

Unified Building Solution

Administration Guide

*Copyright August 2017 Mircom Inc.
All rights reserved.*

Unified Building Solution Administration Guide Version 1.1.

This manual, as well as the software described in it, is provided under licence or other agreements and may be used or copied only in accordance with the terms of such license. The content of this manual is furnished for informational use only. It is subject to change without notice, and should not be construed as a commitment by Mircom. Mircom assumes no responsibility or liability for any errors or inaccuracies that appear in this book.

Except as permitted by such license, no part of this publication may be reproduced, stored in a retrieval system, transmitted in any form by means electronic, mechanical, using any recorded media, or any other format without the prior written permission of Mircom.

Mircom
25 Interchange Way
Vaughan, Ontario
L4K 5W3
905.660.4655
Fax:905.660.4113

Contents

1	Introduction	7
1.1	Unified Building Platform Overview	7
1.2	Components	7
1.3	TX3 InSuite Products	11
1.4	Additional Documentation	11
2	Network Management	12
2.1	Terms	12
2.2	Network Diagram	13
2.3	Collect and Record Information in the Device List	14
2.4	Configure Static IP Addresses	15
2.5	Configure the Router	15
2.6	Configure the Switches	26
2.7	Configure Remote Access	39
3	Virtual Machine Management	44
3.1	Install the Virtual Machine	44
3.2	Start the Virtual Machine	49
3.3	Set the IP Address	49
3.4	Set the Virtual Machine Time	51
3.5	Change your Virtual Machine Password	52
3.6	Disable Call Control	53
3.7	Delete Logs	53
3.8	Configure the Virtual Machine to Start Automatically	55
3.9	Configure the Building Server to Start Automatically	56
3.10	Change the Default Website of the Virtual Machine (Optional)	57
4	ONVIF Camera Management	59
4.1	Install the ONVIF Camera Server Software	59
4.2	Disable the SSL Custom Log	59
4.3	Connect to the Server	61
4.4	Import the License	62
4.5	Add Cameras to the Server	63
4.6	Enable Recording	64
4.7	Configure Resolution and Image Rate	65
4.8	Configure Storage	67
4.9	Create an Administrator User	67
4.10	Create a Restricted User (optional)	68
4.11	Back up your Settings	69
4.12	Back up Video	70
4.13	Delete Video	70

5	SIP Server Management	72
5.1	Terms	72
5.2	Overview	72
5.3	Configure the SIP Server	73
5.4	Configure the User Preferences (Optional)	75
5.5	Configure Kamailio to Call Multiple TX3 InSuites (Optional)	77
6	TX3 Touch Configuration	80
6.1	Discover the MAC address of the TX3 Touch	80
6.2	Configure the TX3 Touch SIP Settings	81
6.3	Set up Residents on the TX3 Touch	83
6.4	Back up the Configuration on the TX3 Touch	84
7	TX3 InSuite Installation	85
7.1	The TX3 InSuite	85
7.2	Install the Ferrite Bead	86
7.3	Mount the TX3 InSuite	87
7.4	Unmount the TX3 InSuite	89
7.5	Configure the TX3 InSuite	89
8	Troubleshooting	92
8.1	Virtual Machine Troubleshooting	92
8.2	ExacqVision Troubleshooting	93
8.3	TX3 InSuite Troubleshooting	94
9	TX3 InSuite Specifications	98
10	Device List	99
	Warranty & Warning Information	101
	Special Notices	104

List of Figures

Figure 1.	Example network diagram	13
Figure 2.	Antaira router - Login page	16
Figure 3.	Antaira router - System Information	16
Figure 4.	Antaira router - WAN Setup	17
Figure 5.	Antaira router - WAN Setup	18
Figure 6.	DNS Servers	19
Figure 7.	Antaira router - Firmware Upgrade	19
Figure 8.	Antaira router - Services tab	20
Figure 9.	Antaira router - Services page	20
Figure 10.	Antaira router - Static Leases	21
Figure 11.	Antaira router - Access Restrictions tab	21
Figure 12.	Antaira router - Access Restrictions	22
Figure 13.	Antaira router - Client IP range	23
Figure 14.	Antaira router - Access Restrictions	24
Figure 15.	Antaira router - Client IP range	25
Figure 16.	Antaira router - Backup and Restore	26
Figure 17.	Antaira switch - IP Configuration	27
Figure 18.	Antaira switch - System Information	28
Figure 19.	Antaira switch - SNTP Configuration	30
Figure 20.	Antaira switch - Syslog Configuration	31
Figure 21.	Antaira switch - System Event Log	32
Figure 22.	Antaira switch - Fault Relay Alarm	33
Figure 23.	Antaira switch - IP Security	34
Figure 24.	Antaira switch - MAC Address Table	35
Figure 25.	Antaira switch - 802.1x/Radius	35
Figure 26.	Antaira switch - Port Configuration	36
Figure 27.	Tftpd32	37
Figure 28.	Tftpd32 - Global tab	37
Figure 29.	TFTPD32 - TFTP tab	38
Figure 30.	Antaira Switch - Backup Configuration	38
Figure 31.	Antaira switch - Power over Ethernet	39
Figure 32.	TeamViewer - Installation	40
Figure 33.	TeamViewer - Main window	40
Figure 34.	TeamViewer - Define personal password	41
Figure 35.	TeamViewer - Options	41
Figure 36.	TeamViewer - Main window	42
Figure 37.	TeamViewer - Sign Up	42
Figure 38.	TeamViewer - Add remote computer	43
Figure 39.	TeamViewer - Properties	43
Figure 40.	VirtualBox - Custom Setup	45
Figure 41.	VirtualBox - Network Interfaces	45
Figure 42.	VirtualBox - Appliance Settings	47
Figure 43.	VirtualBox - Adapter	48
Figure 44.	VirtualBox - MAC address	48
Figure 45.	VirtualBox - Memory	49
Figure 46.	ifconfig	50
Figure 47.	Virtual machine network interface	50
Figure 48.	Virtual machine time server setting	52

Figure 49.	WINS CP navigation menu	54
Figure 50.	WINS CP - navigation menu	54
Figure 51.	Virtual Machine Name	55
Figure 52.	Right-click All Programs	56
Figure 53.	netplwiz	57
Figure 54.	WINS CP navigation menu	58
Figure 55.	exacqVision Client - Add Systems	61
Figure 56.	exacqVision Client - System	62
Figure 57.	exacqVision Client - Add IP Camera	63
Figure 58.	exacqVision Client - Schedule	64
Figure 59.	exacqVision Client - Select all	65
Figure 60.	exacqVision Client - Recording Mode	65
Figure 61.	exacqVision Client - Recording	66
Figure 62.	exacqVision Client - Storage	67
Figure 63.	exacqVision User Settings	68
Figure 64.	exacqVision User Settings	68
Figure 65.	Select cameras	69
Figure 66.	exacqVision Client - System	70
Figure 67.	SIP server - login page	73
Figure 68.	SIP Server - SIP Admin Menu	74
Figure 69.	SIP Server - SIP Admin Modules page	74
Figure 70.	SIP Server - New Subscriber page	75
Figure 71.	SIP Server - User Preferences link	76
Figure 72.	SIP Server - New User	76
Figure 73.	request_route	78
Figure 74.	TX3 Touch - Admin Access	80
Figure 75.	Desktop icon	81
Figure 76.	Control Panel	81
Figure 77.	Large Icons	81
Figure 78.	Desktop icon	81
Figure 79.	TX3 Touch - VOIP Setup	82
Figure 80.	TX3 Touch - Resident VOIP Setup	83
Figure 81.	Figure 78. TX3 Touch - Backup Jobs	84
Figure 82.	Dimensions of the TX3 InSuite	85
Figure 83.	Connections on the back of the TX3 InSuite	86
Figure 84.	TX3 InSuite with ferrite bead	86
Figure 85.	The mounting bracket directly on the wall	87
Figure 86.	Back of the TX3 InSuite	88
Figure 87.	Mounting bracket showing posts	88
Figure 88.	Logged into the TX3 InSuite	89
Figure 89.	TX3 InSuite - exacqVision Settings	90
Figure 90.	TX3 InSuite - SIP Settings	90
Figure 91.	TX3 InSuite - Time server settings	91
Figure 92.	WINS CP	95
Figure 93.	WINS CP - connected to TX3 InSuite	95
Figure 94.	WINS CP - arm32 directory	96
Figure 95.	WINS CP - Navigation menu	96

1 Introduction

This manual provides instructions on installing and configuring the Unified Building Platform.

Installation must be performed by a qualified technician and must adhere to the standards and special notices set by the local regulatory bodies.

This chapter explains:

- Unified Building Platform Overview
- Components
- TX3 InSuite Products
- Additional Documentation

1.1 Unified Building Platform Overview

The Unified Building Platform is a versatile and full-featured security and communication solution for multi-resident condominiums and homes.

1.1.1 Benefits

Benefits of the Unified Building Platform include:

- Intelligent building systems integration for tech savvy tenants
- More secure, more intelligent, more interactive communities
- Improved intra-facility communications and emergency response
- Better communication between tenants and property managers

1.2 Components

1.2.1 TX3 InSuite

The TX3 InSuite is a touch screen tablet located in the condominium unit. Residents use it to communicate with visitors and other residents.

1.2.2 Building Server

The building server computer runs the virtual machine and the ONVIF camera server. It is located on the property.

The recommended requirements are:

- Option 1: IONODES CIRRUS CR47 Compact
 - CPU - Intel Core i7-4790T
 - RAM - 8 GB DDR3
 - GPU - Integrated
 - OS - Windows Embedded 7
 - Boot Drive (OS) - 128 GB SSD SATA3
- Option 2: IONODES CIRRUS CR40 Ultra Compact
 - CPU - Intel Core i3-6100U
 - RAM - 4 GB DDR4
 - GPU - Integrated
 - OS - Windows Embedded 7
 - Boot Drive (OS) - 128 GB SSD SATA3

The building server should include the following programs:

- WINSCP 5.7.5 (<http://winscp.net>)
- Advanced IP Scanner 2.4.2601 (<http://www.advanced-ip-scanner.com/>)
- SADP 2.21.100 (<http://www.hikvision.ca/>)
- Tftpd32 4.50 (http://tftpd32.jounin.net/tftpd32_download.html)
- Teamviewer 11.0.56083 (<http://www.teamviewer.com>)
- Oracle VirtualBox (see section 1.2.3)
- ExacqVision (see section 1.2.4)

1.2.3 Virtual Machine

The virtual machine is hosted on the building server. It enables communication between the TX3 InSuites, the ONVIF cameras, and the TX3 Touch or lobby intercom unit. It includes:

- Oracle VirtualBox 4.3.28, a free open-source virtualization system (<https://www.virtualbox.org/>)
- Linux Ubuntu 10.04 LTS (<http://www.ubuntu.com/>)
- Kamailio 4.0.6: An open-source SIP server (<http://www.kamailio.org/>)

- Siremis 4.1.0: An open-source Web interface for Kamailio (<http://siremis.asipto.com/>)

1.2.4 ONVIF Camera Server

ONVIF is a specification for communication with IP-based video devices.

The ONVIF camera server is installed on the building server, and is used for communicating with security cameras.

An example of a camera server is the exacqVision video management system (<https://exacq.com/>). It includes 3 software packages:

- exacqVision Client 6.6.2.72241
- exacqVision Server 6.6.2.72387
- exacqVision Web service 3.10.4.72058

1.2.5 Router

Mircom recommends the following routers:

- Antaira Industrial VPN Router LNR-3001 with firmware version 1.1 (05/12/16) - build 21995M and kernel version Linux 3.10.81
- Linksys Dual Gigabit WAN VPN Router LRT224 with firmware version 1.0.2.06
- Ubiquiti EdgeRouter ERPoe-5 with firmware version 1.8.0

The router must support the following features:

- WAN port
- DHCP server
- IP and MAC binding
- Access rules
- Ability to back up and restore configuration

1.2.6 Switches

Mircom recommends the following switches:

- Antaira 7-port Industrial Unmanaged Ethernet Switch LNX-0702C-SFP
- Antaira 26-port Industrial Managed Ethernet Switch LNP-2602GN with firmware version 1.21 and kernel version 6.07

The managed switch must support the following features:

- Port to MAC binding
- Power over Ethernet
- 802.1x/Radius
- Ability to power cycle each port
- Ability to back up and restore configuration

1.2.7 Client Computer (Optional)

The client computer is a computer on the property that can be used to configure any TX3 series products, and to run the ONVIF camera client software. It is also used by Mircom to access the system remotely if necessary for technical support.

1.2.8 OpenGN

The OpenGN software provides monitoring, control and software management solutions for the fire detection and asset protection market. It lets you monitor information from fire alarm control panels, card access systems, and TX3 InSuites, using a customized graphical display.

For more information, see LT-1113 OpenGN Administrator Guide on the Mircom Website.

1.2.9 Lobby Intercom

The lobby intercom, for example Mircom's TX3 Touch, is a building access control panel that can make a video call between a visitor to the building and a resident's TX3 InSuite. The video is one-way: the resident can see the visitor, but the visitor cannot see the resident. The lobby intercom controls building access and can unlock the door for the visitor if the resident wishes.

For more information, see LT-995 TX3 Touch Screen Configuration and Administration Manual on the Mircom Website.

1.2.10 Card Access

The TX3-CX Card Access System provides building ready monitoring, control and integrated security solutions.

For more information, see LT-980 TX3-CX Card Access System Installation and Operation Manual on the Mircom Website.

1.2.11 Fire Alarm Panels

For information on integrating fire alarm panels with OpenGN, see LT-1113 OpenGN Administrator Guide on the Mircom Website.

1.3 TX3 InSuite Products

- **TX3-INSUITE-10:** 10 inch touch screen station
- **TX3-INSUITE-BP:** Mounting plate for TX3-INSUITE-10, mounts onto single gang electrical box

1.4 Additional Documentation

For additional documentation, see the following Mircom literature:

- LT-6079 TX3 InSuite User Guide
- LT-995 TX3 Touch Screen Configuration and Administration Manual
- LT-980 TX3-CX Card Access System Installation and Operation Manual
- LT-1113 OpenGN Administrator Guide

2

Network Management

This chapter explains how to configure the network. This includes:

- Terms
- Network Diagram
- Collect and Record Information in the Device List
- Configure the Router
- Configure the Switches
- Configure Remote Access

2.1 Terms

DHCP (Dynamic Host Configuration Protocol): DHCP is a method of automatically assigning IP addresses to devices on a network. On a LAN, the router usually has a DHCP server that assigns IP addresses to all devices on the LAN.

LAN (Local Area Network): A LAN is a network covering a small area, such as a building.

MAC address: Each device's network interface has a MAC (media access control) address. This address uniquely identifies the device on the network.

NTP (Network Time Protocol): A protocol for synchronizing clocks between systems.

Router: A router is a device that connects two or more networks together. For example, a router connects a LAN to the Internet.

SNTP (Simple Network Time Protocol): A simpler implementation of NTP.

Subnet mask: A subnet is a way of dividing a network into groups. When the IP addresses of the devices share the first three octets, for instance 128.15.1.x, then the devices are on the same subnet and the subnet mask is 255.255.255.0.

Some routers require the LAN information in CIDR (classless inter-domain routing) format. A LAN with the IP address range of **128.15.1.x** and subnet mask **255.255.255.0** is written in CIDR format as **128.15.1.0/24**.

Switch: A switch is a device that connects devices to each other on a network.

WAN (Wide Area Network): A WAN is a network covering a wide area, such as the Internet.

2.2 Network Diagram

Figure 1 shows an example wiring layout for a 4 story condominium with a TX3 InSuite in each unit. The number and size of the Power over Ethernet (PoE) switches depends on the building requirements.

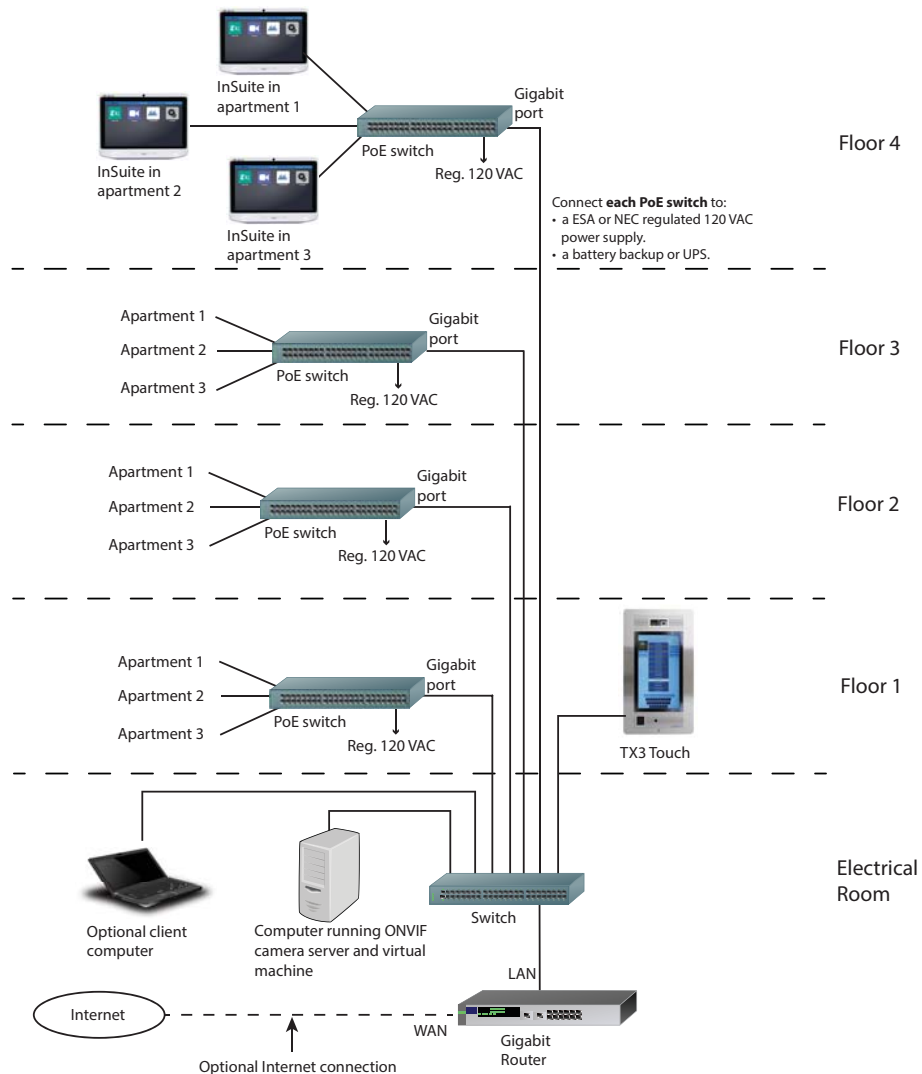


Figure 1. Example network diagram

Note: Connect each switch, router, and server to a battery backup or UPS.

Avoid running Ethernet cables near sources of electrical interference or noise, as per NEC requirements.

2.3 Collect and Record Information in the Device List

Note: The Device List on page 99 is essential for configuring the system correctly. Fill it out completely and keep it available for easy reference.

1. Collect the MAC addresses for each device on the network.
 - Client computer
 - Building server
 - Virtual machine (record this when you configure it; see chapter 3)
 - Router
 - Switch
 - ONVIF camera
 - TX3 Touch or lobby intercom (record this when you configure it; see chapter 5)
 - TX3 InSuite (each TX3 InSuite has its MAC address printed on the back)
2. Record the MAC addresses in the Device List on page 99.
3. Decide on the range of IP addresses for all the devices in the network. This range should have no gaps.
4. Assign an IP address to each device on the network and record this information in the Device List on page 99.

You will configure the router with this information later, so that the router can assign a reserved IP address to each device.
5. Assign SIP usernames and SIP passwords to each TX3 InSuite and lobby intercom on the network, and record them in the Device List on page 99.
 - For each TX3 InSuite, assign a 4 digit number as the SIP username. Use the building number plus the suite number. For example, a TX3 InSuite in suite 500 of building 1 has the SIP username **1500**.
 - For all TX3 InSuites, use **mircom123** as the SIP password.
 - Use a descriptive name like **Lobby** as the SIP username of the lobby intercom, and use **mircom123** as the SIP password of the TX3 Touch.

Note: Do not use spaces in SIP usernames or SIP passwords.

- Only devices that initiate or receive calls need SIP usernames and SIP passwords.

6. Fill out the rest of the fields in the Device List on page 99, including the building and suite that each TX3 InSuite will be installed in, and the switch and port number that it will be connected to.

2.4 Configure Static IP Addresses

The following devices must have static IP addresses:

- Client computer
- Building server
- Virtual machine (see Chapter 3)
- Router (see section 2.5 on page 15)
- Switches (see section 2.6 on page 26)

All the other devices have dynamically assigned IP addresses, although their IP addresses are reserved in the router.

2.5 Configure the Router

Attention: Read the documentation that comes with your router before you start.

The instructions that follow show how to configure the Antaira Industrial VPN Router LNR-3001.

