



TX3 Series

MiConnect Administrator Manual

Company Confidential - For Internal Use Only - Mircom Technologies Ltd. & Affiliates ("Mircom")
This information is confidential and the exclusive property of Mircom. It is intended for internal use and only for the purposes provided, and may not be disclosed to any third party without prior written permission from Mircom.



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

MiConnect Administrator Manual Version 0

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

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

Table of Contents

1	Introduction	5
1.1	MiConnect	5
1.2	MiEntry	5
1.3	Mircom SIP Service	5
1.4	Additional Documentation	6
1.5	Terms	7
2	Administrators	8
2.1	Dashboard	9
2.2	Account(s)	9
2.3	Child Accounts	14
2.4	Locations	19
2.5	Devices	21
2.6	Residents	29
2.7	Inventory	30
2.8	Reporting	32
2.9	Configuration	34
3	Warranty and Warning Information	37

List of Figures

Figure 1.	Dashboard (Administrators)	8
Figure 2.	Account(s)	9
Figure 3.	Add new account	9
Figure 4.	Existing Accounts	12
Figure 5.	Delegate Details	14
Figure 6.	Edit Child Account	15
Figure 7.	Edit User	16
Figure 8.	New User	17
Figure 9.	New Location	19
Figure 10.	Prices	20
Figure 11.	Example MiVision license	20
Figure 12.	New Service menu	21
Figure 13.	Existing Locations	21
Figure 14.	Add New Device	22
Figure 15.	Register Multiple New Devices	23
Figure 16.	Existing Devices	24
Figure 17.	New Resident	29
Figure 18.	Existing Residents	30
Figure 19.	My Vendors	31
Figure 20.	New Vendor	31
Figure 21.	Edit Contact	32
Figure 22.	Add a Vendor - Invoices	32
Figure 23.	Event Log Report	33
Figure 24.	Billing Report	33
Figure 25.	DID Report	34
Figure 26.	Roles & Permissions	35
Figure 27.	New Role	36

1

Introduction

This manual explains how to use Mircom's MiConnect portal.

For warranty and special notices see section 3.

This chapter explains

- MiConnect
- MiEntry
- Mircom SIP Service
- Additional Documentation
- Terms

1.1 MiConnect

The MiConnect portal is Mircom's online center for the management, monitoring and configuration of its online services.

The portal is for Mircom dealers and their customers such as building managers and resellers.

1.2 MiEntry

Mircom's MiEntry is an app for Android and iOS that provides SIP voice and video calling with TX3 voice entry products. MiEntry allows residents to verify the identity of their guests with live video and audio.

The app requires the Mircom SIP Service to receive calls from the lobby panels.

1.3 Mircom SIP Service

The Mircom SIP Service supports audio calls, video calls, and push notifications. Mircom has two SIP services for two different applications: MiVoIP and MiEntry SIP service.

SIP (Session Initiation Protocol) is a protocol that controls multimedia messaging on an IP network. TX3 voice entry products use SIP for IP telephony. To make audio and video calls using SIP, you need at least two SIP clients and one SIP server.

1.3.1 MiVoIP

Telephone Entry Systems can be fitted with a VoIP adapter (ATA) to provide the voice communications from the telephone entry panel to any cellular, home or business phone.

The VoIP adapter is a simple plug and play device that automatically makes all the required connections. A Mircom SIP Service subscription is required for activation.

1.3.2 MiEntry SIP service

MiEntry SIP service is the most reliable SIP service for the MiEntry application. It supports both audio and video communication as well as push notifications.

All usage can be monitored using the MiConnect portal. The MiConnect portal also allows creation, cancellations and suspension of the MiEntry users.

1.4 Additional Documentation

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

- LT-6638 TX3 MiEntry Manual
- LT-6679 MiVision Manual
- LT-6673 SPA112 Installation Guide
- LT-1194 TX3 Nano Configuration Manual
- LT-600213 IP Telephony Guide
- LT-995 TX3 System Configuration and Administration Manual
- LT-6637 TX3 Nano Installation Manual
- LT-600212 TX3-NANO-BB Installation Instructions
- LT-969 TX3 Telephone Access System Installation and Operation Manual
- LT-6906 UL TX3-CX Card Access System Manual
- LT-6082 Unified Building Solution Administration Guide

1.5 Terms

Analog telephone adapter (ATA): An ATA is a device that connects a traditional analog device, such as a telephone line, to a TCP/IP network.

Local Area Network (LAN): An IP network in a limited area, such as a building, that all the devices are connected to.

Registered: All devices that use SIP must be registered with the same SIP server.

SIP (Session Initiation Protocol): A protocol for controlling voice and video communication over an IP network.

SIP account details: A SIP username, SIP password, and address of the SIP server.

SIP Client: SIP clients are devices that communicate with each other using SIP.

SIP Server: A computer or program that monitors and establishes the call between SIP clients.

SIP Trunk: A method of connecting SIP clients to the PSTN or cellular network.

SIP Username: Every SIP client has a unique SIP username.

SIP Password: Every SIP client has a password for registering with the SIP server.

TCP/IP: The group of protocols that specify how computers communicate with each other over the Internet.

VOIP: Voice over IP.

2

Administrators

This portion of the site is only for users who have administrator access.

This chapter explains the following features:

- Dashboard
- Account(s)
- Child Accounts
- Locations
- Devices
- Residents
- Inventory
- Reporting
- Configuration

Note: Access to the options listed above varies based on the user account type. Different user roles (for example dealers, building managers, resellers) may have different permissions.

1. On the MiConnect portal, click **Administrators** in the upper right.

The Admin page appears.



Figure 1. Dashboard (Administrators)

2.1 Dashboard

The dashboard has a top menu option panel and quick action blocks.

The quick action blocks have numbers for reference. For example, in Figure 1 the number 49 in the Accounts block means that there are 49 accounts.

2.2 Account(s)

An account represents an organization. An account can have several users associated with it.

2.2.1 Add New Account

1. Click **Account(s)** in the top panel, then click **Add New Account**.

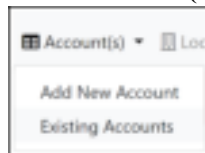


Figure 2. Account(s)

The **Account** window appears.





The screenshot shows the 'Account' form with the following fields and sections:


- Top Bar:** 'Account(s)' dropdown, 'Loc' icon, 'Add New Account', 'Existing Accounts'.
- Form Fields:**
 - Company Name* (e.g. ABCD Inc.)
 - Company Number
 - Dealer Number
 - Status*
 - Account Type* (Select Account Type)
 - Account Level* (Select Account Level)
 - Assigned by Mircom: Parent Account (e.g. N/A)
 - Assigned automatically when saved: MEntry Provider* (e.g. 001)
 - PSTN Provider* (e.g. 001)
 - Approved (checkbox)
- Navigation Tabs:** Profile, Users, Locations, Devices, Reservations, Child-Accounts.
- Form Fields (continued):**
 - First Name* (e.g. Mircom)
 - Last Name* (e.g. Mircom)
 - Street Number (e.g. 10)
 - Street (e.g. 10000 Street South)
 - Unit Abv. (e.g. Suite)
 - Phone (e.g. 0000-000-0000)
 - Mobile (e.g. 0000-000-0000)
 - Country (Select Country)
 - City (e.g. North York)
 - Province / State (Select a Country)
 - Postal Code (Select a Country)
 - Account Expiration
 - Account Disabled (Yes/No)

Figure 3. Add new account

2. Fill out these fields. The fields with asterisks are mandatory.
 - Company Name*
 - Company Number (Assigned by Mircom)
 - Dealer Number (Assigned automatically when saved)

- Status* (Select from Active, Suspend, Closed)
 - Account Type* (Select from Admin, Reseller, Installer, Building Manager)
 - Account Level* (Select from Basic, Premium, or Demo)
 - Parent Account (Select N/A or an account from the list of Existing Accounts)
 - MiEntry Provider* (leave as is)
 - PSTN Provider* (leave as is)
 - Approved (select on or off)
3. Under **Profile**, fill out these fields. The fields with asterisks are mandatory.
- First Name*
 - Last Name*
 - Phone
 - Mobile
 - Email*
 - Street Number
 - Street
 - Unit No
 - Country (select from Canada and United States)
 - City
 - Province / State
 - Postal Code
 - Account Expiration (Select date from calendar, leave blank if there is no expiration date)
4. Click the **Save Changes** button  to save the account.

