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

DL-WINDOWS™ VERSION 5.5.3
NETWORX™ USER'S GUIDE

OI383BLF 11/18

Communication Software for the Trilogy® Networx™ Locks

DL6500
&
ETDLN

PL6500
& ETPLN

PDL6500
&
ETPDLN

PL6100

networx
by Trilogy

AL-IME-USB

PDL6100

NETWORXPANEL

AL-IME2-EXP
AL-IM2-80211
AL-IME2
AL-IME2-POE

ArchiTech
Series

DL6100

Radio and Television Interference

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the 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 does cause 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 one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the 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.

This Class B digital apparatus complies with Canadian ICES-003. Changes and Modifications not expressly approved by Napco can void your authority to operate this equipment under Federal Communications Commissions rules.

About this Manual

This manual is intended to document the DL-Windows computer screens and features used to program Networx wireless door locks and devices.

The word "**lock**" is a generic word used to indicate one of the many Alarm Lock locking devices available, including devices such as the DK series keypads that trigger other locking devices.

The word "**credential**" is also a generic word used to indicate a PIN number pressed into a lock keypad, **or** a proximity card or proximity keyfob.

The word "**Group**" (i.e. "User Group", "Gateway Emergency Group", "Expander Group", etc.) is used throughout this manual and throughout DL-Windows. Generally, the context will determine the type of Group to which the manual refers.

In DL-Windows, the word "**configure**" has a specific meaning--to "configure" is to "assign" discovered physical locks to a Gateway, thus ensuring a fixed wireless communication channel exists between selected physical locks and a selected Gateway.

Throughout this manual, the phrase "**DL-Windows 'Main Screen'** " is often used, and refers to the first screen that opens when the DL-Windows program is launched.

When the word "Gateway" is used in this manual, it may refer to original Gateways, to "version 2" Gateways or the AL-IME-USB Gateway.

Version 2 Gateways

The **AL-IM2-80211**, **AL-IME2** and the **AL-IME2-POE** "version 2" Gateways (notice the "2" in the model name) are the next generation of Networx Gateways. The "version 2" models are virtually the same as the original "version 1" Gateways, but have the added ability to expand your system with up to 7 Expanders. Note also that "version 2" series Gateways CAN be mixed into an existing system that includes the older "non-version 2" Gateways. Important: DL-Windows version 5.4 or later is required to support version 2 Gateways and Expanders.

Important: *Trilogy® is a registered trademark of Alarm Lock. ProxCard® and ProxKey® are trademarks of the HID© Corporation.. Microsoft® and Windows® are trademarks of their the Microsoft Corporation. All other trademarks, service marks, and product or service names described in this manual are for identification purposes only and may be trademarks or registered trademarks of their respective owners. The absence of a name or logo in this document does not constitute a waiver of any and all intellectual property rights that NAPCO Security Technologies, Inc. has established in any of its product, feature, or service names or logos. Screen images, icons and instructions in this guide may vary depending on the software version installed. The information in this manual is for informational purposes only and is subject to change without notice. Companies, names and data used in examples herein are fictitious unless otherwise noted. Alarm Lock assumes no responsibility for incorrect information this manual may contain.*

Changes From Previous Edition

The following changes have been made to this manual (OI383B) since the last edition (OI383A):

Enhanced Emergency Lockdown Functions

- Page 33: The **Transfer lock(s) to Another Gateway** option is supported: Located in **Gateway Configuration** > **Locks**. **Note:** This option is available only during the **Discover Locks** function.
- Page 40: The **Wireless Configuration** names are customizable: Located in the **Wireless** screen, this allows you to type customized names for each **Wireless Configuration**. Click on the **Edit** button to rename; then click **Save**
- Page 44: The **Enable Emergency Indicator** setting is now available for Networx Lock Profiles ETPLN and ETPLNiRx. The **Enable Emergency Indicator** check box is located in **Features** > ***Emergency*** tab
- Page 45: "Exit Only" limited Emergency User configuration is supported: The "Global Users" screen, right-click a User in the User List. The menu option named **Add/Remove Emergency User(s)** has been placed into to the new menu option **Lockdown User** (with additional sub-menu "**Enable/Disable as Reset Lockdown User**"; see page 45 and "**Using Emergency Commands**" in OI382 for details)
- Page 46: The Main Screen's flashing red and yellow **Emergency Lockdown** indicator bar will automatically update. This feature verifies that the DL-Windows display quickly reflects any changes to the system lockdown status should emergency commands be initiated from individual locks (this update occurs each time the **Gateway** screen is opened)
- Page 55: **Manually Unlock Door** menu and functionality are added: Right-click any "Linked" Networx Lock Profile, then click **Manually Unlock Door**
- **Note:** The firmware version of all Networx and ArchiTech locks is now displayed to the right of each *Linked* Lock Profile name located in the "Account List" area of the Main Screen. To initiate or update the firmware information, either select **View Status of Lock** (in the Networx Lock right-click Profile menu) or select **Update Status of All Locks** from the Wireless Actions pull-down

Table of Contents

Ordering Information

Several Gateway device models are available; all have the two antennas used to transmit to the locks via an Alarm Lock proprietary radio connection.

- **Gateway "Wireless/Wired" AL-IM2-80211** - Hardwired/ Wireless Version 2 Gateway Interface Module. Supplied with its own Class 2 transformer to supply power; connection to a network is supported via either a *wired* connection (using a standard RJ-45 Ethernet cable) or a *wireless* connection (using a third antenna for 802.11 transmissions). Ensure adequate 802.11 coverage in the area where the "Wireless/Wired" Gateway is mounted. Supports up to 63 Networx Locks. Ceiling- or wall-mountable.
- **Gateway "Wired" AL-IME2** - Hardwired Version 2 Gateway Interface Module, supports up to 63 Networx Locks, connects directly to a network using a standard RJ-45 Ethernet cable. Ceiling- or wall-mountable; powered with Class 2, 6VAC transformer (supplied).
- **Gateway "Power over Ethernet" AL-IME2-POE** - Hardwired Version 2 Gateway Interface Module + POE (Power Over Ethernet), supports up to 63 Networx Locks, connects directly to a network using a standard RJ-45 Ethernet cable and POE. Ceiling- or wall-mountable.
- **Expander AL-IME2-EXP** - Version 2 Expander Module, extends the coverage area of AL-IME2 series Gateways, allowing control of up to its rated maximum of 63 Networx locks per Gateway. The Expander only requires a connection to an AC outlet. Ceiling- or wall-mountable; Up to 7 Expanders can be added to one version 2 series Gateway. Requires one 6VAC External Power Supply (supplied).
- **Expander AL-IME2-PIE** - Version 2 *Plug-In* Expander Module, extends the coverage area of AL-IME2 series Gateways, allowing control of up to its rated maximum of 63 Networx locks per Gateway. Up to 7 Expanders can be added to one version 2 series Gateway. Occupies one 120VAC outlet. Enclosure Size: 4.3"H x 2.5"W x .875"D (5"H with tab).
- **PDL6100** - Cylindrical Trilogy® Networx™ Wireless Access Control Lock with built in HID Proximity ID Card Reader, full-metal digital keypad, integral bi-directional radio, 4 C-cell battery-operated (batteries supplied), serial number ID card, standard format SC1 keyway for manual key override, 4⅞" ASA Strike (included).
- **DL6100** - Cylindrical Trilogy® Networx™ PIN-Code Wireless Access Control Lock, as above, with metal digital keypad only. Standard format SC1 keyway for manual key override, 4⅞" ASA Strike (included).
- **PL6100** - Cylindrical Trilogy® Networx™ Wireless Access Control Lock with built in HID Proximity ID Card Reader (keypad removed for added security), integral bi-directional radio, 4 C-cell battery-operated (batteries supplied), serial number ID card, standard format SC1 keyway for manual key override, 4⅞" ASA Strike (included).
- **PDL6200** - Cylindrical Trilogy® Networx™ Wireless Access Control Lock with added Door Monitoring features, including logged entry and exit, "Door Ajar" (valid credential entered and door opened but not closed within the programmed time), and "Forced Entry" (door opened without a valid credential entered or without inside lever turned). Includes built in HID Proximity ID Card Reader, full -metal digital keypad, integral bi-directional radio, 4 C-cell battery-operated (batteries supplied), serial number ID card, standard format SC1 keyway for manual key override, 4⅞" ASA Strike (included).
- **PL6200** - Cylindrical Trilogy® Networx™ Wireless Access Control Lock with added Door Monitoring features (see PDL6200 for details). Includes built in HID Proximity ID Card Reader (keypad removed for added security), integral bi-directional radio, 4 C-cell battery-operated (batteries supplied), serial number ID card, standard format SC1 keyway for manual key override, 4⅞" ASA Strike (included).
- **PDL6500** - Mortise Trilogy® Networx™ Wireless Access Control Lock with built in HID Proximity ID Card Reader, full -metal digital keypad, integral bi-directional radio, supplied batteries and serial number ID card. Standard format SC1 keyway for manual key override, 4⅞" ASA Strike (included).
- **DL6500** - Mortise Trilogy® Networx™ Wireless Access Control Lock with full-metal digital keypad, integral bi-directional radio, supplied batteries and serial number ID card. Standard format SC1 keyway for manual key override, 4⅞" ASA Strike (included).
- **PL6500** - Mortise Trilogy® Networx™ Wireless Access Control Lock with built in HID Proximity ID Card Reader (keypad removed for added security), integral bi-directional radio, supplied batteries and serial number ID card. Standard format SC1 keyway for manual key override, 4⅞" ASA Strike (included).
- **PDL6600** - Mortise Trilogy® Networx™ Wireless Access Control Lock with added Door Monitoring features (see PDL6200 for details). Includes built in HID Proximity ID Card Reader, full-metal digital keypad, integral bi-directional radio, supplied batteries and serial number ID card. Standard format SC1 keyway for manual key override, 4⅞" ASA Strike (included).
- **PL6600** - Mortise Trilogy® Networx™ Wireless Access Control Lock with added Door Monitoring features (see PDL6200 for details). Includes built in HID Proximity ID Card Reader (keypad removed for added security), integral bi-directional radio, supplied batteries and serial number ID card. Standard format SC1 keyway for manual key override, 4⅞" ASA Strike (included).
- **PDL7100** - Cylindrical Trilogy® Networx™ Wireless Access Control Lock with built in Proximity **iCLASS** Smart Card Reader, full-metal digital keypad, integral bi-directional

Ordering Information (cont'd)

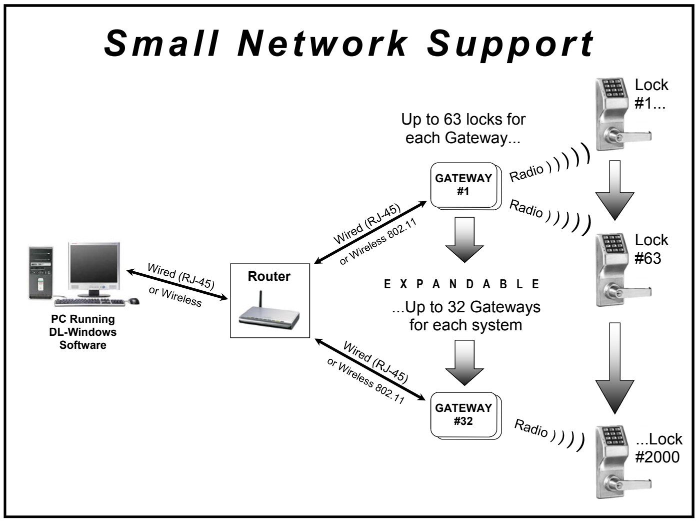
radio, 4 C-cell battery-operated (batteries supplied), serial number ID card, standard format SC1 keyway for manual key override, 4⅞" ASA Strike (included).

- **PL8200** - Same as the PL6200 but includes a built in 13.56MHz proximity Smart Card reader.
- **PDL8200** - Same as the PDL6200 but includes a built in 13.56MHz proximity Smart Card reader.
- **PDL8600** - Mortise Trilogy® Networx™ Wireless Access Control Lock with added Door Monitoring features (see PDL6600 for details). Includes built in 13.56MHz proximity Smart Card reader, full-metal digital keypad, integral bi-directional radio, supplied batteries and serial number ID card. Standard format SC1 keyway for manual key override, 4⅞" ASA Strike (included).
- **PL8600** - Same as the PL6600 but includes a built in 13.56MHz proximity Smart Card reader.
- **ETPDLN, ETDLN & ETPLN** - Exit Trim Trilogy Networx™ Wireless Access Control Locks for most major manufacturers exit devices. **ETPDLN and ETPLN include** built in HID Proximity ID Card Reader (**ETPLN** for proximity -only). **ETPDLN** and **ETDLN include** full-metal digital keypad. All include integral bi-directional radio, 4 C-cell battery-operated (batteries supplied), serial number ID card, standard format SC1 keyway for manual key override.
- **NETDK, NETPDK & NETWORXPANEL** - The NETDK and NETPDK (with proximity card reader) are secured single-door or double-door digital keypads for use within the wireless Networx™ system. One or two keypads can be wired to the dedicated NETWORXPANEL control panel to provide controlled access to a door by releasing a locking device (such as a magnetic lock or electric door strike) when a proper User Code (and/or a proximity credential to the NETPDK) is presented. The NETWORXPANEL inputs support two of any combination of NETDK or NETPDK keypads, PLUS up to two Wiegand devices. See WI1881, WI1855 and WI1856 for additional information.
- **ETPDLNRX & ETPLNRX** - Exit Trim Trilogy Networx™ Wireless stand-alone access control locks for most major manufacturers exit devices with added Door Monitoring features (see PDL6200 for details). The **ETPDLNRX** includes both a 12-button metal keypad and a built in HID Proximity ID Card Reader (**ETPLNRX** for proximity-only). All include integral bi-directional radio, 4 C-cell battery-operated (batteries supplied), serial number ID card, standard format SC1 keyway for manual key override.
- **ETPDNIRX** - An Exit Trim version of the **PDL8600** used with most major manufacturers exit devices for exit door push bar applications.
- **ArchiTech Series** - For architectural and designer applications, virtually unlimited combinations of several hundred architectural trims and finishes, in mortise and cylindrical lock styles, with multi-credential proximity reader technologies. See www.alarmlock.com for a complete list of all available ArchiTech™ Networx™ series devices and manuals (downloadable in PDF format).
- **DL-WINDOWS** - Alarm Lock Trilogy Microsoft Windows-based software application, v4.0.0 or higher, supports Trilogy Networx and Trilogy stand-alone locks, with single database. *Free of charge* and downloadable online at www.alarmlock.com.
- **OI382** - DL-WINDOWS™ Basic User's Guide (non-Networx), replaces OI237K.
- **OI383** - DL-WINDOWS™ NETWORX™ User's Guide (this manual), replaces OI352D.
- **WI2085** - Networx Gateway Installation & Setup Instructions
- **OI362** - Networx Quick Start Guide.
- **WI1790** - PDL6100 Keypad Programming Instructions.
- **WI1820** - DL6100 Keypad Programming Instructions.
- **WI1835** - PDL6500 & ETPDLN Keypad Programming Instructions.
- **WI1836** - DL6500 & ETDLN Keypad Programming Instructions.
- **WI1843** - PL6100 Programming Instructions.
- **WI1844** - PL6500 & ETPLN Programming Instructions.
- **WI1674** - PDL6100 and DL6100 Installation Instructions.
- **WI1676** - PDL6100 and DL6100 Door Installation Template.
- **WI1881** - NETDK & NETPDK Installation Instructions
- **WI1855** - NETWORXPANEL Programming Instructions with the NETDK & NETPDK keypads
- **WI1856** - NETWORXPANEL Installation Instructions
- **WI2024** - PDL6200 & DL6200 Installation Instructions
- **WI2027** - PDL6600 & ETPDLNRX Programming Instructions
- **WI2036** - PDL6600 & DL6600 Template
- **WI2059** - PL6600 & ETPLNRX Programming Instructions
- **WI2126** - PDL8600 & ETPDNIRX Programming Instructions
- **WI2203** - PDL6200 & PDL8200 Programming Instructions

