



ALARM LOCK

345 Bayview Avenue, Amityville, New York 11701
For Sales and Repairs 1-800-ALA-LOCK
For Technical Service 1-800-645-9440
or visit us at <http://tech.nasposecurity.com/>

(Note: Technical Service is for security professionals only)
Publicly traded on NASDAQ Symbol: NSSC

AL-IM3-80211 "Wireless / Wired" Gateway Installation Instructions

© ALARM LOCK 2024

WI2528ALF 11/24

OVERVIEW

The **AL-IM3-80211** "Version 3" Gateways (notice the "3" in the "IM3" model name) are the next generation of Networkx™ "Wireless / Wired" Gateways used within the Trilogy Networkx™ wireless system. The **AL-IM3-80211** is the newest and most versatile Trilogy Networkx Gateway yet.

The objective with all Gateways is to allow DL-Windows to "Discover" the Gateway through the customer's network. For this Discovery process to work, both the Gateway and DL-Windows must be connected to the same customer network. The Gateway's network connection can be wired (through an RJ-45 Ethernet network cable) or wireless (through Wi-Fi).

Like all previous Gateway models, the **AL-IM3-80211** supports the aforementioned RJ-45 Ethernet cable installation. However, all Version 3 Gateways are now equipped with a local wireless network whereby the Gateway can be detected by almost any wireless device (such as a smartphone) and can be configured for any wireless network using a web browser -- all without needing a hard-wired connection nor DL-Windows. There is no need to be physically located at the installation site -- use a browser to *pre-configure* the Gateway with your customer's Wi-Fi network settings from virtually any location.

ALL methods previously used with Version 1 and 2 Gateways to make a wired or Wi-Fi connection to the customer's network can also be used with Version 3 Gateways. Version 3 Gateways are backwards-compatible, and CAN be mixed into an existing system that includes older Version 1 or Version 2 Gateways. Version 3 Gateways also include the added ability to expand your system with up to seven (7) **AL-IME2-EXP** Expanders. **Note:** **AL-IME2-EXP** Expanders cannot communicate with older "non-Version 2" Gateways.

IMPORTANT: **DL-Windows Version 5.5.4** or later is required to support Version 3 Gateways and Expanders.

The **AL-IM3-80211** Gateway is also compatible with Alarm Lock and Continental Access products (refer to the documentation supplied with your software for integration details for your specific product).

Blue ID Card

We strongly recommend that when installing any model Gateway, a **blue-colored** "Gateway ID Card" (OI429) be completed. Gateway physical locations may easily be forgotten. These ID cards may prove very useful when replacing Gateways, when selecting a particular Gateway to use to Discover locks, or whenever an installed Gateway needs to be physically located.

AL-IM3-80211 SPECIFICATIONS

WIRELESS SPECIFICATIONS

Wireless Standards: IEEE 802.11b; 802.11g

Frequency Range: 2.412 - 2.484 GHz

Output Power: 14dBm + 1.5dBm/-1.0dBm

Maximum Receive Level: -10dBm (with PER < 8%)
Data Rates With Automatic Fallback: 54Mbps - 1Mbps
Modulation Techniques: OFDM, DSSS, CCK, DQPSK, DBPSK, 64 QAM, 16 QAM

NETWORK RANGE

Gateway / Expander to Locks: Clear field range 500'.

Typical indoor range: Networkx 75-175'; ArchiTech Networkx: 50-125'.

Gateway / Expander to Expander: Clear field range 500'. Typical indoor range: 75-175'. **Note:** Actual range varies with building construction.

AL RADIO LINK

900 MHz GFSK

50 Channels

10mW power output

POWER - Provided by UL Listed Class 2 Transformer

Peak Supply Current: 650mA

Input Voltage: 5 - 6VAC

AVERAGE POWER CONSUMPTION

1300mW (WLAN mode; maximum data rate)

300mW (WLAN mode; idle)

750mW (Ethernet Mode)

ENVIRONMENTAL

Operating Temperature: -20° to 60°C (-4° to 140°F)

Storage Temperature: -40° to 85°C (-40° to 185°F)

PHYSICAL

Enclosure Size: 4.5"H x 6.0"W x 1.94"D

Weight: 0.5lbs.

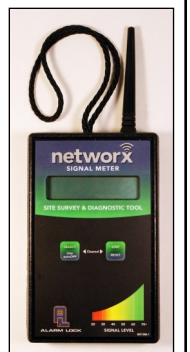
GATEWAY LOCATION GUIDELINES

Before selecting a final mounting location for your Gateway, the following must be taken into consideration:

- Gateways should be located within 175 feet (radially) from

TIP

The **AL-NSM Networkx Signal Meter** tool can help you perform a site survey test of the premises to find the optimum location for Gateways relative to Networkx locks; as well as determine the optimum number of Gateways (or Expanders) needed for signal area coverage. See WI2092 or speak to your Alarm Lock sales representative for more information.



the intended wireless lock locations

- Open areas will increase range while concrete building construction, walls, ceilings and narrow corridors will decrease range
- ArchiTech series locks generally have shorter range to/from a Gateway
- Generally, the Gateway should be within approximately 75 feet (radially) from an **AL-IME2-EXP** Expander (see WI2156)
- If using a wired network connection, select a location that allows for access to an RJ-45 network Ethernet cable connection
- Mount Gateway within acceptable range of wireless router or wireless access point
- Gateways should be mounted in elevated areas; however mounting in a drop ceiling can adversely affect signal strength
- Preferred mounting position = 6 to 12" below standard 8-9 foot ceiling
- Gateways must be mounted vertically; horizontal "flat" mounting should be specifically avoided
- Although wood and wallboard construction can have little effect upon signal strength, concrete or brick can reduce signal strength by up to 35%. Steel-reinforced concrete or metal lath and plaster can reduce signal strength as much as 90%!
- Do NOT mount close to electrical wiring or other metal obstructions such as pipes or conduits
- Installing in computer closets or server rooms can negatively impact signal strength

Helpful Tips

- In difficult installations wherein signal problems exist, the use of (multiple) **AL-IME2-EXP** Expanders throughout the premises is recommended. **AL-IME2-EXP** Expanders extend the coverage area of Version 2 Gateways, allowing control of up to its rated maximum of 63 locks. Up to 7 Expanders can be added to one Version 2 or Version 3 Gateway. For more information, see WI2156.
- We recommend obtaining or creating a layout of your intended system identifying all proposed installation locations, also noting building construction materials to assist in determining optimal Gateway installation locations

IMPORTANT: If you plan to use **AL-IME2-EXP** Expanders with your Gateway, be sure to read the "**EXPANDER GROUP**" **DIALS** section on page 8 before powering your Gateway.

