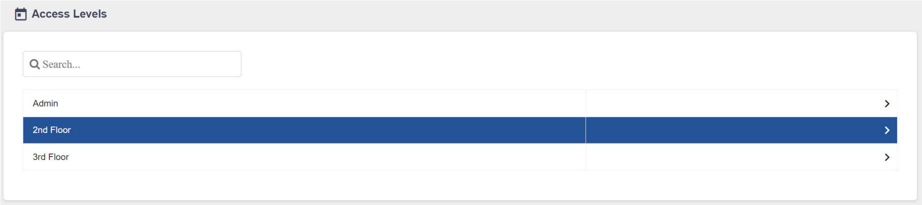
- Panel1: Reader A schedule = Office hours
- Panel1: Reader B schedule = Always
- Panel2: Reader C schedule = Always
- Panel2: Reader D schedule = Always

If a credential is assigned to Access Level 1, the user has access to Reader A on Panel1 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.

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

   The Access Levels screen appears.



Access Levels

Search...

Admin

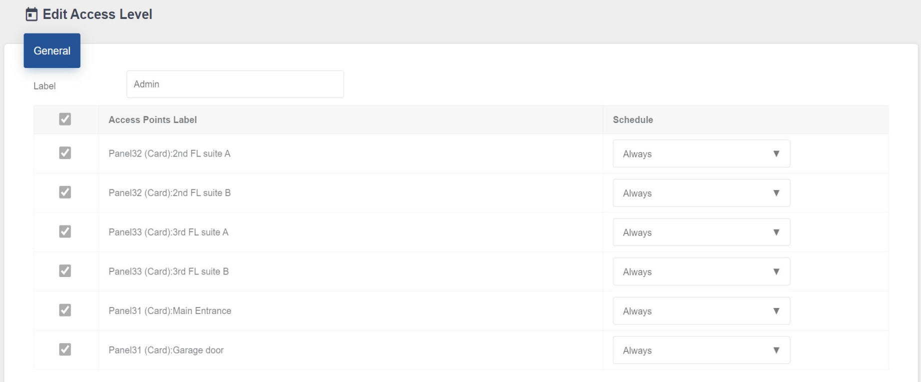
2nd Floor

3rd Floor

Figure 60. Access Levels

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

2. 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 see its details.



Label: Admin

☑	Access Points Label	Schedule
☑	Panel32 (Card):2nd FL suite A	Always ▾
☑	Panel32 (Card):2nd FL suite B	Always ▾
☑	Panel33 (Card):3rd FL suite A	Always ▾
☑	Panel33 (Card):3rd FL suite B	Always ▾
☑	Panel31 (Card):Main Entrance	Always ▾
☑	Panel31 (Card):Garage door	Always ▾

Figure 61. Add or Edit 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 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.

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

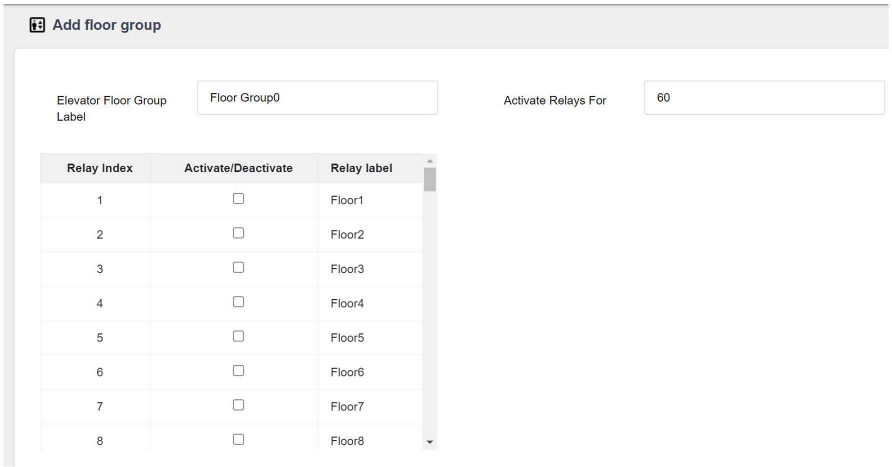
4.7 Floor Groups

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

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

2. 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 see its details.