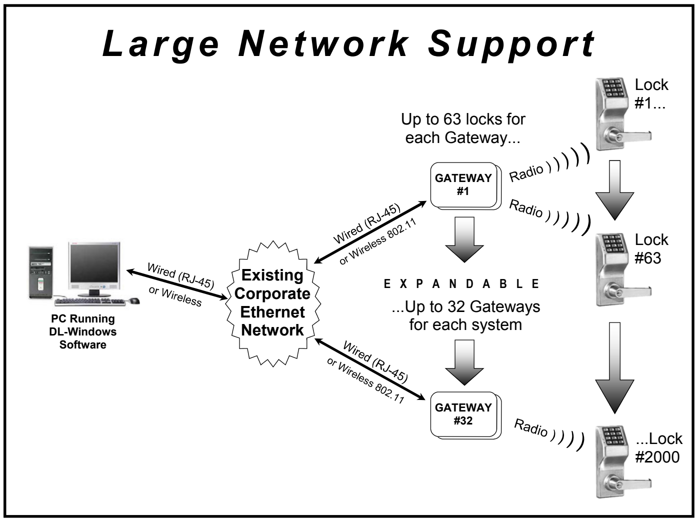
See www.alarmlock.com for a complete list of all available standard Trilogy and Networx™ series devices and manuals (downloadable in PDF format).

Overview

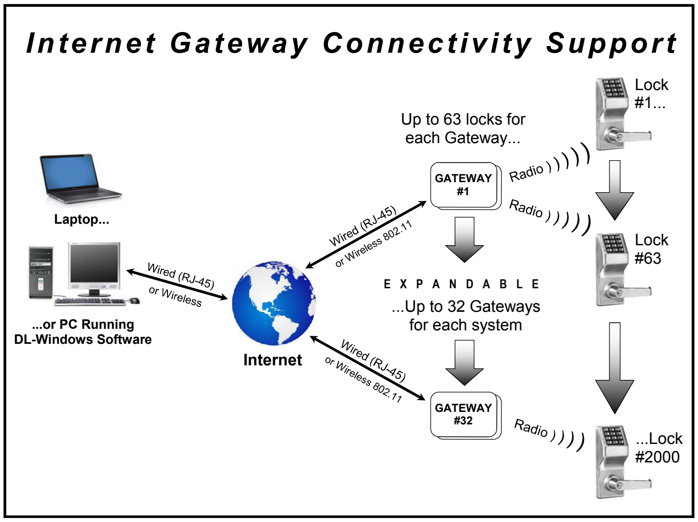
Used with the Trilogy Networx™ series door locks and keypads, DL-Windows (version 4.0.0 software or later) allows you to upload and download programming features ***wirelessly*** using a computer network. With "wireless" communication, the various cables and/or an AL-DTM Data Transfer Module are NOT required to transfer data between DL-Windows and the wireless locks. Simply use your computer to retrieve logs, download User Codes and program features into each wireless lock in the system.


Small Network Support

PC Running DL-Windows Software
Wired (RJ-45) or Wireless
Router
Wired (RJ-45) or Wireless 802.11
GATEWAY #1
Up to 63 locks for each Gateway...
Radio
Radio
EXPANDABLE
...Up to 32 Gateways for each system
Wired (RJ-45) or Wireless 802.11
GATEWAY #32
Radio
Lock #1...
Lock #63
...Lock #2000


Large Network Support

PC Running DL-Windows Software
Wired (RJ-45) or Wireless
Existing Corporate Ethernet Network
Wired (RJ-45) or Wireless 802.11
GATEWAY #1
Up to 63 locks for each Gateway...
Radio
Radio
EXPANDABLE
...Up to 32 Gateways for each system
Wired (RJ-45) or Wireless 802.11
GATEWAY #32
Radio
Lock #1...
Lock #63
...Lock #2000


Internet Gateway Connectivity Support

Laptop...
...or PC Running DL-Windows Software
Wired (RJ-45) or Wireless
Internet
Wired (RJ-45) or Wireless 802.11
GATEWAY #1
Up to 63 locks for each Gateway...
Radio
Radio
EXPANDABLE
...Up to 32 Gateways for each system
Wired (RJ-45) or Wireless 802.11
GATEWAY #32
Radio
Lock #1...
Lock #63
...Lock #2000

DL-Windows software is installed on a computer that is connected to a network (either a small Ethernet network, a large corporate LAN, or over the Internet). Connected to this network is an intermediate device called a *Gateway* that communicates via a private wireless signal to a radio located inside each door lock. In this way, the software allows full programming and control of each lock in the system. **Note:** In this manual, the word "lock" refers to all Networx™ series door locks and the NETWORX-PANEL wireless control panel and its wireless keypads.

To ensure each physical lock is identified correctly by DL-Windows, the factory assigns each lock a unique serial number; after locks are installed on the doors and the Gateways are mounted, the Gateways search for new locks, allowing them to be enrolled into the system.

FLEXIBLE SETUP

In addition to wireless communication, ***these wireless door locks can also be programmed at the keypad*** (see the keypad programming instructions included with the lock). This means that locks can be installed on the doors and *immediately be put into use via keypad programming*--even before a wireless network is set up. Therefore, you can install the locks on the doors before configuring the wireless network, or you can set up the wireless network first and add locks later. If you wish, you can even start by designing a "virtual" system within DL-Windows (creating new Accounts, adding Users and configuring lock features, etc.), then set up the network and install the lock hardware later. But in the end, after your lock hardware is physically installed and the network is up and running, you can run DL-Windows to "Link" the "virtual" system saved on your computer with the "real" lock hardware on the doors.

Note: Keypad programming of User Codes, Features, Time Zones, and Schedules is available as a ***temporary*** convenience to allow the lock to be put into use before installing and configuring a wireless network. Therefore, all lock programming added via the keypad ***cannot*** be retrieved into DL-Windows. If you decide to start programming your wireless lock via the keypad, we recommend you keep hardcopy records (in a secure location) of all Users, their User Codes, and any proximity cards that may have been programmed. Keeping complete and accurate records saves time because after the wireless network is set up, any programming added via the keypad must be re-added to DL-Windows and downloaded back to the lock(s).

CAPACITY

Each installed system can contain from 1 to 32 Gateways--and each Gateway can control up to 63 locks--for a maximum of 2000 locks allowed per Account; and the DL-Windows software can support, in theory, an unlim-

Overview (cont'd)

ited number of Accounts. In addition, each Networx™ lock can contain up to 5000 Users! **Note:** Each Gateway can support up to 7 Expanders. The Gateway and Account capacity does not change with the addition of Expanders to a system.

MINIMUM WIRELESS SYSTEM

As shown in the "overview" drawings above, you do not need a massively complex corporate network to run a working system. In fact, a minimum wireless system may consist of a laptop or desktop **computer** (to run DL-Windows), a **router** (to allow connection to a computer network), and an Alarm Lock **Gateway** module (the intermediary between the network and the locks).

AL-IME-USB Gateway

The **AL-IME-USB** Portable Gateway provides full Networx Gateway functionality without the need for a network connection. The **USB Gateway** is inserted into the USB socket of your PC or laptop and quickly creates a wireless connection to your Networx door locks, with all data routed through the **USB Gateway**. In addition, the **USB Gateway** can be used in an existing system with standard Networx Gateways. See OI386 for more information.

NETWORK SECURITY

The system uses AES (Advanced Encryption Standard) to protect the integrity of the data flow between the wireless router / network and the Gateways.

EXPANDERS

DL-Windows (version 5.4 and later) supports AL-IME2-EXP Expanders. Expanders extend the coverage area of version 2 series Gateways, allowing control of up to its rated maximum of 63 Networx locks per Gateway.
Used in place of additional Gateways, **AL-IME2-EXP** Expanders are useful when a Gateway does not provide sufficient signal strength to a particular area and therefore is unable to communicate with a wireless lock or group of wireless locks. Up to 7 Expanders can be added to one version 2 series Gateway.

IMPORTANT - Please Read This

DL-Windows software is the basis for wireless lock programming. For those unfamiliar with using DL-Windows software or if DL-Windows is not yet installed, **stop here** and review the DL-Windows User Guide (OI382). It may be helpful to create a "test" Account in DL-Windows, where you can add Lock Profiles and become familiar with the DL-Windows program while working through the examples presented in this manual and in OI382.

If you are already familiar with DL-Windows, the transition to working with wireless locks will be straightforward with slight changes in terminology. If you want to get started right away to see the system work, see the **Quick Start** section on page 11. This manual can be read from beginning to end, or can be used with the Table of Contents as a reference manual.

- **To install locks on the doors first**, use the Installation Instructions for the lock model you wish to install, then use the keypad Programming Instructions to put the locks into use.
- **To install and set up Gateways** and configure your network settings, see the **Networx Gateway Installation & Setup Instructions** (WI2085).

DL-WINDOWS SYSTEM REQUIREMENTS

See OI382 for a complete list of the minimum requirements, plus things to consider when upgrading from previous versions, and the step-by-step procedures for installing DL-Windows version 5.

Gateway Specifications

For Gateways, network activity (or bandwidth usage) does NOT occur until you operate DL-Windows software to send programming to (or receive log data from) physical locks. **Exception:** During the Emergency Lockdown Command, Gateways communicate through the network. Gateways will send less than 1000 bytes during these Emergency Commands (for more information regarding Emergency Commands, see page 43).

AL-IME2 Gateway

NETWORK INTERFACE:

Interface: Ethernet, 10Base-T or 100Base-TX (using RJ-45 jack)
Protocols: TCP/IP, UDP/IP, DHCP

NETWORK RANGE

Gateway / Expander to Locks: Clear field range 500'.
Typical indoor range: Networx 75-175'; ArchiTech Networx: 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

Peak Supply Current: 650mA
Input Voltage: 5 - 6VAC

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.

AL-IM2-80211 Gateway

NETWORK INTERFACE

Interface: Ethernet, 10Base-T or 100Base-TX (using RJ-45 jack)
Protocols: TCP/IP, UDP/IP, DHCP

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

SECURITY

SIEEE 802.11 - PSK with AES Encryption 128-bit
Encryption: 128-bit AES Rijndael encryption

NETWORK RANGE

Gateway / Expander to Locks: Clear field range 500'.
Typical indoor range: Networx 75-175'; ArchiTech Networx: 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

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.

AL-IME2-POE Gateway

NETWORK INTERFACE

Interface: Ethernet, 10Base-T or 100Base-TX (using RJ-45 jack)
Protocols: TCP/IP, UDP/IP, DHCP

NETWORK RANGE

Gateway / Expander to Locks: Clear field range 500'.
Typical indoor range: Networx 75-175'; ArchiTech Networx 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

POE Voltage: 48VDC Nominal Class 2
Peak Supply Current: 650mA
Input Voltage: 5 - 6VAC

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.

Expander Specifications

AL-IME2-EXP Expander

Maximum of seven (7) AL-IME2-EXP Expanders per one version 2 series Gateway (addressed as one Group).

NETWORK RANGE
Gateway/Expander to Locks: Clear field range 500'.
Typical indoor range: Networx 75-175'; ArchiTech Networx: 50-125'. **Note:** Actual range varies with building construction.
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
Peak Supply Current: 150mA
Input Voltage: 5 - 6VAC
Requires one (1) 6VAC External Power Supply

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.

AL-IME2-PIE Plug-In Expander

Maximum of seven (7) AL-IME-PIE Expanders per one Version 2 Series Gateway (addressed as one Group)

NETWORK RANGE
Gateway / Expander to Locks: Clear field range 500'.
Typical indoor range: Networx 75-175'; ArchiTech Networx: 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
Peak Supply Current: 150 mA
Input Voltage: 5 - 6VAC
Occupies one (1) 12VAC Outlet as External Power

ENVIRONMENTAL
Operating Temperature: -20˚ to 60˚C (-4˚ to 140˚F)
Storage Temperature: -40˚ to 85˚C (-40˚ to 185˚F)

PHYSICAL
Enclosure Size: 4.3"H x 2.5"W x .875"D (5"H with tab)
Weight: 0.35lbs.

Quick Start

1. **Install the DL-Windows software** (see OI382).

2. **Setup your Network connection and install your Gateway** (see WI2085). **Note:** Complete the blue **Gateway ID Card** specifying its physical location.

3. **Connect the Gateway to the Network, then power up the Gateway** (refer to the documentation that accompanied the device).

4. **Start DL-Windows and add a new Account** (see OI382).

5. **Create Lock Profiles for each physical wireless lock** (see OI382). Lock Profiles will be required for Linking to physical locks after discovery. **Note:** See **Ordering Information** on page 5 for supported lock models.

6. **Add Users, create Schedules and set Features for each lock** (see OI382). **Note:** This step may be performed after the Linking process described in step 13 below.

7. **Set Security Password** (see page 12). You cannot perform the next step without the Security Password being set.

8. Click the **Gateway Config** button (see page 13).

9. **Discover Gateways:** Click **Discover Gateways and Auto Add** button (see page 13).

10. **Discover Expanders** (if applicable)**:** (Refer to the documentation that accompanied the device).

11. **Discover Locks:** In the **Gateway Configuration** screen, click to highlight and select the desired Gateway, set the **Number of Locks to Discover**, then click the **Discover Locks** button (page 15).

12. **Assign Locks:** Select discovered lock(s) by serial number and click **Assign** (page 15).

13. **Link lock(s) to Lock Profile(s)** (page 17). In the **Link/Unlink Lock Profiles** screen:
    a. In the **Available Lock Profiles** field: Click to highlight a **Lock Profile**.
    b. In the **Available Lock(s) By Serial Number** field: Click to select the desired physical lock (by serial number) to be Linked to the Lock Profile.

14. **"Download" Lock Profile to lock(s)** (see OI382).