After you save the account, an email confirmation will be sent to the email associated with the account. The user must verify their email address when they receive it. If they do not receive it, click the **Resend Email Confirmation** button  at the bottom.

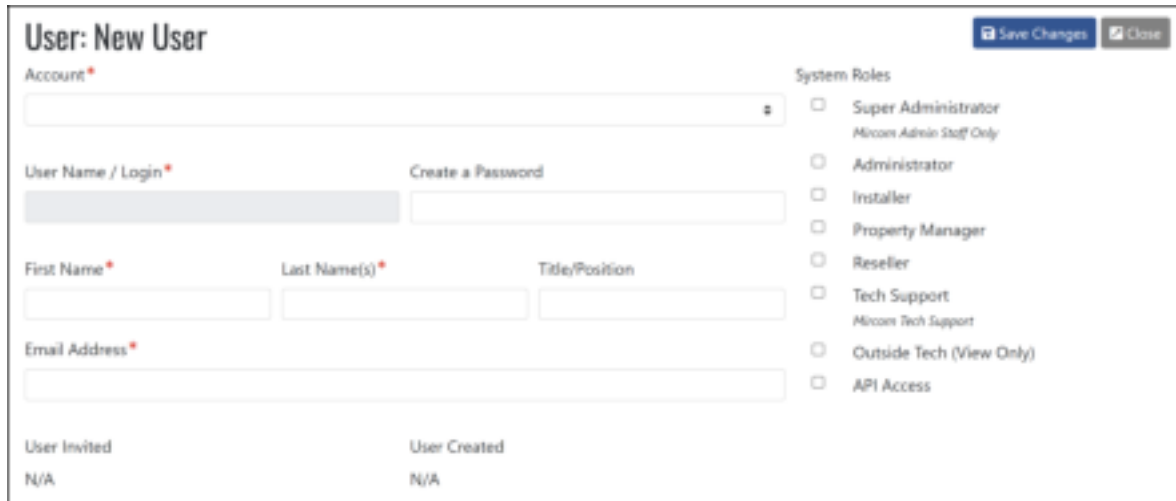
If the email is not verified, the page shows the Unconfirmed  sign next to the email address.

After you save the account, you can access the **Users, Locations, Devices, Residents, Delegates**, and **Child Accounts** tabs. You can also access these features when you click on an existing saved account. You can also delete the account by clicking the **Remove Account** button.

2.2.2 Add New User


An account can have several users associated with it.


1. On the **Users** tab, click the **Add New User** button at the bottom of the window to add a user to the account you just created.



2. Fill out these fields. The fields with asterisks are mandatory.
 - Account* (Select the account that you want to add the user to)
 - User Name/Login* (Select from Active, Suspend, Closed)
 - Create a Password (The user will create a new password when they receive the email confirmation)
 - First Name*
 - Last Name(s)*
 - Title/Position
 - Email Address*
 - System Roles (select one or all)
 - Super Administrator (Mircom Admin Staff Only)
 - Administrator
 - Installer
 - Property Manager
 - Reseller
 - Tech Support
 - Mircom Tech Support
 - Outside Tech (View Only)
 - API Access

- Click the **Save Changes** button  to add the user to the account.

After you save the user, an email confirmation will be sent to the email associated with the user. The user must verify their email address when they receive it. They will also create a new password. If they do not receive the email, click the **Resend Email Confirmation** button  at the bottom.

If the email is not verified, the page will show the Unconfirmed  sign next to the email address.

2.2.3 Edit Existing Account


- Click **Accounts > Existing Accounts** from the top menu panel.

The list of existing accounts appears.



Accounts									
Company		Type	Plan	Contact	City	Province/State	Approved	Status	Created
Building Manager	Basic				New York	NY			2023-11-23 14:03:30
Building Manager	Basic				Test	OH			N/A

Figure 4. Existing Accounts

- To filter the list by location, click the **Provinces/States** menu at the top.
- Click an account to edit it.
- Edit the account profile by following the instructions in section 2.2.1.
- To edit or add users, locations, and devices, and to edit residents, delegates and child accounts, click the corresponding tab and follow the instructions below.
- Click the **Save Changes** button  when you are done.

2.2.4 Users

- Click the Users tab to view users and add new users to this account.
- To edit a user, click a user, then follow the instructions in section 2.2.2.
- To add a user, click **Add New User** at the bottom of the screen, then follow the instructions in section 2.2.2.

2.2.5 Locations

1. Click the Locations tab to view locations and add new locations to this account.
2. To edit a location, click a location, then follow the instructions in section 2.4.1.
3. To add a location, click **Add New Location** at the bottom of the screen, then follow the instructions in section 2.4.1.

2.2.6 Devices

1. Click the Devices tab to view devices and add new devices to this account.
2. To edit a device, click a device, then follow the instructions in section 2.5.1.
3. To add a device, click **Add New Device** at the bottom of the screen, then follow the instructions in section 2.5.1.

2.2.7 Residents


1. Click the Residents tab to view residents and add new residents to this account.
2. To edit a residents, click a resident, then follow the instructions in section 2.6.1.

2.2.8 Delegates

You can grant other people permission to add or remove residents for buildings that you own without giving ownership to another account. These other people are called delegates.

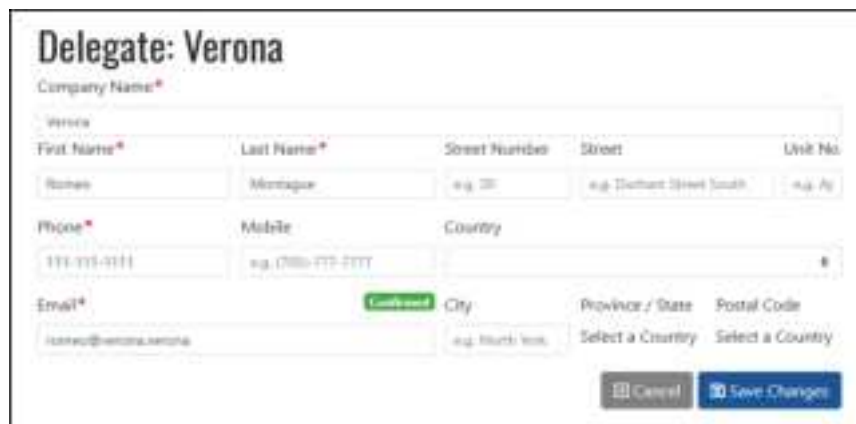
1. Click the Delegates tab to view delegates for this account.

Note: You cannot invite delegates from this screen.

2. To edit a delegate, click the **Edit** button  to the right.

The Delegate Details page lets you edit the delegate's company information, name, address, and email.

Note: When the delegate confirms their email address, the word **Confirmed** appears. If the delegate has not yet confirmed the email address, then the word **Unconfirmed** appears.