The Add floor group window appears.



Add floor group

Elevator Floor Group Label: Floor Group0

Activate Relays For: 60

Relay Index	Activate/Deactivate	Relay label
1	□	Floor1
2	□	Floor2
3	□	Floor3
4	□	Floor4
5	□	Floor5
6	□	Floor6
7	□	Floor7
8	□	Floor8

Figure 62. Add floor group

3. Click the **Activate/Deactivate** button to select the floors that you want in this 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.

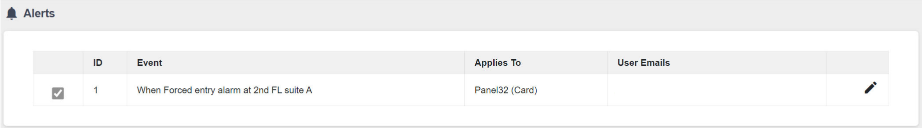
Click the Done button ✓ in the upper right corner to save your changes.

4.8 Alerts

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

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

   The Alerts screen appears.



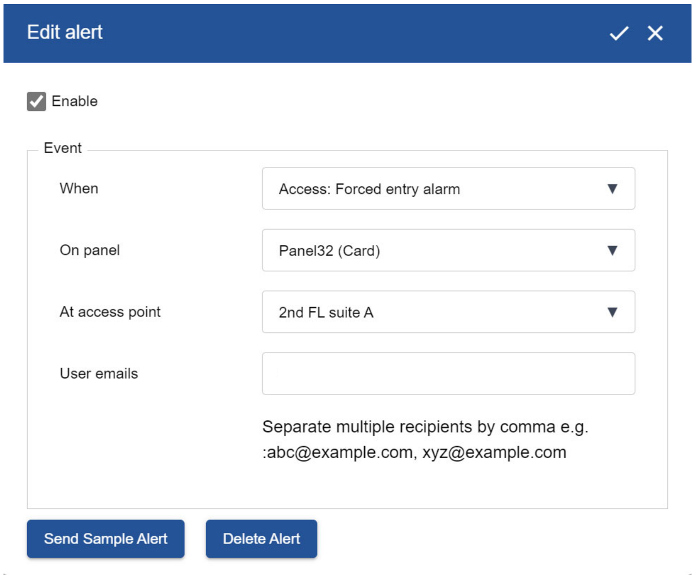
Alerts

	ID	Event	Applies To	User Emails	
☑	1	When Forced entry alarm at 2nd FL suite A	Panel32 (Card)		✎

Figure 63. Alerts

2. Click the pencil ✎ 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

Figure 64. Edit alert

3. Supply the following information:

When. Choose an event that will activate an alert. For a description of the events, see the Event List in LT-995 TX3 System Configuration and Administration Manual.

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 (Panel1 and Panel2) in your TX3 system, you could select from the following options:

Panel1 - Apply the correlation to Panel1 only.

Panel2 - Apply the correlation to Panel2 only.

All panels - Apply the correlation to all Telephone Access, 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.

5 Reports

The **Reports** option lets you generate reports on events, residents and access cards, and lets you print a paper directory.

To see the Reports pane, click the **Options** menu, then click **Reports**.