The above guidelines and tips should be followed for each additional Gateway added to the system.

MOUNTING INSTRUCTIONS

The **AL-IM3-80211** rear housing must be mounted "up" as shown on the page 11 template; i.e. when the front housing is attached, its engraved Networkx logo must be located at the lower right with the front housing positioned "up" in a conventional manner (the unit contains internal antennas that must be positioned vertically). *Horizontal "flat" mounting of the enclosure is to be specifically avoided.*

Mount as follows:

1. Insert a small flat-head screwdriver into the slots at the bottom and twist while applying inward pressure (see Fig. 1; insert the screwdriver closer to the edges of the unit, as shown in the Fig. 1 "inset" image).

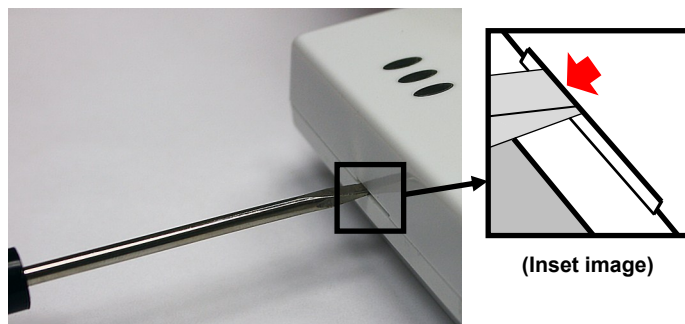


Fig. 1: To separate rear housing from cover
(Inset: Insert flat-head screwdriver closer to the edges of the unit)

2. Using the rear housing as a mounting template, secure the unit to a wall or other flat surface using the hardware provided (see page 11 for printed template). Shown in Fig. 2, the rear housing includes two mounting holes for single-gang (A) and four mounting holes for double-gang (B) electrical utility boxes, as well as four all-purpose holes (C) for mounting to drywall or other surfaces (use minimum #6 screws suitable for the surface).

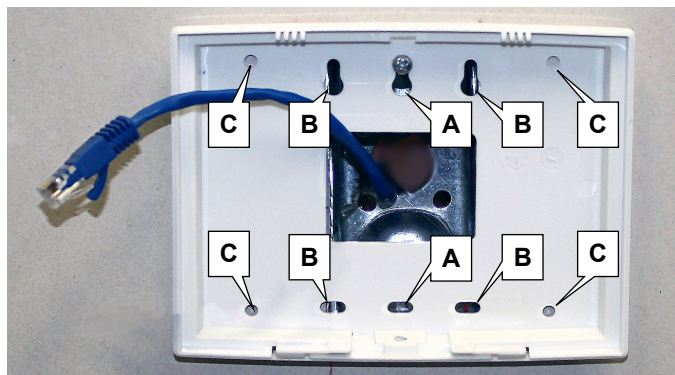


Fig. 2: Rear housing mounting holes for single-gang (A) and double-gang (B) electrical boxes, and four all-purpose holes (C)

BEFORE CONNECTING TO A NETWORK SOME PRELIMINARY INFORMATION

The **AL-IM3-80211** Gateway can be used wired or wirelessly. However, "out of the box", the Gateway is configured for a wired connection only.

IMPORTANT: Gateways can ONLY be Discovered by DL-Windows when the PC running DL-Windows is on the same subnet as the Gateway. Refer to **Subnet** section for more information.



The following sub-sections refer to the DL-Windows software, therefore the following terminology may be better understood by referencing OI383 (included with your Gateway).

Static IP Addresses - Recommendations

Using a static IP address for each Gateway can be helpful:

- DL-Windows software performs faster; no wasted time re-locating Gateways that have had their IP addresses changed by DHCP
- Allows for operation across subnets in large corporate networks (such as those that exist between buildings)
- Allows for Emergency Commands (such as "Emergency Lockdown") to perform properly

Contact the Network Administrator

For large corporate networks with multiple subnets, we recommend contacting the corporate network administrator and request the following:

- IP Address - An address for each Alarm Lock Gateway device
- Subnet Mask - Filtering data ("mask bits") if required by the aforementioned IP address
- Default Gateway - The address of the physical device, such as a router, for the current subnet to which DL-Windows will be connected
- Wireless Network Configuration - The wireless network security settings, authentication, encryption, etc.

Subnets - General Information

To improve security and processing performance, corporate networks are often divided into interconnected but separate "subnet" segments. The network administrator may decide to use routing tables or may specify blocks of addresses through which the two subnets can freely communicate in both directions. However, if the two subnets cannot freely communicate as in Fig. 3, follow the steps below to ensure communication between the subnets:

- Connect the Gateway to the local network (on same subnet as DL-Windows); Gateway receives valid IP address
- Using DL-Windows, Discover and add the Gateway to an Account
- Configure Gateway with the static IP address information of the subnet with which you plan to communicate
- Disconnect from the local network - remove power from the Gateway (Gateway will retain static IP information)
- Re-connect / re-apply power in the desired location / subnet