To configure the router you must:

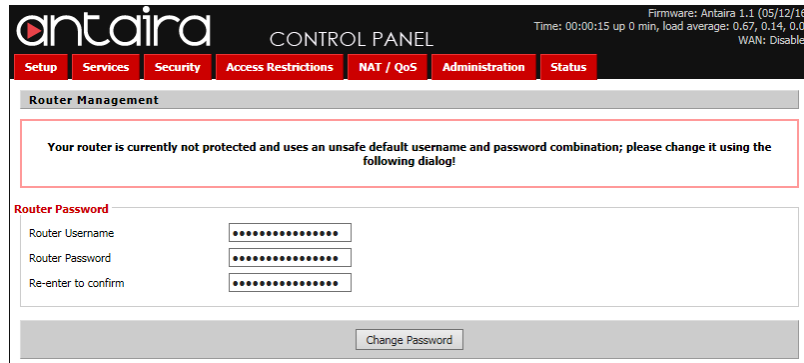
- Configure the Router's IP Information
- Log in to the Router Again
- Update Firmware
- Configure IP and MAC Binding
- Create Access Restrictions
- Back up the Configuration

Follow the instructions below to complete these steps.

2.5.1 Configure the Router's IP Information

By default the router has a static IP address. Consult the router's documentation for more information. On the Antaira Industrial VPN Router LNR-3001, the default IP address is 192.168.1.1.

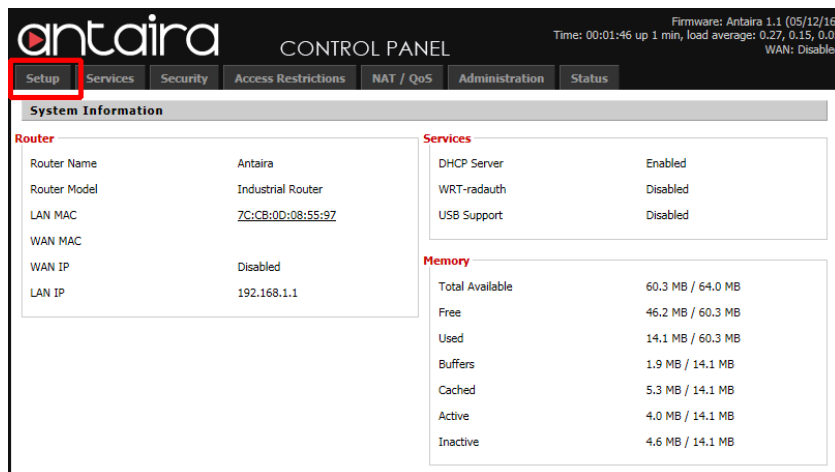
1. Connect the client computer to the ETH1 port of the router with a category 5 cable.
2. Configure the client computer to obtain an IP address automatically.
3. On the client computer, open the Chrome Web browser, type the IP address of the router, and then press Enter.



The screenshot shows the Antaira router's 'CONTROL PANEL' with the 'Router Management' section active. A warning message states: 'Your router is currently not protected and uses an unsafe default username and password combination; please change it using the following dialog!'. Below this, the 'Router Password' section contains three input fields: 'Router Username', 'Router Password', and 'Re-enter to confirm', each with a masked password (dots). A 'Change Password' button is located at the bottom right of the form.

Figure 2. Antaira router - Login page

4. Enter a new username and password for the router, then click **Change Password**.
5. Make a note of the router's new username and password in the Device List on page 99.
6. On the main page, click **Setup** in the upper left.



The screenshot shows the Antaira router's 'CONTROL PANEL' with the 'Setup' tab selected. The 'System Information' section is displayed, showing details for the router and system resources.

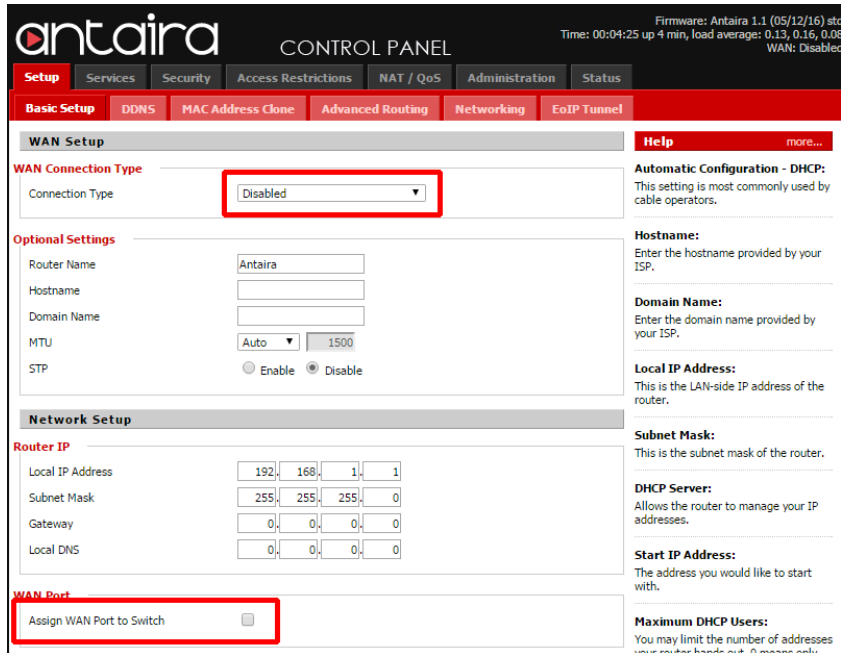
Router		Services	
Router Name	Antaira	DHCP Server	Enabled
Router Model	Industrial Router	WRT-radauth	Disabled
LAN MAC	7C:CB:0D:08:55:97	USB Support	Disabled
WAN MAC			
WAN IP	Disabled		
LAN IP	192.168.1.1		

Memory	
Total Available	60.3 MB / 64.0 MB
Free	46.2 MB / 60.3 MB
Used	14.1 MB / 60.3 MB
Buffers	1.9 MB / 14.1 MB
Cached	5.3 MB / 14.1 MB
Active	4.0 MB / 14.1 MB
Inactive	4.6 MB / 14.1 MB

Figure 3. Antaira router - System Information

7. If the page prompts for a username and password, enter the new username and password, then click **OK**.

8. On the WAN Setup page, select **Assign WAN Port to Switch**.
9. In the Connection Type menu, select **Automatic Configuration - DHCP**.



antaira CONTROL PANEL

Firmware: Antaira 1.1 (05/12/16) stc
Time: 00:04:25 up 4 min, load average: 0.13, 0.16, 0.08
WAN: Disabled

Setup Services Security Access Restrictions NAT / QoS Administration Status

Basic Setup DDNS MAC Address Clone Advanced Routing Networking EoIP Tunnel

WAN Setup Help more...

WAN Connection Type

Connection Type: **Disabled**

Optional Settings

Router Name: Antaira

Hostname:

Domain Name:

MTU: Auto 1500

STP: ☐ Enable ☒ Disable

Network Setup

Router IP

Local IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

Local DNS: 0.0.0.0

WAN Port

Assign WAN Port to Switch: ☐

Automatic Configuration - DHCP:
This setting is most commonly used by cable operators.

Hostname:
Enter the hostname provided by your ISP.

Domain Name:
Enter the domain name provided by your ISP.

Local IP Address:
This is the LAN-side IP address of the router.

Subnet Mask:
This is the subnet mask of the router.

DHCP Server:
Allows the router to manage your IP addresses.

Start IP Address:
The address you would like to start with.

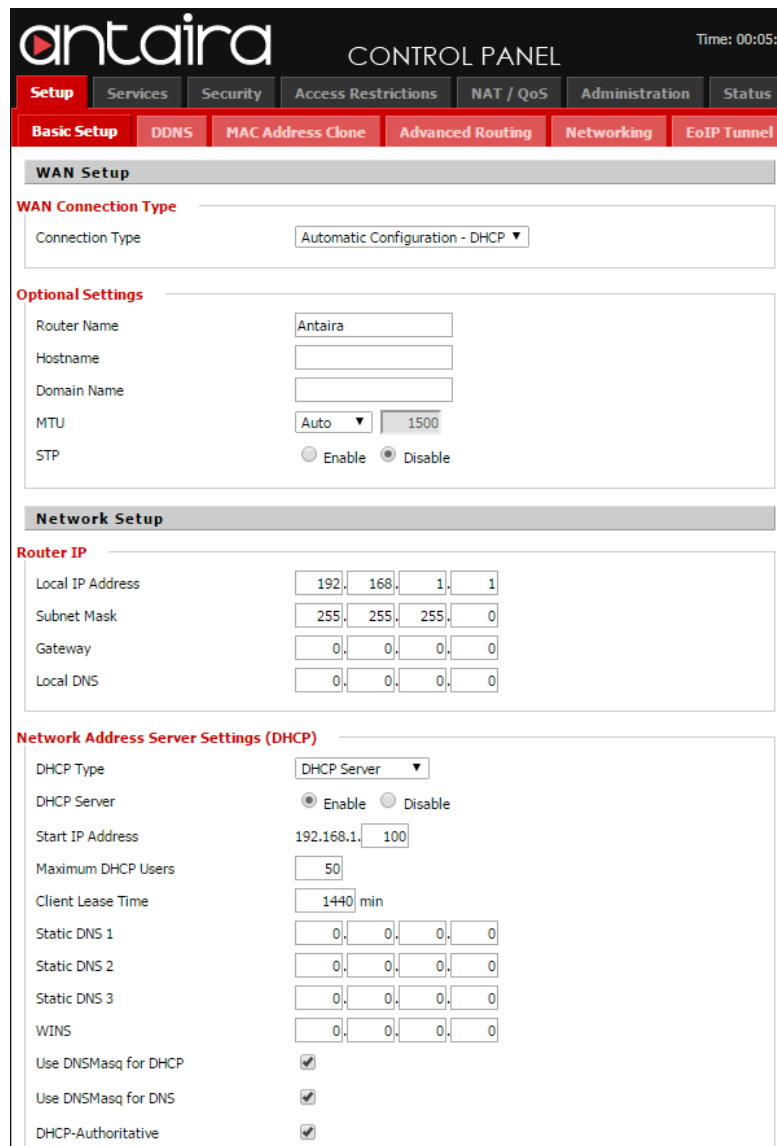
Maximum DHCP Users:
You may limit the number of addresses your router hands out. 0 means only

Figure 4. Antaira router - WAN Setup

10. Provide the following information:
 - **Router Name:** Give your router a name
 - **Hostname:** Same as router name
 - **Local IP Address:** The IP address of the router (see the Device List on page 99)
 - **Subnet Mask:** 255.255.255.0
 - **Gateway:** The IP address of the router (see the Device List on page 99)
 - **DHCP Type:** DHCP Server
 - **Start IP Address:** The IP address of the first device on the LAN (see the Device List on page 99)
 - **Maximum DHCP Users:** The number of devices on the LAN (the Device List on page 99)
 - **Static DNS:** your Internet service provider's DNS servers
11. Click **Save** at the bottom of the window.

12. Click **Apply Settings**.

Note: The router's WAN port is now ETH0.



antaira CONTROL PANEL Time: 00:05:00

Setup Services Security Access Restrictions NAT / QoS Administration Status

Basic Setup DDNS MAC Address Clone Advanced Routing Networking EoIP Tunnel

WAN Setup

WAN Connection Type

Connection Type Automatic Configuration - DHCP ▼

Optional Settings

Router Name Antaira

Hostname

Domain Name

MTU Auto 1500

STP ☐ Enable ☒ Disable

Network Setup

Router IP

Local IP Address 192 168 1 1

Subnet Mask 255 255 255 0

Gateway 0 0 0 0

Local DNS 0 0 0 0

Network Address Server Settings (DHCP)

DHCP Type DHCP Server ▼

DHCP Server ☒ Enable ☐ Disable

Start IP Address 192.168.1.100

Maximum DHCP Users 50

Client Lease Time 1440 min

Static DNS 1 0 0 0 0

Static DNS 2 0 0 0 0

Static DNS 3 0 0 0 0

WINS 0 0 0 0

Use DNSMasq for DHCP ☒

Use DNSMasq for DNS ☒

DHCP-Authoritative ☒

Figure 5. Antaira router - WAN Setup

Some routers require the LAN information in CIDR (classless inter-domain routing) format. This format looks like 128.15.1.0/24, where the first 3 octets are the octets of your IP address range, the fourth octet is 0, and 24 is equivalent to the subnet mask 255.255.255.0.

Discover your Internet service provider's DNS servers

1. Connect a laptop to the Internet service provider's router.
2. Open Command Prompt and type:
ipconfig /all

There IP addresses are listed beside DNS servers. If there is only one IP address, then leave the Static DNS 2 field blank.



Figure 6. DNS Servers

2.5.2 Log in to the Router Again

After you configure the router's IP information, you must log into it again.

3. On the client computer, open the Chrome Web browser, type the IP address of the router, and then press Enter.
4. If the page prompts for a username and password, enter the new username and password, then click **OK**.

2.5.3 Update Firmware

If the firmware version listed in the upper right corner of the control panel is lower than version 1.3 (10/07/16), then you must update the firmware.

1. Click the **Administration** tab, then click the **Firmware Upgrade** tab.

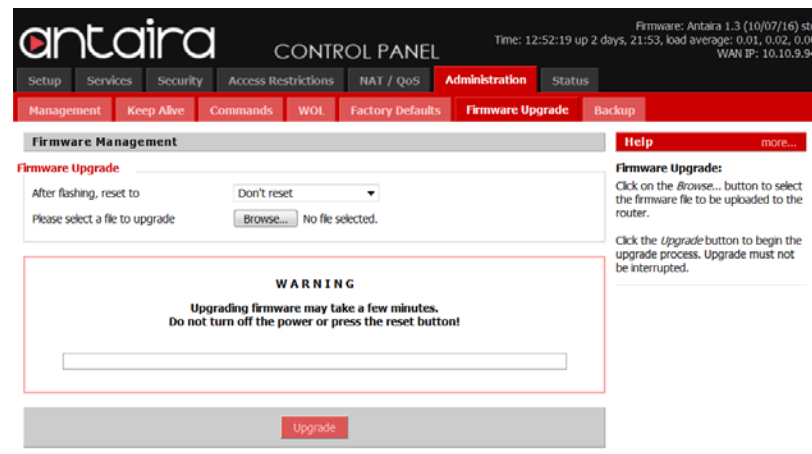


Figure 7. Antaira router - Firmware Upgrade

2. Beside **After flashing, reset to**, select **Don't reset**.

3. Click **Browse**, then select the firmware file on the Client Computer.
4. Click **Upgrade**.

After the firmware is updated, the router restarts.

2.5.4 Configure IP and MAC Binding

IP and MAC binding is also called static MAC/IP mapping or DHCP reservations. This feature reserves an IP address for each device, so that the router always assigns the same IP address to the device.

1. Click the **Services** tab at the top of the window.

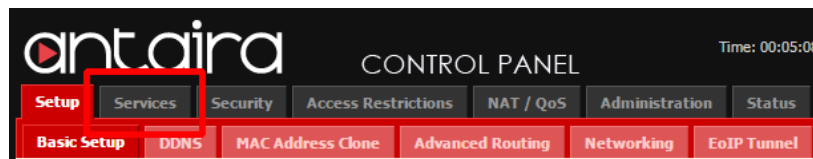


Figure 8. Antaira router - Services tab

The Services page appears.

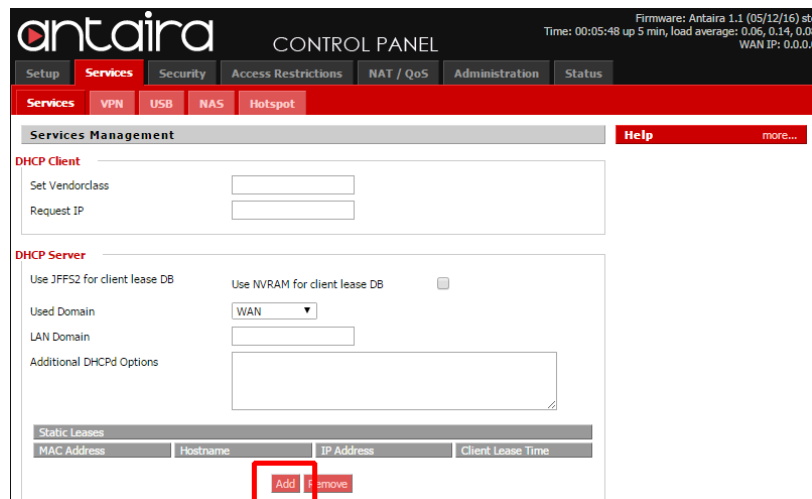


Figure 9. Antaira router - Services page

2. Click **Add**.
- A new row appears under **Static Leases**.
3. Provide the following information (see the Device List on page 99):
 - **MAC Address:** The MAC address of the first device on the network

- **Hostname:** The name of the device
- **IP Address:** The device's IP address
- **Client lease time:** 1440

Static Leases			
MAC Address	Hostname	IP Address	Client Lease Time
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/> min

Figure 10. Antaira router - Static Leases

4. Click **Save** at the bottom of the window.
5. Click **Apply Settings**.
6. Repeat steps 2 to 5 for each device.

2.5.5 Create Access Restrictions

Access restrictions are also called access rules or firewall rules. They prevent and allow access to the Internet for certain devices.

On the Antaira Industrial VPN Router LNR-3001, you must create one policy for every computer or range of computers that you want to allow Internet access to. The following steps describe how to create rules for 2 computers that have the IP addresses 128.15.1.8 and 128.15.1.25.

Allow a computer on the LAN to access the Internet

1. Click the **Access Restrictions** tab.

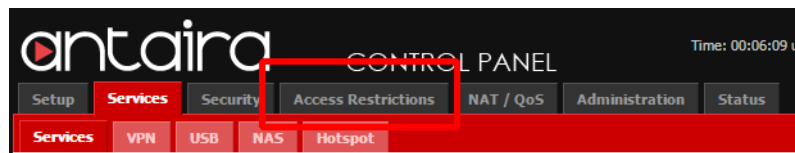


Figure 11. Antaira router - Access Restrictions tab

The WAN Access page appears.

2. Provide the following information:
 - **Policy:** Select 1()
 - **Status:** Enable
 - **Policy Name:** Block Internet Access Group 1
 - **Internet access during selected days and hours:** Deny



Figure 12. Antaira router - Access Restrictions

3. Click **Edit list of clients**.
4. On the page that appears, enter 2 ranges of IP addresses in the **Enter the IP Range of the clients** section. The first range starts at x.x.x.2 and ends before the first IP address or range of IP addresses that you want to allow Internet access to. The second range starts after the first IP address, and ends before the second IP address or range of IP addresses that you want to allow Internet access to.

If there is only one IP address or range of IP addresses, then the second range ends with x.x.x.254.

For example, if you want to allow access to 2 computers with the IP addresses 128.15.1.8 and 128.15.1.9, then the first range is 128.15.1.2 to 128.15.1.7, and the second range is 128.15.1.10 to 128.15.1.254.

For 2 computers with the IP addresses 128.15.1.8 and 128.15.1.25, the first range is 128.15.1.2 to 128.15.1.7, and the second range is 128.15.1.9 to 128.15.1.24 as shown in Figure 13.

192.168.1.1/FilterIPMAC.asp

List of clients

Enter MAC Address of the clients in this format: xx:xx:xx:xx:xx:xx

MAC 01	00:00:00:00:00:00
MAC 02	00:00:00:00:00:00
MAC 03	00:00:00:00:00:00
MAC 04	00:00:00:00:00:00
MAC 05	00:00:00:00:00:00
MAC 06	00:00:00:00:00:00
MAC 07	00:00:00:00:00:00
MAC 08	00:00:00:00:00:00

Enter the IP Address of the clients

IP 01	192.168.1.	0
IP 02	192.168.1.	0
IP 03	192.168.1.	0
IP 04	192.168.1.	0
IP 05	192.168.1.	0
IP 06	192.168.1.	0

Enter the IP Range of the clients

IP Range 01	192.	15.	1.	2	~	192.	15.	1.	7
IP Range 02	192.	15.	1.	9	~	192.	15.	1.	24

Save Apply Settings Cancel Changes Close

Figure 13. Antaira router - Client IP range

5. Click **Save** at the bottom of the window.
6. Click **Apply Settings**.
7. Click **Close**.
8. On the WAN Access page, click **Save** at the bottom, then click **Apply Settings**.

Allow a second computer on the LAN to access the Internet

1. On the WAN Access page, provide the following information:
 - **Policy:** Select 2()
 - **Status:** Enable
 - **Policy Name:** Block Internet Access Group 2
 - **Internet access during selected days and hours:** Deny

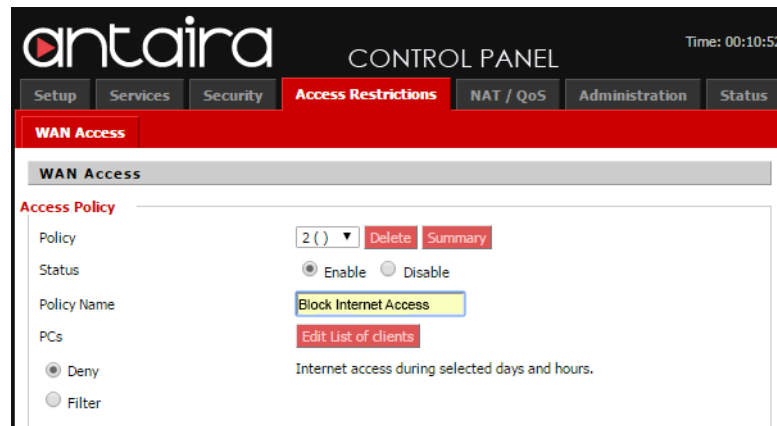


Figure 14. Antaira router - Access Restrictions

2. Click **Edit list of clients**.
3. On the page that appears, enter 2 ranges of IP addresses in the **Enter the IP Range of the clients** section. The first range starts after the second IP address that you want to allow Internet access to and ends before the third IP address that you want to allow Internet access to. The second range starts after the third IP address, and ends before the fourth IP address that you want to allow Internet access to. If there are only 2 IP addresses, then the first range ends at x.x.x.254 and the second range is all zeros.