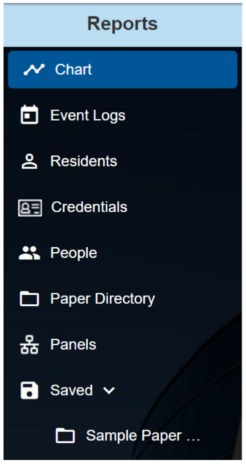


Figure 65. The Reports Pane

5.1 Saving and Exporting 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.

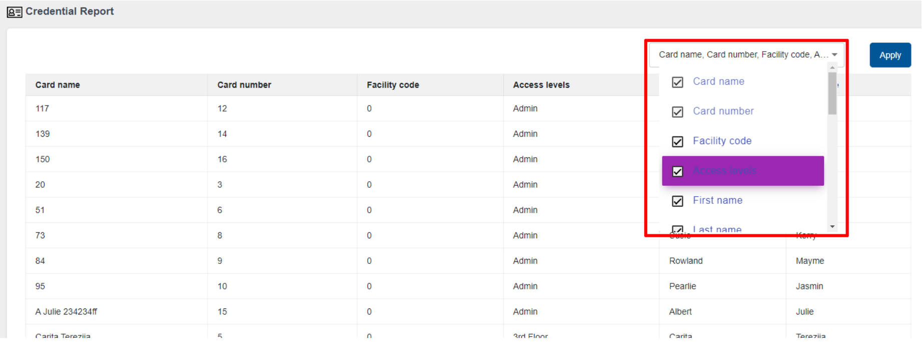
Click the Export button in the upper right to save the report as a PDF, XSLX, or CSV file.

5.2 Showing and Hiding 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.



Credential Report

Card name, Card number, Facility code, A…

- ☑ Card name
- ☑ Card number
- ☑ Facility code
- ☑ Access levels
- ☑ First name
- ☑ Last name

Card name	Card number	Facility code	Access levels		
117	12	0	Admin		
139	14	0	Admin		
150	16	0	Admin		
20	3	0	Admin		
51	6	0	Admin		
73	8	0	Admin	Susie	Kerry
84	9	0	Admin	Rowland	Mayme
95	10	0	Admin	Pearlie	Jasmin
A Julie 234234ff	15	0	Admin	Albert	Julie
Carita Tereziia	5	0	3rd Floor	Carita	Tereziia

Figure 66. Showing and Hiding Columns

3. Click **Apply**.

5.3 Chart

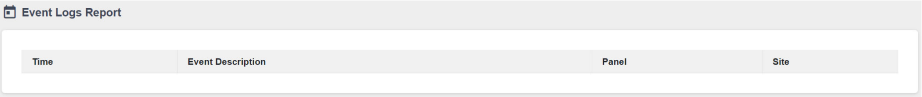
This chart is the same as the chart described in Section 3.4.

5.4 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.

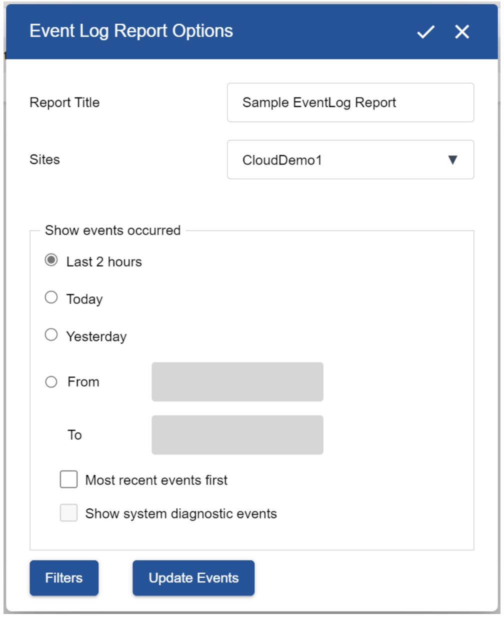


Event Logs Report

Time	Event Description	Panel	Site

Figure 67. Event Log Report

2. Click the Edit button ✎ to edit the event log.



Event Log Report Options ✓ ✕

Report Title: Sample EventLog Report

Sites: CloudDemo1 ▼

Show events occurred

● Last 2 hours

○ Today

○ Yesterday

○ From

To

□ Most recent events first

□ Show system diagnostic events

Figure 68. 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.

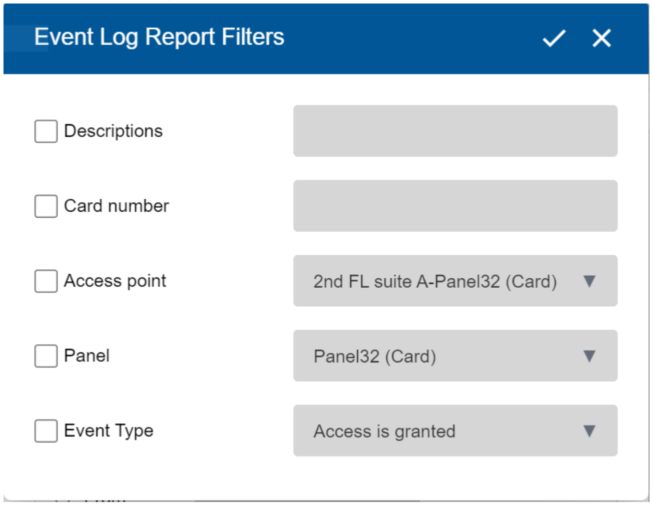
   Most recent events first. Select this option to display the most recent events at the top of the report.