    Congratulations! Locks can now communicate wirelessly. Use the **Communication** button in the **Lock** screen (see OI382), or communicate with multiple locks using the **Wireless** screen (page 40).

Security Password

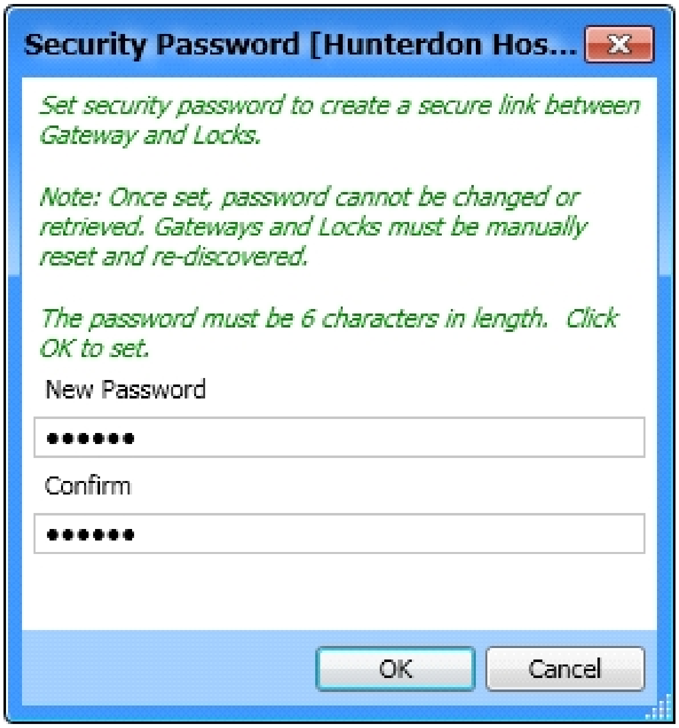
Overview

Before Gateways and locks can be discovered and configured, a Security Password must be set for the Account. The Security Password creates a secure connection between DL-Windows, your Gateways and the physical locks. Once set, the Security Password is embedded within the radio transmissions, also preventing separate Accounts from overlapping their wireless signals.

IMPORTANT: ***The Security Password cannot be changed and cannot be retrieved****.* If you wish to change or remove the Security Password, the Account may be *cloned* to remove the Security Password in the new Account (see OI382 for more information about "cloning" Accounts). To change or remove the Security Password in the locks and/or the Gateways, each lock (or Gateway) must be manually defaulted and re-downloaded with the new (or blank) Security Password.

To set the Security Password, click **Tools** > **Set Security Password**. **Note:** After a Security Password has been created, the **Tools** > **Set Security Password** will no longer be available for the selected Account.

In the screen that appears (shown below), type a unique 6 character (no more, no less) password in the **New Password** field. Retype the password in the **Confirm** field and click **OK** to set the Security Password, or click **Cancel** to exit without saving changes.



Set security password to create a secure link between Gateway and Locks.

Note: Once set, password cannot be changed or retrieved. Gateways and Locks must be manually reset and re-discovered.

The password must be 6 characters in length. Click OK to set.

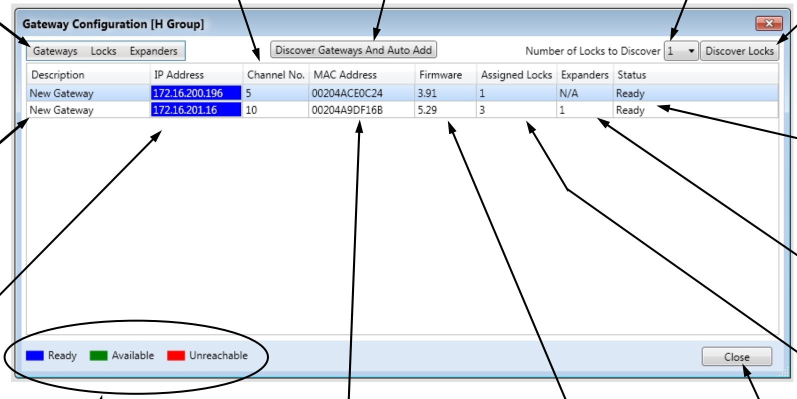
New Password: ●●●●●●

Confirm: ●●●●●●

"Gateway Configuration" Screen - Field and Button Definitions

The **Gateway Configuration** screen allows for the discovery, addition and configuration of Gateways, Expanders and locks. additionally, this screen serves as the main hub for all Networx devices and displays all pertinent status information.

Click the **Gateway Config** button to access the **Gateway Configuration** screen. Gateway Config


Gateway Configuration [H Group]
Gateways
Locks
Expanders
Discover Gateways And Auto Add
Number of Locks to Discover
1
Discover Locks
Ready
Available
Unreachable
Close

Description	IP Address	Channel No.	MAC Address	Firmware	Assigned Locks	Expanders	Status
New Gateway	172.16.200.196	5	00204ACE0C24	3.91	1	N/A	Ready
New Gateway	172.16.201.16	10	00204A9DF16B	5.29	3	1	Ready

Gateways
Click to display the **Gateway** menu selections.

Locks
Click to display the **Locks** menu selections.

Expanders
Click to display the **Expanders** menu selections.

Note: The new simplified menu selections are intended to guide you to the proper selection based on the device you need to configure.

Channel No.
Displays the internal channel number assigned to the Gateway.

Discover Gateways And Auto Add
This button combines two actions: The "**Discover New Gateway(s)**" process and the "**Add Gateway To Account**" process, in one button.
The Gateways that are found on the network (but not already configured) are automatically added to the current Account and listed below.

Number of Locks to Discover
Click to set the number of locks you wish to discover (1 - 63).

Discover Locks
Click to start the lock discovery process. The signal will be transmitted based upon the number of locks selected in "**Number of Locks to Discover**". **Note:** Only those locks within range that have not already been assigned to a Gateway will respond.

Status
Displays the current state or the last-known condition of the Gateway.

Description
Default name is "New Gateway".
Double-click to manually edit the Gateway Description.

Expanders
Indicates the total number of Expanders added to the version 2 Gateway.

Assigned Locks
Indicates the total number of locks assigned to the Gateway / Expanders.

IP Address
Specifies the IP address currently assigned to the Gateway from the network. This column is color coded; see "**Color Definitions**" on the next page.

Firmware
Indicates the current firmware version the Gateway is running.

Close
Click to save changes and exit.

Color Key
The **IP Address** column is color coded to describe the status of the Gateway (see next page for complete descriptions).

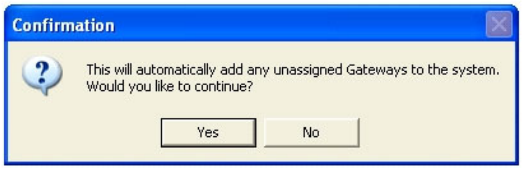
- Blue = Ready
- Green = Available
- Red = Unreachable

MAC Address
A unique serial number assigned to the Gateway that identifies that Gateway from all others. Inside the Gateway housing, the MAC address is located on a square sticker (look under the bar code) and has 12 digits, grouped in 6 pairs separated by dashes.

Discovering / Adding Gateways

Once connected to the network, Gateways must be discovered and added to the Account. This can be accomplished in one of 3 ways:

- In the **Gateway Configuration** screen, click the **Discover Gateways And Auto Add** button. This one-click option discovers and adds **ALL** "**Available**" (see **Color Definitions** below) Gateways to the selected Account.



Confirmation

This will automatically add any unassigned Gateways to the system.
Would you like to continue?

- In the **Gateway Configuration** screen **Gateways** menu, click **Discover New Gateway(s)**. This action will find **ALL** "**Available**" Gateways and list them on the screen. **Note:** The IP addresses of "**Available**" Gateway(s) will be highlighted green (see **Color Definitions** below). The next step is to click to select a Gateway you wish to add, then click **Gateways** > **Add Gateway to Account**. Click **Yes** in the confirmation popup and when added, the IP address of the Gateway will be highlighted in blue. This two-step option allows you to first discover Gateways, then selectively decide which Gateways to add.

Note: USB Gateways are added using either of the two methods described above (see OI386).

- In the **Gateway Configuration** screen, click **Gateways** > **Manually Add a Gateway**. This option opens the **Manual Gateway Addition** screen, where the MAC Address of the Gateway is manually typed and saved to the database. A connection will then be attempted to the Gateway over the network, and if successful, the Gateway will be added to the system. When Gateways cannot be added to the system, it will be colored red. See **Color Definitions** below.

> **TIP** For a Gateway to be considered "**Available**", it must be on the network, have a dynamically obtained IP address, and manually reset (see WI2085 for reset GW procedure). A Gateway may also be considered "**Available**" if it already contains the same Security Password as the Security Password set for the Account. See section **Gateways > Import Gateway and Assigned Lock(s)** for more information.

Things to Remember

1. **IMPORTANT:** Gateways must be on the same Subnet as DL-Windows to allow for successful discovery. Once Gateways are added to the system, its static IP address, Wireless settings, etc., may then be configured. See **Gateways > Configure/Edit Network Settings** for more information.
2. All added Gateways are put into **Gateway Emergency "GROUP A"** by default. For more information, see **Automatic Gateway Grouping** on page 44.
3. Since Gateways are discovered and added using DHCP (Dynamic Host Configuration Protocol), and are therefore not yet static, a reminder "**red siren**" symbol will be displayed in the DL-Windows "Main Screen" status bar upon Gateway addition. The "**red siren**" symbol is a reminder that keypad-initiated Emergency commands may not function correctly if the Gateway has not been configured with a *static* IP address. See 38 for important information.

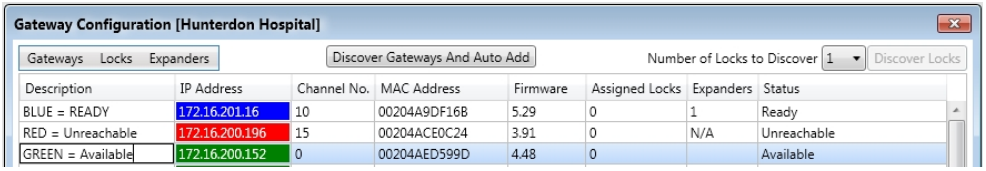
Color Definitions

The **IP Address** column is color coded, as follows:

- **Blue**: **Gateway Status = Ready**.
  Indicates the Gateway has been discovered on the network successfully, and added to an existing Account within DL-Windows. **Note:** This Gateway may or may not have physical locks assigned (may or may not have a Lock Table assigned).
- **Green**: **Gateway Status = Available**.
  Indicates a Gateway has been successfully discovered on the network, but has not been added to the Account within DL-Windows.
- **Red**:
  Gateway Status = Unreachable.
  Indicates a Gateway that has been previously discovered and added to an Account, but is currently not reachable on the network. **Note:** Gateway can be re-located by clicking **Gateways** > **Relocate Gateways Displayed in red**. This red color can signify a security mismatch, detailed below.

  OR

  Red:
  Gateway Status = Security Mismatch.
  Indicates the Gateway Security Password and the Security Password set for the Account are not the same, therefore a successful connection cannot be established. **Note:** Gateway may require latest configuration data. See page 21 ("**Gateways > Send Config Table to the Gateway**") and the **TIP** on page 28 (the page for "**Gateway Configuration > Gateways > Relocate Gateways (Displayed in red)**") for more information.



Gateway Configuration [Hunterdon Hospital]

Description	IP Address	Channel No.	MAC Address	Firmware	Assigned Locks	Expanders	Status
BLUE = READY	172.16.201.16	10	00204A9DF16B	5.29	0	1	Ready
RED = Unreachable	172.16.200.196	15	00204ACE0C24	3.91	0	N/A	Unreachable
GREEN = Available	172.16.200.152	0	00204AED599D	4.48	0		Available

Discovering / Assigning Wireless Locks

After Gateways have been discovered and added to the Account, physical locks may now be discovered and assigned to the Gateways (or Expanders). More commonly, this is accomplished in two steps: First discovering the locks, then assigning them to the Gateway(s)/Expander(s).

Note: After lock discovery and lock assignment to a Gateway, locks are then "Linked" to Lock Profiles. Therefore, before proceeding, we recommend that you create Lock Profiles for each physical lock you wish to assign to a Gateway.

STOP If you plan to use Expanders, it is recommend to add the Expanders to the Gateway **before** discovering locks. Locks may receive stronger signals from an Expander and cannot be quickly moved from a Gateway to an Expander after assignment. Refer to page 34 for information regarding Expander discovery .

DISCOVERING LOCKS

The lock "discovery" process (search) can be performed in one of two ways:

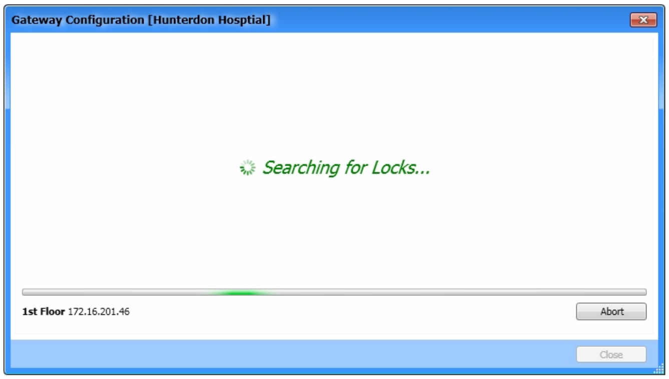
- In the **Gateway Configuration** screen, click to select the desired Gateway to which the installed lock will be assigned. Then in the **Number of Locks to Discover** pull-down, select the number of physical locks you wish to attempt to discover, then click **Discover Locks**. **Note:** The selected Gateway will transmit a discovery request radio signal. Only the locks that are close enough to receive the signal will respond. In addition, only locks that not yet been assigned to a Gateway (or Expander) will respond. By selecting the number of physical locks to be discovered, the discovery process will stop the instant the selected number of locks are found.

  The lock discovery procedure will then be carried out by each added expander (if applicable). **Note:** Lock discovery time increases by approximately 30 seconds with each added Expander.

  The discovery process may also be stopped at any time by clicking the **Abort** button (this will also return the list of locks found up until the time the **Abort** button was clicked).

- This second procedure is identical to the above procedure, except the lock discovery process is started using **Locks** > **Discover Locks**.

TIP For a lock to be considered "unassigned" to a Gateway, it must be manually reset ("defaulted"). See the programming instructions that came with the lock for the reset procedure.