Delegate: Verona

Company Name*

Verona

First Name* Last Name* Street Number* Street* Unit No.*

Romeo Montague e.g. 20 e.g. 1234567890 e.g. A

Phone* Mobile* Country*

111-111-1111 e.g. (111) 111-1111

Email* City* Province/State* Postal Code*

romeo@verona.com e.g. North York Select a Country Select a Country

Confirmed

Cancel Save Changes

Figure 5. Delegate Details

- Click the **Save Changes** button  to save the delegate.

2.3 Child Accounts

An account represents an organization, with users and locations associated with it. A child account is a subdivision of that organization, or a related organization, with its own users and locations. For example, a child account can be a reseller that buys products from the parent account company. A child account has all the same permissions that the parent account does.

- In the Accounts screen, click the Child Accounts tab to view child accounts for this account.
- To edit a child account, click the child account you want to edit.

The Edit Child Account screen appears.

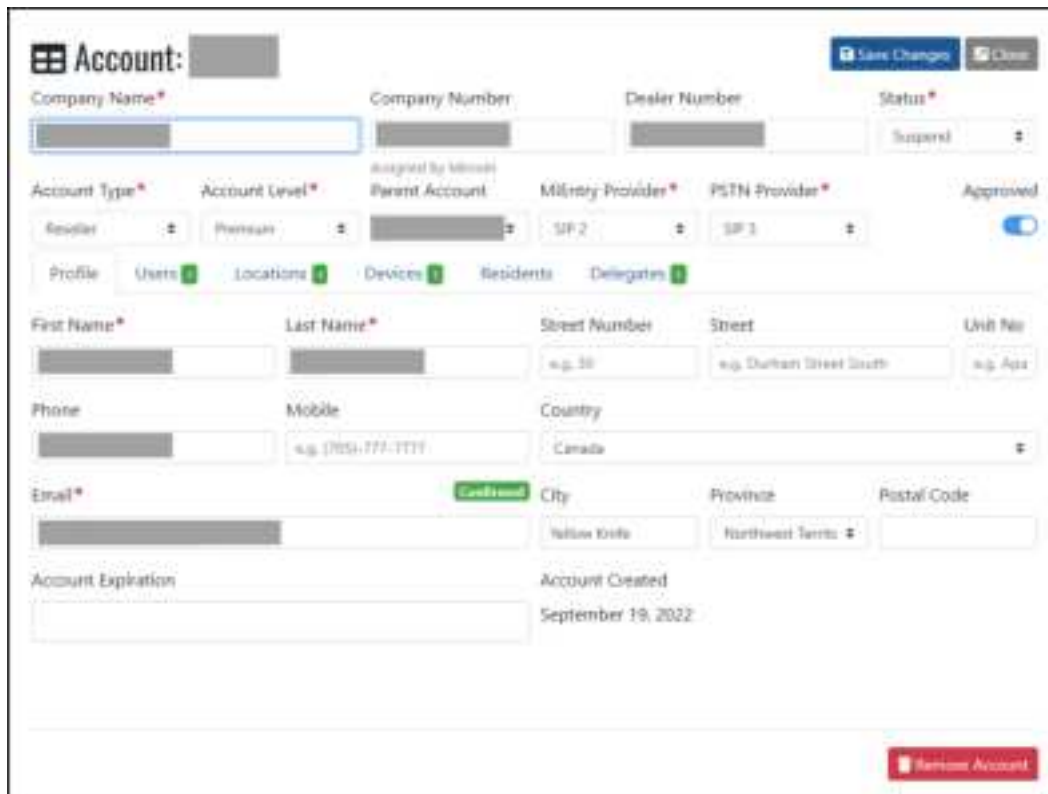



Figure 6. Edit Child Account

Provide the following information:

- Company Name
 - Company Number
 - Dealer Number
 - Account Type
 - Status: Select **Active**, **Suspend**, or **Closed**.
 - Account Level
 - Parent Account
 - MiEntry Provider
 - PSTN Provider
 - Approved: An administrator must approve every child account.
3. Click the **Save Changes** button  to save your changes.

2.3.1 Child account profile

1. Click the **Profile** tab to edit the child account's profile.
2. Provide the following information:
 - First Name
 - Last Name
 - Phone
 - Email Address
 - Account Expiration: This field is not used.
 - Address
 - Account Expiration
 - Account Created: This is automatically generated.

2.3.2 Child account users

Edit a User

1. Click the Users tab to view users and add new users to this child account.
1. Click the user you want to edit.

The Edit User screen appears.

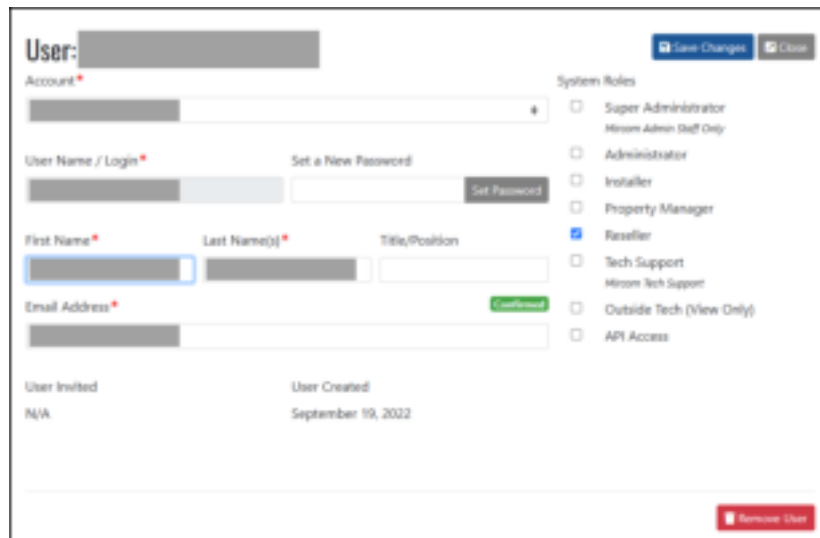


Figure 7. Edit User

The fields that can be edited are:

- Account

- Password
- First Name
- Last Name
- Position
- Email Address
- System Roles

Note: **Confirmed** status will appear next to the user if their email is verified, and **Unconfirmed** if the email is not verified.

2. Click the **Save Changes** button  to save your changes.

Remove a User

1. Click the **Remove User** button at the bottom of the Edit User screen.
2. Click **OK** to remove the user. Or click **CANCEL** to go back.

Add a User

1. Click the **Add New User** button at the bottom of the list of users.

The New User screen appears.