   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.



Event Log Report Filters

□ Descriptions

□ Card number

□ Access point: 2nd FL suite A-Panel32 (Card)

□ Panel: Panel32 (Card)

□ Event Type: Access is granted

Figure 69. Event Log Report Filters

6. Provide the following information if you want to narrow down the report results.

   Descriptions. Type the percent sign (**%**), then type the text to search for in the event description. The report shows only events that contain this text in the event description.

   For example, to search for events that contain the facility code 1, type **%1**.

   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.

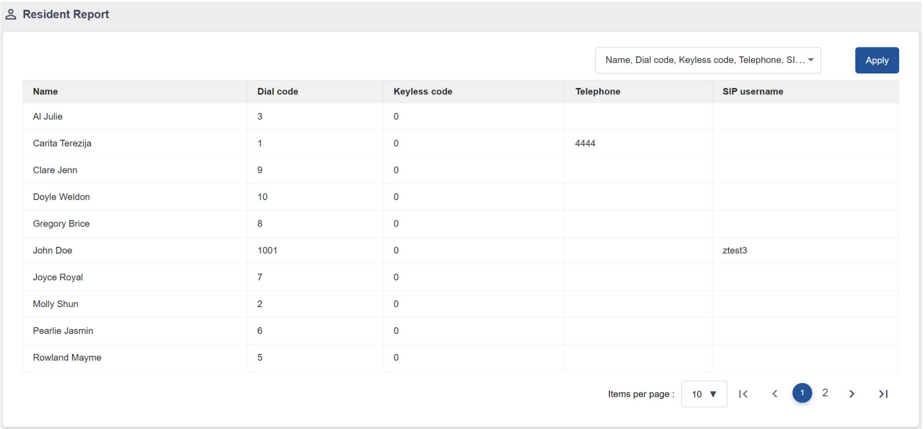
   Event Type. The report shows only events for this event type.

5.5 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.



Resident Report

Name, Dial code, Keyless code, Telephone, SI...

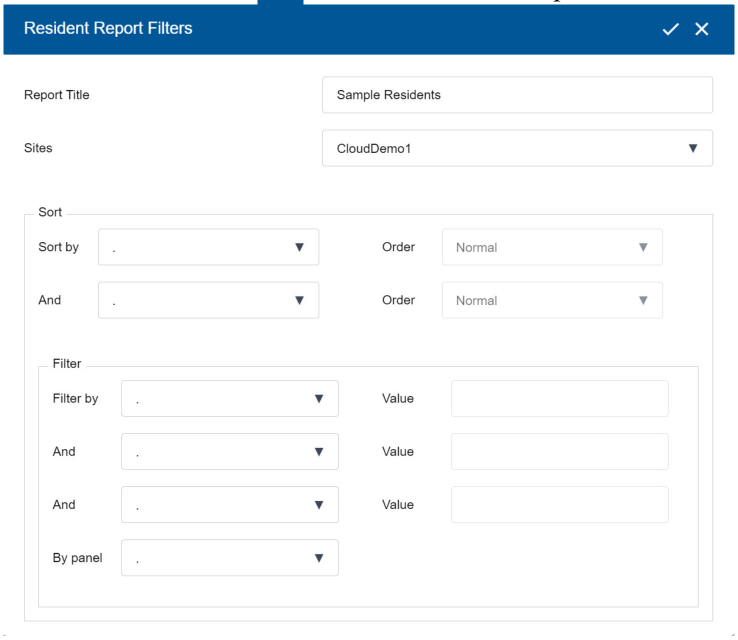
Apply

Name	Dial code	Keyless code	Telephone	SIP username
Al Julie	3	0		
Carita Terezija	1	0	4444	
Clare Jenn	9	0		
Doyle Weldon	10	0		
Gregory Brice	8	0		
John Doe	1001	0		ztest3
Joyce Royal	7	0		
Molly Shun	2	0		
Pearlie Jasmin	6	0		
Rowland Mayme	5	0		