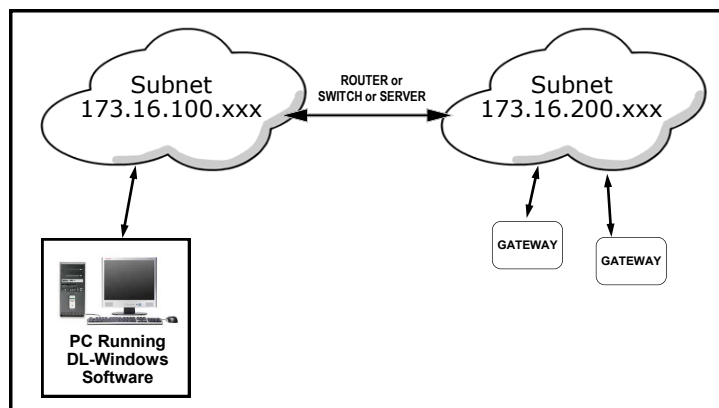


Fig. 3: Gateways on different subnets within a network

FIRST POWER UP: GATEWAY RESET

IMPORTANT: Before selecting one of the 3 network connection methods (see page 3), ALWAYS reset the Gateway, even if it is new "out of the box" and/or has never been used previously. This reset procedure clears the Gateway memory, user data and configuration data (such as static IP information). You can also reset the Gateway any time after the Gateway is powered.

Read and understand the following steps before performing them:

1. Remove the Gateway front housing cover. Take note of the **RESET** button (see Fig. 4 on page 8).
 2. Wait until the green LED starts blinking, then press and hold **RESET** button until the **Red** LED turns on solid; keep holding until the **Yellow** LED also turns on solid, then release the **RESET** button.
 3. Both the **Yellow** and **Red** LEDs will remain on solid for 2 minutes.
 4. The Red LED will turn off, the **Yellow** LED will remain on solid and the **Green** LED will start to flash rapidly.
- You are now ready to configure your Gateway. Select one of the three network connection methods in the next section:

SELECT A GATEWAY NETWORK CONNECTION METHOD

Select one of the 3 ways to connect your **AL-IM3-80211** Gateway to your customer's network, listed below. The first two are methods previously used with Version 1 and Version 2 Gateways that can ALSO be used with Version 3 Gateways. See the DL-WINDOWS NETWORKX User's Guide (OI383) for details about programming with DL-Windows software.

The 3 basic methods are:

1. **Wired Ethernet Using DL-Windows** (skip to page 4)
2. **Wi-Fi Using DL-Windows for Wi-Fi Configuration** (skip to page 5)
3. **Wi-Fi Using the Local Web Server for Wi-Fi Configuration (New to Version 3 Gateways)** (skip to page 6)

Method 1: Wired Ethernet Using DL-Windows

- The simplest and most common method usually performed at the installation site
- Use a permanently-wired Ethernet network connection
- Can also be used with Version 1 and Version 2 Gateways
 - 1a. If not already done, perform a factory reset of the Gateway (see "**FIRST POWER UP: GATEWAY RESET**" on page 3).
 - 1b. If not already done, connect one end of an RJ-45 Ethernet network cable to the back of the Gateway.
 - 1c. If not already done, connect the other end of the RJ-45 cable to the physical network infrastructure.
 - 1d. The Gateway will search for a valid IP address from the network via DHCP.
Be patient; searching for an IP address *could* take up to 1 minute.
 - 1e. With a PC running DL-Windows connected to the same network described in previous step 1c, use DL-Windows to Discover and add the Gateway to an Account.

The RJ-45 network cable remains permanently connected to the Gateway.

If you are assigning a static IP address to your Gateway, then proceed as follows:

- In the **Gateway Configuration** screen, click to highlight your new Gateway in the list, then click **Gateways > Configure / Edit Network Settings**.
- In the **Network Configuration** screen, click the **Network Mode** drop-down and select **Wired Ethernet**.
- Add a check to the **Use Static IP Address** checkbox.
- Configure the other network settings, including: **IP Address**, **Subnet Mask** and the **Default Gateway**. **Note:** The **Gateway MAC Address** will automatically populate, therefore there is no need to change it.

IMPORTANT: For security, we recommend changing the default **Username** and **Password** that is used to access the Gateway web page to prevent unauthorized access to the Gateway (use **Gen 3 Web Page Username and Password** section). **IMPORTANT:** **Username** and **Password** MUST NOT contain any spaces!

- When finished, click **Send**.

The RJ-45 network cable remains permanently connected to the Gateway.

You are now ready to use your new Gateway to Discover locks and to perform other tasks.

The screenshot shows the 'Network Configuration [Method 1]' window. It has two main sections: 'IP Address Setup' and 'Wireless Network Configuration'. In the 'IP Address Setup' section, 'Network Mode' is set to 'Wired Ethernet' and 'DHCP Name' is 'ALGateway'. The 'Use DHCP IP Address' checkbox is unchecked, and 'Use Static IP Address' is checked. The 'IP Address' is '172. 16. 200. 100', 'Subnet Mask' is '255. 255. 254. 0', 'Default Gateway' is '172. 16. 1. 1', and 'Gateway MAC Address' is '0080A38B34FF'. The 'Remote Configuration' section shows 'WAN Address' as '0. 0. 0. 0' and 'Port' as '10001', with a note '(Required only for internet access)'. The 'Wireless Network Configuration' section has 'Network Name (SSID)' and 'Password' fields, a 'Retype Password' field, and a 'Security Type' dropdown set to 'None'. At the bottom, there is a 'Gen 3 Web Page Username and Password' section with 'Username' set to 'admin' and a 'Password' field with masked characters. At the very bottom are 'Save', 'Send', and 'Close' buttons.

Method 2: Wi-Fi Using DL-Windows for Wi-Fi Configuration

- Connect your PC running DL-Windows to an Ethernet network, and connect your Gateway to the same Ethernet network
- Use DL-Windows to configure the Gateway for Wi-Fi communication
- At the end of this procedure, the Gateway will be configured for Wi-Fi, ready to be Discovered
- Create a temporary DL-Windows Account for use with this method
- Contact the Network Administrator and have the broadcast Network Name (SSID) and network Password ready before you proceed

2a. If not already done, perform a factory reset of the Gateway (see page 3 "**FIRST POWER UP: GATEWAY RESET**").