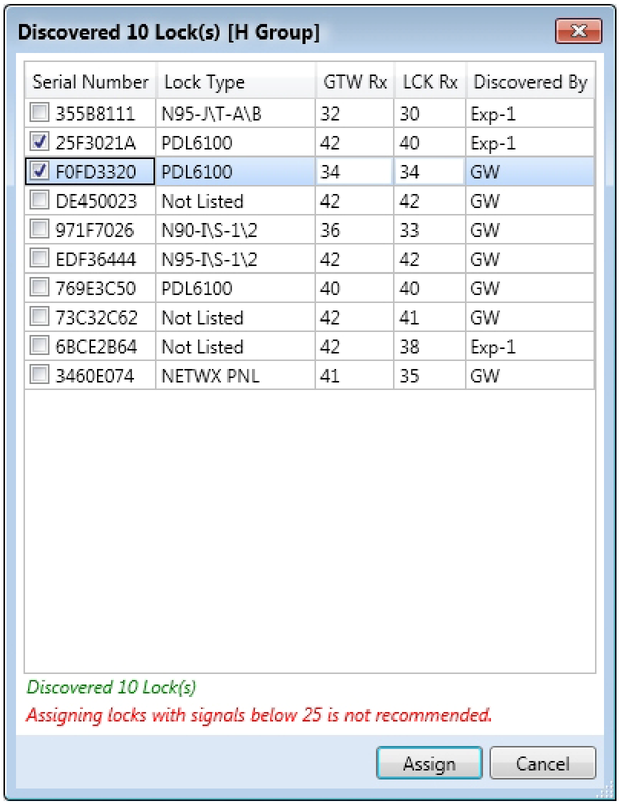

Gateway Configuration [Hunterdon Hosptial]

Searching for Locks...

1st Floor 172.16.201.46

ASSIGNING LOCKS

After locks are discovered, the following **Discovered Locks** popup automatically appears listing the successfully discovered locks for the selected Gateway:


Discovered 10 Lock(s) [H Group]

Serial Number	Lock Type	GTW Rx	LCK Rx	Discovered By
☐ 355B8111	N95-J\T-A\B	32	30	Exp-1
☑ 25F3021A	PDL6100	42	40	Exp-1
☑ F0FD3320	PDL6100	34	34	GW
☐ DE450023	Not Listed	42	42	GW
☐ 971F7026	N90-I\S-1\2	36	33	GW
☐ EDF36444	N95-I\S-1\2	42	42	GW
☐ 769E3C50	PDL6100	40	40	GW
☐ 73C32C62	Not Listed	42	41	GW
☐ 6BCE2B64	Not Listed	42	38	Exp-1
☐ 3460E074	NETWX PNL	41	35	GW

Discovered 10 Lock(s)

Assigning locks with signals below 25 is not recommended.

The discovered locks displayed in the screen above are those physical locks that were able to be discovered based on their range to the selected Gateway or Expander. (For more information about signal levels, see page 52 for definitions of GTW Rx and LCK Rx). The "Discovered By" column will display either "GW" (for Gateway) or "Exp-#" (for Expander number).

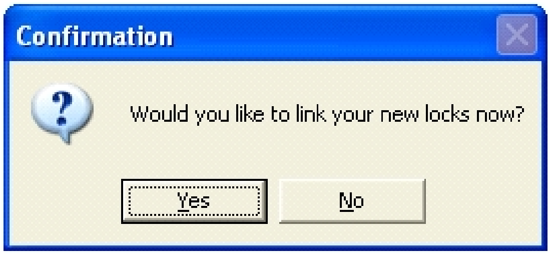
Click to add a check to the checkbox next to the serial number for each lock you wish to assign to the selected Gateway (or Expander), then click **Assign**. The following message appears as locks are assigned:

Assigning locks.. Please wait...

After locks are assigned to the selected Gateway (or

Discovering / Assigning Wireless Locks (cont'd)

Expander), the following popup appears to begin the required procedure of "Linking" the assigned locks to Lock Profiles. See the next section on page 17 for procedures.



Confirmation

Would you like to link your new locks now?

TIP If a lock(s) fails to be assigned to the Gateway, reattempt the lock assignment by clicking **Gateway** > **Send Config Table to the Gateway** or in the **Gateway Lock Table** click the "**Re-Configure Unassigned Locks**" button (see page 30).

MANUAL LOCK ASSIGNMENT

In the **Gateway Configuration** screen, click **Locks** > **Manually Add a Lock by Serial Number**. In the screen that appears, type the lock serial number and select the lock model from the **Lock Type** pull-down. **Note:** For version 2 Gateways, another pull-down ("**Assign To:**") is available allowing for adding a lock by serial number to an Expander. Then click **Add Lock**. This feature adds the lock(s) to the database; when finished adding locks, click **Gateways** > **Send Config Table to the Gateway**. All locks in the database will then attempt to be assigned to the Gateway (or Expander). For more information with using this feature, see page 21.

Linking Lock Profiles

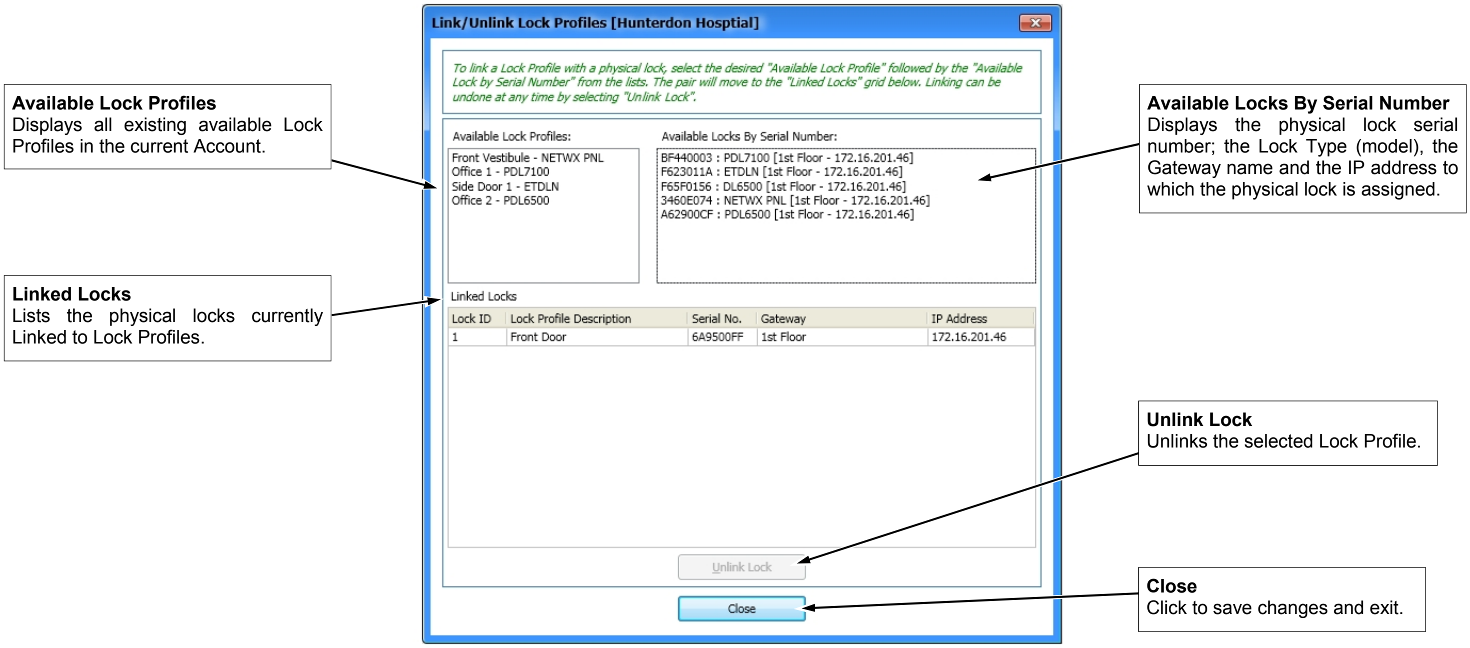
After physical locks are successfully assigned to the Gateway / Expander, they must be "Linked" to Lock Profiles (locks not Linked cannot be downloaded). In DL-Windows, the word "Link" is used to describe the specific action of associating a Lock Profile to the physical lock assigned to the Gateway / Expander (by serial number). The Lock Type (model) of the Lock Profile MUST match the assigned lock to which you wish to Link. The **Link/Unlink Lock Profiles** screen may be accessed in one of two ways:

- More commonly, the screen is accessed immediately following lock assignment (click **Yes** to confirmation popup shown on previous page);

or

- At a later time, from the DL-Windows "Main Screen", click **Locks** > **Link/Unlink Lock Profiles**.

Note: A condensed version of the screen may be accessed via the right-click options from the Lock Profile (right-click the Lock Profile and select "**Link/Unlink Lock Profile**"). See page 53 for more information.



Link/Unlink Lock Profiles [Hunterdon Hosptial]

To link a Lock Profile with a physical lock, select the desired "Available Lock Profile" followed by the "Available Lock by Serial Number" from the lists. The pair will move to the "Linked Locks" grid below. Linking can be undone at any time by selecting "Unlink Lock".

Available Lock Profiles:

Front Vestibule - NETWX PNL
Office 1 - PDL7100
Side Door 1 - ETDLN
Office 2 - PDL6500

Available Locks By Serial Number:

BF440003 : PDL7100 [1st Floor - 172.16.201.46]
F623011A : ETDLN [1st Floor - 172.16.201.46]
F65F0156 : DL6500 [1st Floor - 172.16.201.46]
3460E074 : NETWX PNL [1st Floor - 172.16.201.46]
A62900CF : PDL6500 [1st Floor - 172.16.201.46]

Linked Locks

Lock ID	Lock Profile Description	Serial No.	Gateway	IP Address
1	Front Door	6A9500FF	1st Floor	172.16.201.46

Available Lock Profiles
Displays all existing available Lock Profiles in the current Account.

Linked Locks
Lists the physical locks currently Linked to Lock Profiles.

Available Locks By Serial Number
Displays the physical lock serial number; the Lock Type (model), the Gateway name and the IP address to which the physical lock is assigned.

Unlink Lock
Unlinks the selected Lock Profile.

Close
Click to save changes and exit.

LINKING PROCEDURE

To Link a Lock Profile to an assigned lock, in the **Available Lock Profiles** field, click to select a Lock Profile, then in the **Available Locks By Serial Number** field, click the physical lock to which you want to Link. The pair will automatically move down to the **Linked Locks** grid at the bottom. **Note:** Since Lock Types (models) must match for successful Linking, when a Lock Profile is selected, the **Available Locks By Serial Number** field automatically filters and displays only matching Lock Types.

If an incorrect Linking was made, or if you wish to undo a Linking, simply select the Linked lock from the **Linked Locks** grid and click the **Unlink Lock** button (the Lock Profile and the available locks will return to their respective lists, and are thereafter available for Linking.

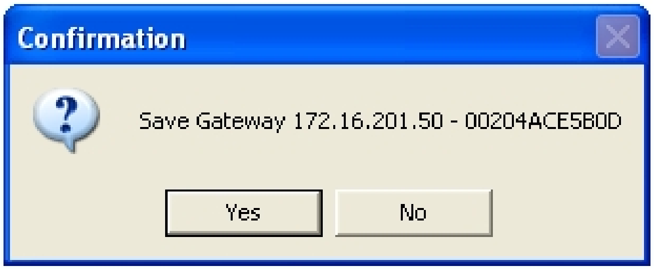
CONGRATULATIONS! Your locks have been Linked, and are now able to be downloaded with Lock Profile data. To add Users, Schedules, etc., see OI382.

Gateway Configuration > Gateways > Discover New Gateway(s)

In the **Gateway Configuration** screen, click **Gateways** > **Discover New Gateway(s)**. Upon selection, an attempt is made to discover all new Gateway devices on the network. Gateways that are not yet added and are therefore "**Available**" will be listed in the **Gateway Configuration** screen with the IP address highlighted in green. This option is used when using the two -step approach indicated in the **Discovering / Adding Gateways** section on page 14 of this manual. In addition, this option may be used to rebuild a database by importing an existing Gateway and its lock configuration data (see page 26, **Gateways** > **Import Gateway and Assigned Lock(s)**).

Gateway Configuration > Gateways > Add Gateway to Account

In the **Gateway Configuration** screen, after using the **Discover New Gateways** feature, select an "**Available**" Gateway, then click **Gateways** > **Add Gateway to Account**. A confirmation popup appears:



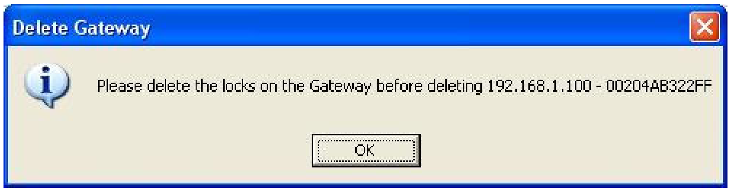
Confirmation

Save Gateway 172.16.201.50 - 00204ACE5B0D

Click **Yes** in the confirmation popup to complete the Gateway addition. **Note:** This action is used when adding newly discovered ("**Available**") Gateways to the Account (Gateway IP address highlighted in green). See page 14 for more information about **Discovering / Adding Gateways**.

Gateway Configuration > Gateways > Remove Gateway from Account

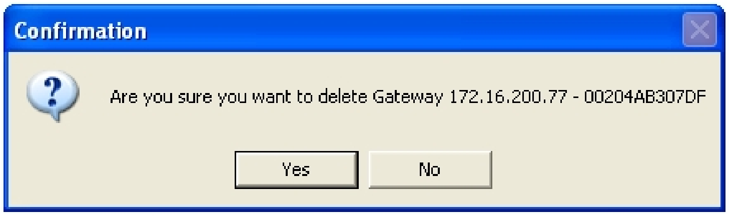
In the **Gateway Configuration** screen, click to highlight a specific Gateway in the list, then click **Gateways** > **Remove Gateway from Account**. Before the Gateway can be removed from the Account, *any locks already assigned to the selected Gateway must first be deleted ("un-assigned") from that Gateway*. If all locks have already been deleted from the Gateway, or if there are no locks assigned to the Gateway, upon selection, and after confirmation, the Gateway will be deleted from the Account. **Note:** In addition, if Expanders have been added to the Gateway, those Expanders must be removed in order to successfully remove the Gateway. For more information about removing Expanders, see page 35.



Delete Gateway

Please delete the locks on the Gateway before deleting 192.168.1.100 - 00204AB322FF

For more information regarding removing locks, see page 31.