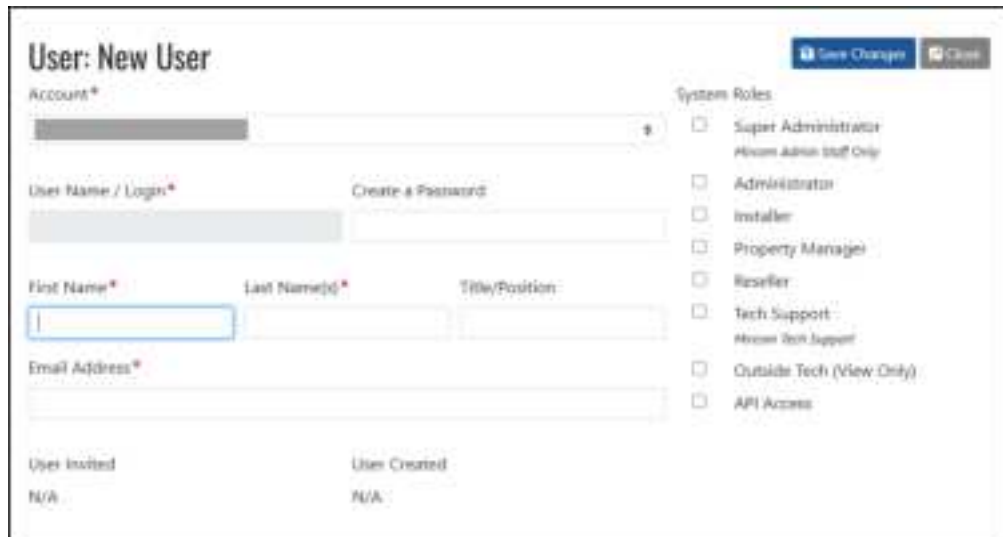



Figure 8. New User

2. Provide the following information:
 - Account: Select the child account this user is for

- User Name/Login
 - Create a Password
 - First Name
 - Last Name (optional)
 - Position (optional)
 - Email Address
 - System Roles
3. Click the **Save Changes** button  to save your changes.

2.3.3 Child account locations

1. Click the Locations tab to view locations associated with this child account.
2. To edit a location, click a location, then follow the instructions in section 2.4.1.
3. To add a location, click **Add New Location**, then follow the instructions in section 2.4.1.


2.3.4 Child account devices

1. Click the Devices tab to add a device to this child account.
2. To edit a device, click a device, then follow the instructions in section 2.5.3.
3. To add a device, click **Add New Device**, then follow the instructions in section 2.5.1.

2.3.5 Child account residents

1. Click the Residents tab to view the residents for this child account.
2. To edit a resident, click a resident, then follow the instructions in section 2.6.1.

2.3.6 Child account delegates

1. Click the Delegates tab to view the delegates for this child account.
2. To edit a delegate, click the **Edit** button  to the right.
3. See section 2.2.8.

2.3.7 Remove a child account

1. In the Edit Child Account screen (Figure 6), click the **Remove Account** button at the bottom.
2. Click **OK**.

2.4 Locations

A location is a building. You can add locations to an account.

2.4.1 Add New Location

1. Click **Location > Add New Location** from the top menu panel.

Note: This is the same as clicking **Add New Location** in the **Location** tab of an Account.



Figure 9. New Location

2. Fill out these fields. The fields with asterisks are mandatory.
 - Location Name/ Designation*
 - Owner*
3. In the **Physical Address** tab, fill out these fields. The fields with asterisks are mandatory.
 - Street Number*
 - Street Name*
 - Unit No
 - Country (Select from Canada and United States)
 - City
 - Province / State (Select from drop-down list)
 - Postal Code
4. Click the **Installed Devices** tab, then click a device to edit it (section 2.5.3), or click **Add New Device** (section 2.5.1).
5. Click the **Residents** tab, then click **Add New Resident** and follow the instructions in section 2.6.1.

6. Click the **Prices** tab, then enter the reseller's price charged to the building per user.



Figure 10. Prices

7. Click the **MiVision Licenses** tab.

The registered site license attached to that location is listed. If there is none, you can create one.

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

8. Click the **Create Site License** button.

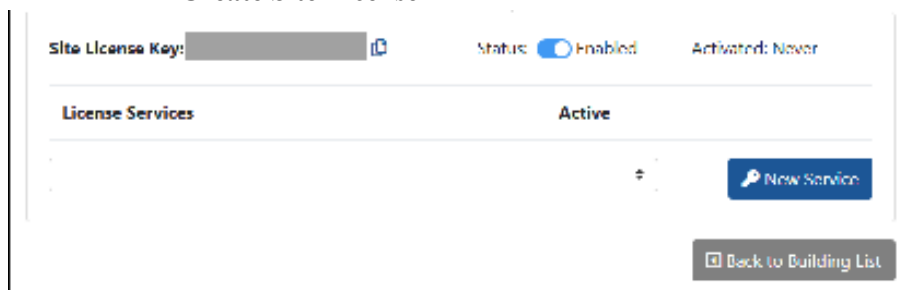



Figure 11. Example MiVision license

- Site License Key: This is automatically generated. Click the icon  beside this number to copy it, and then paste it into the Site Subscription window in MiVision. See LT-6679 MiVision Manual.
9. Select **Enabled** or **Disabled** for the status.
- Activated: When the license is activated (by pasting the Site License Key into MiVision), the activation date appears here.

10. Select a service from the menu next to the **New Service** button, then click **New Service** to activate it.



Figure 12. New Service menu

11. Click the **Save Changes** button. 

2.4.2 Edit Existing Location

1. Click **Locations** > **Existing Locations** from the top menu panel.

The list of existing locations appears.

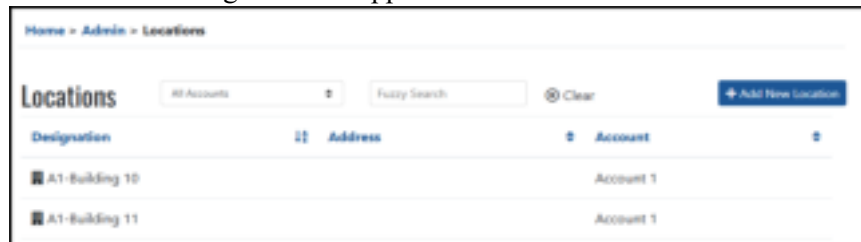


Figure 13. Existing Locations

2. To filter the list by account, click the **Accounts** menu at the top.
3. Click a location to edit it. The procedure for editing a location is the same as adding (section 2.4.1).

2.5 Devices

You can add devices to an account and a location. This helps keep track of which devices are installed in which buildings.

2.5.1 Add New Device

1. Click **Device > Add New Device** from the top menu panel.

Note: This is the same as clicking **Add New Device** in the **Device** tab of an Account.