For example, for 2 computers with the IP addresses 128.15.1.8 and 128.15.1.25, the first range is 128.15.1.26 to 128.15.1.254. The second range is 0.0.0.0 to 0.0.0.0 as shown in Figure 15. The first range excludes 128.15.1.25 and since there is no third computer, there is no need for a second range.

① 192.168.1.1/FilterIPMAC.asp

List of clients

Enter MAC Address of the clients in this format: xx:xx:xx:xx:xx:xx

MAC 01	<input type="text" value="00:00:00:00:00:00"/>
MAC 02	<input type="text" value="00:00:00:00:00:00"/>
MAC 03	<input type="text" value="00:00:00:00:00:00"/>
MAC 04	<input type="text" value="00:00:00:00:00:00"/>
MAC 05	<input type="text" value="00:00:00:00:00:00"/>
MAC 06	<input type="text" value="00:00:00:00:00:00"/>
MAC 07	<input type="text" value="00:00:00:00:00:00"/>
MAC 08	<input type="text" value="00:00:00:00:00:00"/>

Enter the IP Address of the clients

IP 01	<input type="text" value="192.168.1."/> <input type="text" value="0"/>
IP 02	<input type="text" value="192.168.1."/> <input type="text" value="0"/>
IP 03	<input type="text" value="192.168.1."/> <input type="text" value="0"/>
IP 04	<input type="text" value="192.168.1."/> <input type="text" value="0"/>
IP 05	<input type="text" value="192.168.1."/> <input type="text" value="0"/>
IP 06	<input type="text" value="192.168.1."/> <input type="text" value="0"/>

Enter the IP Range of the clients

IP Range 01	<input type="text" value="192."/> <input type="text" value="15."/> <input type="text" value="1."/> <input type="text" value="26~"/>	<input type="text" value="192."/> <input type="text" value="15."/> <input type="text" value="1."/> <input type="text" value="254"/>
IP Range 02	<input type="text" value="0."/> <input type="text" value="0."/> <input type="text" value="0."/> <input type="text" value="0~"/>	<input type="text" value="0."/> <input type="text" value="0."/> <input type="text" value="0."/> <input type="text" value="0"/>

Figure 15. Antaira router - Client IP range

4. Click **Save** at the bottom of the window.
5. Click **Apply Settings**.
6. Click **Close**.
7. On the WAN Access page, click **Save** at the bottom, then click **Apply Settings**.

2.5.6 Back up the Configuration

1. Click the Administration tab.
2. Click the **Backup** tab.
3. On the Backup page, click **Backup**.

A backup of the configuration is saved to your computer.

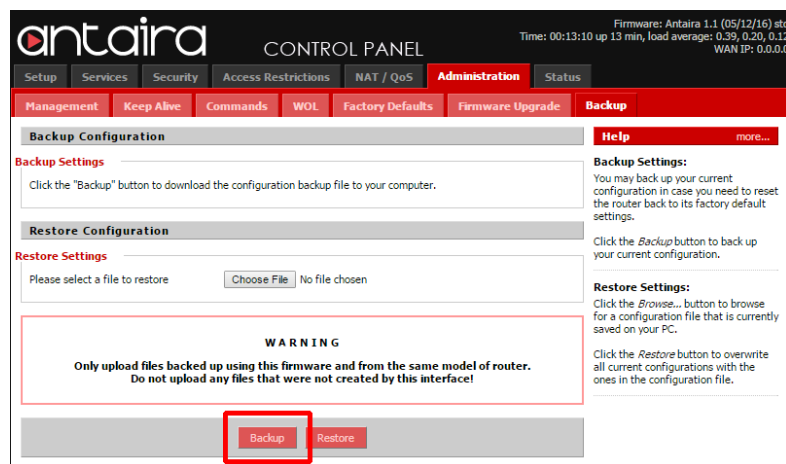


Figure 16. Antaira router - Backup and Restore

2.6 Configure the Switches

Attention: Read the documentation that comes with your switches before you start.

The instructions that follow show how to configure the Antaira 26-port Industrial Managed Ethernet Switch LNP-2602GN.

To configure the switches you must:

- Change the IP Address
- Log in to the Switch
- Configure the Name and Description
- Update Firmware
- Set the Time
- Enable Logging
- Configure the Fault LEDs
- Configure Security
- MAC and Port Binding
- Back up the Configuration
- Power Cycling

Follow the instructions below to complete these steps.

2.6.1 Change the IP Address

By default the switch has a static IP address. Consult the switch's document for more information.

1. Configure your computer directly to the switch and configure it so that it is on the same network as the switch.
2. In a Web browser on the client computer, type the IP address of the switch, and then press Enter.
3. Log in to the switch with the username and password for the switch. Consult the switch's documentation for the default username and password. For the Antaira LNP-2602GN, the username and password are **root** and **root**.
4. In the left sidebar, click **IP Configuration**.
5. Enter the following information:
 - **DHCP Client:** Disable
 - **IP Address:** The switch's IP address (see the Device List on page 99)
 - **Subnet Mask:** 255.255.255.0
 - **Gateway:** The IP address of the router (see the Device List on page 99)
6. Click **Apply**.
7. In the left sidebar, click **Save Configuration**, then click **Save**.

IP Configuration

DHCP Client :

IP Address	128.15.1.2
Subnet Mask	255.255.255.0
Gateway	128.15.1.1
DNS1	0.0.0.0
DNS2	0.0.0.0

Figure 17. Antaira switch - IP Configuration

2.6.2 Log in to the Switch

1. Connect the client computer to the LAN and configure it with its assigned IP address (see the Device List on page 99).
2. In a Web browser on the client computer, type the new IP address of the switch, and then press Enter.
3. Log in to the switch with the username and password for the switch. Consult the switch's documentation for the default username and password. For the Antaira LNP-2602GN, the username and password are **root** and **root**.

2.6.3 Configure the Name and Description

1. In the left sidebar, click **System**, then click **System Information**.
2. Enter the following information:
 - **System Name:** A name for the switch
 - **System Description:** The a description of the switch
 - **System Location:** The location of the switch

This information is helpful for identifying the switch later, so be as descriptive as you can.

3. Click **Apply**.
4. In the left sidebar, click **Save Configuration**, then click **Save**.

System Information

System Name	LNP-2602GN
System Description	24 10/100TX PoE + 2 10/100/1000T/Mini-GBIC Combo Managed Industrial Sw
System Location	Mircom Group of Companies - Engineering Lab
System Contact	Mircom Group of Companies

Firmware Version	v1.20
Kernel Version	v6.06
MAC Address	7CCB0D001DAA
Serial Number	53780150400070

Figure 18. Antaira switch - System Information

2.6.4 Update Firmware

If the firmware and kernel version on the System Information page (Figure 18) are lower than firmware version 1.21 and kernel version 6.07, then you must update the firmware.

1. Ensure that the client computer has administrator rights as described in section 2.6.10 on page 36.
2. On the building server, open Tftdp32.
3. In the Tftdp32 window, click **Browse** and select the directory where the firmware is located.
4. Click the menu beside **Server Interfaces** and select the network interface that is connected to the LAN.
5. Click **Settings**, then click the **Global** tab.
6. Unselect **Syslog Server** and **DHCP Server**.
7. Click the **TFTP** tab.
8. Click **Browse** and select the same directory that you selected in step 3.
9. Select **Allow "\" As virtual root**.
10. Click **OK**.
11. Quit Tftdp32 and start it again.
12. In a Web browser, log in to the switch.
13. Click the **TFTP** tab under the **System** menu.
14. Click the **Update Firmware** tab.
15. Type the address of your laptop in the **TFTP Server** field.
16. Type the name of the firmware in the field.

Note: The firmware name must exactly match the file name of the firmware on the computer.

17. Click **Apply**.

After the firmware is updated, the switch restarts.

2.6.5 Set the Time

1. In the left sidebar, click **SNTP**.
2. Enter the following information:
 - **SNTP Client:** Enable
 - **Daylight Savings Time:** Enable
 - **UTC Timezone:** Your time zone

- **SNTP Server URL:** The IP address of the building server (see the Device List on page 99)
 - **Daylight Saving Period:**
 - **Daylight Saving Offset:** 60
3. Click **Apply**.
 4. In the left sidebar, click **Save Configuration**, then click **Save**.

SNTP Configuration

SNTP Client :

Daylight Saving Time :

UTC Timezone	<input type="text" value="(GMT-05:00)Eastern Time (US & Canada)"/>	
SNTP Server URL	<input type="text" value="128.15.1.3"/>	
Switch Timer	<input type="text" value="9/14/2016, 2:36:37 PM"/>	
Daylight Saving Period	<input type="text" value="20160307 00:00"/>	<input type="text" value="20161106 00:00"/>
Daylight Saving Offset(mins)	<input type="text" value="60"/>	

Figure 19. Antaira switch - SNTP Configuration

2.6.6 Enable Logging

Enable the system event log

1. In the left sidebar, click **System Event Log**.
2. Click the **Syslog Configuration** tab.
3. Enter the following information:
 - **Syslog Mode:** Both
 - **Syslog Server IP Address:** 0.0.0.0
4. Click **Apply**.
5. In the left sidebar, click **Save Configuration**, then click **Save**.

System Event Log - Syslog Configuration

Syslog Configuration
SMTP Configuration
Event Configuration

Syslog Mode	Both ▼	<input type="button" value="Apply"/>
Syslog Server IP Address	0.0.0.0	

44: Jan 1 00:37:41 : System Log Enable!
43: Jan 1 00:11:56 : Port.25: Link Up!
42: Jan 1 00:11:54 : Port.25: Link Down!
41: Jan 1 00:00:50 : Port.01: Link Up!
40: Jan 1 00:00:48 : Port.01: Link Down!
39: Jan 1 00:00:24 : Port.24: Link Up!
38: Jan 1 00:00:22 : Port.24: Link Down!
37: Jan 1 00:00:21 : Port.07: Link Up!
36: Jan 1 00:00:21 : Port.06: Link Up!
35: Jan 1 00:00:21 : Port.05: Link Up!
34: Jan 1 00:00:20 : Port.04: Link Up!
33: Jan 1 00:00:20 : Port.03: Link Up!
32: Jan 1 00:00:20 : Port.02: Link Up!
31: Jan 1 00:00:19 : Port.07: Link Down!
30: Jan 1 00:00:19 : Port.06: Link Down!
29: Jan 1 00:00:18 : Port.05: Link Down!
28: Jan 1 00:00:18 : Port.04: Link Down!
27: Jan 1 00:00:18 : Port.03: Link Down!
26: Jan 1 00:00:17 : Port.02: Link Down!
25: Jan 1 00:00:17 : Port.25: Link Up!

Page.1 ▼

Figure 20. Antaira switch - Syslog Configuration

Configure the switch to report a message in the log when a device is connected or disconnected from the port

1. Click the **Event Configuration** tab.
2. For each port that has a device connected to it, select **Link Up & Link Down** in the **Syslog** column.
3. Click **Apply**.
4. In the left sidebar, click **Save Configuration**, then click **Save**.

System Event Log - Event Configuration

Syslog Configuration
SMTP Configuration
Event Configuration

System Event Selection		
Event Type	Syslog	SMTP
Device cold start	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device warm start	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Authentication failure	<input checked="" type="checkbox"/>	<input type="checkbox"/>
X-Ring topology change	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Port Event Selection		
Port	Syslog	SMTP
Port.01	Disable ▼	Disable ▼
Port.02	Link Up & Link Down ▼	Disable ▼
Port.03	Disable ▼	Disable ▼
Port.04	Disable ▼	Disable ▼
Port.05	Disable ▼	Disable ▼
Port.06	Disable ▼	Disable ▼
Port.07	Disable ▼	Disable ▼
Port.08	Disable ▼	Disable ▼
Port.09	Disable ▼	Disable ▼
Port.10	Disable ▼	Disable ▼
Port.11	Disable ▼	Disable ▼
Port.12	Disable ▼	Disable ▼
Port.13	Disable ▼	Disable ▼
Port.14	Disable ▼	Disable ▼
Port.15	Disable ▼	Disable ▼
Port.16	Disable ▼	Disable ▼
Port.17	Disable ▼	Disable ▼
Port.18	Disable ▼	Disable ▼
Port.19	Disable ▼	Disable ▼
Port.20	Disable ▼	Disable ▼
Port.21	Disable ▼	Disable ▼
Port.22	Disable ▼	Disable ▼
Port.23	Disable ▼	Disable ▼
Port.24	Disable ▼	Disable ▼

Figure 21. Antaira switch - System Event Log

2.6.7 Configure the Fault LEDs

1. In the left sidebar, click **Fault Relay Alarm**.
2. Select the checkboxes to enable the LEDs for power failure.
3. Select the checkboxes to enable the LEDs for each port.

When these options are enabled, the fault LED on the switch for a programmed port illuminates when a device is disconnected from that port.

4. Click **Apply**.
5. In the left sidebar, click **Save Configuration**, then click **Save**.

Fault Relay Alarm

Power Failure	
<input type="checkbox"/> Power 1	<input type="checkbox"/> Power 2
Port Link Down/Broken	
<input type="checkbox"/> Port.01	<input checked="" type="checkbox"/> Port.02
<input type="checkbox"/> Port.03	<input type="checkbox"/> Port.04
<input type="checkbox"/> Port.05	<input type="checkbox"/> Port.06
<input type="checkbox"/> Port.07	<input type="checkbox"/> Port.08
<input type="checkbox"/> Port.09	<input type="checkbox"/> Port.10
<input type="checkbox"/> Port.11	<input type="checkbox"/> Port.12
<input type="checkbox"/> Port.13	<input type="checkbox"/> Port.14
<input type="checkbox"/> Port.15	<input type="checkbox"/> Port.16
<input type="checkbox"/> Port.17	<input type="checkbox"/> Port.18
<input type="checkbox"/> Port.19	<input type="checkbox"/> Port.20
<input type="checkbox"/> Port.21	<input type="checkbox"/> Port.22
<input type="checkbox"/> Port.23	<input type="checkbox"/> Port.24
<input type="checkbox"/> Port.25	<input type="checkbox"/> Port.26

Figure 22. Antaira switch - Fault Relay Alarm

2.6.8 Configure Security

Prevent unwanted computers from accessing the switch's Web configuration

1. In the left sidebar, click **IP Security**.
2. Enter the following information:
 - **IP Security Mode:** Enable
 - **Enable HTTP Server:** Enable
 - **Enable Telnet Server:** Enable
 - **Security IP1:** The IP address of the building server (see the Device List on page 99)
 - **Security IP2:** The IP address of the client computer (see the Device List on page 99)
 - **Security IP3:** The IP address of any technician's computer that needs to access the switch's Web configuration
3. Click **Apply**.
4. In the left sidebar, click **Save Configuration**, then click **Save**.

IP Security

IP Security Mode: Enable ▼

☒ Enable HTTP Server

☒ Enable Telnet Server

Security IP1	198.162.1.18
Security IP2	0.0.0.0
Security IP3	0.0.0.0
Security IP4	0.0.0.0
Security IP5	0.0.0.0
Security IP6	0.0.0.0
Security IP7	0.0.0.0
Security IP8	0.0.0.0
Security IP9	0.0.0.0
Security IP10	0.0.0.0

Apply
Help

Figure 23. Antaira switch - IP Security

2.6.9 MAC and Port Binding

Bind each port to the MAC address of the device connected to it

1. In the left sidebar, click **Security**, then click **MAC Address Table**.
2. Click the **Static Mac Addresses** tab.
3. For each port that has a device connected to it, enter the following information:
 - **MAC Address:** The MAC address of the device that is connected to this port (see the Device List on page 99)
 - **Port No.:** The port that this device is connected to (see the Device List on page 99)
 - **VLAN ID:** 1
4. Click **Add**.
5. Repeat steps 3 to 4 for each port that has a device connected to it.
6. In the left sidebar, click **Save Configuration**, then click **Save**.

MAC Address Table - Static MAC Addresses

Static MAC Addresses
MAC Filtering
All Mac Addresses
Multicast Filtering

MAC Address	Port	VLAN ID
FCC23D07A506	Port.01	1

MAC Address

Port No.

VLAN ID

Port.01

Add
Delete
Help

Figure 24. Antaira switch - MAC Address Table

Enable 802.1x

The 802.1x protocol works in conjunction with MAC and port binding to allow and deny connections to ports.

1. In the left sidebar, click **802.1x/Radius**.
2. Beside **802.1x Protocol**, select **Enable**.

802.1x/Radius - System Configuration

System Configuration
Port Configuration
Misc Configuration

802.1x Protocol	Enable
Radius Server IP	0.0.0.0
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	NAS_L2_SWITCH

Apply
Help

Figure 25. Antaira switch - 802.1x/Radius

3. Click the **Port Configuration** tab.
4. For each port except the uplink ports and the port connected to the router, enter the following information:
 - Select the port, then select **Authorize**.

5. Click **Apply**.
6. Repeat steps 4 to 5 for each port that has a device connected to it.

Leave the uplink ports and the port connected to the router as Disabled.

If a device is connected to a port that is configured as Authorize, the switch allows access only if the device's MAC address matches the MAC address bound to the port.

802.1x/RADIUS - Port Configuration

System Configuration
Port Configuration
Misc Configuration

Port
Port.01
Port.02
Port.03
Port.04
Port.05

State
<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;"> Authorize ▼ </div>

Apply
Help

Port Authorization

Port	State
Port.01	Authorize
Port.02	Authorize
Port.03	Authorize
Port.04	Authorize
Port.05	Authorize
Port.06	Authorize
Port.07	Authorize
Port.08	Authorize
Port.09	Authorize
Port.10	Authorize
Port.11	Authorize
Port.12	Authorize
Port.13	Authorize

Figure 26. Antaira switch - Port Configuration

7. In the left sidebar, click **Save Configuration**, then click **Save**.

2.6.10 Back up the Configuration

This section describes how to save a backup of the configuration in case you need to restore it later.

1. On the client computer, click **Control Panel > User Accounts**.
2. Click **Manage User Accounts** to check whether or not your user account has administration rights.
3. If you do not have administration rights:
 - a. Highlight **Administrator** and click **Reset Password**.
 - b. Enter a new password.
 - c. Log into the administrator account with the newly password.
4. On the building server, open Tftpd32.

5. In the Tftpd32 window, click **Browse** and select the directory where you want to save the backup.

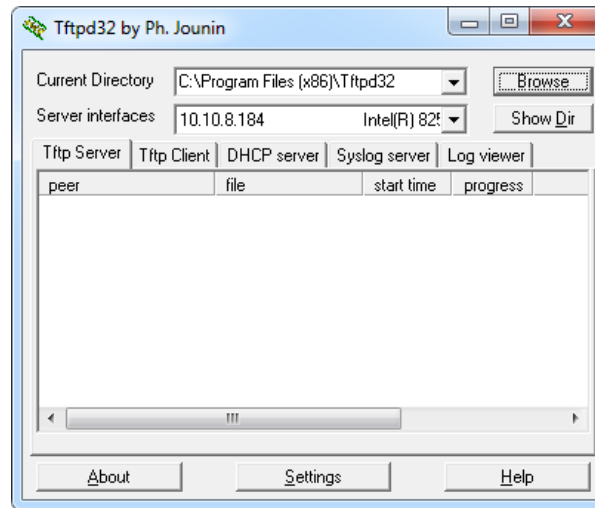


Figure 27. Tftpd32

6. Click the menu beside **Server Interfaces** and select the network interface that is connected to the LAN.
7. Click **Settings**, then click the **Global** tab.
8. Unselect **Syslog Server** and **DHCP Server**.

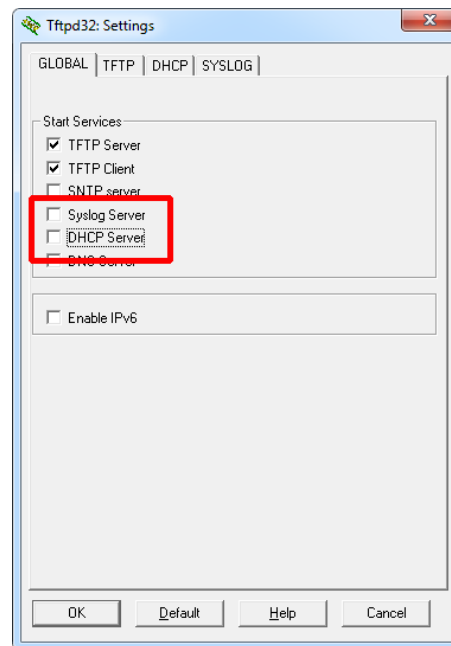


Figure 28. Tftpd32 - Global tab

9. Click the **TFTP** tab.
10. Click **Browse** and select the same directory that you selected in step 5.
11. Select **Allow "\" As virtual root**.

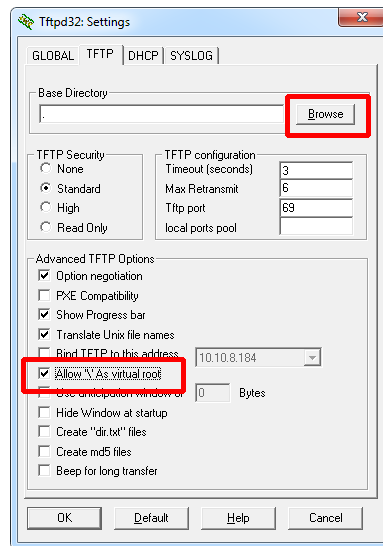


Figure 29. TFTP32 - TFTP tab

12. Click **OK**.
13. Quit Tftdp32 and start it again.
14. In a Web browser, log in to the switch.
15. Click the **TFTP** tab under the **System** menu.
16. Click the **Backup Configuration** tab.