Confirmation

Are you sure you want to delete Gateway 172.16.200.77 - 00204AB307DF

Confirmation Popup

Gateway Configuration > Gateways > Replace Gateway with New One

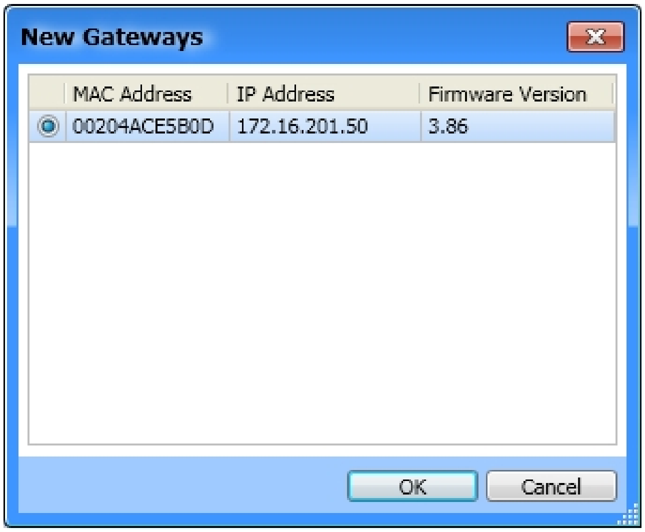
In the **Gateway Configuration** screen, click to highlight an "unreachable" (IP address highlighted red) Gateway in the list, then click **Gateways** > **Replace Gateway with New One**. Upon selection, the Gateway discovery process is started, and all newly discovered Gateways will be listed in the **New Gateways** screen. Select the desired Gateway from the list, then click **OK**. All existing Gateway configuration data (radio channel, security data, etc.) and the replaced Gateway's Lock Table (existing assigned locks) will be sent to (and used by) the new Gateway. **Note:** Functional Gateways (Status = **Ready**; IP address highlighted blue) may also be replaced, if desired.

This option is typically used when a working Gateway (discovered on the network, added to an Account and operational with physical locks assigned) becomes faulty and needs to be physically replaced.

Before replacing the Gateway, be sure to check the network and the Gateway connections outlined in the **Gateways**, **Relocate Gateways (Displayed in red)** on page 28.

Physically replace the Gateway device: Disconnect the power wires and the RJ-45 plug from the old device, then reconnect all wires to the new device. Remember to press the "**RESET**" button on the new Gateway PC board to clear the Gateway memory (see the instructions in WI2085 for resetting the Gateway).

In the **Gateway Configuration** screen, click to select the Gateway you wish to replace. Then click **Gateways** > **Replace Gateway with New One**. The following screen appears showing newly discovered Gateways:



	MAC Address	IP Address	Firmware Version
●	00204ACE5B0D	172.16.201.50	3.86

Click the radio button to select the desired Gateway and click **OK**. DL-Windows will automatically replace the old Gateway with the new Gateway, copying the Gateway configuration data (radio channel, security data, etc.) and existing assigned locks into the new Gateway.

Version 2 Gateway Replacement Considerations

The following should be considered when using version 2 Gateways:

- Older "version 1" Gateways can be replaced by version 2 Gateways (and vice versa)
- When replacing a version 2 Gateway, it is vital to ensure the "Expander Group" dials of the new Gateway are set identically to the Gateway being replaced
- If the Gateway being replaced has Expanders, upon replacement the Expander Configuration Table (Routing Table) will be transferred into the new Gateway (along with other configuration data such as radio channel, security data, etc.)
  - See page 35 for more information about Expander Routing Table

USB Gateway Replacement Considerations

- Networx Gateways ("version 1" or "version 2") *cannot* be replaced with a USB Gateway (model AL-IME-USB)
- A USB Gateway **can** be replaced by a Networx Gateway
- If you wish to replace a USB Gateway with a new USB Gateway, do not use this "**Gateways** > **Replace Gateway with New One**" feature. Instead, see OI386 for complete step by step instructions.

Gateway Configuration > Gateways > View Gateway Status

In the **Gateway Configuration** screen, click to highlight a specific Gateway in the list, then click **Gateways** > **View Gateway Status**. Upon selection, the **Gateway Status** is retrieved and displays the operational status of the selected Gateway. In addition, if Expanders have been added to the Gateway, their status will also be retrieved and displayed. **Note:** This screen appears automatically after updating Gateway or Expander firmware.

Description
Displays the text of the **Description** field from the **Gateway Configuration** screen. Default = "New Gateway".

IP Address
Displays the network address currently assigned to the Gateway.

Firmware Version
Displays the current firmware edition (or "release") the Gateway is running.

Firmware Update
Indicates the result of the last Gateway firmware upgrade process. "Good" signifies that the last firmware upgrade was completed without errors. "Bad" signifies the last firmware upgrade was completed unsuccessfully. See **Gateways** > **Update Gateway Firmware** on page 21 for more information.

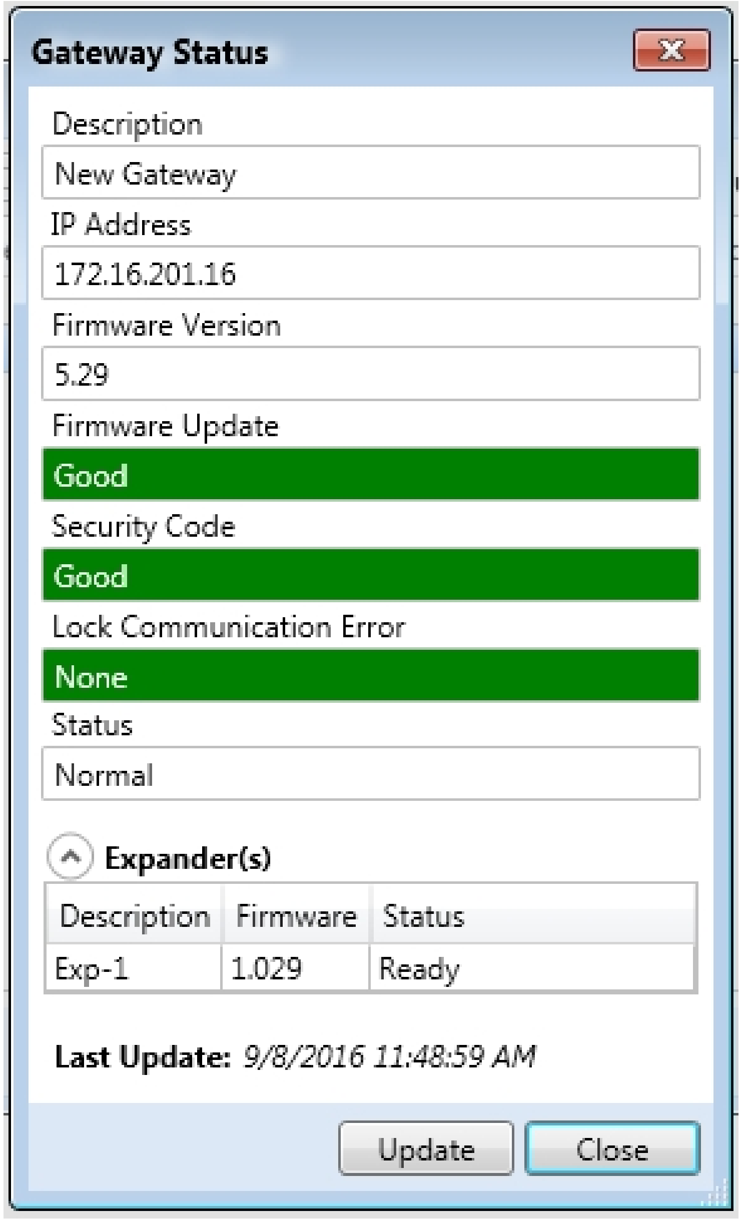
Security Code ("Security Password")
Indicates the status of the Security Password by comparing the Security Password in the Gateway with the Security Password in DL-Windows. If Passwords are not identical, the field indicates "Security Mismatch", thus disabling DL-Windows-to-Gateway communications.

Lock Communication Error
Indicates if locks assigned to the selected Gateway previously failed to communicate with that Gateway.
If "**Communication Error**" appears in this field, a lock communication failure was detected. Click **Locks** > **View Gateway's Lock Table** to determine which lock failed to communicate.

Status
Displays the current state (or condition) of the Gateway. Indicates status such as "**Normal**" to indicate a normal condition; "**Emergency Lock Down**" if an Emergency Lock Down Command was sent; and "**Emergency Passage**" if an Emergency Passage Command was sent.

Expander(s) (table not displayed for non-version 2 Gateways)
This table displays the **Description**, **Firmware** version and latest **Status** of the Expanders added to the selected Gateway. Each time the Gateway status is updated, this table is also refreshed.

Last Updated
Displays the date and time of the latest Gateway status update (the last time the **Gateway Status** was retrieved).



Description: New Gateway
IP Address: 172.16.201.16
Firmware Version: 5.29
Firmware Update: Good
Security Code: Good
Lock Communication Error: None
Status: Normal

Expander(s)

Description	Firmware	Status
Exp-1	1.029	Ready

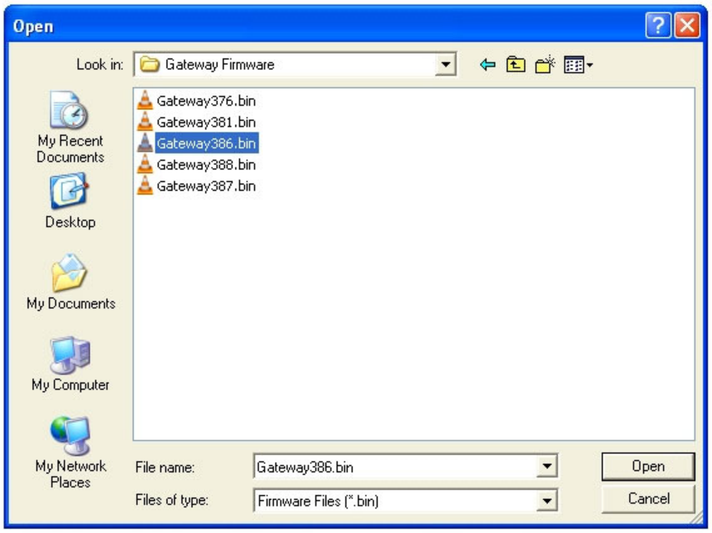
Last Update: *9/8/2016 11:48:59 AM*

Update (button)
Click to request an updated Gateway / Expander status from the Gateway. All fields will be refreshed upon Gateway status retrieval.

Gateway Configuration > Gateways > Update Gateway Firmware

In the **Gateway Configuration** screen, click to highlight a specific Gateway in the list, then click **Gateways** > **Update Gateway Firmware**.

Upon selection, the standard Windows **Open** dialog box appears (shown at right), allowing you to browse for the binary ".bin" file containing the Gateway firmware.



Open

Look in: Gateway Firmware

Gateway376.bin
Gateway381.bin
Gateway386.bin
Gateway388.bin
Gateway387.bin

File name: Gateway386.bin

Files of type: Firmware Files (*.bin)

Select Gateway firmware file, then click **Open** to initiate the update process.

The system will check the integrity of the firmware, burn it into the Gateway memory, reboot the Gateway and verify if the Gateway is functioning properly. Upon completion, a **Gateway Status** screen will automatically open. Verify that the **Firmware Update** field is green, reads "**Good**", and the Gateway firmware version has been updated in the **Firmware Version** field.

Gateway Configuration > Gateways > Send Config Table to the Gateway

In the **Gateway Configuration** screen, click **Gateways** > **Send Config Table to the Gateway**. Upon selection, the Gateway (and Expander) will be updated with the latest configuration data and will attempt to assign locks (if necessary).

In DL-Windows, the word "**configure**" has a specific meaning--to "configure" is to "assign" discovered physical locks to a Gateway, thus ensuring a fixed wireless communication channel exists between selected physical locks and a selected Gateway.

The Gateway sends "configuration data" in the form of a "Lock Configuration Table" to the selected locks. This "configuration data" contains items (an internal lock designation, a specific radio channel and security data) that are all embedded in the "Lock Configuration Table". The "configuration data" then instructs the physical lock(s) to communicate ONLY with that Gateway, thus preventing other Gateways from communicating with the physical lock(s).

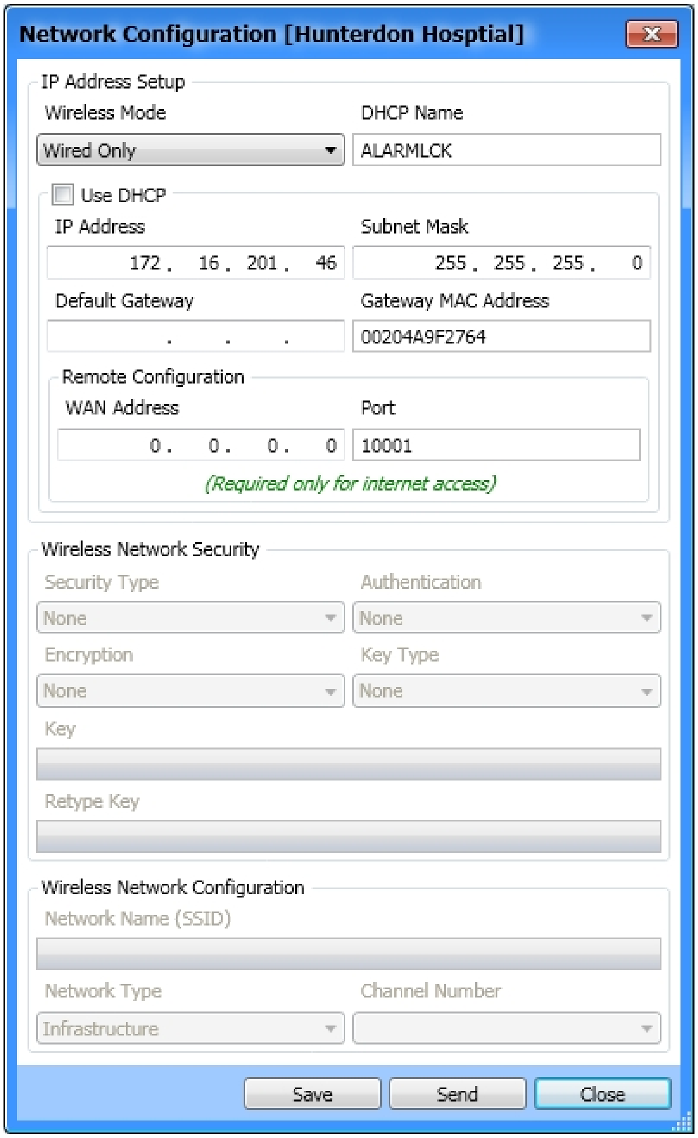
Although other applications exist, the three most common uses for sending the Lock Configuration Table to a Gateway are:

- **Assignment Retry** - Lock was successfully discovered, but was unable to be assigned to the Gateway.
- **Completing Manual Lock Addition** - Requirement after manually assigning locks to the Gateway database.
- **Security Mismatch** - "**Gateway Configuration Data**" area elements do not match those elements within the DL-Windows database.

Note: If Expanders have been added to the Gateway, the "Lock Configuration Table" will be sent to each Expander. Thus, the applications also apply to Expanders.

Gateway Configuration > Gateways > Configure / Edit Network Settings

In the **Gateway Configuration** screen, click to highlight a specific Gateway in the list, then click **Gateways** > **Configure / Edit Network Settings**. Upon selection, the **Network Configuration** screen will open, allowing for Gateway network settings to be configured or edited. This screen is typically used to configure the Gateway with a static IP address, configure for "Internet Gateway Connectivity" (**Remote Configuration** settings) and/or wireless Gateway configuration. **Important:** For more information about configuring your Gateway with a static IP address, "Internet Gateway Connectivity" (**Remote Configuration** settings), and/or **Wireless Network Configuration**, see WI2085.
The following is a brief description of each field as it applies to DL-Windows; see your network administrator for more information if needed.