Items per page : 10 ▼ |< < 1 2 > >|

Figure 70. Resident Report

2. Click the Edit button to edit the resident report.



Resident Report Filters ✓ ✕

Report Title: Sample Residents

Sites: CloudDemo1 ▼

Sort

Sort by: . ▼ Order: Normal ▼

And: . ▼ Order: Normal ▼

Filter

Filter by: . ▼ Value:

And: . ▼ Value:

And: . ▼ Value:

By panel: . ▼

Figure 71. Resident 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 **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.

Filter. Select up to 3 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,** select **Name** in the **Filter by** menu, then type **S** in the **Value** field.

To search for something within a name or number, use the percent sign (**%**).

For example, 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.

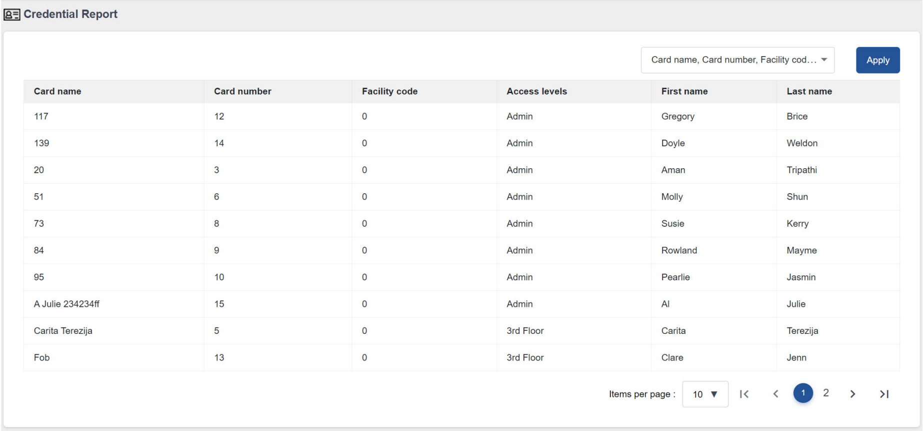
b. Select **Dial Code** in the **And** menu, then type **%5** in the **Value** field.

5.6 Credentials

You can generate a report of some or all of the credentials.

1. Click **Credentials** in the **Reports** pane.

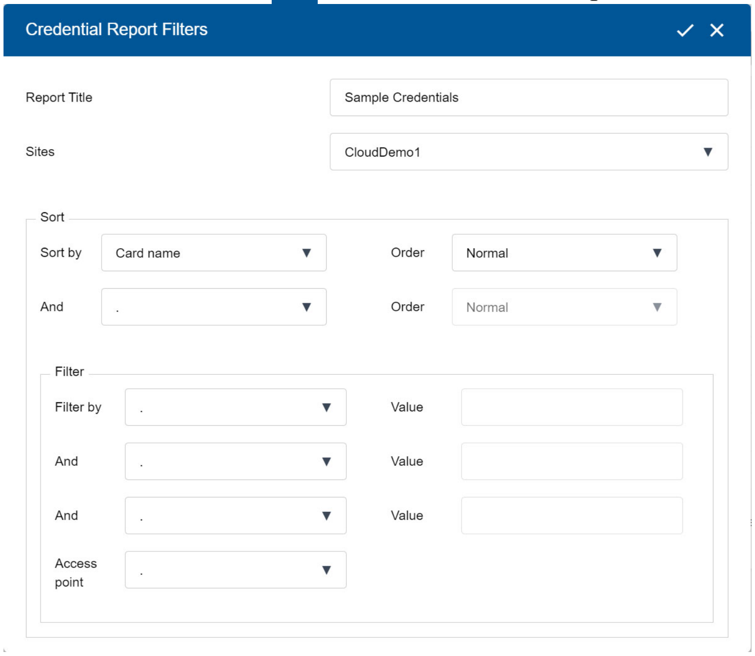
   The Credential Report window appears.