TFTP - Backup Configuration

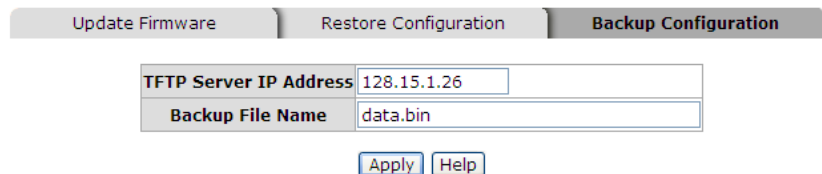


Figure 30. Antaira Switch - Backup Configuration

17. Type the address of your laptop in the **TFTP Server IP Address** field.
18. Click **Apply**.

The firmware is downloaded to the client computer. Its name is the same name in the **Backup File Name** field.

2.6.11 Power Cycling

The switch should provide the ability to power cycle each port from the switch's Web configuration. If there is a problem with a device, you can power cycle the port that the device is connected to.

1. In the left sidebar, click **Power over Ethernet**.
2. Unselect the checkbox under **Enable State** then click **Apply** to turn off the corresponding port.

Power over Ethernet

Maximum Power Available	400 W	Actual Power Consumption	64 W
System Power Limit	400 W	Main Supply Voltage	476 dV

Firmware Version2.04

Port Knockoff Disabled☒

AC Disconnect☒

Capcitive Detection☒

Start☒

Apply

Port	Enable state	Power Limit From Classification	Legacy	Priority	Power Limit (<22600) (mW)	Mode	Current (mA)	Voltage (V)	Power (mW)	Determined Class
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low ▾	22600	InvalidPD	0	0.0	0	0:15.4W
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low ▾	22600	Detecting	0	0.0	0	0:15.4W
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low ▾	22600	Detecting	0	0.0	0	0:15.4W
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low ▾	22600	Detecting	0	0.0	0	0:15.4W
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low ▾	22600	Detecting	0	0.0	0	0:15.4W
6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low ▾	22600	Detecting	0	0.0	0	0:15.4W
7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low ▾	22600	Detecting	0	0.0	0	0:15.4W
8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low ▾	22600	InvalidPD	0	0.0	0	0:15.4W
9	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low ▾	22600	Detecting	0	0.0	0	0:15.4W
10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low ▾	22600	Detecting	0	0.0	0	0:15.4W
11	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low ▾	22600	Detecting	0	0.0	0	0:15.4W
12	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low ▾	22600	Detecting	0	0.0	0	0:15.4W
13	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low ▾	22600	Pwr(IEEE)	112	47.4	5297	0:15.4W
14	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low ▾	22600	Pwr(IEEE)	112	47.5	5333	0:15.4W
15	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low ▾	22600	Pwr(IEEE)	113	47.8	5398	0:15.4W
16	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low ▾	22600	Pwr(IEEE)	111	47.5	5286	0:15.4W
17	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low ▾	22600	Pwr(IEEE)	110	47.5	5258	0:15.4W
18	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Low ▾	22600	Pwr(IEEE)	110	47.7	5238	0:15.4W

Figure 31. Antaira switch - Power over Ethernet

2.7 Configure Remote Access

This section describes how to configure a remote access program such as TeamViewer so that the technician can control the site remotely.

1. Download the remote access program on two computers: the building server or the client computer if there is one, and the remote computer.
2. Install and configure the remote access program on both computers.

3. During the installation select **Basic** and **Personal / Non-commercial use**.

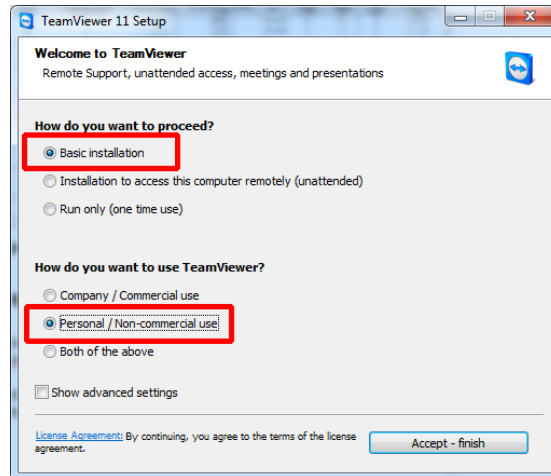


Figure 32. TeamViewer - Installation

4. When TeamViewer starts, make a note of the 9 digit number in the **Your ID** field. You will use this number to connect to the computer remotely.
5. Configure the program to start when Windows starts.

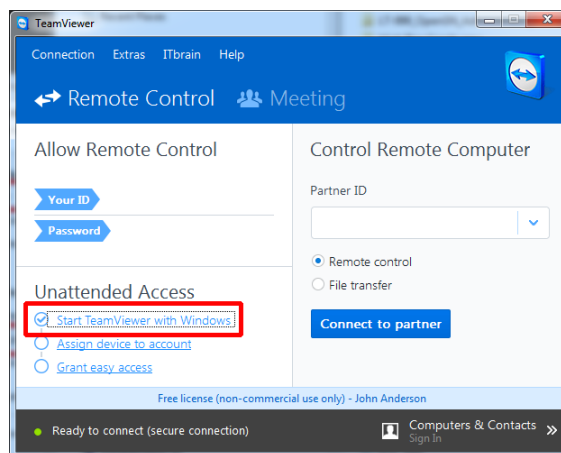


Figure 33. TeamViewer - Main window

6. Click **Connection > Setup unattended access**.
7. Create a computer name and password for connecting with the building server or client computer.

A technician can use this computer name and password to connect to this computer remotely. This password should not change.



Figure 34. TeamViewer - Define personal password

8. Click **Extras > Options**.
9. Click **Security**.
10. Beside **Windows login**, select **Allowed for all users**.

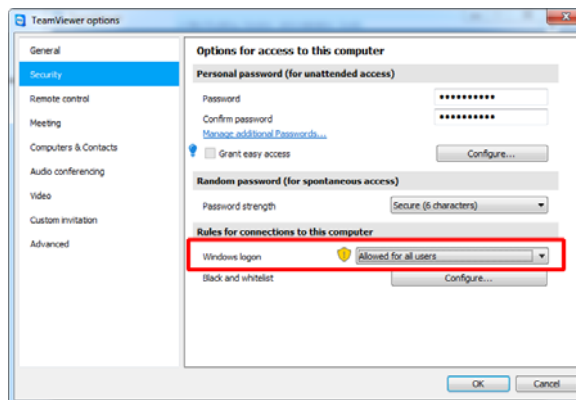


Figure 35. TeamViewer - Options

11. Click **OK**.

2.7.1 Connect to a Computer Remotely

To connect to a computer remotely

1. On the remote computer, open the remote access program.

2. Enter the 9 digit number in the **Partner ID** field.
3. Enter the password you created in step 7 above.

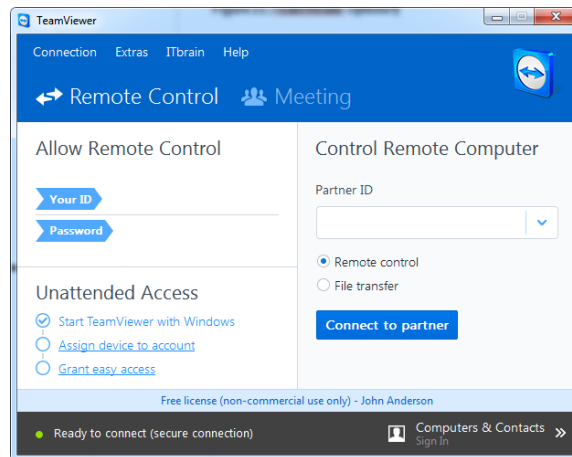


Figure 36. TeamViewer - Main window

2.7.2

Create an Account to Manage Multiple Job Sites

TeamViewer lets you easily manage more than one job site.

1. In the main TeamViewer window, click **Computers & Contacts**.
2. Click **Sign Up**, and create a TeamViewer account.

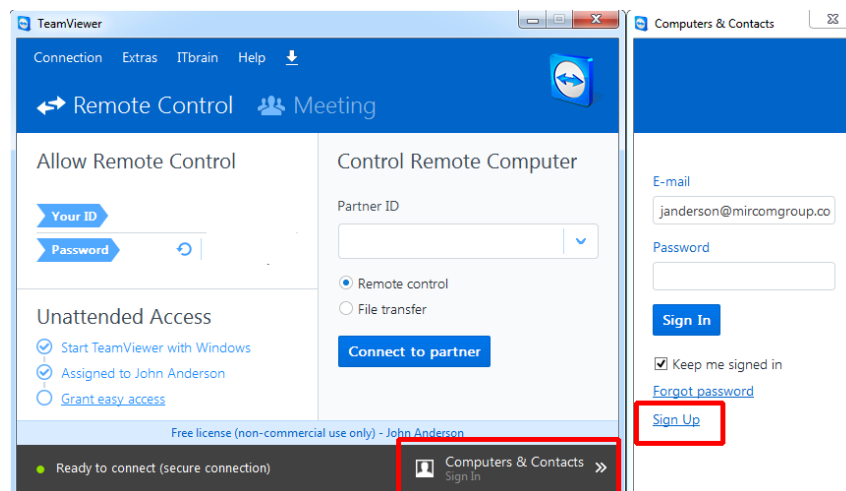


Figure 37. TeamViewer - Sign Up

3. After you have created an account, click the icon shown in Figure 38 and click **Add remote computer**.

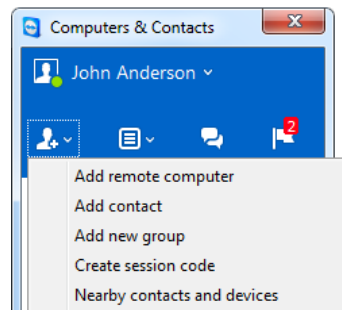


Figure 38. TeamViewer - Add remote computer

4. In the TeamViewer ID field, enter the 9 digit number and password associated with the computer that you want to connect to.

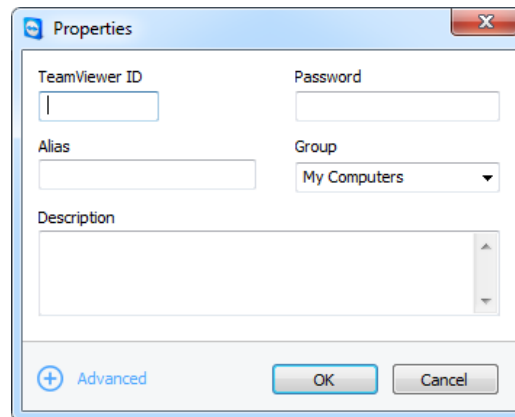


Figure 39. TeamViewer - Properties

5. Type a descriptive **Alias** and **Description** for the computer.
6. Click **OK**.
7. Repeat these steps for each computer that you want to connect to.

3 Virtual Machine Management

This chapter explains how to install the virtual machine.

- Install the Virtual Machine
- Start the Virtual Machine
- Set the IP Address
- Set the Virtual Machine Time
- Change your Virtual Machine Password
- Disable Call Control
- Delete Logs
- Configure the Virtual Machine to Start Automatically
- Configure the Building Server to Start Automatically
- Change the Default Website of the Virtual Machine (Optional)

3.1 Install the Virtual Machine

A virtual machine is a software environment that emulates computer hardware and software.

The virtual machine can run on Oracle VirtualBox, which is free open-source virtualization software. There are versions for Windows, Mac OS X, Linux, and Solaris. The operating system in the virtual machine is Linux Ubuntu 10.04 LTS (<http://www.ubuntu.com/>).

To install the virtual machine you must:

- Verify the system requirements
- Install VirtualBox
- Import the virtual machine into VirtualBox
- Start the virtual machine

Follow the instructions below to complete these steps.

3.1.1 Install VirtualBox

1. Ensure that the Ethernet network is configured and that the building server is connected to the building network.

2. On the building server, download the version of Oracle VM VirtualBox for your operating system:
<https://www.virtualbox.org/wiki/Downloads>
3. Run the VirtualBox installer.
4. Click **Next** on the Welcome window.
5. On the first **Custom Setup** window, click **Next**.

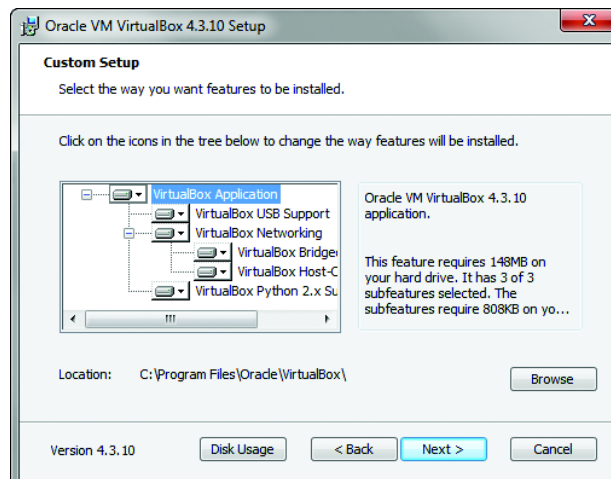


Figure 40. VirtualBox - Custom Setup

6. On the second **Custom Setup** window, click **Next**.
7. On the **Network Interfaces** window, click **Next**. The VirtualBox installer temporarily disconnects you from your network.



Figure 41. VirtualBox - Network Interfaces

Attention: When you install VirtualBox, you are temporarily disconnected from your network.

8. On the **Ready to Install** window, click **Install**.


The VirtualBox Installer installs software for network and USB adapters.

9. When Windows asks you if you want to install device software, click **Install**.

After Windows has installed the device software, a window appears saying that the installation is complete.

10. Click **Finish**.

3.1.2 Import the Virtual Machine into VirtualBox

1. On the **Welcome to VirtualBox** window, click **File**, then click **Import Appliance**.
2. Click the folder icon , select the virtual machine image, and then click **Next**.
3. On the **Import Virtual Appliance** window, select **Reinitialize the MAC address of all network cards**.
4. Scroll to the bottom of the window and ensure that the location of the Virtual Disk Image is a drive with enough space.

For example, if the C:\ drive has 500 GB, and the D:\ drive has 2 TB, then double-click the Virtual Disk Image and change it to **D:**.

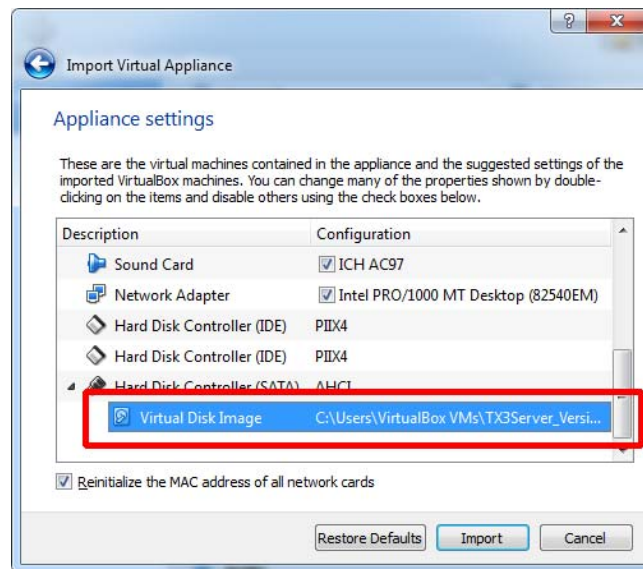


Figure 42. VirtualBox - Appliance Settings

5. Click **Import**.

The VirtualBox Manager imports the virtual machine.

3.1.3 Configure the Network

1. On the VirtualBox Manager window, select the virtual machine that you just imported.
2. Click **Settings**.
3. In the Settings window, select **Network** on the left.
4. Select **Bridged Adapter** in the menu next to **Attached to**.

5. Select the network adapter that the building server is using in the menu next to **Name**.

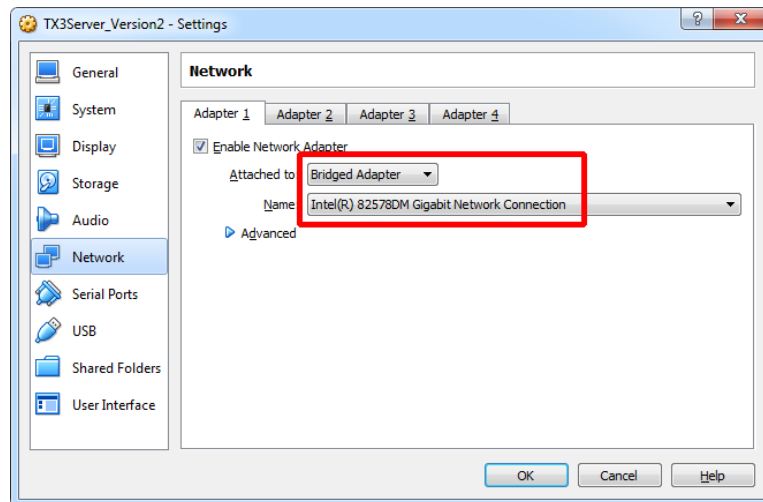


Figure 43. VirtualBox - Adapter

6. Click **Advanced**, and record the virtual machine's MAC address in the Device List on page 99.

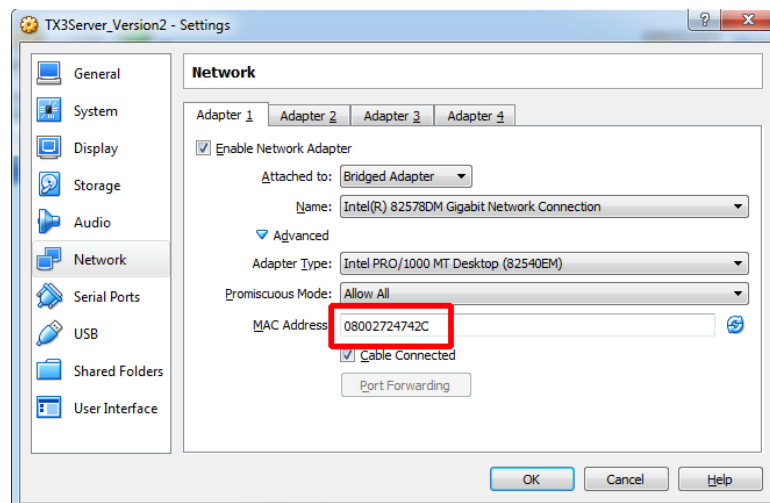


Figure 44. VirtualBox - MAC address

7. Select **System** on the left.

8. Ensure that the slider beside **Base Memory** is not in the red. If it is, the virtual machine might not run.

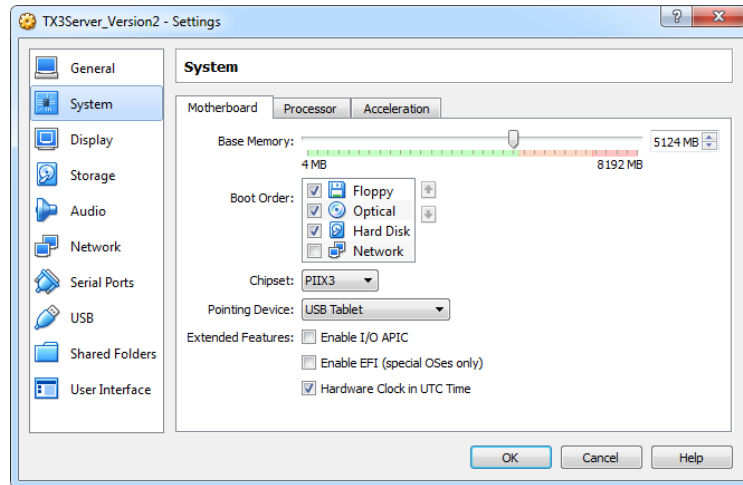



Figure 45. VirtualBox - Memory

9. Click **OK**.

3.2 Start the Virtual Machine

1. On the VirtualBox Manager window, click **Start**. 
2. On the login window, double-click **mircom**, type **mircom** for the password, and then click **Log In**.

To change your password, see section 3.5 on page 52.

3.3 Set the IP Address

By default, the virtual machine has a dynamically assigned IP address. You must change this to a static IP address.

1. Double-click the **Terminal** icon on the desktop.
2. Type the following command, then press Enter.

ifconfig



- ```
sudo vi /etc/network/interfaces
```

- Terminal displays the network interface information for the virtual machine.



6. Use the arrow keys to move the cursor down to the **address** line, and then press the **i** key to enter editing mode.
7. Type the IP address of the virtual machine after **address**. See the Device List on page 99.
8. Move down to the next four lines and type the following pieces of information:
  - **netmask:** 255.255.255.0
  - **network:** The first 3 octets of your IP address range, with **0** as the fourth octet. For example, if your IP range is 128.15.1.1 to 128.15.1.100, then type **128.15.1.0** here.
  - **broadcast:** The first 3 octets of your IP address range, with **255** as the fourth octet. For example, if your IP range is 128.15.1.1 to 128.15.1.100, then type **128.15.1.255** here.
  - **gateway:** The IP address of the router. See the Device List on page 99.
9. Edit the **eth** number so that it matches the **eth** number that you noted in step 3.