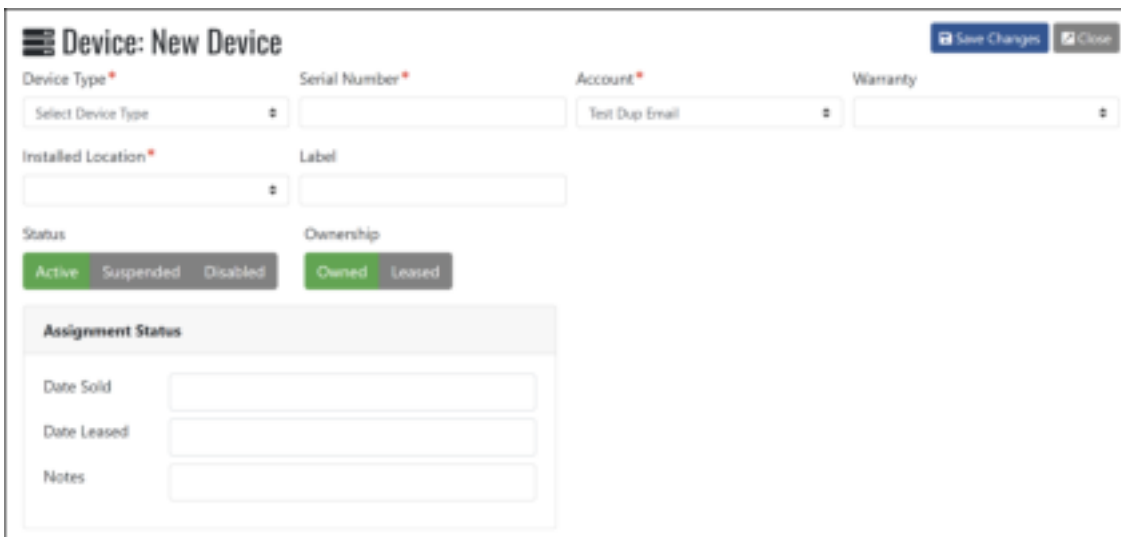



Figure 14. Add New Device

2. Fill out the fields. The fields with asterisks are mandatory.
 - Device Type* (select from list of devices)
 - Serial Number* (The serial number is printed on an orange sticker, which is on the back of the TX3 Nano, and on the inside metal chassis of the TX3 Touch. It is on the back of the SPA112 and on the bottom of the HT801/HT802.)
 - MAC Address* (if present. The MAC address is a 12 digit address that identifies each device. It is printed on the bottom of the SPA112 and HT801/HT802. Press and hold the Home button on the TX3 Nano for 10 seconds to see its MAC address. TX3 Touch devices do not require MAC addresses.)
 - Account* (Select from list of existing accounts)
 - Warranty (Select from No Warranty, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 years)
 - Installed Location* (Select from list of existing locations)
 - Label (type a descriptive label for the device)
 - Status (Select from Active, Suspended, Disabled. If a device is suspended, it will not be added to the billing report.)
 - Ownership (Select from Owned and Leased)

- Assignment Status (Fill in details for Date Sold, Date Leased, and add Notes if needed)

3. Click the **Save Changes** button  to save the device.

2.5.2 Register Multiple New Devices

You can add more than one of the same type of device at once.

1. Click **Devices** in the top panel, then click **Bulk Add Devices**.



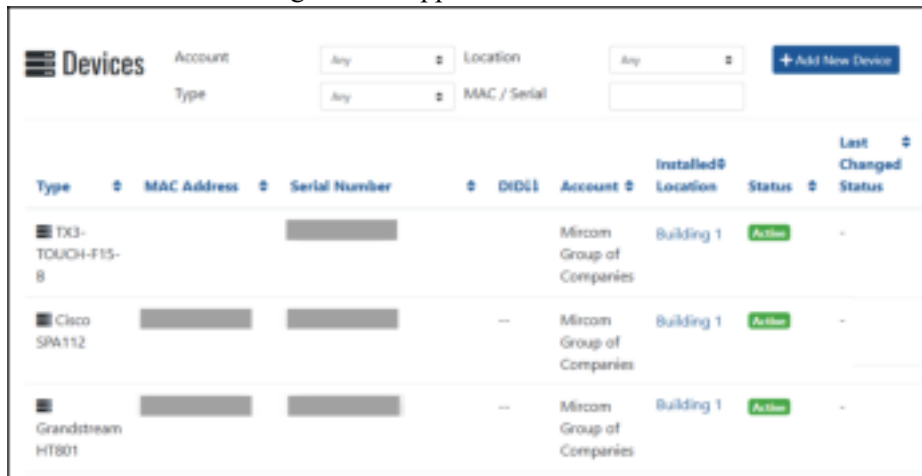
Figure 15. Register Multiple New Devices

2. Fill out these fields. The fields with asterisks are mandatory.
- Device Type* (select from list of devices)
 - Number of Devices*
 - Warranty (Select from No Warranty, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 years)
 - Serial Number and MAC Address* (Enter the serial number and MAC address for each device. TX3 Touch devices do not require MAC addresses)
3. Click **Save Changes**.

2.5.3 Edit Existing Device

1. Click **Devices > Existing Devices** from the top menu panel.

The list of existing devices appears.



The screenshot shows a web interface for managing devices. At the top, there are filter menus for 'Account' (Any), 'Location' (Any), 'Type' (Any), and 'MAC / Serial'. A '+ Add New Device' button is on the right. Below the filters is a table with columns: Type, MAC Address, Serial Number, DID, Account, Location, Status, and Last Changed Status. Three devices are listed: a TX3-TOUCH-F15-8, a Cisco SPA112, and a Grandstream HT801. All are installed in 'Building 1' and have an 'Active' status.

Type	MAC Address	Serial Number	DID	Account	Location	Status	Last Changed Status
TX3-TOUCH-F15-8				Mircom Group of Companies	Building 1	Active	-
Cisco SPA112			--	Mircom Group of Companies	Building 1	Active	-
Grandstream HT801			--	Mircom Group of Companies	Building 1	Active	-

Figure 16. Existing Devices

2. To filter the list, click one of the menus at the top: **Account**, **Type**, **Location**, **MAC / Serial**.

3. Click a device to edit it. The procedure for editing a device is the same as adding (section 2.5.1).

The device's details consist of the following information.

Table 1: Cisco SPA112 and Grandstream HT801/HT802 Device Details

Device Type	Grandstream HT801, Grandstream HT802, or SPA112.
Serial Number	The serial number is printed on the back or bottom of the device.
MAC Address	A unique 12 digit address that identifies each device. It is printed on the bottom of the device.
Account	Select an account that the device belongs to.
Warranty	Select from No Warranty, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 years.
Installed Location	The location where the device is installed. Note: if the device does not have a location, then its Status is Inactive in the My Devices list.
Label	A label for identifying the device.
PSTN Provider	
DID Number	The direct inward dialing (DID) number is a local telephone number assigned to the device.
Display Name	This name appears on phones that the device calls.
Provisioning Status	This indicates whether the provisioning server has configured the device.
Last Communication	This is the last time that the device has called the provisioning server. The device calls the provisioning server every 30 minutes.
Timezone	The time zone of the location where the device is installed.
Device Lock	

Table 1: Cisco SPA112 and Grandstream HT801/HT802 Device Details (Continued)

Status	Select Active to provision the device. When the device is active it is working normally and is billable. Select Suspended to suspend the device. When suspended, it is still billable, but it cannot make calls. Select Disabled to disable the device. When disabled, it cannot make calls, its DID number and display name are erased, and it is not billable.
Ownership	Owned: Mircom will unlock the device if you cancel your account. Leased: The device is locked and cannot be reset.
Reset Password When Saved	See <i>Reset a device's password (SPA112 and Grandstream HT801/HT802)</i> on page 28.
Device Reload	
Device Expiration	Select a date for expiration, or leave blank if there is no expiration.
Device Activated	The date the device was activated.
Hardware	HT801/HT802 only. This information is automatically generated.
Firmware	
Last Reboot	
IPv4	
IPv6	
Load Device Information	HT801/HT802 only. Click this button to display information on the HT801/HT802.
Date Sold	Select the date the device was sold.
Date Leased	Select the date the device was leased.
Notes	Any notes for the device.

Table 1: Cisco SPA112 and Grandstream HT801/HT802 Device Details (Continued)

Reboot	HT801/HT802 only. Click this button to restart the device.
Firmware Upgrade	
Factory Reset	

Table 2: TX3 Device Details

Device Type	TX3 Nano or TX3 Touch.
Serial Number	The serial number is printed on an orange sticker, which is on the back of the TX3 Nano, and on the inside chassis of the TX3 Touch.
Account	Select an account that the device belongs to.
Warranty	Select from No Warranty, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 years
Installed Location	The location where the device is installed. Note: if the device does not have a location, then its Status is Inactive in the My Devices list.
Label	A label for identifying the device.
MiEntry Provider	
MAC Address	TX3 Nano only. A 12 digit address that identifies each device. Press and hold the Home button on the TX3 Nano for 10 seconds to see its MAC address.
SIP Username	This information is automatically generated and must be entered in the TX3 Configurator before the TX3 device can make VOIP calls. See LT-995 <i>TX3 System Configuration and Administration Manual</i> .
Auth Username	
SIP Password	
SIP Domain	
SIP Proxy Domain	

Table 2: TX3 Device Details (Continued)

Status	Select Active to provision the device. When the device is active it is working normally and is billable. Select Suspended to suspend the device. When suspended, it is still billable, but it cannot make calls. Select Disabled to disable the device. When disabled, it cannot make calls, its DID number and display name are erased, and it is not billable.
Ownership	Select Owned or Leased .
Device Expiration	Select a date for expiration, or leave blank if there is no expiration.
Device Activated	The date the device was activated.
Date Sold	Select the date the device was sold.
Date Leased	Select the date the device was leased.
Notes	Any notes for the device.