Card name	Card number	Facility code	Access levels	First name	Last name
117	12	0	Admin	Gregory	Brice
139	14	0	Admin	Doyle	Weldon
20	3	0	Admin	Aman	Tripathi
51	6	0	Admin	Molly	Shun
73	8	0	Admin	Susie	Kerry
84	9	0	Admin	Rowland	Mayme
95	10	0	Admin	Pearlie	Jasmin
A Julie 234234ff	15	0	Admin	Al	Julie
Carita Terezija	5	0	3rd Floor	Carita	Terezija
Fob	13	0	3rd Floor	Clare	Jenn

Figure 72. Credential Report

2. Click the Edit button ✎ to edit the credential report.



Credential Report Filters

Report Title: Sample Credentials

Sites: CloudDemo1 ▼

Sort

Sort by: Card name ▼ Order: Normal ▼

And: . ▼ Order: Normal ▼

Filter

Filter by: . ▼ Value:

And: . ▼ Value:

And: . ▼ Value:

Access point: . ▼

Figure 73. 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 3 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**, select **Facility Code** in the **Filter by** menu, and then type **1** in the **Value** field.

To search for something within a name or number, use the percent sign (**%**).

For example, 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.

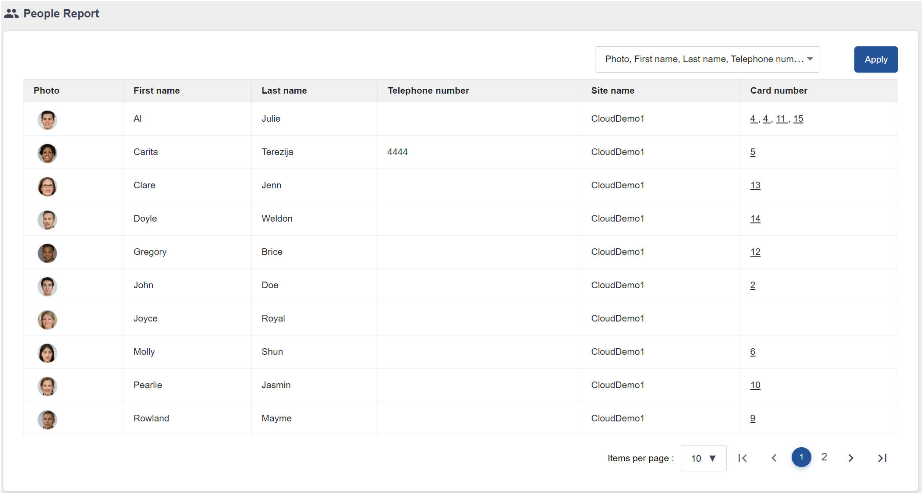
b. Select **Card Number** in the **And** menu, then type **%2** in the **Value** field.

5.7 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.