For example, if ifconfig listed **eth4**, then change the two lines in the Terminal that begin with **auto** and **iface** so that they are:

  - **auto eth4**
  - **iface eth4 inet static**
10. In the Terminal, press the Esc key, then type **:wq** and press Enter to exit the editing program.
11. In the Terminal, type the following command to restart the network interface:

```
sudo /etc/init.d/networking restart
```

## 3.4 Set the Virtual Machine Time

1. In the virtual machine, open Terminal and type:

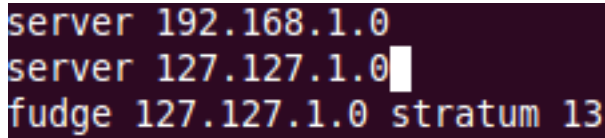
```
sudo vi /etc/ntp.conf
```

and then press Enter.
2. Type the virtual machine password and press Enter.

Terminal displays the timer server information for the virtual machine.
3. Press the **i** key to enter editing mode.

4. Change the IP address on the first line to the IP address of the Building Server (see the Device List on page 99). For example, if the building server's IP address is 192.168.1.0, then change the line so that it reads:

**server 192.168.1.0**



```
server 192.168.1.0
server 127.127.1.0
fudge 127.127.1.0 stratum 13
```

**Figure 48. Virtual machine time server setting**

5. Press the Esc key, then type **:wq** and press Enter to exit the editing program.
6. Type the following to restart the time interface:

**sudo service ntp restart**

and press Enter.

## 3.5 Change your Virtual Machine Password

The default password for the **mircom** account is **mircom**. You should change the password as soon as possible.

### To change your password

1. In the virtual machine, click the System menu, click Preferences, and then click About Me.
2. Click **Change Password**.
3. Type your current password, and then click **Authenticate**.
4. Type your new password in the fields, and then click **Change password**.  
Your new password must be at least 6 characters long.
5. Click **Close**.

## 3.6 Disable Call Control

Disabling call control ensures that there is no limit on calls between TX3 InSuites.

### To disable call control

1. In the virtual machine, double-click the **Terminal** icon on the desktop.
2. Type the following command, then press Enter.  
**sudo service call-control stop**
3. Type **mircom** for the password, and then press Enter.

## 3.7 Delete Logs

### Back up logs

1. On the building server, start WINSCP and enter the following information:
  - File Protocol: **SCP**
  - Host name: IP address of the virtual machine
  - Username: **root**
  - Password: **mircom**
2. Click **Login**.

In WINSCP, the left pane shows the contents of the building server, and the right pane shows the contents of the virtual machine.

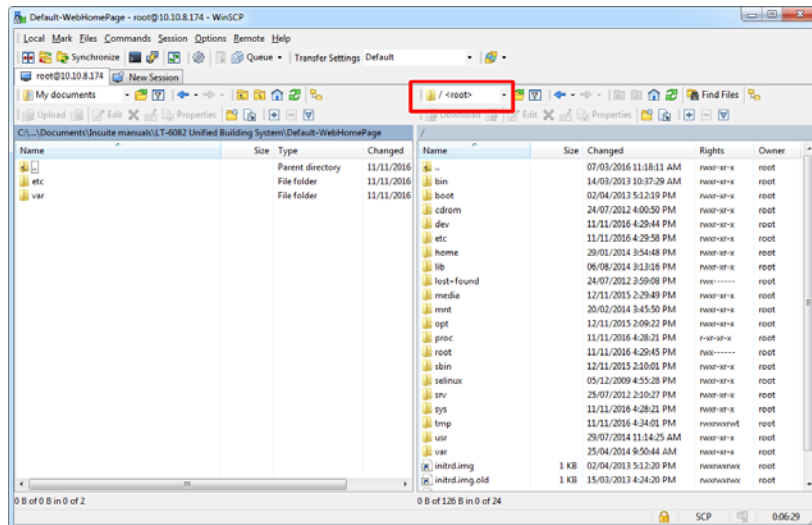


Figure 49. WINSCP navigation menu

3. In the right pane, click the navigation menu and select /<root>, then select /var/log.

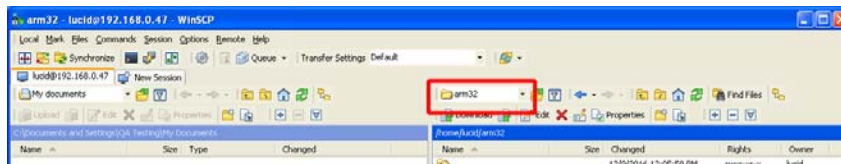


Figure 50. WINSCP - navigation menu

4. Transfer all the files beginning with **syslog** from the /var/log directory.

### Delete logs

1. In the virtual machine, double-click the **Terminal** icon on the desktop.
2. Type the following command, then press Enter.
3. Type **mircom** for the password, and then press Enter.
4. Type the following command, then press Enter.

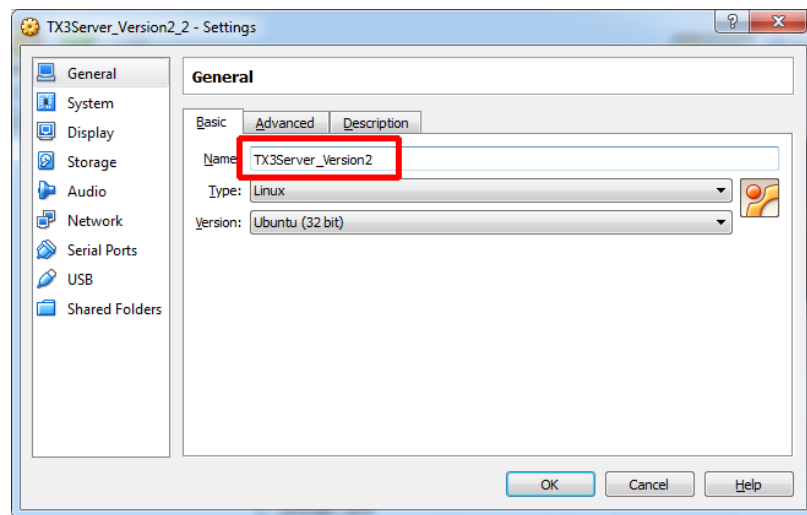
```
sudo rm -r -f /var/log/syslog
```

```
sudo rm -r -f /var/log/syslog.*
```

## 3.8 Configure the Virtual Machine to Start Automatically

### Get the name of the Virtual Machine

1. On the VirtualBox Manager window, select the virtual machine.
2. Click **Settings**.
3. Make a note of the name in the **Name** field.



**Figure 51. Virtual Machine Name**

### Create a startup script

1. On the Building Server, create a text document and copy and paste the following 2 lines into it.

```
cd /D "c:\Program Files\Oracle\VirtualBox"
```

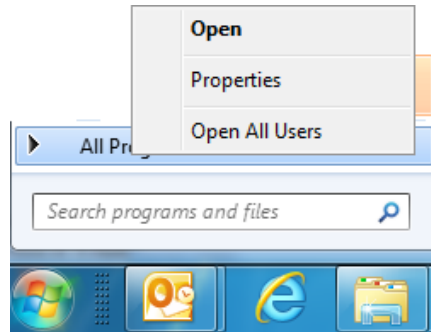
```
VBoxManage.exe startvm --type gui TX3Server_Version2
```

Change the path in the first line to the path of the Virtual Box program.

Change the virtual machine name in the second line to the name of the virtual machine that you noted above.

2. Name the text document **TX3Server-VM-AutoStart.bat**.

3. Click the **Start** menu, right-click **All Programs**, then click **Open**.



**Figure 52. Right-click All Programs**

4. In the window that appears, double-click **Programs**, then double-click **Startup**.
5. Copy **TX3Server-VM-AutoStart.bat** into the **Startup** folder.

## 3.9 Configure the Building Server to Start Automatically

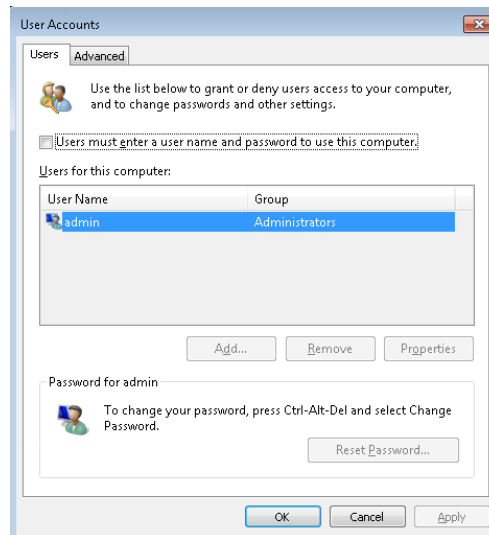
You should configure Windows on the building server so that it does not prompt for a password when it starts.

### To configure the building server to start automatically

1. Click the **Start** button, and type **netplwiz**.
2. Press **Enter**.



3. In the netplwiz window, select the admin account.



**Figure 53. netplwiz**

4. Unselect **Users must enter a user name and password to use this computer.**
5. Click **Apply**, and enter the password for the Building Server.
6. Click **OK**.

## 3.10 Change the Default Website of the Virtual Machine (Optional)

These instructions describe how to replace the default Website with a Website that you have received from Mircom.

You need:

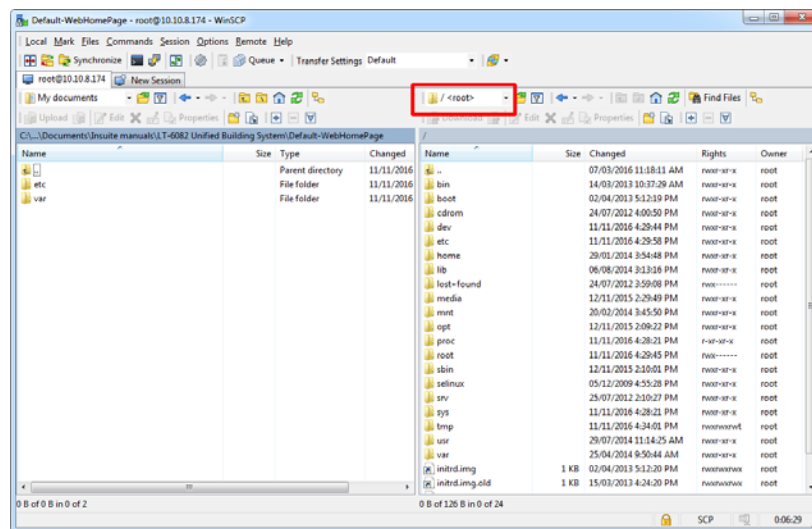
- The **Default-WebHomePage** directory from Mircom.
1. Copy the **Default-WebHomePage** directory to the building server.
  2. On the building server, navigate to the **Default-WebHomePage/var/www/smartcondo** directory.
  3. Open all the directories and delete all **.DS\_Store** files.
  4. Open the **lab** directory and copy **index.html**.
  5. Navigate back to the **smartcondo** directory and paste the **index.html** file here.

6. Start WINSXP and enter the following information:

- File Protocol: **SCP**
- Host name: IP address of the virtual machine
- Username: **root**
- Password: **mircom**

7. Click **Login**.

In WINSXP, the left pane shows the contents of the building server, and the right pane shows the contents of the virtual machine.



**Figure 54. WINSXP navigation menu**

8. In the right pane, click the navigation menu and select / <root>.
9. In the left pane, navigate to the **Default-WebHomePage** directory.
10. Copy both the **etc** and **var** directories from the building server to the **root** directory of the virtual machine.
11. Select **Yes to All**.
12. In the virtual machine, open Terminal and type:  
**sudo service apache2 restart**  
and then press Enter.
13. Type your password.
14. On the client machine, open a Web browser, enter the IP address of the virtual machine, and verify that the new Website appears.

# 4 ONVIF Camera Management

This chapter explains how to configure the cameras. This includes:

- Install the ONVIF Camera Server Software
- Disable the SSL Custom Log
- Connect to the Server
- Import the License
- Add Cameras to the Server
- Enable Recording
- Configure Storage
- Create an Administrator User
- Create a Restricted User (optional)
- Back up your Settings
- Back up Video
- Delete Video

---

**Attention:** Read the documentation that comes with your cameras and camera software before you start. The instructions that follow are not specific to any brand of camera software, so it is important to be familiar with the details of how to configure your cameras.

---

## 4.1 Install the ONVIF Camera Server Software

1. Install the ONVIF camera server and Web service on the building server.
2. Install the ONVIF client software on the optional client computer, or on the building server.

## 4.2 Disable the SSL Custom Log

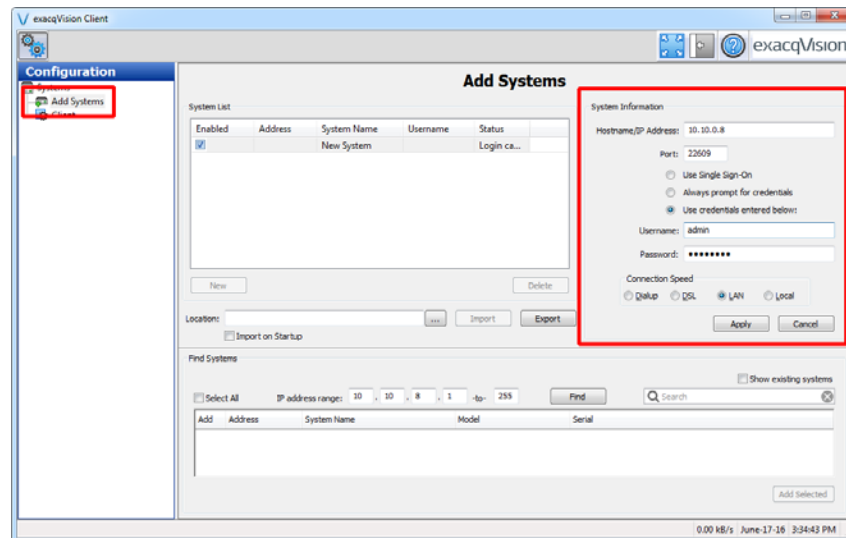
If you are installing exacqVision on Windows, follow these instructions to disable the SSL custom log.

1. On the building server, open the Control Panel.

2. Click **Administrative Tools**, then double-click **Services**.
3. Select **exacqVision Server** and then click **Stop**.
4. Select **exacqVision Web Service** and then click **Stop**.
5. Select **evApache** and then click **Stop**.
6. In Windows Explorer, open this folder:  
**C:\Program Files(x86)\eqxacqVision\webservice\Apache\conf**
7. Open the file **httpd.conf** with Notepad.
8. Comment out any lines that start with the word **Custom** by inserting # at the start of the line.
9. Save the file.
10. In Windows Explorer, open this folder:  
**C:\Program Files(x86)\eqxacqVision\webservice\Apache\conf\extra**
11. Open the file **httpd-ssl.conf** with Notepad.
12. Comment out any lines that start with the word **Custom** by inserting # at the start of the line.
13. Save the file.
14. In Windows Explorer, open this folder:  
**C:\Program Files(x86)\eqxacqVision\webservice\Apache\conf\extra**
15. Open the file **httpd-sni.conf** with Notepad.
16. Comment out any lines that start with the word **Custom** by inserting # at the start of the line.
17. Save the file.
18. Restart the computer.

## 4.3 Connect to the Server

1. Start the ONVIF client.
2. Select **Add Systems** on the left.

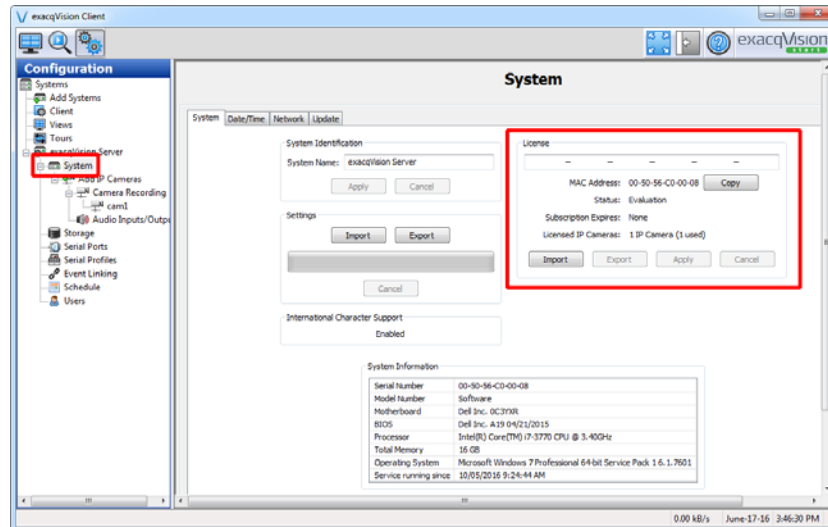


**Figure 55. exacqVision Client - Add Systems**

3. Under **System Information**, type the IP address of the ONVIF server (the same as the building server). See the Device List on page 99.
4. Select **Use credentials entered below**, and type the username and password for the server. By default the username is **admin** and the password is **admin256**.
5. Under **Connection Speed**, select **LAN**.
6. Click **Apply**.
7. The server appears in the left pane.

## 4.4 Import the License

1. In the left pane, click **System** below the server that you added.

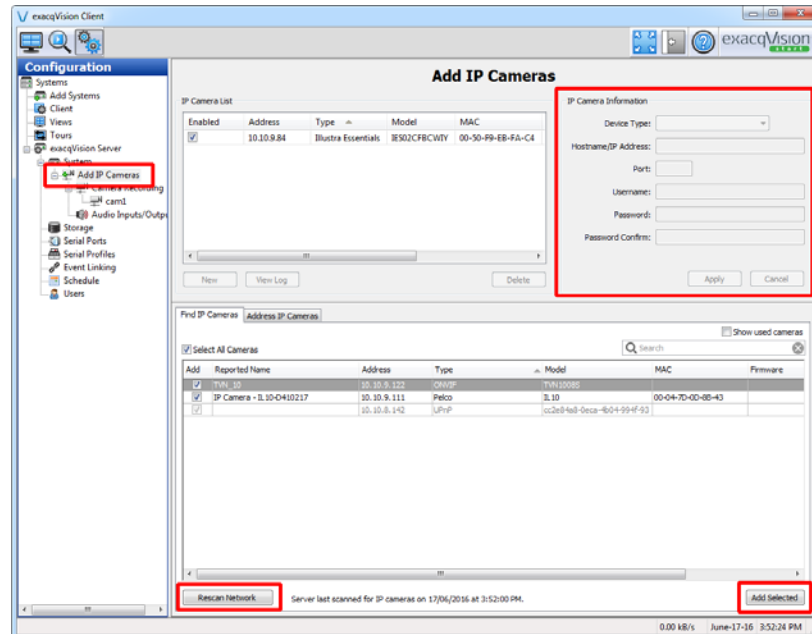


**Figure 56. exacqVision Client - System**

2. Click **Import**, then browse to your exacqVision license.
3. After you import the license, click **Export** and save the license in a secure location.

## 4.5 Add Cameras to the Server

1. In the left pane, double-click **Add IP Cameras**.



**Figure 57. exacqVision Client - Add IP Camera**

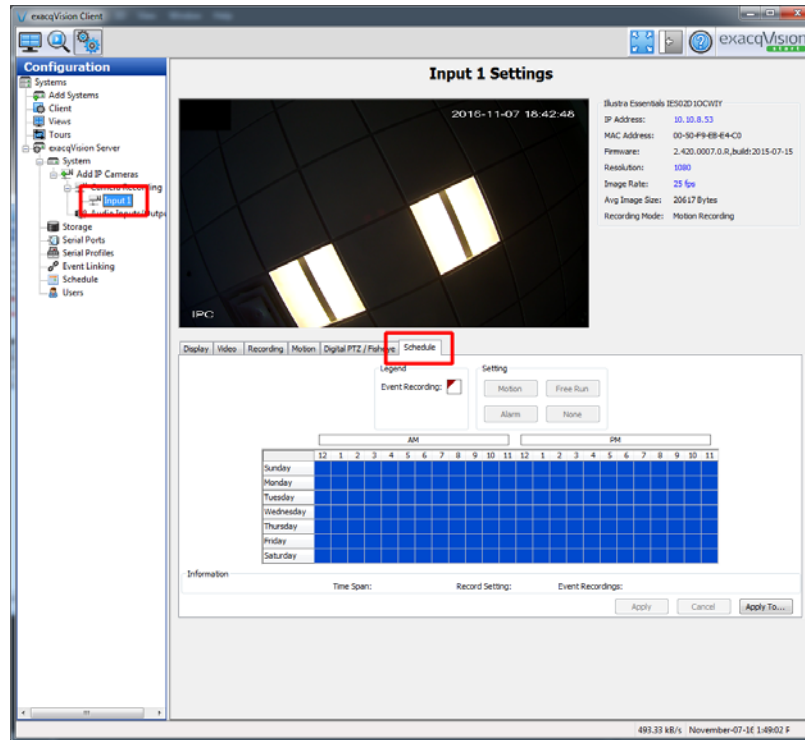
2. Click **Rescan Network**.
3. In the list of cameras that appears, select the camera that you want to add and click **Add Selected**.
4. Type the **Username** and **Password** for the camera in the upper right pane. Consult the camera's documentation for more information.
5. Type **80** for the **Port**, if it is empty.
6. Click **Apply**.
7. Select the camera that you just added from the list on the left, and type a name for the camera in the **Name** field.

**Note:** For an IP camera in the TX3 Touch, the **Name** of this camera in exacqVision must match the SIP **Display Name** of the TX3 Touch (see chapter 5).