Reset a device's password (SPA112 and Grandstream HT801/HT802)

1. Click the button beside **Reset Password When Saved**.
2. Click **Save Changes**.
3. Click the device in the **My Devices** list to view the new password.


Note: If you reset a device's password, it can take up to 30 minutes for the change to take effect. You can restart the device to force the change to take effect immediately.

2.6 Residents

2.6.1 Add New Resident

1. Click **Residents** in the top panel, then click **Add New Resident**.

Figure 17. New Resident

2. Fill out these fields. The fields with asterisks are mandatory.
 - Account* (Select the account of the building manager or reseller that this resident is linked to)
 - First Name(s)*
 - Last Name(s)*
 - Phone
 - Mobile
 - Email* (Once email is verified, the sign **Confirmed** will appear)
3. Click the **Save Changes** button  to save the resident to the account.

When the resident is saved, the Residency and MiEntry Accounts tabs appear.

4. Click the **Residency** tab, then click the **Add Resident to Building** button.
5. Fill out these fields.
 - Building
 - Unit
 - Primary Residence (Select if this building is the resident's primary residence)
6. Click the **Add Residency** button.

7. Click the **MiEntry Accounts** tab.

Note: You cannot edit this tab until the resident's email is confirmed.

8. If this resident does not have a MiEntry account, click the **Add MiEntry Account** button to add one. The username is automatically generated. An email is sent to the resident with instructions on creating a MiEntry password.

Note: The **MiEntry Card Access** tab is not used.

2.6.2 Edit Existing Resident

1. Click **Residents > Existing Residents** from the top menu panel.

The list of existing residents appears.



Figure 18. Existing Residents

2. To filter the list by account, click the **All Accounts** menu at the top.
3. Click a resident to edit it. The procedure for editing a resident is the same as adding (section 2.6.1).

2.7 Inventory

Inventory is a list of devices and vendors.

2.7.1 Inventory

1. Click **Inventory** in the top panel, then click **Inventory**.
2. See section 2.5.3.

2.7.2 Vendors

1. Click **Inventory** in the top panel, then click **Vendors**.

The list of existing vendors appears.



Home > Admin > Devices > Vendors

My Vendors

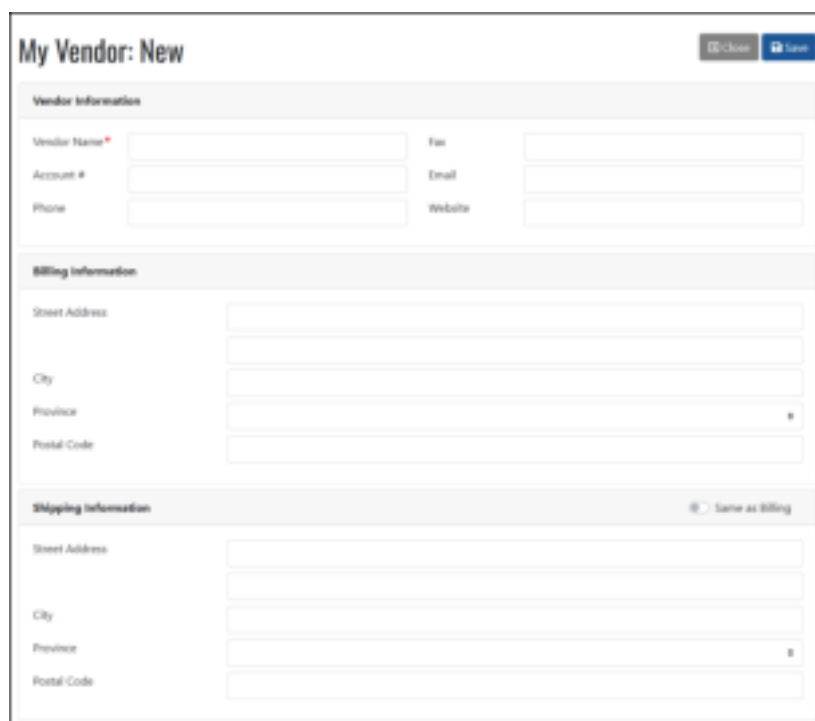
Vendor	City	Phone	Email	Website
Gentek				
Mircom				http://mircom.com

[Add a Vendor](#)

Figure 19. My Vendors

Add a Vendor

- Click **Add a Vendor** to add a vendor.



My Vendor: New

[Clear](#) [Save](#)

Vendor Information

Vendor Name* Fax

Account # Email

Phone Website

Billing Information

Street Address

City

Province

Postal Code

Shipping Information ☐ Same as billing

Street Address

City

Province

Postal Code

Figure 20. New Vendor

- Fill out the fields. Only the Vendor Name is mandatory.

4. Click **Add a Contact** to add a contact to the vendor, then click **Save** to save the contact.




Figure 21. Edit Contact

5. In the **Invoices** section, add an invoice by entering the **Invoice Number**, selecting the **Invoice Date**, and choosing a file to upload.



Figure 22. Add a Vendor - Invoices

6. Click the **Save** button at the top to save vendor.

Edit Existing Vendor

1. Click a vendor in the **My Vendors** list. The procedure for editing a vendor is the same as adding (*Add a Vendor* on page 31).

2.8 Reporting

The Reporting feature lets you download event logs and billing logs.

2.8.1 View Event Log

1. Click **Reporting > View Event Log** from the top menu panel.

The event log report appears.



The interface shows two calendar pickers for selecting a date range. The 'From' calendar is for July 2024, and the 'To' calendar is for August 2024. Both calendars have the 19th of the month selected. A 'Generate Report' button is located at the bottom right.

Figure 23. Event Log Report

2. Select a **From** date and a **To** date, then click **Generate Report** to download the report in a CSV (comma separated value) file to the Downloads folder of the local computer.

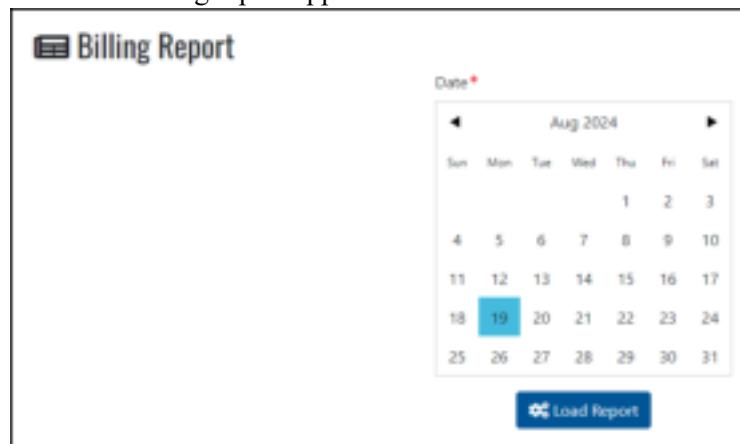
2.8.2 View Billing Log

This feature is not used.