2b. If not already done, connect one end of an RJ-45 Ethernet network cable to the back of the Gateway.

2c. If not already done, connect the other end of the RJ-45 cable to the physical network infrastructure.

2d. With DL-Windows connected to the same network described in previous step **2c**, use DL-Windows to Discover and add the Gateway to the temporary DL-Windows Account, then proceed as follows:

- In the **Gateway Configuration** screen, click to highlight your new Gateway in the list, then click **Gateways > Configure / Edit Network Settings**.
- In the **Network Configuration** screen, click the **Network Mode** drop-down and select **Wireless (Wi-Fi)**.

Option 1: If using a *static* IP address, check **Use Static IP Address** and type the static IP in the **IP Address** field. Add the **Subnet Mask**, **Default Gateway** and all other fields, if required. **Note:** The **Gateway MAC Address** will automatically be populated.

Option 2: To *auto-assign* an IP address, check **Use DHCP IP Address**. In the **Wireless Network Configuration** area, type the broadcast **Network Name (SSID)** and network **Password** (and **Retype Password** to confirm). Select the **Security Type** from the drop-down as recommended by your Network Administrator. *An incorrect selection will require resetting the Gateway!*

- **IMPORTANT:** For security, we recommend changing the default **Username** and **Password** that is used to access the Gateway web page to prevent unauthorized access to the Gateway (use **Gen 3 Web Page Username and Password** section). **IMPORTANT:** **Username** and **Password** MUST NOT contain any spaces!
- Click **Send**. Wait until the Gateway green LED starts flashing, then proceed.
- Click **OK** in the warning popup that appears, then close the **Network Configuration** screen.
- In the **Gateway Configuration** screen, the Gateway we just converted to Wi-Fi will be highlighted in red ("unreachable"). Click this red Gateway in the list, then click **Gateways > Remove Gateway from Account**. Click **OK** in the warning popup that appears.

Be patient, this may take some time; when finished, the Gateway will be configured for Wi-Fi.

- Press and hold **RESET** and release immediately after the red LED turns on.

2e. Disconnect the RJ-45 network cable from the local network and the Gateway will retain the Wi-Fi information. Relocate the Gateway and re-power. **Note:** The Gateway will be using this cable for power only; a network connection is not required.

- Use DL-Windows to Discover the Gateway.
- The Gateway's Wi-Fi MAC address will be displayed (notice that the last digit of the Wi-Fi MAC address is incremented by 1 (in hex) when compared to the Ethernet MAC address).
- Add the Gateway to your Account. The Gateway will then communicate wirelessly through the network. **Note:** Both MAC addresses are listed on the supplied blue "**GATEWAY ID CARD**" (OI429).

Method 3: Wireless Using the Local Gateway Network

Version 3 Gateways include a locally-generated web page ("xPico® 240") that allows you to pre-configure the Gateway to conform to your customer's Wi-Fi network before adding the Gateway to a DL-Windows account. Use any wireless device (a laptop, a tablet, etc.) to connect and configure the Gateway, then the Gateway will be ready to be Discovered and added to your customer's DL-Windows account. Add your customer's Wi-Fi settings from any location -- *you and the Gateway do NOT need to be physically located at the installation site!* **Note:** A laptop will be used in the steps below, but any convenient wireless device can be used.

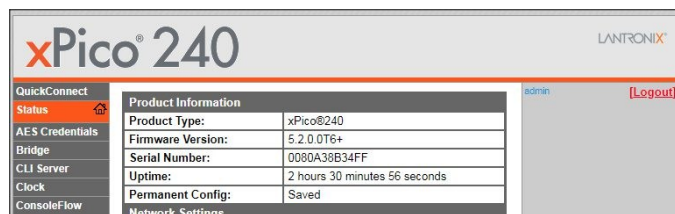
- 3a. Perform a factory reset of the Gateway (see page 3, "FIRST POWER UP: GATEWAY RESET").
- 3b. At this point the **Green** LED will be flashing rapidly, then press and release the Gateway **RESET** button. The Gateway will broadcast its SSID.
- 3c. Use your wireless laptop (or other wireless device) to display the list of "Available networks".
- 3d. Connect your laptop to the Gateway's local wireless network: In the list of "Available networks", look for "**AL_**" followed by the last 6 characters (last 3 bytes) of the Gateway's **ETHERNET MAC ADDRESS** printed on the supplied blue "**GATEWAY ID CARD**" (OI429). In the example blue card shown below, this Gateway will broadcast the SSID "**AL_789012**".



Connect to the "**AL_**" SSID using the method required by your PC. Some PCs will ask you for the network security password which is "**Alarmlock**" (both are cAsE SeNsItiVe; quotes omitted).

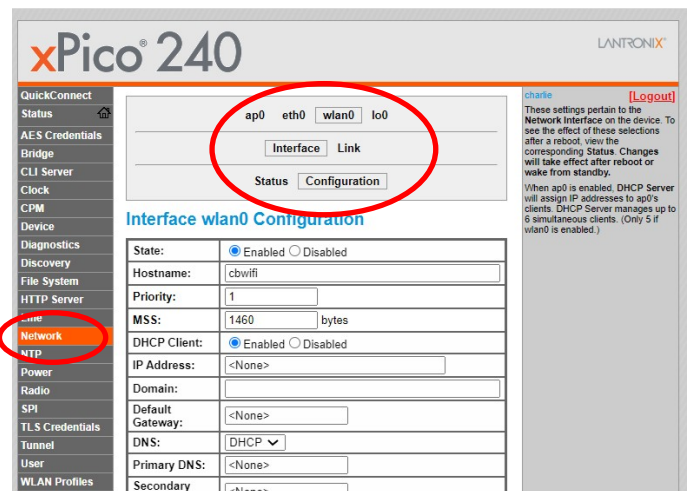
- 3e. At your laptop, open a browser and in the address bar, type **192.168.0.1**, then press **Enter**. **Note:** If the xPico login screen does not appear, go back to step **3b** and start again.
- 3f. In the login dialog, type the default Username "**admin**" and the default Password "**Alarmlock**" (both are cAsE SeNsItiVe; quotes omitted) and press **Enter**. **Note:** You can change this Password later. **Note:** If using an Alarm Lock or MVP Access Gateway configured with Cloud firmware, the default password to the GUI is "**MVPAccess**".