8. Repeat steps 3 to 7 for each camera in your network.

## 4.6 Enable Recording

1. Select a camera in the **Configuration** menu.
2. Click the **Schedule** tab.



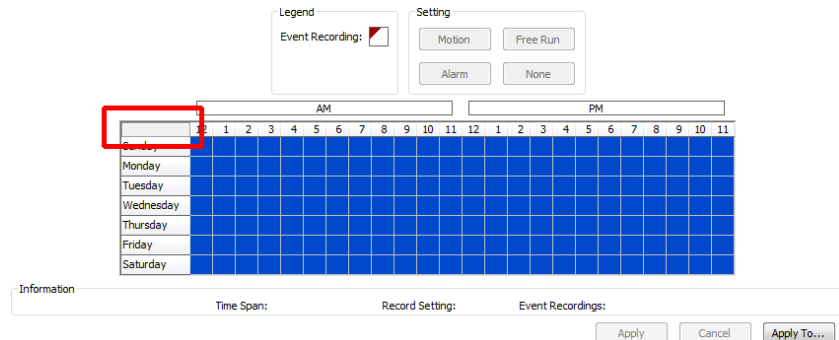
**Figure 58. exacqVision Client - Schedule**

By default, the schedule is white, which means that the camera is not recording.



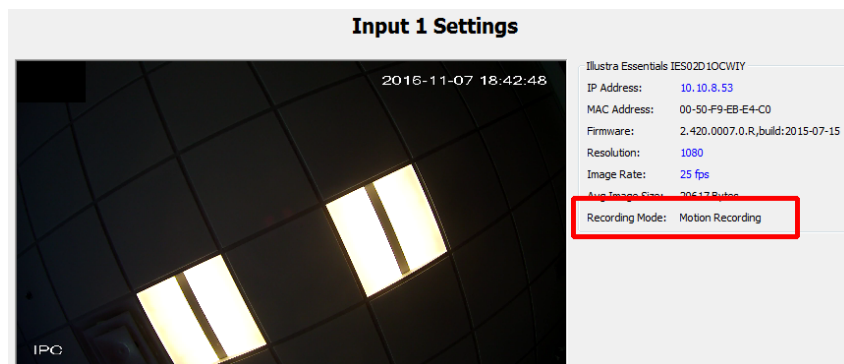
### To set the camera to record on motion

1. Click the box shown in Figure 59 to select the whole schedule.



**Figure 59. exacqVision Client - Select all**

2. Click **Motion**.
3. Note the Recording Mode as shown in Figure 60 to make sure that it is correct.



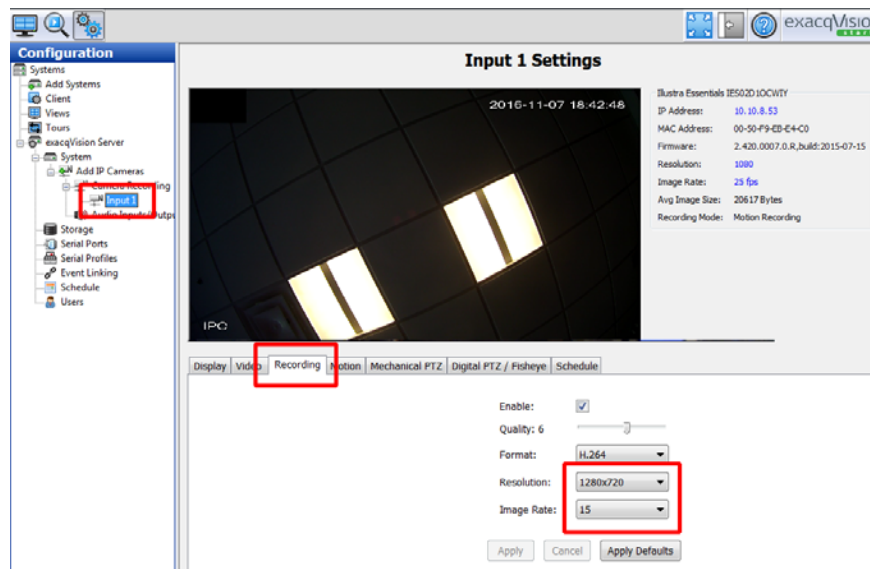
**Figure 60. exacqVision Client - Recording Mode**

4. Adjust the schedule to allow the camera to record all the time (Free Run) or when it detects motion, as desired.
5. Repeat these steps for every camera.

## 4.7 Configure Resolution and Image Rate

1. Select a camera in the **Configuration** menu.

2. Click the **Recording** tab.

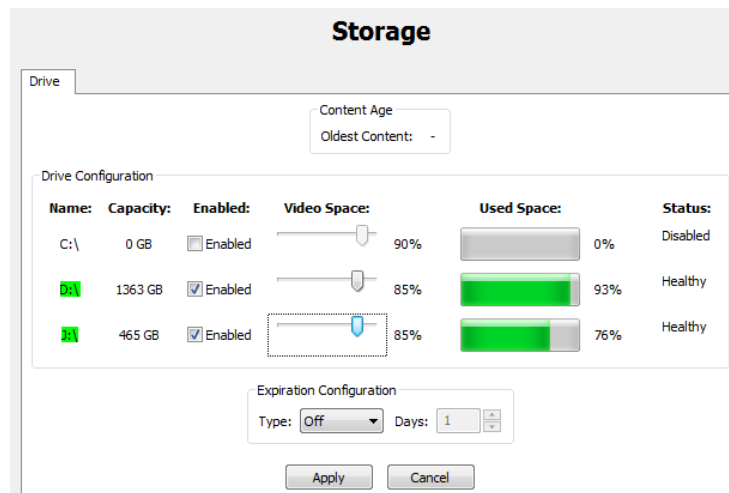


**Figure 61. exacqVision Client - Recording**

3. Select **1280x720** in the Resolution menu.
4. Select **15** in the Image Rate menu.
5. Click **Apply**.
6. Repeat these steps for every camera.

## 4.8 Configure Storage

1. In the left pane, select **Storage**.
2. Change the storage to **85%**. If possible, use a second hard drive for ONVIF camera storage, not the computer's primary hard drive.



**Figure 62. exacqVision Client - Storage**

3. Click **Apply**.

## 4.9 Create an Administrator User

The administrator user has permission to view all the camera feeds. By default, the TX3 InSuites are configured as this user and can view all the camera feeds (section 7.5.2 on page 89).

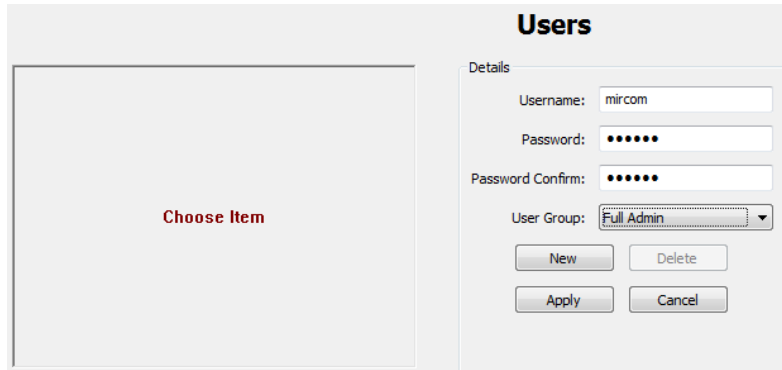
1. In the left pane, select **Users**.
2. Click **New**, and type **mircom** as the Username and **mircom** as the Password.

---

**Note:** The TX3 InSuites use this username and password to connect to the camera.

---

3. In the **User Group** menu, select **Full Admin**.



**Figure 63. exacqVision User Settings**

4. Click **Apply**.

## 4.10 Create a Restricted User (optional)

If you want to restrict some TX3 InSuites so that they can view the feeds from only some cameras, follow the instructions below.

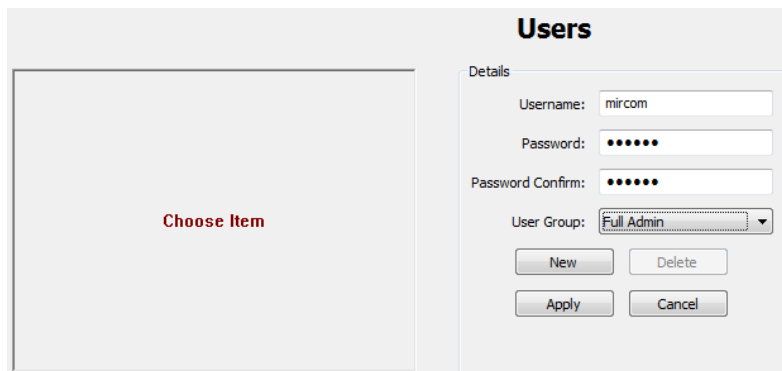
1. In the left pane, select **Users**.
2. Click **New**, and type a Username and Password.

---

**Note:** The Username and Password can be anything other than **mircom**.

---

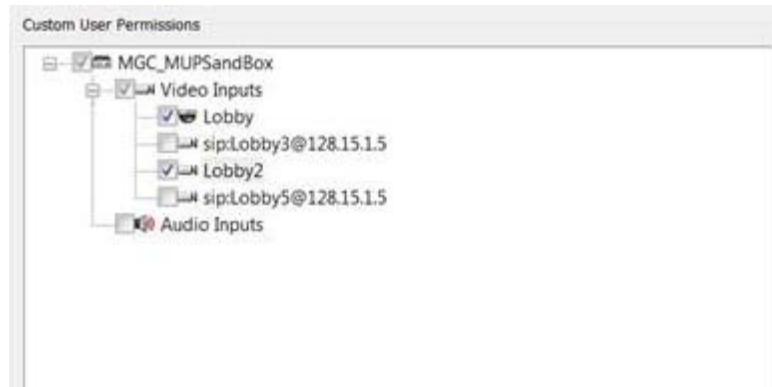
3. In the **User Group** menu, select **Full Admin**.



**Figure 64. exacqVision User Settings**

4. Click **Apply**.
5. Click **Edit**, then change the **User Group** menu to **Restricted**.

6. Select the cameras that you want this user to view.



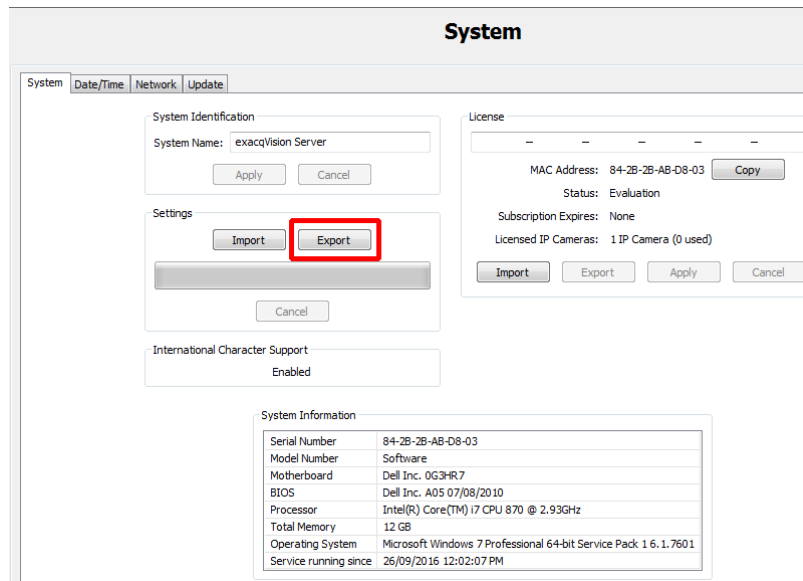
**Figure 65. Select cameras**

7. Click **Apply**.
8. For each TX3 InSuite that you want to restrict, follow the instructions in section 7.5 on page 89 to log into the TX3 InSuite and open the **smart\_home\_insuite.ini** file.
9. On the **[Exacq]** lines, change the password and username to the values that you assigned in step 2 above.
10. Press the Esc key, then type **:wq** and press Enter to exit the editing program.
11. Type the following command to restart the TX3 InSuite:  
**sudo init 6**

## 4.11 Back up your Settings

1. In the left pane, select **System**.

2. Click **Export** and save your settings to a safe place.




The screenshot shows the 'System' settings window in the exacqVision Client. The window has tabs for 'System', 'Date/Time', 'Network', and 'Update'. The 'System' tab is active. It contains several sections: 'System Identification' with a 'System Name' field set to 'exacqVision Server' and 'Apply'/'Cancel' buttons; 'Settings' with 'Import' and 'Export' buttons (the 'Export' button is highlighted with a red rectangle); 'License' with fields for 'MAC Address' (84-2B-2B-AB-D8-03), 'Status' (Evaluation), 'Subscription Expires' (None), and 'Licensed IP Cameras' (1 IP Camera (0 used)), along with 'Copy', 'Import', 'Export', 'Apply', and 'Cancel' buttons; 'International Character Support' set to 'Enabled'; and 'System Information' which lists hardware and software details in a table.

| System Information    |                                                                 |
|-----------------------|-----------------------------------------------------------------|
| Serial Number         | 84-2B-2B-AB-D8-03                                               |
| Model Number          | Software                                                        |
| Motherboard           | Dell Inc. 0G3HR7                                                |
| BIOS                  | Dell Inc. A05 07/08/2010                                        |
| Processor             | Intel(R) Core(TM) i7 CPU 870 @ 2.93GHz                          |
| Total Memory          | 12 GB                                                           |
| Operating System      | Microsoft Windows 7 Professional 64-bit Service Pack 1 6.1.7601 |
| Service running since | 26/09/2016 12:02:07 PM                                          |

**Figure 66. exacqVision Client - System**

## 4.12 Back up Video

Follow these steps to find and back up specific videos.

1. Click the Search button. 
2. Select the camera that has the video that you want to back up.
3. Select the date range and time in the **Search Range** section at the bottom of the window.
4. Click **Search**.
5. Click **Quick Export** and save the video in a secure location.

## 4.13 Delete Video

You can delete video by date or time. When you delete video, you delete it for all cameras; there is no way to delete video from some cameras and not others.

---

**Note:** Before you delete video, make sure that you have backed up any video that you want to save (see section 4.12 on page 70).

---

1. In Windows Explorer, go to the drive where video is stored (see section 4.8 on page 67).

2. Navigate to the day or hour that you want to delete.

Video is stored in directories in the format **year\month\day\hour**.

For example, to delete all video for 3:00 pm on November 8 2016, navigate to the directory:

**C:\2016\11\08\15**

3. Delete the files in the directory.

# 5 SIP Server Management

This chapter explains how to configure the SIP server.

## 5.1 Terms

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

**SIP (Session Initiation Protocol):** A protocol for controlling messaging on an IP network.

**SIP username (SIP ID):** Every device communicating on the IP network has a unique SIP username (also called SIP ID).

**SIP password:** Most SIP usernames must have a password.

## 5.2 Overview

The SIP server runs on the virtual machine. All SIP enabled devices are each configured with a unique SIP username and SIP password, as well as the IP address of the SIP server. After all the devices are registered with the server, the devices can communicate with each other.

This chapter explains how to:

- Configure the SIP Server with SIP usernames and passwords for each TX3 InSuite and lobby intercom
- Configure the User Preferences (Optional)
- Configure Kamailio to Call Multiple TX3 InSuites (Optional)

Follow the instructions below to complete these steps.



## 5.3 Configure the SIP Server

1. From the virtual machine, open Firefox and type the IP address of the virtual machine followed by **siremis** and then press Enter.

For example, if the virtual machine's IP address is 192.168.0.10, then type:

**192.168.0.10/siremis**

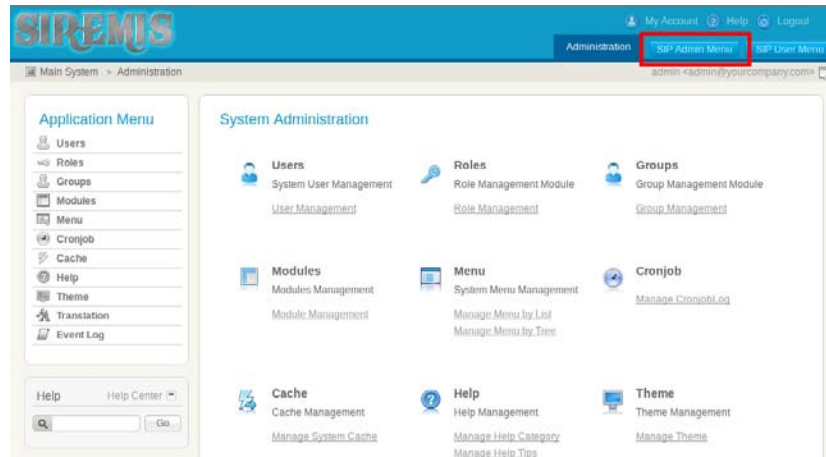


**Figure 67. SIP server - login page**

2. Type the username and password and then click **Login**. Consult the SIP server's documentation for more information.

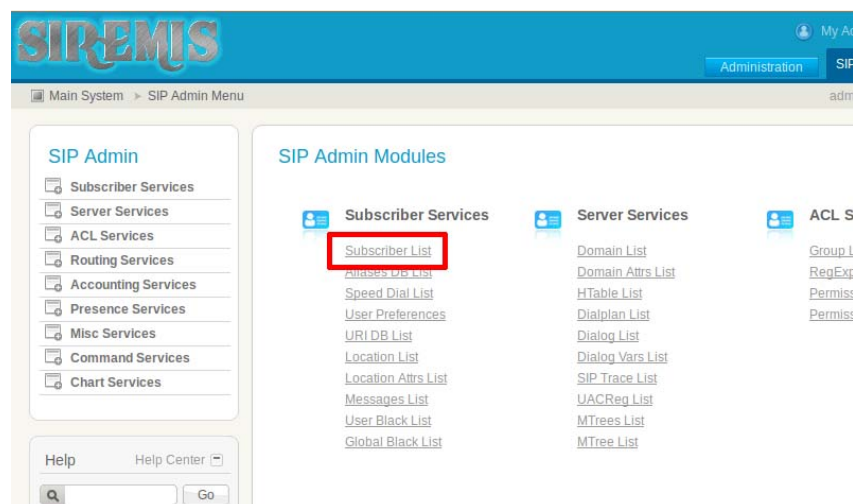
The default username and password are both **admin**.

3. Click SIP Admin Menu.




**Figure 68. SIP Server - SIP Admin Menu**

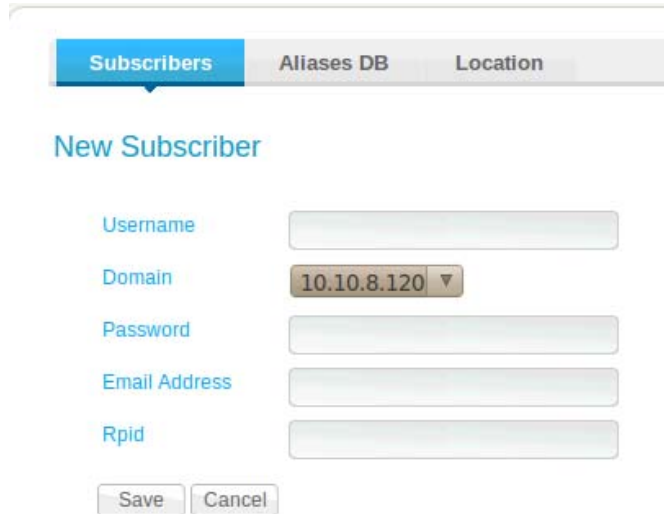
4. Click **Subscriber List**.



**Figure 69. SIP Server - SIP Admin Modules page**

5. Click **Add**. 
6. For each SIP-enabled device (for instance TX3 InSuite and lobby intercom), create a SIP username and SIP password. See the Device List on page 99.

7. Enter **mircom123** as the SIP password for the TX3 Insuites and TX3 Touch.



**Figure 70. SIP Server - New Subscriber page**

8. Save your changes.
9. Repeat steps 5 to 8 for each SIP-enabled device on the network.

## 5.4 Configure the User Preferences (Optional)

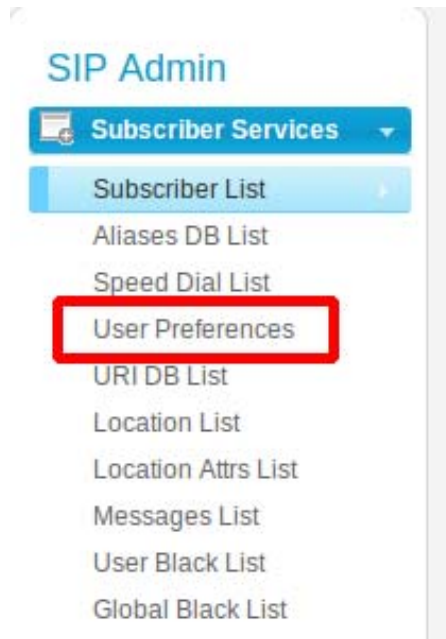
This section describes how to create names for each SIP account. When you create a name for a SIP account, the name and SIP ID appears in the contact list of every TX3 InSuite. For this reason, follow the instructions in this section only if you want the contact list to appear on the TX3 InSuites.