Network Configuration [Hunterdon Hosptial]

IP Address Setup

Wireless Mode: Wired Only

DHCP Name: ALARMLCK

□ Use DHCP

IP Address: 172 . 16 . 201 . 46

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: . . .

Gateway MAC Address: 00204A9F2764

Remote Configuration

WAN Address: 0 . 0 . 0 . 0

Port: 10001

(Required only for internet access)

Wireless Network Security

Security Type: None

Authentication: None

Encryption: None

Key Type: None

Key:

Retype Key:

Wireless Network Configuration

Network Name (SSID):

Network Type: Infrastructure

Channel Number:

IP Address Setup

Wireless Mode
Configures the selected Gateway for either wireless or wired communication with the computer network. Select either **Wired Only** or **Wireless Only** from this pull-down menu. If **Wireless Only** is selected, the **Wireless Network Security** area and the **Wireless Network Configuration** area both become active and available for selection.

DHCP Name
To aid in locating the Gateway on the network, specify a name to describe the domain name and hostname of the corresponding IP address assigned to the selected Gateway. The **DHCP Name** entered here will be used for the DNS configuration (default = **ALARMLCK**).

Use DHCP (checkbox)
Use DHCP (Dynamic Host Configuration Protocol) is checked (enabled) by default. When checked, DL-Windows allows the selected Gateway to accept the dynamic assignment of an IP address by the TCP/IP network. *Note that Emergency Commands may **NOT** function properly using DHCP*. Uncheck **Use DHCP** to allow the manual assignment of a static IP address to the selected Gateway (a warning popup appears that the Gateway may be unreachable until it is installed on the correct network). The **IP Address**, **Subnet Mask** and **Default Gateway** fields become active. Un-checking **Use DHCP** also activates the fields in the **Remote Configuration** area for "**Internet Gateway Connectivity**" support (though not required unless using for Internet access).

IP Address
This field allows the (static) IP address to be manually assigned to the selected Gateway.

Subnet Mask
The IP protocol makes use of a Subnet Mask to more efficiently route packets to their correct network destinations.

Default Gateway
This field is the IP address of the physical device, such as a router, for the current subnet to which you want to be connected. *This field is **not** to be confused with the IP address of the Alarm Lock Gateway device installed in the system.*

Gateway MAC Address
This field represents the unique 12-digit MAC Address of the Gateway. This field cannot be edited or changed.

WAN Address (**Remote Configuration** area)
This field allows DL-Windows to communicate with a Gateway over a Wide Area Network (Internet).

Port (**Remote Configuration** area)
Default = 10001. Identifies the default Gateway communication port setting.

Wireless Network Security

Security Type
Click the pull-down menu to specify the 802.11 security protocol (encryption method) to be used when the selected Gateway is connected to the wireless network. The selections are:

- **WEP** (Wired Equivalent Privacy) The WEP encryption method was designed to provide wireless networks with the "equivalent" security available in traditional wired "landline" networks.
- **WPA** (Wi-Fi Protected Access) A security protocol from the Wi -Fi alliance for 802.11 wireless networks. It uses the Temporal Key Integrity Protocol (TKIP) to provide stronger encryption than the earlier WEP (Wired Equivalent Privacy) method. Derived from, and a subset of, the IEEE 802.11i security standard, WPA includes 802.1x authentication.
- **WPA2** (Wi-Fi Protected Access 2) Supports additional security features of the IEEE 802.11i standard that are not already included in the WPA security protocol.

Note: For each Security Type selected, different choices appear for the other fields in the **Wireless Network Security** area of this screen.

Authentication
Click the pull-down menu to specify the 802.11 authentication protocol to be used when the selected Gateway is connected to the wireless network. When **WEP Security Type** is selected, the options for the selected Gateway are:

- **Open/None**: Requires no Authentication for the data transmissions between the selected Gateway and the router.
- **Shared**: Requires a shared symmetric code (encryption "key") for all data transmissions between the router and the Gateway.

When **WPA** or **WPA2 Security Type** is selected, the option is:

- **Pre-Shared Key (PSK)**: Allows the use of manually-entered keys or passwords (encryption "key") to initiate WPA security.

Encryption
The reversible transformation of data from its original format into a concealed format as a process for securing its accessibility, authenticity and integrity. Encryption uses an encryption algorithm (sequence) and one or more encryption keys (numeric codes).
When **WEP Security Type** is selected, the options for the selected Gateway are:

- **64 bits**: Although the 64-bit WEP data encryption method uses a five-character key size (forty bits or five bytes) for symmetric encryption, plus an additional 24 factory-set bits, this method represents a relatively low level of security.
- **128 bits**: Stronger than 64-bit WEP, 128-bit WEP uses a string of 26 hexadecimal characters (0-9 and A-F), each representing four bits of the key.

When **WPA Security Type** is selected, the option for the selected Gateway is:

- **TKIP**: (Temporal Key Integrity Protocol), a security protocol algorithm that compliments WPA encryption with increased security measures such as extended key lengths and data integrity checks.

When **WPA2 Security Type** is selected, the options for the selected Gateway are:

- **CCMP**: (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) improves upon both WPA and TKIP. CCMP is a required option for Robust Security Network (RSN) compliant networks.
- **TKIP**: See above.

Key Type
A "key" is a numeric code used to encrypt data, and is used to secure the data traffic between the router and the Gateways. The key "type" can be "**Passphrase**" or "**Hex**" (a hexadecimal string, for example, '45D3 E454 3523 EDC2'). To ease encryption key entry, a password or passphrase can be entered instead of the cryptic hexadecimal characters.

Key
Retype Key
Type your key in the **Key** field, and re-type in the **Retype Key** field to confirm it. Maximum character entry dependant upon selections made above.

Wireless Network Configuration

Network Name (SSID)
This field allows you to specify the SSID (Service Set IDentifier) name assigned to the wireless Wi-Fi (802.11) network. Wireless Gateway models in a system must use this name to allow for network communication. **Note:** This field is case-sensitive and can be up to 32 bytes in length.

Network Type
Click the pull-down menu to select the network communication mode. With "**Infrastructure**" selected, the Gateways communicate to a wired LAN via access points. With "**Ad Hoc**" selected, the Gateways can communicate directly in a peer-to-peer fashion.

Channel Number
Click the pull-down menu to manually specify the number (1 - 11) of the carrier frequency (subchannel pathway) between the selected Gateway and the wireless Wi-Fi (802.11) network.

Save (button)
Click to record all network configuration data to the database. Use this option when connection to the Gateway failed due to incorrect network configuration entry. **Note:** Network configuration data will **NOT** be sent to the Gateway.

Send (button)
Click to save all network configuration data to the database and send all network configuration data to the Gateway.

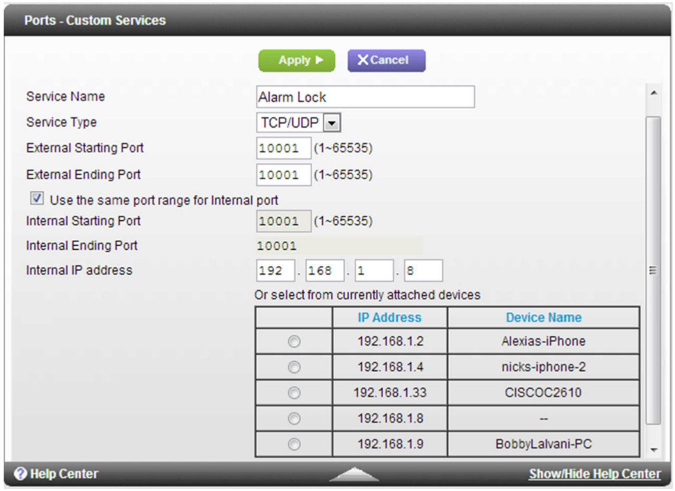
Close (button)
Click "**X**" or the **Close** button to exit the screen without saving changes.

Setting Up a Remote Gateway

Remote Gateway Set Up Scenario 1

For remote connectivity only: Use these steps when DL-Windows will NOT be used or installed where the Networx Gateway is installed.

1. Discover and add Gateway locally.
2. Set the static IP information for the **remote** location, the WAN address (router Internet address) and port number. Can use the default port number 10001 for the first Gateway installed.
3. Disconnect - Send to Remote Location.
4. At the **remote** location, configure router: Set In/Out Port (must be the same) for the static IP address. **Note:** You will likely need to find the setting and disable "Block anonymous Internet requests".
5. Plug in Gateway. May need to close and re-open the **Gateway Configuration** screen.



Service Name	Alarm Lock
Service Type	TCP/UDP
External Starting Port	10001 (1~65535)
External Ending Port	10001 (1~65535)
☑ Use the same port range for Internal port	
Internal Starting Port	10001 (1~65535)
Internal Ending Port	10001
Internal IP address	192 . 168 . 1 . 8

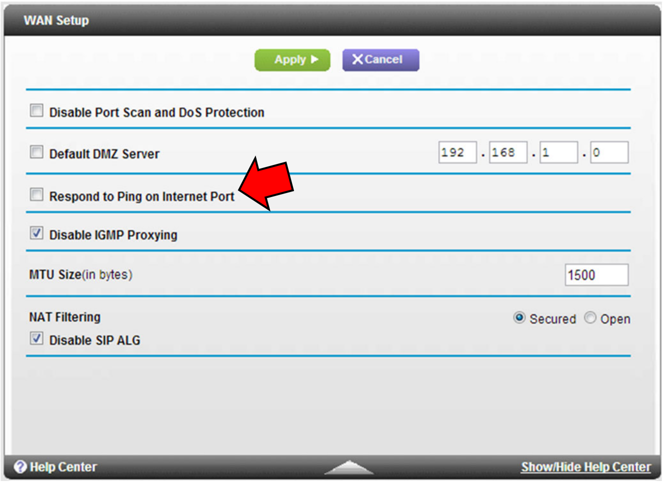
Or select from currently attached devices

	IP Address	Device Name
○	192.168.1.2	Alexias-iPhone
○	192.168.1.4	nicks-iphone-2
○	192.168.1.33	CISCOC2610
○	192.168.1.8	--
○	192.168.1.9	BobbyLalvani-PC

Remote Gateway Set Up Scenario 2

Use these steps for remote and local connectivity (e.g., for laptop use).

1. Discover and add the Gateway locally.
2. Set the static IP address information (**Local** location), the WAN address (router Internet address), and port number. You can use the default port number 10001 for the first Gateway installed.
3. At **local** location, configure router: Set In/Out Port (must be the same) for the static IP address.
   Note: You will likely need to find the setting and disable "Block anonymous Internet requests". When the connection cannot be made locally, connection to the WAN address will be attempted and the connection will be made over the Internet (and vice versa)



□ Disable Port Scan and DoS Protection

□ Default DMZ Server 192 . 168 . 1 . 0

□ Respond to Ping on Internet Port

☑ Disable IGMP Proxying

MTU Size(in bytes) 1500

NAT Filtering ● Secured ○ Open

☑ Disable SIP ALG

Remote Gateway Set Up Scenario 3

Use this scenario when installing two instances of DL-Windows in order to facilitate setup. For example, where User 1 installs DL-Windows where the router is installed, in order to configure the system, and User 2 will always be connecting remotely.

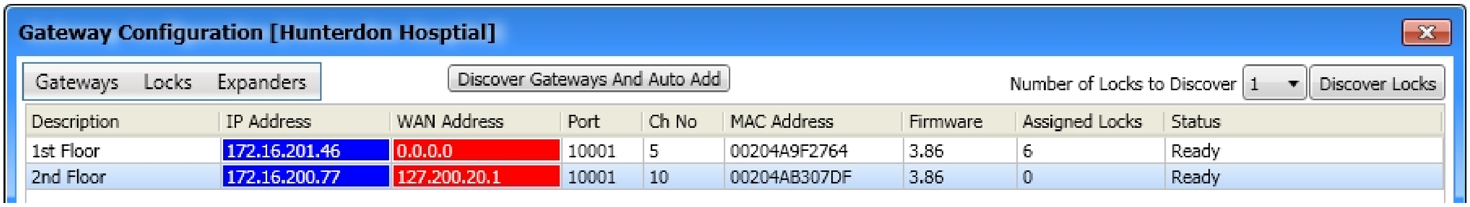
1. User 1 installs DL-Windows, Discovers and adds Networx Gateway.
2. Set the static IP address information for the User 1 location.
3. **Important:** Remove Gateway from the DL-Windows Account.
4. At User 1 location, configure the router: Set In/Out Port (must be the same) for the static IP address. **Note:** You will likely need to find the setting and disable "Block anonymous Internet requests".
5. User 2 installs DL-Windows (if not installed already).
6. User 2 *Manually adds the Networx Gateway* to the DL-Windows Account. Enters the MAC address, the WAN address (User 1 router Internet address) and Port information. Be sure to save entered information to the DL-Windows database. The connection will be made automatically.

Gateway Configuration > Gateways > Ping Gateway

In the **Gateway Configuration** screen, click **Gateways** > **Ping Gateway**. Upon selection, a **Ping** (**P**acket **IN**ternet **G**roper) command will test whether the IP address of the Gateway is reachable on the network. Ping sends a packet out on the network and waits for a response; the result of the ping is indicated by a splash screen on the DL-Windows "Main Screen". A successful test displays the IP address of the Gateway with the word "**found**"; an unsuccessful test displays the IP address of the Gateway with the words "**not found**".

Gateway Configuration > Gateways > Show WAN / Port Information

In the **Gateway Configuration** screen, click **Gateways** > **Show WAN / Port Information**. This feature expands the **Gateway Configuration** screen to show the **WAN Address** column and **Port** column. To collapse these columns, click **Gateways** > **Hide WAN / Port Information**.


Gateway Configuration [Hunterdon Hosptial]
Gateways
Locks
Expanders
Discover Gateways And Auto Add
Number of Locks to Discover
1
Discover Locks

Description	IP Address	WAN Address	Port	Ch No	MAC Address	Firmware	Assigned Locks	Status
1st Floor	172.16.201.46	0.0.0.0	10001	5	00204A9F2764	3.86	6	Ready
2nd Floor	172.16.200.77	127.200.20.1	10001	10	00204AB307DF	3.86	0	Ready

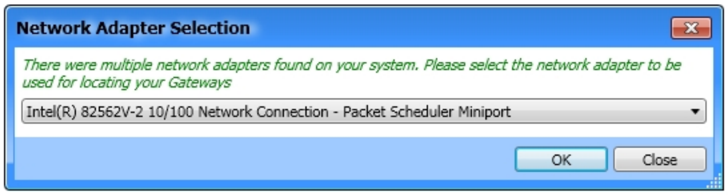
When using the "**Internet Gateway Connectivity**" support features (connection to the Gateway is made remotely over the Internet), the **WAN** (Wide Area Network) **Address** and Gateway **Port** setting are required. These **Remote Configuration** settings, previously set in the **Network Configuration** screen, are not automatically displayed in the **Gateway Configuration** screen. Therefore you must click **Gateways** > **Show WAN / Port Information** to view your connection status. See **Color Definitions** on page 14 for more information about Gateway connection conditions. For more information about setting the "**Internet Gateway Connectivity**" support features, see "**Configure / Edit Network Settings** on page 22 and WI2085.