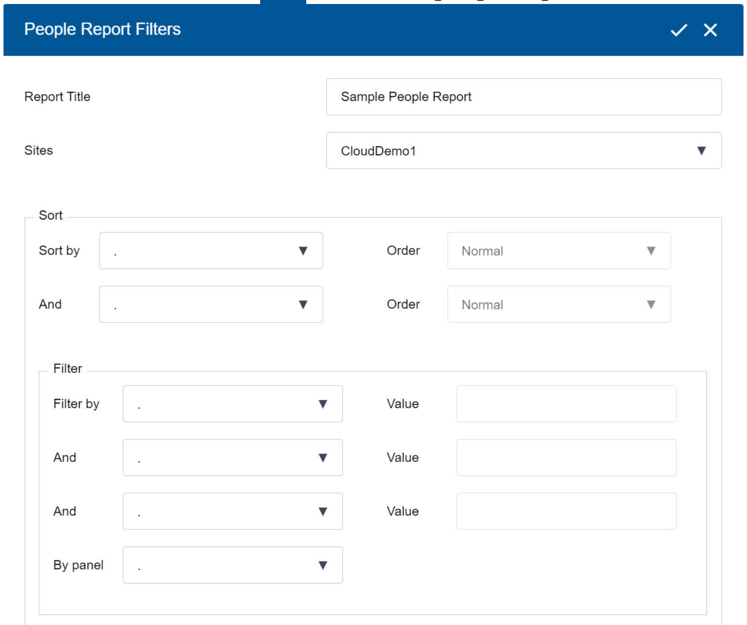
People Report

Photo	First name	Last name	Telephone number	Site name	Card number
	Al	Julie		CloudDemo1	4 , 4 , 11 , 15
	Carita	Terezija	4444	CloudDemo1	5
	Clare	Jenn		CloudDemo1	13
	Doyle	Weldon		CloudDemo1	14
	Gregory	Brice		CloudDemo1	12
	John	Doe		CloudDemo1	2
	Joyce	Royal		CloudDemo1	
	Molly	Shun		CloudDemo1	6
	Pearlie	Jasmin		CloudDemo1	10
	Rowland	Mayme		CloudDemo1	9

Items per page : 10

Figure 74. 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 75. 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 3 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,** select **Last Name** in the **Filter by** menu, then type **S** in the **Value** field.

To search for something within a name or number, use the percent sign (**%**).

For example, 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.

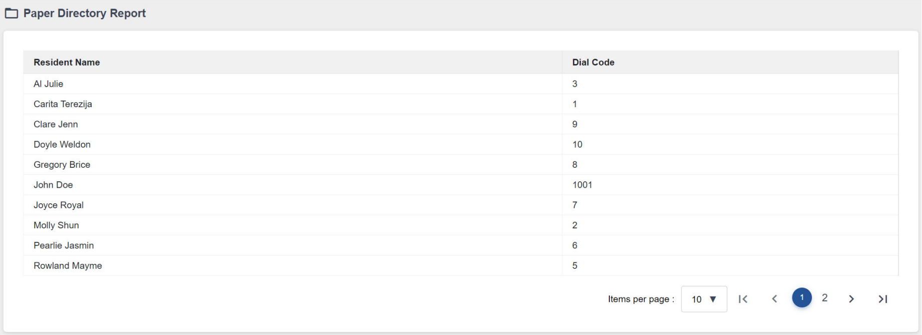
b. Select **Dial Code** in the **And** menu, then type **%5** in the **Value** field.

5.8 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.



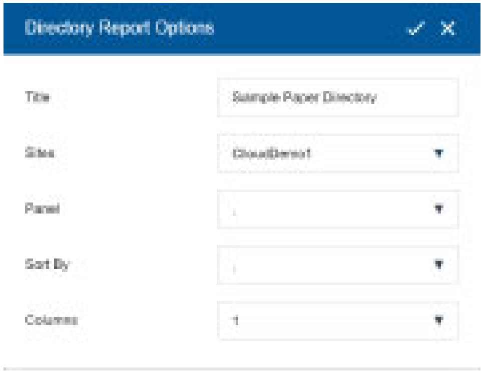
Paper Directory Report

Resident Name	Dial Code
Al Julie	3
Carita Terezija	1
Clare Jenn	9
Doyle Weldon	10
Gregory Brice	8
John Doe	1001
Joyce Royal	7
Molly Shun	2
Pearlie Jasmin	6
Rowland Mayme	5

Figure 76. Paper Directory Report

2. Click the Edit button ✎.

   The Directory Report Options window appears.



Directory Report Options

Title: Sample Paper Directory

Sites: CloudDemo1

Panel:

Sort By:

Columns: 1

Figure 77. 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.

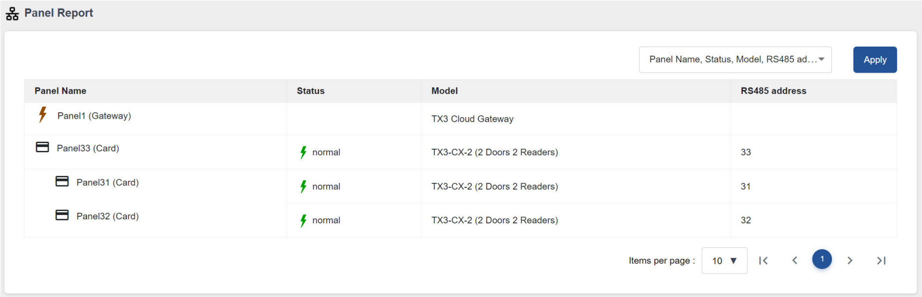
Columns. Select the number of columns. The report can have1, 2, or 3 columns per page.