2.8.3 View Billing Log V2

1. Click **Reporting > View Billing Log V2** from the top menu panel.

The billing report appears.



The interface shows a single date picker for August 2024. The 19th of the month is selected. A 'Load Report' button is located at the bottom right.

Figure 24. Billing Report

2. Select a date, then click **Load Report**.

The report appears.

3. Click **Download CSV File** to download the report in a CSV (comma separated value) file to the Downloads folder of the local computer.

2.8.4 DID Report

The DID (direct inward dialing) number is a local telephone number assigned to the SPA112 and HT801/HT802. The DID report shows the active DIDs.

1. Click **Generate PDF** or **Generate CSV** to download a PDF or CSV version of the DID report to the Downloads folder of the local computer.



ID	Company Number	Company Name	Location	DID	Start Date
493		Mircom Group of Companies	Building 2		2024-08-16
492			Building 1		2024-06-28
474			Building 1		2024-06-10
473			Building 1		2024-05-22
472			Building 1		2024-05-22

Figure 25. DID Report

2.9 Configuration

2.9.1 Add New Users

This feature is the same as section 2.2.2.

2.9.2 Existing Users

1. Click **Configuration > Existing Users** from the top menu panel.
The screen shows all the existing users that you have access to.
2. To edit a user, click the user, then follow the instructions in section 2.2.2.

There is a difference between this screen and the Add New User screen in section 2.2.2: you can resend the user's email verification from this screen.

2.9.3 Manage Roles and Permissions

There are eight roles:

- Super Administrator
- Administrator
- Installer

- Property Manager
- Reseller
- Tech Support
- Outside Tech (View Only)
- API Access



Role Name	Description
<input checked="" type="checkbox"/> Super Administrator	Mircom Admin Staff Only
<input checked="" type="checkbox"/> Administrator	
<input checked="" type="checkbox"/> Installer	
<input checked="" type="checkbox"/> Property Manager	
<input checked="" type="checkbox"/> Reseller	
<input checked="" type="checkbox"/> Tech Support	Mircom Tech Support
<input checked="" type="checkbox"/> Outside Tech (View Only)	
<input checked="" type="checkbox"/> API Access	

Figure 26. Roles & Permissions

1. Click a role to change its permissions, or click **Add New Role** to make a new role.
2. Type a **Role Name** and **Description**.
3. Select the permission for the role.

4. Click **Save Changes**.



Role: New Role

Role Name *

Description

Action Permissions for this Role

<input type="checkbox"/> VIEW_ACCOUNT_LIST	<input type="checkbox"/> EDIT_ACCOUNT	<input type="checkbox"/> ADD_ACCOUNT
<input type="checkbox"/> DELETE_ACCOUNT	<input type="checkbox"/> EDIT_OWNED_ACCOUNT_PROFILE	<input type="checkbox"/> VIEW_LOCATION_LIST
<input type="checkbox"/> EDIT_LOCATION	<input type="checkbox"/> ADD_LOCATION	<input type="checkbox"/> DELETE_LOCATION
<input type="checkbox"/> VIEW_DEVICE_LIST	<input type="checkbox"/> EDIT_DEVICE	<input type="checkbox"/> ADD_DEVICE
<input type="checkbox"/> DELETE_DEVICE	<input type="checkbox"/> VIEW_USER_LIST	<input type="checkbox"/> EDIT_USER
<input type="checkbox"/> ADD_USER	<input type="checkbox"/> DELETE_USER	<input type="checkbox"/> VIEW_ROLE_LIST
<input type="checkbox"/> EDIT_ROLE	<input type="checkbox"/> ADD_ROLE	<input type="checkbox"/> DELETE_ROLE
<input type="checkbox"/> VIEW_GROUP_LIST	<input type="checkbox"/> EDIT_GROUP	<input type="checkbox"/> ADD_GROUP
<input type="checkbox"/> DELETE_GROUP	<input type="checkbox"/> VIEW_RESIDENT_LIST	<input type="checkbox"/> EDIT_RESIDENT
<input type="checkbox"/> ADD_RESIDENT	<input type="checkbox"/> DELETE_RESIDENT	<input type="checkbox"/> VIEW_ADMMAL_DASHBOARD
<input type="checkbox"/> VIEW_ACCOUNT_TYPE_LIST	<input type="checkbox"/> EDIT_ACCOUNT_TYPE	<input type="checkbox"/> DELETE_ACCOUNT_TYPE
<input type="checkbox"/> ADD_ACCOUNT_TYPE	<input type="checkbox"/> RECEIVE_ACTIVATION_EMAILS	<input type="checkbox"/> IDDOO
<input type="checkbox"/> VIEW_EVENT_LOG	<input type="checkbox"/> VIEW_BILLING_LOG	<input type="checkbox"/> EDIT_TOOLTIPS
<input type="checkbox"/> VIEW_SIP_PROVIDERS	<input type="checkbox"/> EDIT_SIP_PROVIDERS	<input type="checkbox"/> EDIT_PROVISIONING
<input type="checkbox"/> ADD_AFFILIATE	<input type="checkbox"/> EDIT_DEVICE_LOCK	<input type="checkbox"/> EDIT_DISPLAY_NAME
<input type="checkbox"/> EDIT_DID	<input type="checkbox"/> ADD_VENDOR	<input type="checkbox"/> EDIT_VENDOR
<input type="checkbox"/> DELETE_VENDOR	<input type="checkbox"/> GSM_RESET	<input type="checkbox"/> GSM_RESET
<input type="checkbox"/> GSM_UPGRADE	<input type="checkbox"/> API	<input type="checkbox"/> ADD_CHILD_ACCOUNT
<input type="checkbox"/> VIEW_LICENSE_LIST	<input type="checkbox"/> EDIT_LICENSE	<input type="checkbox"/> ADD_LICENSE
<input type="checkbox"/> DELETE_LICENSE		

Figure 27. New Role

2.9.4 Manage Account Types

This feature is not used.

2.9.5 Manage Help Tooltips

This feature is not used.

3

Warranty and Warning Information

WARNING!

Please read this document **CAREFULLY**, as it contains important warnings, life-safety, and practical information about all products manufactured by the Mircom Group of Companies, including Mircom and Secutron branded products, which shall include without limitation all fire alarm, nurse call, building automation and access control and card access products (hereinafter individually or collectively, as applicable, referred to as “**Mircom System**”).

NOTE TO ALL READERS:

1. **Nature of Warnings.** The within warnings are communicated to the reader out of an abundance of caution and create no legal obligation for Mircom Group of Companies, whatsoever. Without limiting the generality of the foregoing, this document shall NOT be construed as in any way altering the rights and obligations of the parties, governed by the legal documents that apply in any given circumstance.
2. **Application.** The warnings contained in this document apply to all Mircom System and shall be read in conjunction with:
 - a. the product manual for the specific Mircom System that applies in given circumstances;
 - b. legal documents that apply to the purchase and sale of a Mircom System, which may include the company’s standard terms and conditions and warranty statements;
 - c. other information about the Mircom System or the parties’ rights and obligations as may be application to a given circumstance.
3. **Security and Insurance.** Regardless of its capabilities, no Mircom System is a substitute for property or life insurance. Nor is the system a substitute for property owners, renters, or other occupants to act prudently to prevent or minimize the harmful effects of an emergency situation. Building automation systems produced by the Mircom Group of Companies are not to be used as a fire, alarm, or life-safety system.