Gateway Configuration > Gateways > Select Network Adapter

In the **Gateway Configuration** screen, click **Gateways** > **Select Network Adapter**. This feature may also be accessed from the DL-Windows "Main Screen", click **Tools** > **Select Network Adapter**. **Note:** If only one network adapter is detected, these options will be unavailable.

The **Network Adapter Selection** screen allows you to identify and select the "network interface card" (NIC) you are using inside your computer to communicate with the Gateway devices in your system. Some computers have the network adapter built into the motherboard, thus precluding the need to make a selection (network adapter is automatically detected). Other computers may use external network adapters (i.e. a USB network adapter). When both are a present, the **Network Adapter Selection** screen may automatically appear when opening the **Gateway Configuration** screen, thus requiring the selection of the desired network adapter. Remember, the router or corporate Ethernet network is connected to an Ethernet adapter with an Ethernet cable (RJ-45 plug).

Network Adapter Selection
Click the pull-down menu to select the network card used by the computer.
Click **OK** to save the selection or **Cancel** to exit without saving. **Note:** Clicking **OK** in this screen saves the selection *only for the duration of the current DL-Windows session*. Quitting and restarting DL-Windows may require re-opening this screen and re-selecting the network adapter. **Note:** If the network adapter settings change when the DL-Windows program is running, DL-Windows may require you to close and re-open the program.



There were multiple network adapters found on your system. Please select the network adapter to be used for locating your Gateways

Intel(R) 82562V-2 10/100 Network Connection - Packet Scheduler Miniport

Gateway Configuration > Gateways > Set Gateway Groups

In the **Gateway Configuration** screen, click **Gateways** > **Set Gateway Groups**.
For information about setting Emergency Grouping, see the section "**Using Emergency Commands**" on page 44.

Gateway Configuration > Gateways > Import Gateway and Assigned Lock(s)

In the **Gateway Configuration** screen, after using the **Discover New Gateways** feature, select an "**Available**" Gateway, then click **Gateways** > **Import Gateway and Assigned Lock(s)**. This feature is used to rebuild a DL-Windows database by importing existing Gateway, Expander (if applicable) and lock configuration data.

When the Account information stored in DL-Windows is lost (such as with a stolen laptop)--AND--the DL-Windows back-up files are either non-existent, inadequate or lost, the above "Import" option can be used.

Once you have successfully re-created pertinent data (Accounts, Lock Profiles, Global Users, etc.), the following steps may be used to recreate your wireless system. **Note:** To successfully restore your wireless system, you MUST know the existing Security Password previously set for the Gateway and locks.

1. In the DL-Windows "Main Screen", click **Tools** > **Set Security Password**.
2. Type the Security Password that was previously set for the Gateway and locks you wish to import (see page 12 for more information regarding Security Passwords).
3. Click the **Gateway Config** icon to open the **Gateway Configuration** screen.
4. Click **Gateways** > **Discover New Gateway(s)**. The Gateway(s) appear in the **Gateway Configuration** screen (IP address highlighted in green color; Status = "**Available**").
   IMPORTANT: Do NOT select **Gateways** > **Add Gateway to Account**.
5. Click to highlight the Gateway you wish to import from the list.
6. Click **Gateways** > **Import Gateway and Assigned Lock(s)**.

The Gateway will be added to the system; the Expander Config Table (if applicable) and the Lock Configuration Table will be imported and written into the DL-Windows database.

Gateway Configuration > Gateways > Manually Add a Gateway

In the **Gateway Configuration** screen, click **Gateways** > **Manually Add a Gateway**. Upon selection, the **Manual Gateway Addition** screen opens, where you can *manually* add a Gateway by adding its unique MAC address.
This screen is typically used to add a Gateway to an Account without needing to perform the Gateway discovery process. Manually type the unique MAC address of the Gateway in the **Gateway MAC Address** field, then click **Save**. The Gateway MAC address will be saved to the database and added to the Account, and a connection to the Gateway will be attempted. If the Gateway connection is established successfully, the IP address will be highlighted blue (if unsuccessful, it will be highlighted red). When manually adding a Gateway to an Account, keep in mind the following:

- The Gateway you wish to manually add to the Account must be on the network and "**Available**" (dynamically obtained IP address and manually reset). See WI2085 for more information.

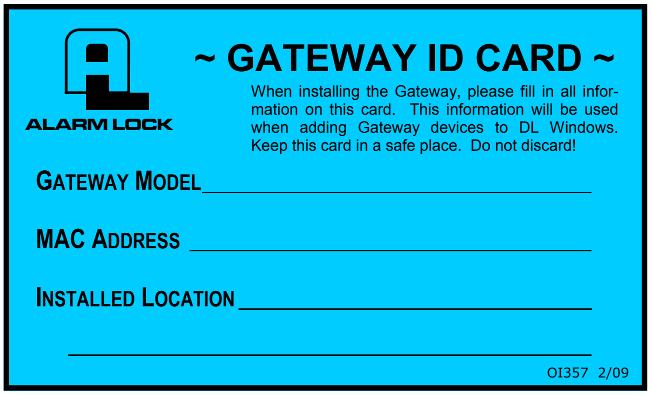
> **TIP** For a Gateway to be considered "**Available**", it must be on the network, have a dynamically obtained IP address, and manually reset (see WI2085 for reset Gateway procedures). A Gateway may also be considered "**Available**" if it already contains the same Security Password as the Security Password set for the Account. See section **Gateways > Import Gateway and Assigned Lock(s)** for more information.

- The Gateway must be successfully saved and added to the Account before configuring a static IP address or wireless settings.
- When using the "**Internet Gateway Connectivity**" feature, uncheck **Use DHCP** and type the required **Remote Configuration** settings (**WAN Address** and **Port**). See WI2085.

Gateway MAC Address
Carefully type the Gateway's unique 12-character factory MAC Address located on the square sticker under the bar code. Each Networx Gateway is identified in DL-Windows by this unique number. Type all characters of the MAC Address, **do not include dashes or spaces**. **Note:** The **Save** button will be enabled after 12 characters are typed.

Save (button)
Click to manually add the Gateway into the DL-Windows database. A connection will be attempted and if successful, the Gateway will be ready for use.

> **TIP** We recommend that when installing a Gateway, a blue-colored "**GATEWAY ID CARD**" (see image below) be completed. These blue cards are a useful way to organize Gateway information, including the MAC Address and physical location of the Gateway.



ALARM LOCK

~ GATEWAY ID CARD ~

When installing the Gateway, please fill in all information on this card. This information will be used when adding Gateway devices to DL Windows. Keep this card in a safe place. Do not discard!

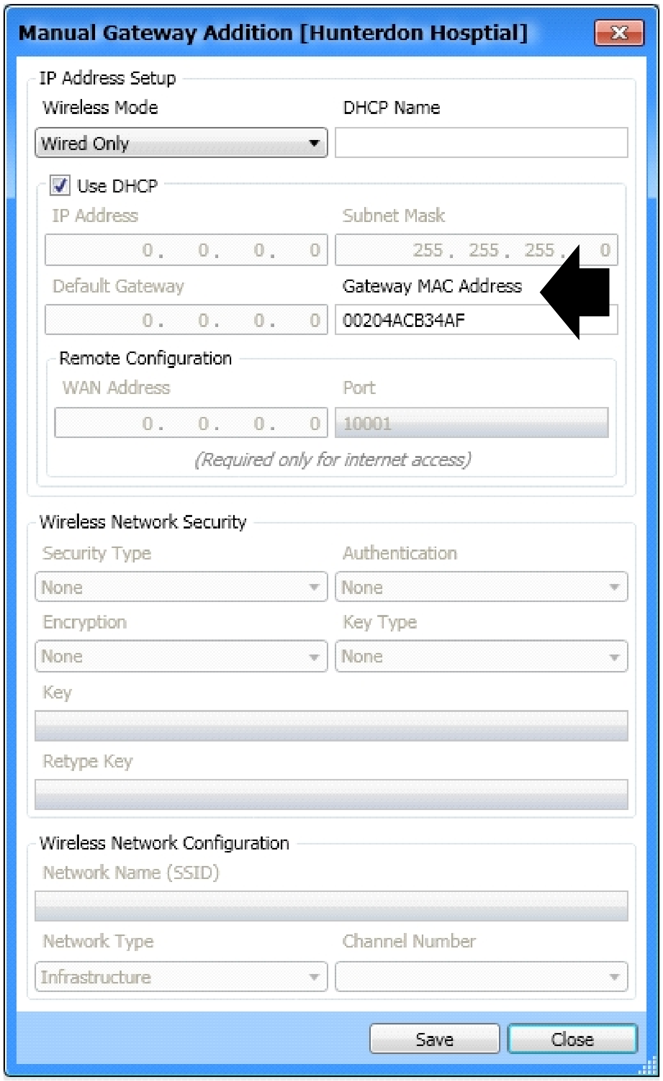
GATEWAY MODEL______________________

MAC ADDRESS ______________________

INSTALLED LOCATION ______________________

____

OI357 2/09



Manual Gateway Addition [Hunterdon Hosptial]

IP Address Setup

Wireless Mode: Wired Only

DHCP Name:

☑ Use DHCP

IP Address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 0 . 0 . 0 . 0

Gateway MAC Address: 00204ACB34AF

Remote Configuration

WAN Address: 0 . 0 . 0 . 0

Port: 10001

(Required only for internet access)

Wireless Network Security

Security Type: None

Authentication: None

Encryption: None

Key Type: None

Key:

Retype Key:

Wireless Network Configuration

Network Name (SSID):

Network Type: Infrastructure

Channel Number:

Gateway Configuration > Gateways > Relocate Gateways (Displayed in red)

In the **Gateway Configuration** screen, click **Gateways** > **Relocate Gateways (Displayed in red)**. Upon selection, an attempt is made to "relocate" (re-establish a connection) with all of the Gateways that have their IP addresses highlighted in ***red*** (Status = "**Unreachable**"). **Note:** If Status = "**Security Mismatch**", see **TIP** below.

A configured Gateway (discovered on the network, added to an Account and operational) is listed in the **Gateway Configuration** screen with its IP address highlighted ***blue*** (Status = "**Ready**"). When a configured Gateway has subsequently lost communication with the network and the **Gateway Configuration** screen is opened, the Gateways IP address will be highlighted ***red*** (Status = "**Unreachable**").

If a Gateway(s) is unreachable with its IP address highlighted ***red***, by clicking **Gateways** > **Relocate Gateways (Displayed in red)**, an attempt is made to re-connect with that Gateway(s).

If a Gateway IP address is highlighted in red, and therefore a connection could not be established, try the following:

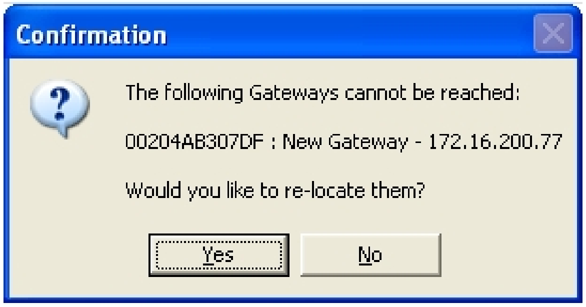
1. **Check the network.** Re-fresh the **Gateway Configuration** screen (by closing and re-opening the screen). If other Gateways exist in the Account and are listed highlighted in blue, this indicates that part of the network is still operational. You may need to contact your network administrator to assist in finding the source of the network problem.

2. **Check your physical connections to the Gateway.**
   - The RJ-45 socket on the Gateway contains two LEDs; the green LED should be lit continually when the RJ-45 plug is inserted and properly connected. The yellow LED flickers when data is being send to or from the Gateway. If these two LEDs are not functioning, you can suspect the problem lies with the RJ-45 cable or the network. Try replacing the RJ-45 cable. **Note:** Both LEDs are **not** lit when the Gateway is configured for wireless (802.11) use.
   - If the RJ-45 socket LEDs are operational, remove the Gateway housing cover, power down and power up the Gateway by removing and replacing the power wires at the Gateway power terminals.

3. **Check your network configuration settings.** Click **Gateways** > **Configure / Edit Network Settings**. Edit any fields that may be incorrect. Click **Save** to save the changes to the database.

4. **Replace the Gateway.** If the network and the physical connections are found to be in working order, the Gateway device itself may need to be replaced. Open the Gateway housing cover on the new Gateway device (it may be helpful to make note of the new Gateway's MAC Address located on a square sticker (the MAC Address is located under the bar code and has 12 digits, grouped in 6 pairs separated by dashes). Disconnect the power wires and the RJ-45 plug from the old Gateway and reconnect all wires to the new Gateway. Continue with the **Gateways** > **Replace Gateway with New One** procedures on page 19.

Note: Upon opening the **Gateway Configuration** screen, connection to each configured Gateway is verified before proceeding. If the Gateway cannot be reached, the following message is displayed providing the option to relocate the Gateway.



The following Gateways cannot be reached:

00204AB307DF : New Gateway - 172.16.200.77

Would you like to re-locate them?

TIP If the Status = "**Security Mismatch**", the Security Password in the Gateway does not match the Security Password in DL-Windows. Try manually resetting the Gateway (partial reset) then click **Gateways > Send Config Table to the Gateway**. See the instructions in WI2085 for resetting the Gateway.

Gateway Configuration > Gateways > Signal Test Mode

In the **Gateway Configuration** screen, click to highlight a specific Gateway in the list, then click **Gateways** > **Signal Test Mode**. Upon selection, the **Gateway Signal Test** screen opens (shown below) where you can set the duration of time (minutes) the Gateway (or Expander) will continuously generate a signal to the **AL-NSM** ***Networx Signal Meter*** (required). For new and existing installations, this option is used to perform a site survey test of the premises to help you find the optimum location for Gateways relative to the door locks or Gateways relative to Expanders. This helps to determine the optimum number of Gateways or Expanders needed to cover the number of locks you plan to install. **IMPORTANT**: This feature will only operate with Gateway firmware version 3.88 or later.

Test time in minutes

Click the pull-down menu to select the time (in minutes) the Gateway will generate a signal to the AL-NSM (Networx Signal Meter). 1 - 30 minutes can be selected (default is 30 minutes).