5.9 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.

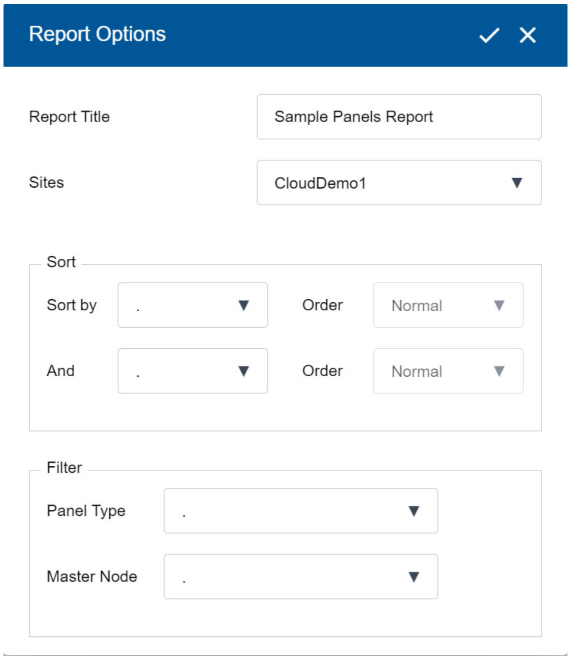


Panel Report

Panel Name	Status	Model	RS485 address
⚡ Panel1 (Gateway)		TX3 Cloud Gateway	
Panel33 (Card)	⚡ normal	TX3-CX-2 (2 Doors 2 Readers)	33
Panel31 (Card)	⚡ normal	TX3-CX-2 (2 Doors 2 Readers)	31
Panel32 (Card)	⚡ normal	TX3-CX-2 (2 Doors 2 Readers)	32

Figure 78. 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 79. 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 3 criteria to filter by. The report shows only entries that begin with the criteria that you select.

6 Compatible Products

TX3 Vision is compatible with the following products.

TX3 Product	Firmware Version
TX3-ER-8-A TX3-ER-8-B	SO-468 3.7.128 or higher SO-254 3.7.x or higher
TX3-NSL-12K-C	SO-467 3.7.3 or higher SO-460 3.7.2 or higher SO-255 3.0.x or higher SO-223 1.0.x, 1.1.x, 2.0.x
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
TX3-TOUCH-S22-D TX3-TOUCH-F22-D TX3-TOUCH-S22-E TX3-TOUCH-F22-E	SO-441 V3.x.x or higher
TX3-TOUCH-S15B-WR TX3-TOUCH-S15S-WR	SO-411 V3.x.x or higher
TX3-TOUCH-S15-E TX3-TOUCH-F15-E	SO-470 V3.x.x or higher
TX3-TOUCH-S22-F TX3-TOUCH-F22-F	SO-472 V3.x.x or higher
TX3-TOUCH-S15B-WR-A TX3-TOUCH-S15S-WR-A	SO-478 V3.x.x or higher

7 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.

4. **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:

5. **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.

6. **Inadequate Testing.** Most problems that would prevent an alarm a Mircom System from operating as intended can be discovered by 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:

7. **Inadequate Testing and Maintenance.** It is imperative that the systems be periodically tested and subjected to preventative maintenance. Best practices and local authority having jurisdiction 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.

8. **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.

9. **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.

10. **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.

11. **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.

12. **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.

13. **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.

14. **Wireless Devices Placement Proximity.** Moreover all wireless devices must be a minimum and maximum distance away from large metal objects, such as refrigerators. 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.

15. **Failure to Trigger Sensors.** Moreover, Mircom Systems may fail to operate as intended if motion, heat, 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.

3. **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.

4. **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.

5. **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.

6. **Telephone Lines Malfunction.** Telephone service can cause system failure where telephone lines are relied upon by a Mircom System. Alarms and information coming from a Mircom System may not be transmitted if a phone line is out of service or busy for a certain period of time. Alarms and information may not be transmitted where telephone lines have been compromised by criminal tampering, local construction, storms or earthquakes.

7. **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.

8. **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.

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