The browser will connect to the Gateway's local wireless network and display the following web page "xPico 240" Home screen (partial example shown below):

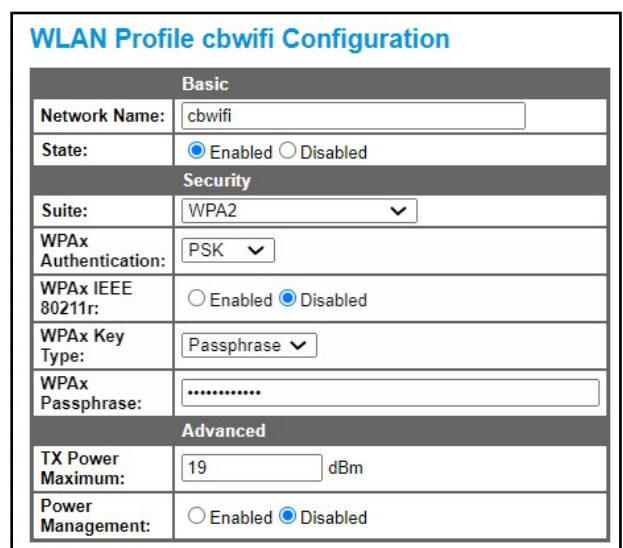


3g. In the "xPico 240" Status/Home screen:

- In the left side column, click **Network** (wait for rotating "busy" circle to finish)
- At the top of the screen, click **wlan0** (wait again)
- At the top of the screen, click **Interface** (wait again)
- At the top of the screen, click **Configuration** (wait again)
- You will now see the **Interface wlan0 Configuration** screen (partial example shown below):



- Set **State** to **Disabled** (wait again)
 - At the bottom of the screen, click **Submit** (wait again)
- 3h. Create a new LAN Profile and add the parameters of your customer's Wi-Fi network:
- In the left side column, click **WLAN Profiles** (wait again)
 - Click in the **Create New WLAN Profile** field. Type the SSID of your customer's network for the **WLAN Profile** name
 - Click **Apply** and the newly created Profile will appear
- 3i. Click the newly created Profile name created in the previous step (wait again). Configure this Profile with the parameters of your customer's Wi-Fi network. *Be sure to record (in writing) the Network Name and all Security information; you may need to add this information into DL-Windows later.*



- The **Network Name** must be the exact SSID of your customer's network (in the above example it is "**cbwifi**")

- Verify the **State** is **Enabled**
- From the **Suite** drop-down, select a Wi-Fi security protocol that matches the protocol used by the customer's network
- For **WPAX Authentication**, select **PSK**
- For **WPAX Key Type**, select **Passphrase** from the drop-down (if not already selected)
- In the **WPAX Passphrase** field, type the exact password of your customer's network (cAsE SeNsItiVe)
- Re-verify all settings, then click **Submit** (and re-confirm)
- Wait for the rotating "busy" circle to finish

3j. On the left side, click **Network**.

- At the top of the screen, click **wlan0** (wait again)
- At the top of the screen, click **Interface** (wait again)
- At the top of the screen, click **Configuration** (wait again)
- For **State**, select the **Enabled** radio button
- If shown, verify the **Hostname** is correct, otherwise, enter the exact SSID of your customer's network
- Verify **DHCP Client** is **Enabled**. If customer uses a static IP address, disable the **DHCP Client** and complete the other fields, including the static **IP Address**, **Default Gateway** and **Primary DNS**
- At the bottom of the screen, click **Submit** ("Submit" will only appear if changes were made to this screen)
- If not already selected, on the left side, click **Network**.
- At the top of the screen, click **eth0** (wait again). Verify that both **Interface** and **Configuration** are selected (with rectangles around each word; if not select each in turn)
- Set the **State** to **Disabled**
- At the bottom of the screen, click **Submit** (wait again)

IMPORTANT: For security, we recommend changing the default **Password** that is used to access the Gateway web page to prevent unauthorized access to the Gateway.
IMPORTANT: **Password** MUST NOT contain any spaces!

3k. On the left side, click **User**.

- At the top of the screen, click **admin** (wait again)
- In the **Password** field, type a new password, then click **Submit** (wait again)
- In the new **Sign in** popup that appears, type the new password again and click **Sign in**

3l. In the left side column, click **Device**.

CLI Server	Property	Status
Clock	Product Type:	xPico@240
ConsoleFlow	Product ID:	Y2
Device	Product SKU:	XPC240100
Diagnostics	Antenna:	U.FL
Discovery	Serial Number:	0080A38B34FF
File System	Configuration Version:	[unversioned]
HTTP Server	Configuration Modified:	Yes
Line	Firmware Version:	5.2.0.0T6+
Network	Active Partition:	1
NTP	Build Date:	Jun 13 2022 (16:53:08)
Power	Bootloader Version:	1.3.0.0R1
Radio	Bootloader Date:	Jun 28 2018 09:58:10
SPI	Uptime:	2 hours 17 minutes 48 seconds
TLS Credentials	Permanent Config:	Saved
Tunnel		[Save]
User		[Reboot]
WLAN Profiles		[Factory Defaults]

- Near the bottom of the screen, click **Reboot**
- Near the top of the screen, click **"Okay"** in the confirmation message. **Note:** Upon clicking the confirmation, your wireless laptop's browser connection to the Gateway's access point will be lost (this is normal). This also indicates that the Gateway is now configured to be connected to the customer's network via Wi-Fi when the physical Gateway is brought within physical proximity of the customer's Wi-Fi signal.