---

**Note:** The contact list is public; it appears on every TX3 InSuite.

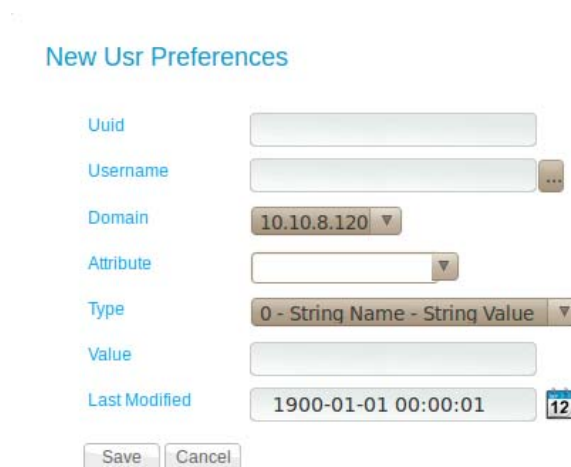
---

1. Click **User Preferences** on the left sidebar of the Siremis site.




**Figure 71. SIP Server - User Preferences link**

2. Click **Add**. 



The image shows a form titled 'New User Preferences'. The fields are: Uuid (text input), Username (text input with a dropdown arrow), Domain (dropdown menu showing '10.10.8.120'), Attribute (text input with a dropdown arrow), Type (dropdown menu showing '0 - String Name - String Value'), Value (text input), and Last Modified (calendar icon showing '1900-01-01 00:00:01'). At the bottom are 'Save' and 'Cancel' buttons.

**Figure 72. SIP Server - New User**

3. Click the button beside **Username**,  select one of the users that you created, and then click **Select**.
4. In the Attribute field, type **first\_name**.
5. In the Value field, type the first name of the resident.

6. Click **Save**.
7. Repeat steps 3 to 6, but type **last\_name** in the Attribute field, and the resident's last name in the Value field.
8. Repeat steps 3 to 6, but type **display\_name** in the Attribute field, and the resident's full name in the Value field. This **display\_name** will appear on the TX3 InSuites' contact list.
9. Restart all the TX3 InSuites. See section 7.5.4 on page 91.

## 5.5 Configure Kamailio to Call Multiple TX3 InSuites (Optional)

This section describes how to create a SIP username that represents a group of TX3 InSuites. When a lobby intercom calls this SIP username, all the TX3 InSuites in the group will ring. The maximum number of TX3 InSuites in one group is 12.

1. Make a list of the SIP usernames of the TX3 InSuites that you want to be in the group.
2. Follow the instructions in section 5.3 on page 73 to create a SIP username. This SIP username represents a group of TX3 InSuites.
3. On the virtual machine, open Terminal and type:  
**cd /etc/kamailio**  
and then press Enter.
4. Type:  
**sudo vi kamailio.cfg**  
and then press Enter.
5. Type **mircom** for the password, and then press Enter.  
Terminal displays the Kamailio configuration file.
6. Type:  
**/request\_route**  
and then press Enter.  
The cursor should be on the line that begins **request\_route**.

7. Press **i** to enter insert mode.

```

#ifdef WITH_DEBUG
---- debugger params ----
modparam("debugger", "cfgtrace", 1)
#endif

Routing Logic

Main SIP request routing logic
- processing of any incoming SIP request starts with this route
- note: this is the same as route { ... }
request_route {

 # per request initial checks
 route(REQINIT);

 # NAT detection
 route(NATDETECT);

```

**Figure 73. request\_route**

8. Type or copy and paste the following code above the line **request\_route {**.

Instead of **1100**, use the SIP username that you created in step 2.

Instead of **1101@128.15.1.4**, **1102@128.15.1.4**, and so on, use the SIP usernames of the InSuites in the group. For the IP address, use the IP address of the virtual machine.

---

**Note:** The maximum number of TX3 InSuites in one group is 12.

---

```

route {

 if($rU == 1100) { *Note: The value 1100 can be
 changed to any number. This number is used by the
 Intercom Entry System to call all InSuite Units

 seturi("sip:1101@128.15.1.4"); *Note: sip:SIP
 username of the first InSuite@IP address of the
 virtual machine

 append_branch("sip:1102@128.15.1.4"); *Note: SIP
 username of the second InSuite@IP address of the
 virtual machine

 append_branch("sip:1103@128.15.1.4");

 append_branch("sip:1104@128.15.1.4");

 append_branch("sip:1105@128.15.1.4");

 append_branch("sip:1106@128.15.1.4");
 }
}

```

```
t_relay();
```

```
break;
```

```
}
```

```
}
```

9. Press the Esc key, then type **:wq** and press Enter to exit the editing program.

10. Type:

```
sudo service kamailio restart
```

and then press Enter.

11. Restart all the TX3 InSuites. See section 7.5.4 on page 91.

When you call the SIP username that you created in step 2, Kamailio will call all the TX3 InSuites in the group.

# 6 TX3 Touch Configuration

This chapter describes how to:

- Discover the MAC address of the TX3 Touch
- Configure the TX3 Touch SIP Settings
- Set up Residents on the TX3 Touch
- Back up the Configuration on the TX3 Touch

---

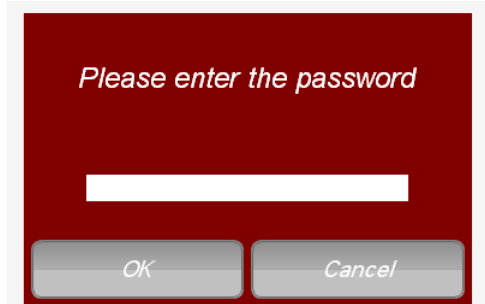
**Note:** See LT-995 “TX3 Touch Screen Configuration and Administration Manual” on the Mircom Website for details on TX3 Touch Configuration.

---

## 6.1 Discover the MAC address of the TX3 Touch

1. From the main TX3 Touch display, enter **9999**.

The administrator access code window appears.

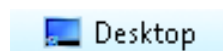


**Figure 74. TX3 Touch - Admin Access**

2. Enter the password to log in to the system and press **OK** (by default there is no password).

The main configuration window appears.

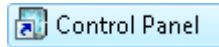
3. Select **File - Exit to Windows** from the Menu Bar.
4. Click **Yes**.
5. Double-click the **Desktop** icon in the upper left corner of the window.



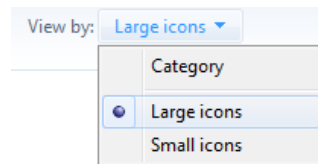


**Figure 75. Desktop icon**

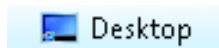
6. Double-click the **Control Panel** icon.

**Figure 76. Control Panel**

7. In the Control Panel window, click **Category** and select **Large Icons**.

**Figure 77. Large Icons**

8. Double-click **Network and Sharing Centre**.
9. Click **Local Area Connection**.
10. In the Local Area Connection Status window, click **Details**.  
The number beside Physical Address is the MAC address.
11. Record the TX3 Touch's MAC address in the Device List on page 99.
12. Double-click the **Desktop** icon in the upper left corner of the window.

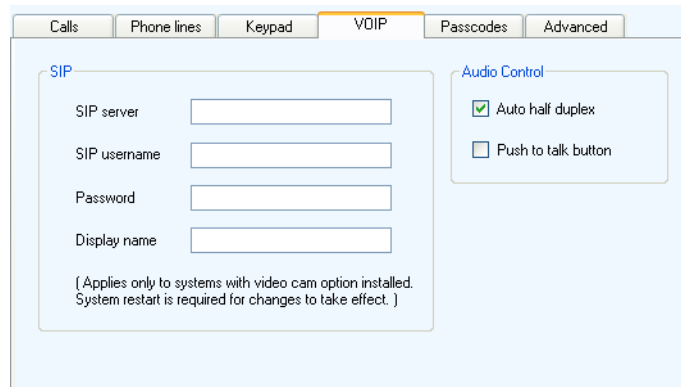
**Figure 78. Desktop icon**

13. Double-click the **Restart** icon.

## 6.2 Configure the TX3 Touch SIP Settings

1. On the client computer or the computer that manages the TX3 Touch, open the TX3 Configurator.
2. Click **Connect** to connect to the TX3 Touch.
3. Select the TX3 Touch in the job tree.
4. Click **VOIP** in the Panel Configuration window.

The VOIP window appears.

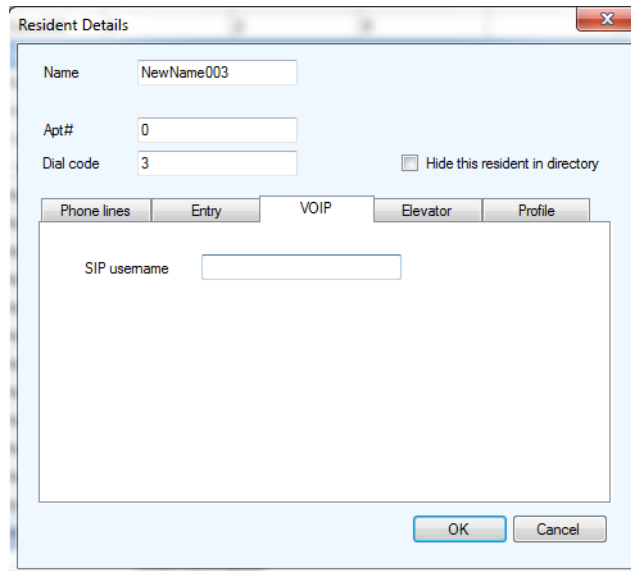


**Figure 79. TX3 Touch - VOIP Setup**

- **SIP server.** The IP address of the virtual machine (see the Device List on page 99)
  - **SIP username.** The SIP username of the TX3 Touch (see the Device List on page 99)
  - **Password.** The SIP password for the TX3 Touch (see the Device List on page 99)
  - **Display name.** This name must match the **Name** of the TX3 Touch camera in exacqVision (if there is one). It appears on the TX3 InSuite when the TX3 Touch calls a resident
  - **Auto half duplex.** Use this selection to turn on automatic half duplex. When one speaker is talking, the other speaker's voice will not be transmitted
  - **Push to talk button.** Use this selection to enable a **Push to Talk** button on the TX3 Touch during SIP calls. The visitor must push and hold the **Push to Talk** button in order to talk to the resident
  - Both **Auto half duplex** and **Push to talk button** help to reduce echo. You can enable either one or the other, but not both. If echo persists when **Auto half duplex** is enabled, then enable **Push to talk button** instead.
5. Click **Send** from the Tool Bar.
  6. Restart the TX3 Touch.

## 6.3 Set up Residents on the TX3 Touch

1. Follow the instructions in LT-995 “TX3 Touch Screen Configuration and Administration Manual” for adding residents.
2. For each resident, click the **VOIP** tab, and type the SIP username for the resident’s TX3 InSuite in the **SIP username** field. See the Device List on page 99.



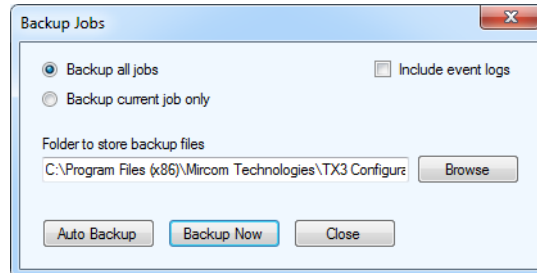
The image shows a 'Resident Details' dialog box with a light blue background. At the top, there's a title bar with 'Resident Details' and a close button. Below the title bar, there are three input fields: 'Name' with the value 'NewName003', 'Apt#' with the value '0', and 'Dial code' with the value '3'. To the right of the 'Dial code' field is a checkbox labeled 'Hide this resident in directory'. Below these fields are five tabs: 'Phone lines', 'Entry', 'VOIP' (which is selected), 'Elevator', and 'Profile'. Under the 'VOIP' tab, there is a large text area labeled 'SIP username' with an empty input field. At the bottom right of the dialog box are two buttons: 'OK' and 'Cancel'.

**Figure 80. TX3 Touch - Resident VOIP Setup**

3. Click **OK**.
4. Repeat steps 2 to 3 for each resident.
5. Click **Send** from the Tool Bar.
6. Restart the TX3 Touch.

## 6.4 Back up the Configuration on the TX3 Touch

1. Select **File > Backup** from the Menu Bar.



**Figure 81. Figure 78. TX3 Touch - Backup Jobs**

2. Enter the following parameters about the Job:

**Backup all jobs.** Select this option to backup all Jobs in the database to the backup folder. Backup files have the extension **.t3**.

**Backup current Job only.** Select this option to backup the current Job only to the backup folder.

**Include event logs.** Select this option if the event logs are to be backed up as well.

**Folder to store backup files.** Select a folder to store the backup files.

3. Click **Backup Now**.

# 7 TX3 InSuite Installation

This chapter explains how to install and configure the TX3 InSuite. This includes:

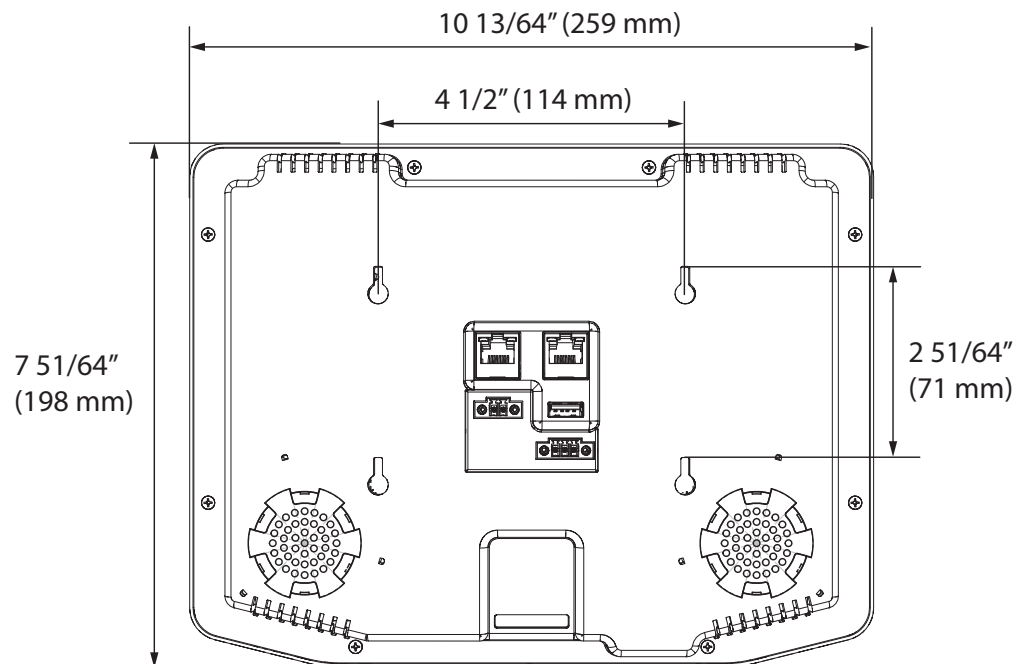
- The TX3 InSuite
- Install the Ferrite Bead
- Mount the TX3 InSuite
- Unmount the TX3 InSuite
- Configure the TX3 InSuite

## 7.1 The TX3 InSuite

### 7.1.1 Included parts

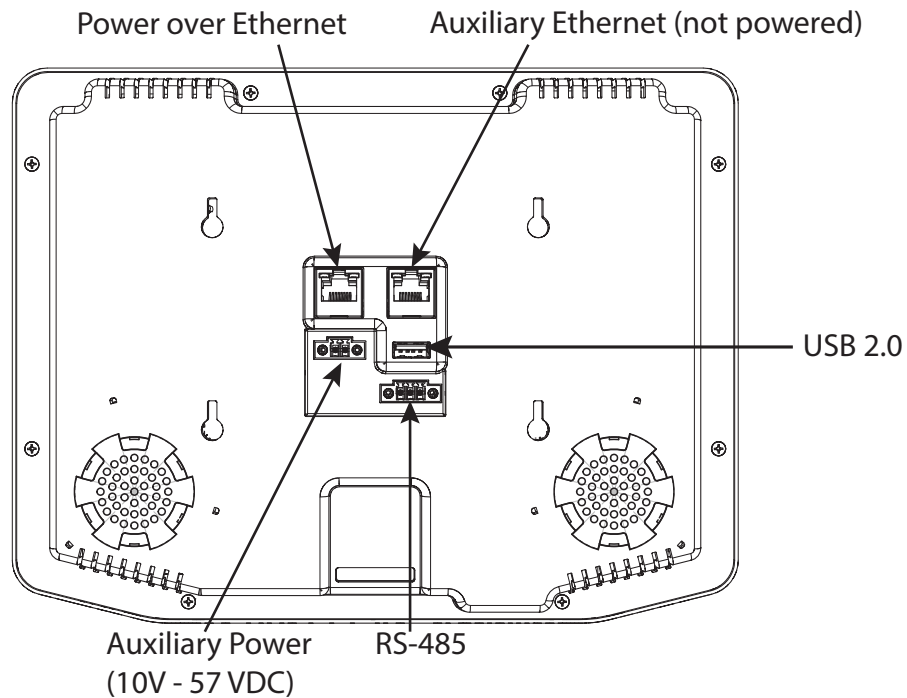
- TX3 InSuite
- TX3 InSuite mounting bracket (sold separately)

### 7.1.2 Dimensions



**Figure 82. Dimensions of the TX3 InSuite**

### 7.1.3 Connections



**Figure 83. Connections on the back of the TX3 InSuite**

## 7.2 Install the Ferrite Bead

If you are powering the TX3 InSuite with PoE, attach the ferrite bead to the Ethernet cable as shown in Figure 84.



**Figure 84. TX3 InSuite with ferrite bead**

## 7.3 Mount the TX3 InSuite

Install the TX3 InSuite:

- At least 1 foot away from mirrors and large metallic surfaces (for example, cable ladders).
- At least 13 feet away from Wi-Fi routers, radio transmitters, and other sources of electromagnetic interference (for example, microwave ovens, electric motors, and other high power electrical equipment).
- At least 54" (137.16 cm) high from the finished ground.

Attach the TX3 InSuite mounting bracket to:

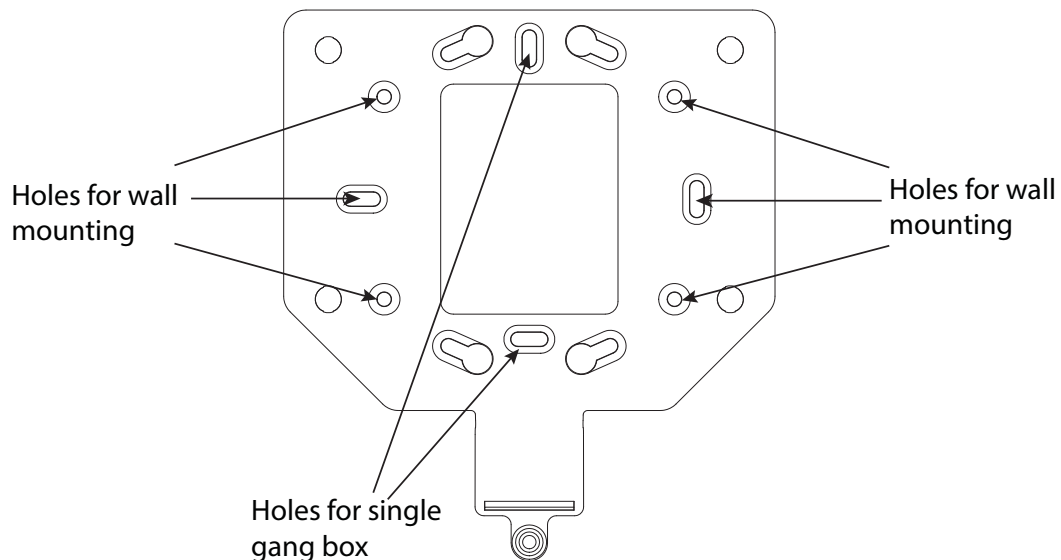
- a single gang box
- a dual gang box
- or the wall directly.

In all cases, connect the TX3 InSuite to:

- a Power over Ethernet cable connected to the building network
- or a non-powered Ethernet cable connected to the building network, and a power cable.

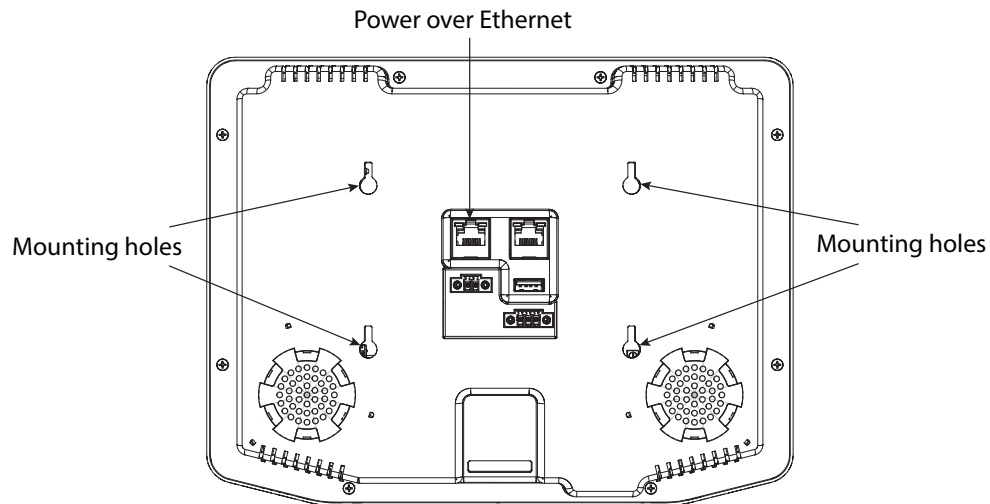
### To mount the TX3 InSuite

1. Screw the mounting bracket over a single gang electrical box.  
Or screw the mounting bracket directly to the wall with the holes shown in Figure 85.