NOTE TO INSTALLERS:

All Mircom Systems have been carefully designed to be as effective as possible. However, there are circumstances where they may not provide protection. Some reasons for system failure include the following. As the only individual in contact with system users, please bring each item in this warning to the attention of the users of this Mircom System. Failure to properly inform system end-users of the circumstances in which the system might fail may result in over-reliance upon the system. As a result, it is imperative that you properly inform each customer for whom you install the system of the possible forms of failure:

4. **Inadequate Installation.** All Mircom Systems must be installed in accordance with all the applicable codes and standards in order to provide adequate protection. National standards require an inspection and approval to be conducted by the local authority having jurisdiction following the initial installation of the system and following any changes to the system. Such inspections ensure installation has been carried out properly.
5. **Inadequate Testing.** Most issues and/or problems that would prevent a Mircom System alarm from operating as intended, can be identified through regular testing and maintenance. The complete system should be tested by the local authority having jurisdiction immediately after a fire, storm, earthquake, accident, or any kind of construction activity inside or outside the premises. The testing should include all sensing devices, keypads, consoles, alarm indicating devices and any other operational devices that are part of the system.

NOTE TO USERS:

All Mircom Systems have been carefully designed to be as effective as possible. However, there are circumstances where they may not provide protection. Some reasons for system failure include the following. The end user can minimize the occurrence of any of the following by proper training, testing and maintenance of the Mircom Systems:

6. **Inadequate Testing and Maintenance.** It is imperative that the systems be periodically tested and subjected to preventative maintenance. Best practices, local codes, applicable laws and industry regulations, and any local authority having jurisdiction to do so, determine the frequency and type of testing that is required at a minimum. Mircom System may not function properly, and the occurrence of other system failures identified below may not be minimized, if the periodic testing and maintenance of Mircom Systems is not completed with diligence and as required.
7. **Improper Operation.** It is important that all system users be trained in the correct operation of the alarm system and that they know how to respond when the system indicates an alarm. A Mircom System may not function as intended during an emergency situation where the user is unable to operate

a panic or emergency switch by reason of permanent or temporary physical disability, inability to reach the device in time, unfamiliarity with the correct operation, or related circumstances.

8. **Insufficient Time.** There may be circumstances when a Mircom System will operate as intended, yet the occupants will not be protected from the emergency due to their inability to respond to the warnings in a timely manner. If the system is monitored, the response may not occur in time enough to protect the occupants or their belongings.
9. **Carelessness or Safety Hazards.** Moreover, smoke detectors may not provide timely warning of fires caused by carelessness or safety hazards such as smoking in bed, violent explosions, escaping gas, improper storage of flammable materials, overloaded electrical circuits or children playing with matches or arson.
10. **Power Failure.** Some Mircom System components require adequate electrical power supply to operate. Examples include: smoke detectors, beacons, HVAC, and lighting controllers. If a device operates only by AC power, any interruption, however brief, will render that device inoperative while it does not have power. Power interruptions of any length are often accompanied by voltage fluctuations which may damage Mircom Systems or other electronic equipment. After a power interruption has occurred, immediately conduct a complete system test to ensure that the system operates as intended.
11. **Battery Failure.** If the Mircom System or any device connected to the system operates from batteries it is possible for the batteries to fail. Even if the batteries have not failed, they must be fully charged, in good condition, and installed correctly. Some Mircom Systems use replaceable batteries, which have a limited life-span. The expected battery life is variable and in part dependent on the device environment, usage and type. Ambient conditions such as high humidity, high or low temperatures, or large temperature fluctuations may reduce the expected battery life. Moreover, some Mircom Systems do not have a battery monitor that would alert the user in the event that the battery is nearing its end of life. Regular testing and replacements are vital for ensuring that the batteries function as expected, whether or not a device has a low-battery monitor.
12. **Physical Obstructions.** Motion sensors that are part of a Mircom System must be kept clear of any obstacles which impede the sensors' ability to detect movement. Signals being communicated by a Mircom System may not reach the receiver if an item (such as metal, water, or concrete) is placed on or near the radio path. Deliberate jamming or other inadvertent radio signal interference can also negatively affect system operation.
13. **Wireless Devices Placement Proximity.** Moreover all wireless devices must be a minimum and maximum distance away from large metal objects, such as refrigerators. As the end user, you are required to consult the specific Mircom System manual and application guide for any maximum distances required between devices and suggested placement of wireless devices for optimal functioning.

14. **Failure to Trigger Sensors.** Moreover, Mircom Systems may fail to operate as intended if, motion, heat, carbon monoxide (CO) and/or smoke sensors, are not triggered.
 - a. Sensors in a fire system may fail to be triggered when the fire is in a chimney, walls, roof, or on the other side of closed doors. Smoke and heat detectors may not detect smoke or heat from fires on another level of the residence or building. In this situation the control panel may not alert occupants of a fire.
 - b. Sensors in a nurse call system may fail to be triggered when movement is occurring outside of the motion sensors' range. For example, if movement is occurring on the other side of closed doors or on another level of the residence or building the motion detector may not be triggered. In this situation the central controller may not register an alarm signal.
15. **Interference with Audible Notification Appliances.** Audible notification appliances may be interfered with by other noise sources such as stereos, radios, televisions, air conditioners, appliances, or passing traffic. Audible notification appliances, however loud, may not be heard by a hearing-impaired person.
16. **Other Impairments.** Alarm notification appliances such as sirens, bells, horns, or strobes may not warn or waken a sleeping occupant if there is an intervening wall or door. It is less likely that the occupants will be alerted or awakened when notification appliances are located on a different level of the residence or premise.
17. **Software Malfunction.** Most Mircom Systems contain software. No warranties are provided as to the software components of any products or stand-alone software products within a Mircom System. For a full statement of the warranties and exclusions and limitations of liability please refer to the company's standard Terms and Conditions and Warranties.
18. **Telephone Line/Network Malfunction.** Telephone service can cause system failure where telephone lines/networks are relied upon by a Mircom System. Alarms and information coming from a Mircom System may not be transmitted if a phone line/network is out of service or busy for a certain period of time. Alarms and information may not be transmitted where telephone lines/networks have been compromised by criminal tampering, local construction, storms or earthquakes.
19. **Component Failure.** Although every effort has been made to make this Mircom System as reliable as possible, the system may fail to function as intended due to the failure of a component.

20. **Integrated Products.** Mircom System might not function as intended if it is connected to a non-Mircom product or to a Mircom product that is deemed non-compatible with a particular Mircom System. A list of compatible products can be requested and obtained.
21. A Mircom System's Auto Configuration feature is intended to assign the Alarm process type to all inputs and to provide an initial set up by detecting connected devices and generates a basic job configuration upon the initial installation of the Mircom System. Mircom makes no representations, warranties or guarantees regarding the accuracy or suitability of the basic job configuration generated upon installation, for any specific site requirements.
The end user shall be solely and exclusively responsible to thoroughly review the basic job generated by the auto configuration feature upon initial installation and to implement necessary adjustments and modifications to customize the job configuration in accordance with the functional and/or technical requirements of the site. Mircom expressly disclaims any responsibility or liability for any failure, malfunction or defective operation of a Mircom System and any associated components, resulting from the end user's failure to customize or adjust the job configuration accordingly.
By installing and utilizing the Mircom System, the user acknowledges and agrees that Mircom shall not be liable for any claims, losses, damages, or defects arising from the failure of the user or installer and those for whom it is responsible at law, to customize the basic job configuration generated on the initial set-up in accordance with the requirements of the site.

Warranty

Purchase of all Mircom products is governed by:

<https://www.mircom.com/product-warranty>

<https://www.mircom.com/purchase-terms-and-conditions>

<https://www.mircom.com/software-license-terms-and-conditions>