3m. Visit the customer's premises and power the Gateway. Upon power up, the Gateway will automatically connect to the customer's network via Wi-Fi. Launch DL-Windows (that must also be connected to the customer's network), and as per the normal DL-Windows procedure, Discover the new Gateway:

- In the DL-Windows **Gateway Configuration** screen **Gateways** menu, click **Discover New Gateway(s)**. After a short wait, this action will find ALL "Available" Gateways and list them on the screen.
- Find the **Wi-Fi MAC ADDRESS** listed on the supplied blue "GATEWAY ID CARD" (OI429) that matches the MAC address shown in the **Gateway Configuration** screen (highlighted in green).
- Click to select that matching Gateway, then click **Gateways > Add Gateway** to the Account. Click **Yes** in the confirmation popup and when added, the IP address of the Gateway will be highlighted in blue.

Note: On the blue "GATEWAY ID CARD", notice the last 6 characters (last 3 bytes) of the **Wi-Fi MAC ADDRESS** will always be incremented by 1 (in hex) as compared to the **ETHERNET MAC ADDRESS**.

~ **GATEWAY ID CARD** ~

When physically installing the Gateway, fill in a card. This information will be used when adding to DL-Windows. Keep this card in a safe place

GATEWAY MODEL >	AL-IM3-80211
ETHERNET MAC ADDRESS >	12-34-56-78-90-12
Wi-Fi MAC ADDRESS >	WIFI: 123456789013

CONNECTED! Your new Gateway is now connected to your customer's network through Wi-Fi. You are now ready to use your new Gateway to Discover locks and to perform other tasks.

Change the xPico® 240 Username & Password

Every Gateway leaves the factory with the same **xPico® 240** default Username ("**admin**") and default Password ("**Alarmlock**"), therefore we **STRONGLY** recommend using the DL-Windows **Network Configuration** screen to change the username and password.

Important: If you configured the Gateway for Wi-Fi use using the local access point procedure (method 3 on page 6), and you want to make any changes to the network configuration using **Network Configuration** screen, you **MUST** be certain **ALL** settings in the **Network Configuration** screen must exactly match all settings in the "**xPico 240**" web page screens, or else the Gateway's connection will be lost!

Be patient. You may need to wait several minutes for the data to be sent from DL-Windows to the new Gateway. In addition, consult your IT department if you used non-standard settings in the "**xPico 240**" screens.

Launch DL-Windows and open the **Gateway Configuration** screen. Click to highlight your new Gateway in the list, then click **Gateways > Configure / Edit Network Settings** to open the **Network Configuration** screen:

In the **Gen 3 Web Page Username and Password** area, enter a new unique **Username** and **Password**.

Before clicking **Send**, verify that each of the following settings is correct: **IP Address**, **Subnet Mask**, **Default Gateway**, wireless **Network Name (SSID)** and **Password**.

GATEWAY LED INDICATIONS

Yellow	Receiver On (normal operation)
Red	Transmitter On
Green	(Gateway Status)
	Not configured - Rapid blinking / flashing
	Idle / configured - 1 blink per second
	Lock Communication Fail - 2 blinks (continuously)
	Expander Communication Fail - 4 blinks (continuously)

"EXPANDER GROUP" DIALS

Inside the Gateway are 2 rotary dials (see Fig. 4). These dials are used to set the "Expander Group" when you wish to add **AL-IME2-EXP** Expanders in your system (all **AL-IME2-EXP** Expanders include an identical set of dials). *Therefore, the dial values set on your Gateway **MUST** then match the dial values set on your **AL-IME2-EXP** Expanders. **IMPORTANT:** Each Gateway in your system **MUST** be set to a different "Expander Group" value along with its associated Expanders. The "Expander Group" dial setting determines which Expanders are associated with which Gateway, thus preventing Gateways from Discovering unintended Expanders. See WI2156 for more information about installing **AL-IME2-EXP** Expanders in your system.*

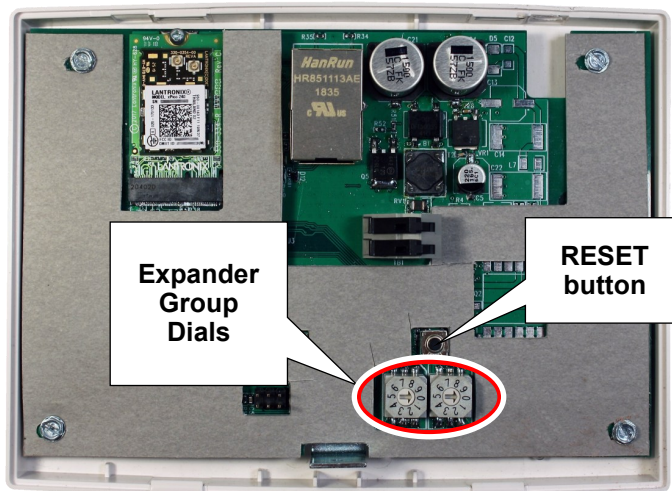


Fig. 4: "RESET" button and two "Expander Group" dials

Expander Group values of "**00**" through "**99**" are valid selections.

IMPORTANT: The small "selection arrow" on each dial must be pointing directly to the desired Group value. In Fig. 5 (below), the Group value is set to "**50**". Use a small flat-head screwdriver to turn the dials and make the selections. *Be sure to orient the Gateway as shown above with the **RESET***

button ABOVE the dials to ensure proper Group setting!