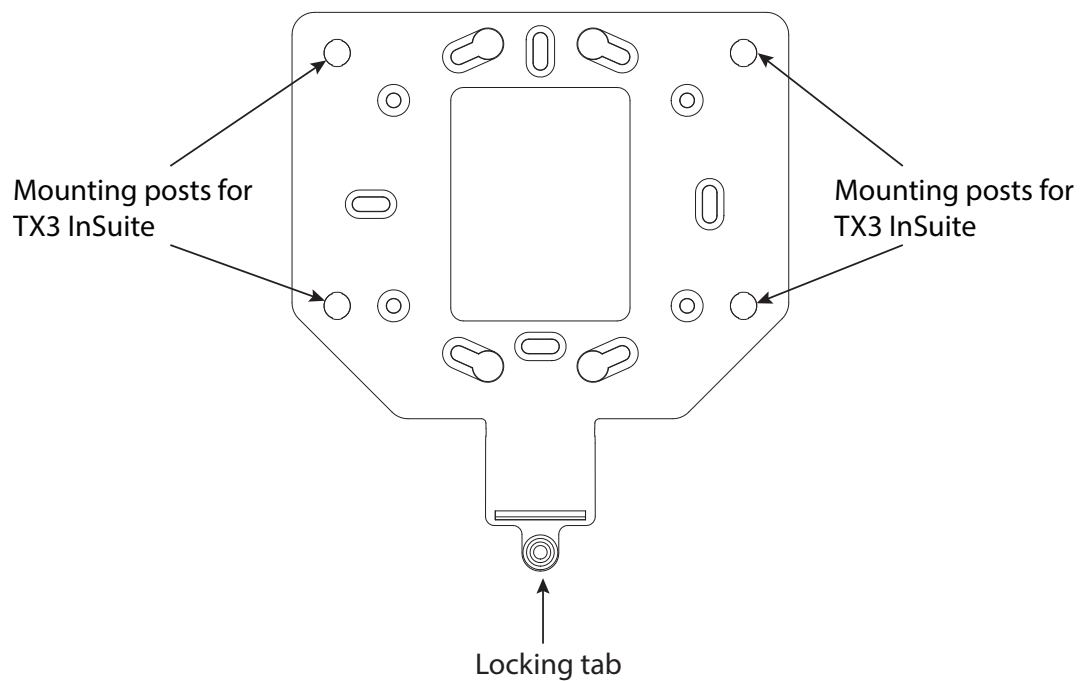
**Figure 85. The mounting bracket directly on the wall**

2. Connect the Ethernet cable from the gang box to the Power over Ethernet port on the TX3 InSuite. The port is shown in Figure 86 (the leftmost Ethernet port if you are looking at the back of the station).



**Figure 86. Back of the TX3 InSuite**

3. Align the 4 holes on the back of the TX3 InSuite with the 4 mounting posts on the mounting bracket. See Figure 87.



**Figure 87. Mounting bracket showing posts**



4. Push the station onto the 4 mounting posts, and then slide the station down until it clicks into place.

## 7.4 Unmount the TX3 InSuite

### To unmount the TX3 InSuite

1. Push the locking tab (shown in Figure 87) towards the wall, and lift the TX3 InSuite up.
2. Pull the TX3 InSuite off the mounting posts.

## 7.5 Configure the TX3 InSuite

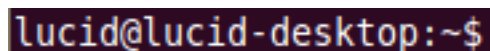
### 7.5.1 Log into the TX3 InSuite

1. In the virtual machine, double-click the **Terminal** icon on the desktop.
2. Type **ssh lucid@** followed by the IP address of the first TX3 InSuite. For example, if the TX3 InSuite's IP address is 198.162.0.1, then type:

**ssh lucid@198.162.0.1**

3. Press Enter.
4. Type **lucid** for the password, and then press Enter.

When the terminal prompt shows **lucid@lucid-desktop**, then you are logged into the TX3 InSuite.



**Figure 88. Logged into the TX3 InSuite**

### 7.5.2 Configure the Server Settings

1. Type the following command, then press Enter.

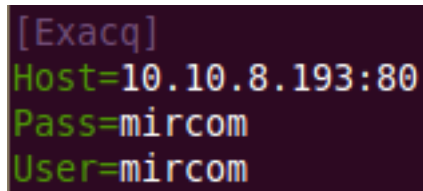
**cd arm32/**

2. Type the following command, then press Enter.

**vi smart\_home\_insuite.ini**

Terminal displays the configuration information for the TX3 InSuite.

3. Use the arrow keys to move the cursor down to the **[Exacq]** line, and then press the **i** key to enter editing mode.



```
[Exacq]
Host=10.10.8.193:80
Pass=mircom
User=mircom
```

**Figure 89. TX3 InSuite - exacqVision Settings**

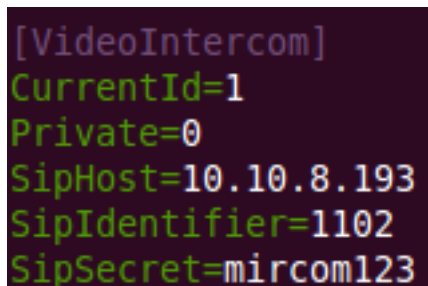
4. On the **Host** line, type the IP address of the ONVIF camera server, followed by a colon and **80**. For example, if the IP address of the ONVIF camera server is 192.168.1.1, then type:

**192.168.1.1:80**

The ONVIF camera server's IP address is the same as the building server's IP address. See the Device List on page 99.

The username and password are **mircom** by default so you do not need to change them. (You defined this username and password in the ONVIF camera client in chapter 4.)

5. Use the arrow keys to move the cursor down to the **[VideoIntercom]** line.



```
[VideoIntercom]
CurrentId=1
Private=0
SipHost=10.10.8.193
SipIdentifier=1102
SipSecret=mircom123
```

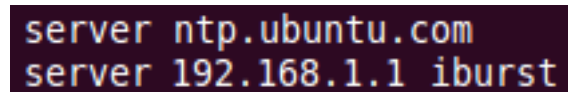
**Figure 90. TX3 InSuite - SIP Settings**

6. On the **SipHost** line, type the IP address of the virtual machine. See the Device List on page 99.
7. On the **SipIdentifier** line, type the SIP username of the TX3 InSuite. See the Device List on page 99.
8. On the **SipSecret** line, type **mircom123**. This is the SIP password for all TX3 InSuites.
9. Press the Esc key, then type **:wq** and press Enter to exit the editing program.

### 7.5.3 Configure the Time Server

1. Type  
  
**sudo vi /etc/ntp.conf**  
  
and then press Enter.
2. Type **lucid** for the password, and then press Enter.  
  
Terminal displays the time server information for the TX3 InSuite.
3. Use the arrow keys to move the cursor down to the **iburst** line, and then press the **i** key to enter editing mode.
4. Change the IP address to the IP address of the virtual machine (see the Device List on page 99). For example, if the virtual machine's IP address is 192.168.1.1, then change the line so that it reads:

**server 192.168.1.1 iburst**



```
server ntp.ubuntu.com
server 192.168.1.1 iburst
```

**Figure 91. TX3 InSuite - Time server settings**

5. Press the Esc key, then type **:wq** and press Enter to exit the editing program.

### 7.5.4 Restart the TX3 InSuite

1. Type the following command to restart the TX3 InSuite:  
  
**sudo init 6**
2. Repeat all the steps in section 7.5 for each TX3 InSuite.

# 8 Troubleshooting

## 8.1 Virtual Machine Troubleshooting

### 8.1.1 Error with the Virtual Machine

Could not start the machine TX3Server\_1 because the following physical network interfaces were not found: Intel(R) Centrino(R) Wireless-N 2230 (adapter 1)

1. Shut down the virtual machine.
2. In the **Oracle VM VirtualBox Manager** window, right-click the virtual server, and then click **Settings**.
3. Click **Network** on the left.
4. Make sure that **Bridged Adapter** is selected in the menu next to **Attached to**.
5. Select the network adapter that the building server is using in the menu next to **Name**.
6. Click **OK**.
7. Start the virtual machine.

### 8.1.2 If the MAC Address of the Virtual Machine Changes

It is possible to change the MAC address of the virtual machine in the Virtual Box settings. If the MAC address changes, follow the instructions in section 3.3 on page 49 to set the correct **eth** number in network interfaces.

### 8.1.3 Get Information on the SIP Server

#### To see if the SIP server is running

1. In the virtual machine, double-click the **Terminal** icon on the desktop.
2. Type the following command, then press Enter.  
**sudo service kamailio status**
3. Type **mircom** for the password, and then press Enter.

A message appears saying whether Kamailio is running or not running.

### To see the SIP usernames that are registered with the SIP server

1. Type the following command, then press Enter.  
**sudo kamctl ul show**
2. Type **mircom** for the password, and then press Enter.  
The list of registered SIP usernames appears.

#### 8.1.4 After the Virtual Machine Restarts

Whenever the virtual machine restarts, you must disable call control and delete the logs. Follow the instructions in section 3.6 on page 53 and section 3.7 on page 53.

## 8.2 ExacqVision Troubleshooting

### 8.2.1 Problems with the ExacqVision Server

If there is a problem with the ExacqVision server, try these tips.

#### Try to access the exacqVision Web server

1. Open a Web browser and access the IP address of the building server.  
The Web page for the ExacqVision Web server should appear.

#### Restart all ExacqVision services

1. Ensure that all TX3 InSuites are showing the Home screens.
2. On the building server, open the Control Panel.
3. Click **Administrative Tools**, then double-click **Services**.
4. Select **exacqVision Server** and then click **Stop**.
5. Select **exacqVision Web Service** and then click **Stop**.
6. Select **evApache** and then click **Stop**.
7. Wait for 10 seconds.
8. Select **exacqVision Server** and then click **Start**.
9. Select **exacqVision Web Service** and then click **Start**.
10. Select **evApache** and then click **Start**.

### Restart the Web service

1. Open a Web browser and access:  
**127.0.0.1/service.web**
2. Log in with the username and password of the exacqVision server.
3. Click **Restart Web Service**.
4. Click **Yes**.

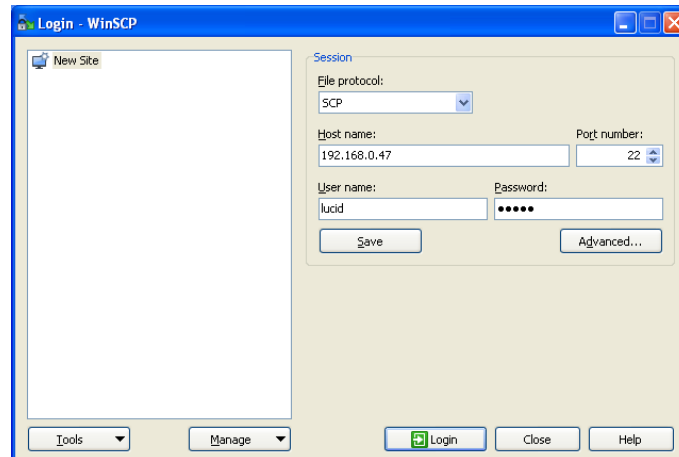
## 8.3 TX3 InSuite Troubleshooting

### 8.3.1 Get the Log Files from a TX3 InSuite

There are 3 kinds of log files:

- **tracelog** (Opal log)
  - **appxLogFile** (application log)
  - **syslog** (system log)
1. On the building server, start WINSCP and enter the following information:
    - File Protocol: **SCP**
    - Host name: IP address of the TX3 InSuite
    - Username: **lucid**
    - Password: **lucid**

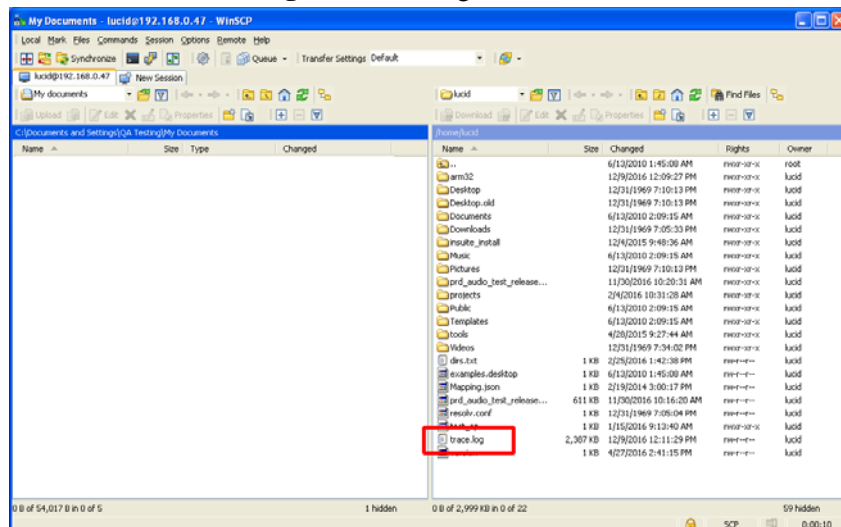
2. Click **Login**.



**Figure 92. WINSCP**

In WINSCP, the left pane shows the contents of the building server, and the right pane shows the contents of the TX3 InSuite.

3. Transfer the file **tracelog** to the building server.



**Figure 93. WINSCP - connected to TX3 InSuite**

4. Double-click the **arm32** directory.

5. Transfer all files beginning with **appxLogFile** from the **arm32** directory to the building server.

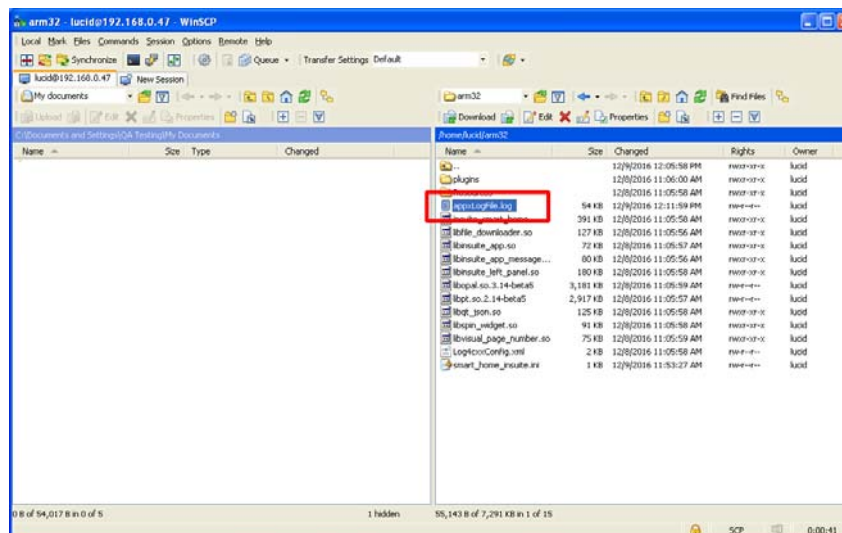


Figure 94. WINSCP - arm32 directory

6. In the right pane, click the navigation menu and select **/<root>**, then select **/var/log**.

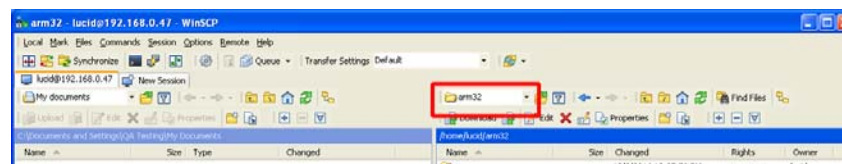


Figure 95. WINSCP - Navigation menu

7. Transfer all files beginning with **syslog** from the **/var/log** directory to the building server.

### 8.3.2 Check if a Service is Running on a TX3 InSuite

1. Log into the TX3 InSuite as described in section 7.5.1 on page 89.
2. Type the following command, then press Enter.

```
sudo netstat -tunlp
```

A list of running services appears.

### 8.3.3 Check the Firmware Version on a TX3 InSuite

1. Log into the TX3 InSuite as described in section 7.5.1 on page 89.



2. Type the following command, then press Enter.

**cat version**

A change log of the TX3 InSuite firmware versions appears.

3. Scroll up to the top of the list to see the latest version.

# 9 TX3 InSuite Specifications

|                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>Dimensions</b>                                                                                                                    |
| 259 mm x 198 mm x 41 mm (10 13/64" x 7 51/64" x 1 5/8")                                                                              |
| <b>Weight</b>                                                                                                                        |
| 0.86 kg (1.90 lb)                                                                                                                    |
| <b>Power over Ethernet</b>                                                                                                           |
| IEEE 802.3af/at                                                                                                                      |
| <b>Auxiliary power input</b>                                                                                                         |
| 12V - 48V DC / 15 W                                                                                                                  |
| <b>Display</b>                                                                                                                       |
| 10.1" Touchscreen display with projective capacitive touch, 1024 x 600 (WSVGA) LCD                                                   |
| <b>Camera</b>                                                                                                                        |
| 5 MP camera with autofocus                                                                                                           |
| <b>Audio</b>                                                                                                                         |
| Two stereo digital microphones<br>2.5W D-Class Stereo Amplifier                                                                      |
| <b>Audio Codecs</b>                                                                                                                  |
| G.711-uLaw-64k, G.711-aLaw-64k                                                                                                       |
| <b>Operating Temperature</b>                                                                                                         |
| 0° C - 50° C (32° F - 122° F)                                                                                                        |
| <b>Connections</b>                                                                                                                   |
| 2 Ethernet 10/100 ports (one with PoE+ function)<br>1 USB 2.0 port<br>1 Auxiliary power input<br>1 RS-485 port<br>1 SD/MMC card slot |





# Warranty & Warning Information

## Limited Warranty

Mircom Technologies Ltd. together with its subsidiaries and affiliates (collectively, the “Mircom Group of Companies”) warrants the original purchaser that for a period of two years from the date of manufacture, the product shall be free of defects in materials and workmanship under normal use. During the warranty period, Mircom shall, at its option, repair or replace any defective product upon return of the product to its factory, at no charge for labour and materials. Any replacement and/or repaired parts are warranted for the remainder of the original warranty or ninety (90) days, whichever is longer. The original owner must promptly notify Mircom in writing that there is defect in material or workmanship, such written notice to be received in all events prior to expiration of the warranty period.

## International Warranty

The warranty for international customers is the same as for any customer within Canada and the United States, with the exception that Mircom shall not be responsible for any customs fees, taxes, or VAT that may be due.

## Conditions to Void Warranty

This warranty applies only to defects in parts and workmanship relating to normal use. It does not cover:

- damage incurred in shipping or handling;
- damage caused by disaster such as fire, flood, wind, earthquake or lightning;
- damage due to causes beyond the control of Mircom such as excessive voltage, mechanical shock or water damage;
- damage caused by unauthorized attachment, alterations, modifications or foreign objects;
- damage caused by peripherals (unless such peripherals were supplied by Mircom);
- defects caused by failure to provide a suitable installation environment for the products;
- damage caused by use of the products for purposes other than those for which it was designed;
- damage from improper maintenance;

- damage arising out of any other abuse, mishandling or improper application of the products.

## Warranty Procedure

To obtain service under this warranty, please return the item(s) in question to the point of purchase. All authorized distributors and dealers have a warranty program. Anyone returning goods to Mircom must first obtain an authorization number. Mircom will not accept any shipment whatsoever for which prior authorization has not been obtained.

**Caution:** Unless specific pre-authorization in writing is obtained from Mircom management, no credits will be issued for custom fabricated products or parts or for complete fire alarm system. Mircom will at its sole option, repair or replace parts under warranty. Advance replacements for such items must be purchased.

---

**Note:** Mircom's liability for failure to repair the product under this warranty after a reasonable number of attempts will be limited to a replacement of the product, as the exclusive remedy for breach of warranty.

---

## Disclaimer of Warranties

This warranty contains the entire warranty and shall be in lieu of any and all other warranties, whether expressed or implied (including all implied warranties of merchantability or fitness for a particular purpose) and of all other obligations or liabilities on the part of Mircom neither assumes nor authorizes any other person purporting to act on its behalf to modify or to change this warranty, nor to assume for it any other warranty or liability concerning this product.

This disclaimer of warranties and limited warranty are governed by the laws of the province of Ontario, Canada.

## Out of Warranty Repairs

Mircom will at its option repair or replace out-of-warranty products which are returned to its factory according to the following conditions. Anyone returning goods to Mircom must first obtain an authorization number. Mircom will not accept any shipment whatsoever for which prior authorization has not been obtained.

Products which Mircom determines to be repairable will be repaired and returned. A set fee which Mircom has predetermined and which may be revised from time to time, will be charged for each unit repaired.

Products which Mircom determines not to be repairable will be replaced by the nearest equivalent product available at that time. The current market price of the replacement product will be charged for each replacement unit.

## WARNING

Mircom recommends that the entire system be completely tested on a regular basis. However, despite frequent testing, and due to, but not limited to, criminal tampering or electrical disruption, it is possible for this product to fail to perform as expected.

## NOTE

Under no circumstances shall Mircom be liable for any special, incidental, or consequential damages based upon breach of warranty, breach of contract, negligence, strict liability, or any other legal theory. Such damages include, but are not limited to, loss of profits, loss of the product or any associated equipment, cost of capital, cost of substitute or replacement equipment, facilities or services, down time, purchaser's time, the claims of third parties, including customers, and injury to property.

**MIRCOM MAKES NO WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO ITS GOODS DELIVERED, NOR IS THERE ANY OTHER WARRANTY, EXPRESSED OR IMPLIED, EXCEPT FOR THE WARRANTY CONTAINED HEREIN.**

## Special Notices

### FCC Regulatory Statements

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference.
- (2) This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the Federal Communication Commission (FCC) rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment causes harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by doing one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

### IC Regulatory Statements

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

CAN ICES-3 (B)/NMB-3(B)