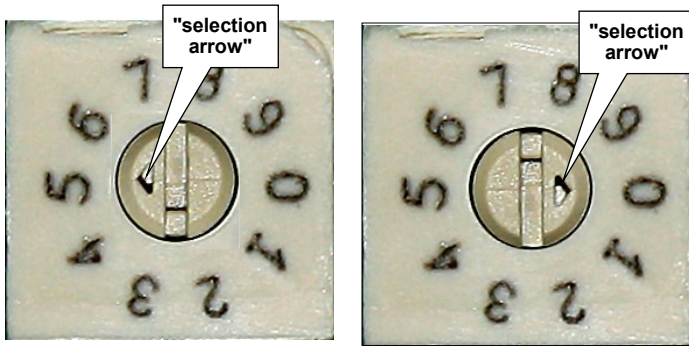


Fig. 5. Example: The above Expander Group dials are set to "50"

HARDWIRED INPUT TO ACTIVATE EMERGENCY LOCK DOWN

The hardwired input integral to all Networkx "Version 3" Gateways can be used to activate Emergency Lock Down. The input consists of a plug and header socket located on the PC board, shown below (see arrow):

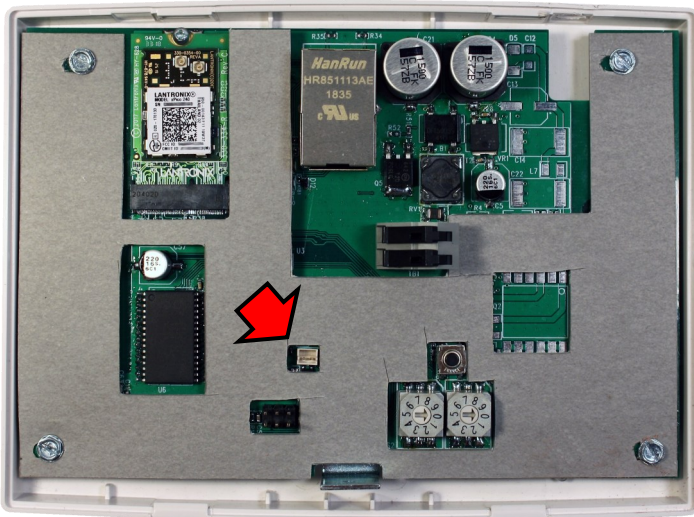


Fig. 6: Location of plug and header socket (arrow)

Connect these two wires to a set of dry contacts, a push button, a switch or a control panel. A closure of at least 1 second activates Emergency Lock Down for all Gateways (both "Version 1" and "Version 2") and therefore for all assigned Networkx locks in the system. In a predominantly "Version 1" Gateway system, it is only necessary to have one "Version 2" Gateway enrolled; in addition, adding multiple "Version 2" Gateways allows for Lock Down to be initiated from various locations and/or by various means.

IMPORTANT: This input can ONLY INITIATE Emergency Lock Down *but CANNOT exit from Lock Down.*

To "Return to Normal", you must use one of the following:

- **DL-Windows**
- **A Networkx lock keypad** (Administrative Users 1 through 11. Users 12 and above must be added to the Emergency Users list (see OI383 for details))

- **A Wireless Remote Release Keyfob** (for example, a model RR-4BKEYFOB)

CLOSE HOUSING COVER

Close the housing cover by first engaging the hooks at the top, then snapping the bottom together. Secure the cover with the Bottom Screw provided as shown in Fig. 7.

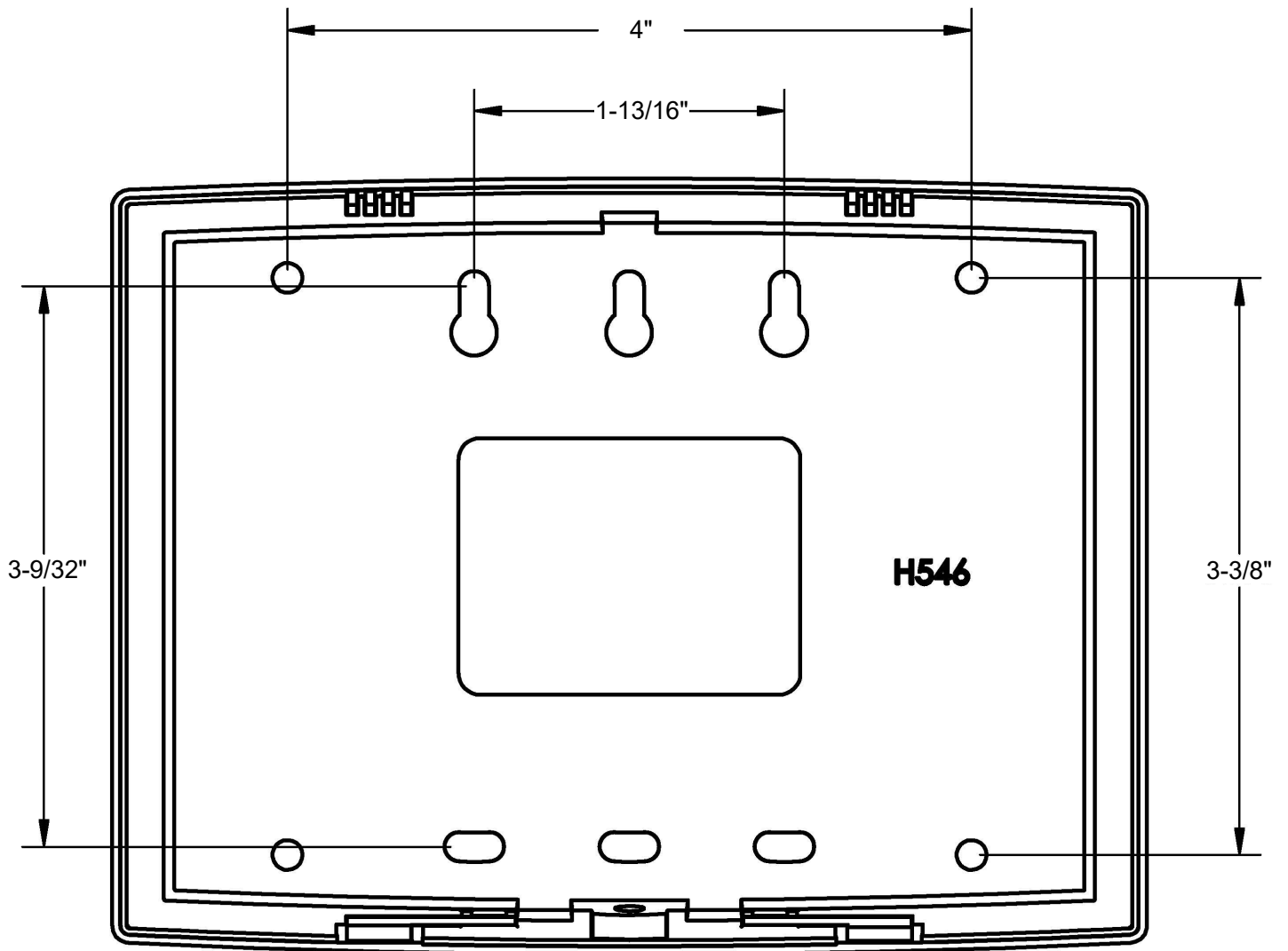


Fig. 7: Bottom Screw

Congratulations! You're finished! Now go to the DL-WINDOWS™ for Networkx™ V5 USER'S GUIDE (OI383) for instructions about Discovering your Gateway from DL-Windows.

This page intentionally left blank.

AL-IM3-80211 Mounting Template



ALARM LOCK LIMITED WARRANTY

ALARM LOCK SYSTEMS, INC. (ALARM LOCK) warrants its products to be free from manufacturing defects in materials and workmanship for twenty four months following the date of manufacture. ALARM LOCK will, within said period, at its option, repair or replace any product failing to operate correctly without charge to the original purchaser or user.

This warranty shall not apply to any equipment, or any part thereof, which has been repaired by others, improperly installed, improperly used, abused, altered, damaged, subjected to acts of God, or on which any serial numbers have been altered, defaced or removed. Seller will not be responsible for any dismantling or reinstallation charges, environmental wear and tear, normal maintenance expenses, or shipping and freight expenses required to return products to ALARM LOCK. Additionally, this warranty shall not cover scratches, abrasions or deterioration due to the use of paints, solvents or other chemicals.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, WHICH EXTEND BEYOND THE DESCRIPTION ON THE FACE HEREOF. THERE IS NO EXPRESS OR IMPLIED WARRANTY OF MERCHANTABILITY OR A WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE. ADDITIONALLY, THIS WARRANTY IS IN LIEU OF ALL OTHER OBLIGATIONS OR LIABILITIES ON THE PART OF ALARM LOCK.

Any action for breach of warranty, including but not limited to any implied warranty of merchantability, must be brought within the six months following the end of the warranty period.

IN NO CASE SHALL ALARM LOCK BE LIABLE TO ANYONE FOR ANY CONSEQUENTIAL OR INCIDENTAL DAMAGES FOR BREACH OF THIS OR ANY OTHER WARRANTY, EXPRESS OR IMPLIED, EVEN IF THE LOSS OR DAMAGE IS CAUSED BY THE SELLER'S OWN NEGLIGENCE OR FAULT.

In case of defect, contact the security professional who installed and maintains your security system. In order to exercise the warranty, the product must be returned by the security professional, shipping costs prepaid and insured to ALARM LOCK. After repair or replacement, ALARM LOCK assumes the cost of returning products under warranty. ALARM LOCK shall have no obligation under this warranty, or otherwise, if the product has been repaired by others, improperly installed, improperly used, abused, altered, damaged, subjected to accident, nuisance, flood, fire or acts of God, or on which any serial numbers have been altered, defaced or removed. ALARM LOCK will not be responsible for any dismantling, reassembly or reinstallation charges, environmental wear and tear, normal maintenance expenses, or shipping and freight expenses required to return products to ALARM LOCK. Additionally, this warranty shall not cover scratches, abrasions or deterioration due to the use of paints, solvents or other chemicals.

This warranty contains the entire warranty. It is the sole warranty and any prior agreements or representations, whether oral or written, are either merged herein or are expressly cancelled. ALARM LOCK neither assumes, nor authorizes any other person purporting to act on its behalf to modify, to change, or to assume for it, any other warranty or liability concerning its products.

In no event shall ALARM LOCK be liable for an amount in excess of ALARM LOCK's original selling price of the product, for any loss or damage, whether direct, indirect, incidental, consequential, or otherwise arising out of any failure of the product. Seller's warranty, as hereinabove set forth, shall not be enlarged, diminished or affected by and no obligation or liability shall arise or grow out of Seller's rendering of technical advice or service in connection with Buyer's order of the goods furnished hereunder.

ALARM LOCK RECOMMENDS THAT THE ENTIRE SYSTEM BE COMPLETELY TESTED WEEKLY.

Warning: Despite frequent testing, and due to, but not limited to, any or all of the following; criminal tampering, electrical or communications disruption, it is possible for the system to fail to perform as expected. ALARM LOCK does not represent that the product/system may not be compromised or circumvented; or that the product or system will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; nor that the product or system will in all cases provide adequate warning or protection. A properly installed and maintained alarm may only reduce risk of burglary, robbery, fire or otherwise but it is not insurance or a guarantee that these events will not occur. CONSEQUENTLY, SELLER SHALL HAVE NO LIABILITY FOR ANY PERSONAL INJURY, PROPERTY DAMAGE, OR OTHER LOSS BASED ON A CLAIM THE PRODUCT FAILED TO GIVE WARNING. Therefore, the installer should in turn advise the consumer to take any and all precautions for his or her safety including, but not limited to, fleeing the premises and calling police or fire department, in order to mitigate the possibilities of harm and/or damage.

ALARM LOCK is not an insurer of either the property or safety of the user's family or employees, and limits its liability for any loss or damage including incidental or consequential damages to ALARM LOCK's original selling price of the product regardless of the cause of such loss or damage.

Some states do not allow limitations on how long an implied warranty lasts or do not allow the exclusion or limitation of incidental or consequential damages, or differentiate in their treatment of limitations of liability for ordinary or gross negligence, so the above limitations or exclusions may not apply to you. This Warranty gives you specific legal rights and you may also have other rights which vary from state to state.