Send To: (not shown for non-version 2 Gateways)

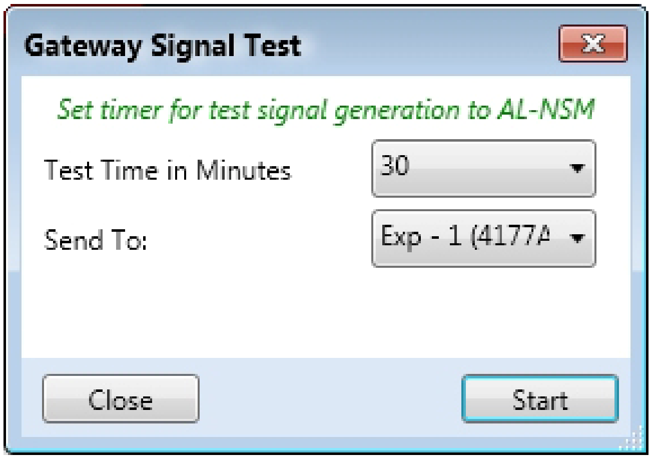
From this pull-down list, select the Gateway or Expander to generate a signal to the **AL-NSM** ***Networx Signal Meter***.

Start (button)

Click to initiate the test signal generation from the selected Gateway or Expander to the AL-NSM (Networx Signal Meter), for the time selected. **Note:** A countdown (time remaining) will display (see image below right). Notice that the **Start** button changes to an **Abort** button that can be clicked to cancel the test signal generation.

Abort (button)

The **Start** button changes to this **Abort** button. Click **Abort** to cancel the test signal generation to the AL-NSM (Networx Signal Meter).

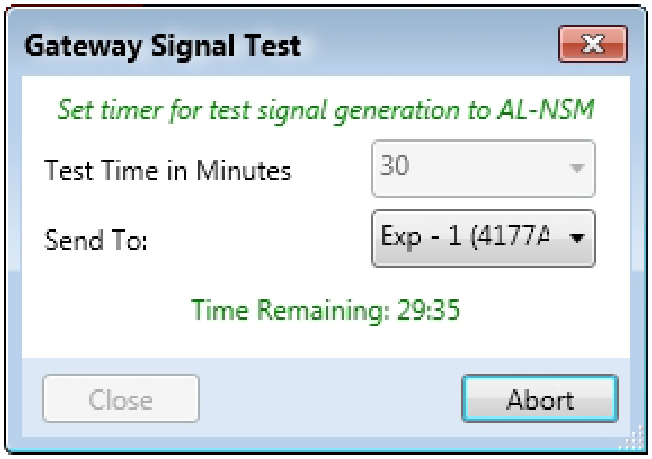


Gateway Signal Test

Set timer for test signal generation to AL-NSM

Test Time in Minutes: 30

Send To: Exp - 1 (4177A



Gateway Signal Test

Set timer for test signal generation to AL-NSM

Test Time in Minutes: 30

Send To: Exp - 1 (4177A

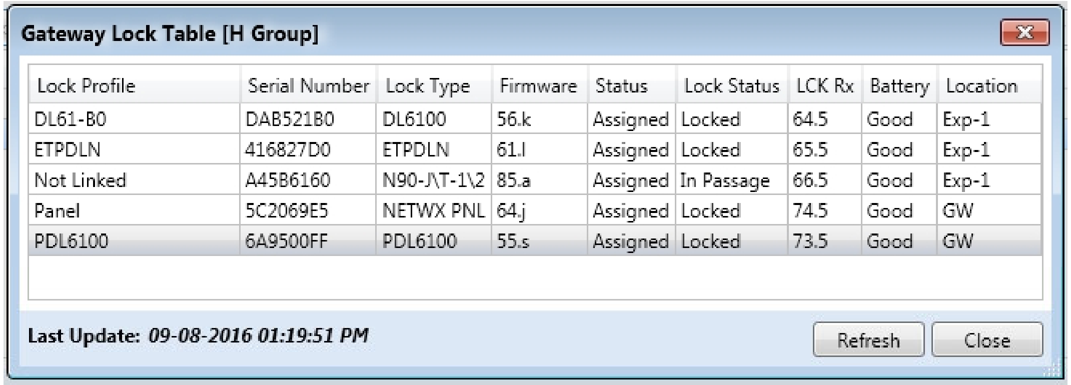
Time Remaining: 29:35

Gateway Configuration > Locks > Discover Locks

In the **Gateway Configuration** screen, click to highlight a specific Gateway in the list, then click **Locks** > **Discover Locks**. This option is **identical** in operation to the **Discover Locks** button found in the **Gateway Configuration** screen. See page 15 for more information about discovering wireless locks.

Gateway Configuration > Locks > View Gateway's Lock Table

In the **Gateway Configuration** screen, click to highlight a specific Gateway in the list, then click **Locks** > **View Gateway's Lock Table**. Upon selection, the Gateway's internal "Lock Table" is displayed, showing each lock assigned to the selected Gateway (and/or Expander), and their status as of the last time the table was updated (date and time shown at bottom left). Use this screen as a tool to verify successful communication with your locks, and their configuration status. Click **Refresh** to retrieve and display the latest information.



Gateway Lock Table [H Group]

Lock Profile	Serial Number	Lock Type	Firmware	Status	Lock Status	LCK Rx	Battery	Location
DL61-B0	DAB521B0	DL6100	56.k	Assigned	Locked	64.5	Good	Exp-1
ETPDLN	416827D0	ETPDLN	61.l	Assigned	Locked	65.5	Good	Exp-1
Not Linked	A45B6160	N90-J\T-1\2	85.a	Assigned	In Passage	66.5	Good	Exp-1
Panel	5C2069E5	NETWX PNL	64.j	Assigned	Locked	74.5	Good	GW
PDL6100	6A9500FF	PDL6100	55.s	Assigned	Locked	73.5	Good	GW

Last Update: *09-08-2016 01:19:51 PM*

Lock Profile
Displays name of the Lock Profile Linked to the physical lock. If not Linked, the text reads "**Not Linked**".

Serial Number
Displays the lock's unique number assigned and programmed into the lock firmware at the factory. Each Networx lock is identified in the system by this unique serial number.

Lock Type
Specifies the model of the Trilogy Networx series locking devices, such as "PDL6100", "DL6100" or "PL6100".

Firmware
Indicates the firmware source code edition currently residing in each physical lock.

Status
Indicates whether the physical lock is currently **Assigned** (was successfully added and configured) or **Unable to Configure** (added, but failed to be assigned).

Re-Configure Unassigned Locks (button)
This button appears when any lock in the table was added but failed to be assigned. Click to re-send the Config Table to the Gateway thus attempting re-configuration of all unassigned locks in the table.

Lock Status
Indicates the latest condition of the physical lock (i.e. "**Locked**", "**Passage**", etc.). If status is unknown or unable to be retrieved, "**Communication Error**" will be displayed.

LCK Rx (Signal)
Indicates the radio transmission strength, as measured between the Gateway (or Expander) to the physical lock (GTW Rx). *A **higher** number indicates **stronger** signal.*

Battery
Displays the status of the battery powering each physical lock.

Location
Displays *where* the physical lock is assigned (either **GW** (Gateway) or **Exp-#** (Expander number).

Refresh (button)
Click to retrieve and update the contents of this **Gateway Lock Table** screen.

Gateway Configuration > Locks > Link/Unlink Lock Profiles

After physical locks are successfully assigned, they must be "Linked" to Lock Profiles (locks not Linked cannot be downloaded). In DL-Windows, the word "Link" is used to describe the specific action of associating a Lock Profile to the physical lock assigned to the Gateway / Expander (by serial number). The Lock Type (model) of the Lock Profile MUST match the assigned lock to which you wish to Link. See page 17 for more information and how to use the **Link/Unlink Lock Profiles** screen.

Gateway Configuration > Locks > Delete Lock(s) by Serial Number(s)

In the **Gateway Configuration** screen, click **Locks** > **Delete Lock(s) by Serial Number(s)**. Upon selection, a table displaying all physical locks discovered by all Gateways (and/or Expanders) in the Account is displayed. Multiple locks can be removed from multiple Gateways (or Expanders) by checking their respective checkboxes and clicking **Delete**. **Note:** The removal command is first sent to the Gateway / Expander, then is sent to each selected physical lock to break the relationship between them. Once removed, the lock becomes unassigned and thus able to be re-discovered.

Lock Information

Displays **Lock ID** number and Lock Profile name. If not Linked to a Gateway, "**Not Linked**" is displayed.

Serial Number

Displays the physical lock's unique serial number assigned and programmed into the lock firmware at the factory. Each Networx lock is identified in the system by this unique serial number.

Lock Type

Specifies the model of the Trilogy Networx series locking devices, such as "PDL6100", "DL6100" or "PL6100".

Description

Description displays the text of the **Description** field from the **Gateway Configuration** screen.

Gateway

Displays the IP address of each Gateway in the Account to which the lock is assigned.

Location

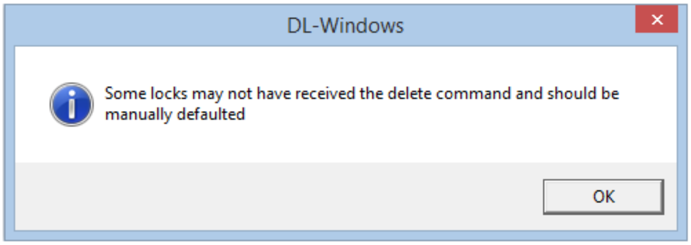
Displays *where* the physical lock is assigned (either **GW** (Gateway) or **Exp-#** (Expander number).

Delete (button)

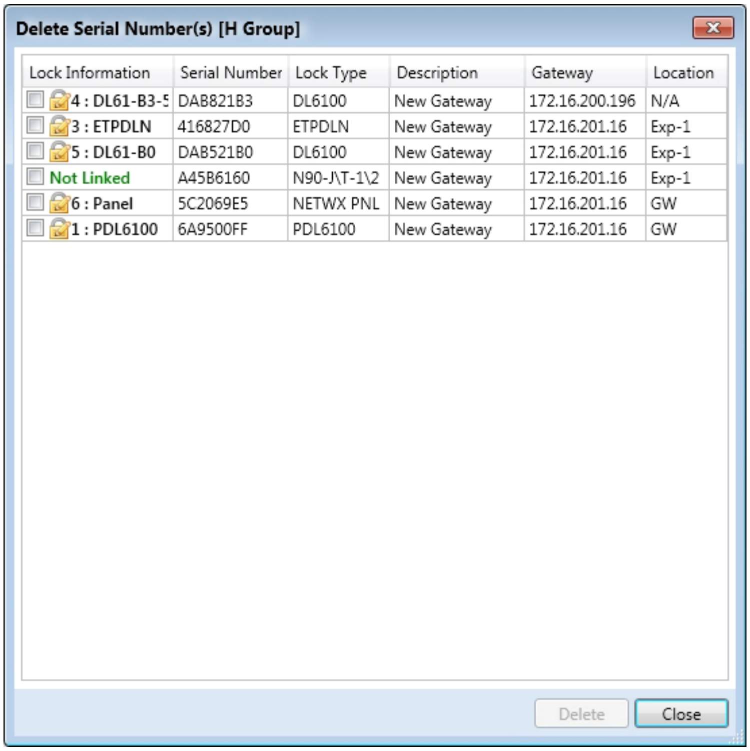
Click to send a delete command to the Gateway / Expander and to the selected (checked) physical locks.

Unresponsive Lock(s)

If some locks could not be reached and therefore could not receive the delete command, although the locks will be removed from the **Gateway Lock Table** (see previous page), each lock should be manually reset ("defaulted") to remove their lock assignments (thus allowing for re-discovery). See the programming instructions that came with the lock for the reset procedure.



Some locks may not have received the delete command and should be manually defaulted

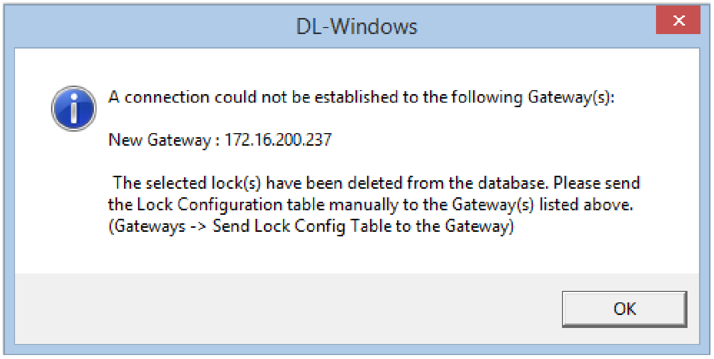


Lock Information	Serial Number	Lock Type	Description	Gateway	Location
□ 4 : DL61-B3-5	DAB821B3	DL6100	New Gateway	172.16.200.196	N/A
□ 3 : ETPDLN	416827D0	ETPDLN	New Gateway	172.16.201.16	Exp-1
□ 5 : DL61-B0	DAB521B0	DL6100	New Gateway	172.16.201.16	Exp-1
□ Not Linked	A45B6160	N90-J\T-1\2	New Gateway	172.16.201.16	Exp-1
□ 6 : Panel	5C2069E5	NETWX PNL	New Gateway	172.16.201.16	GW
□ 1 : PDL6100	6A9500FF	PDL6100	New Gateway	172.16.201.16	GW

Unresponsive Gateway(s) / Expander(s)

If a Gateway or Expander could not be reached and therefore could not receive the delete command, the selected locks will be removed from the DL-Windows Gateway database. The Gateway / Expander(s) will be updated later when the Gateway connection is re-established.

Note: Since the Gateway or Expander could not be reached, the selected locks could not be reached either. Therefore, although the selected locks will be removed from the **Gateway Lock Table** (see previous page), these locks must be manually reset ("defaulted") to remove their lock assignments. See the programming instructions that came with the lock for the reset procedure.



A connection could not be established to the following Gateway(s):

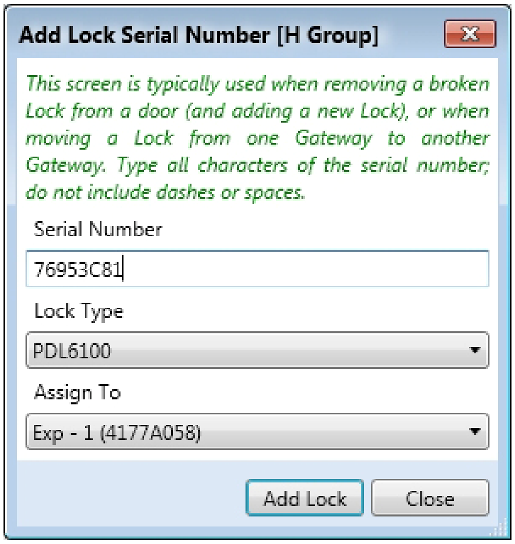
New Gateway : 172.16.200.237

The selected lock(s) have been deleted from the database. Please send the Lock Configuration table manually to the Gateway(s) listed above. (Gateways -> Send Lock Config Table to the Gateway)

Gateway Configuration > Locks > Manually Add a Lock by Serial Number

In the **Gateway Configuration** screen, click to highlight a specific Gateway in the list, then click **Locks** > **Manually Add a Lock by Serial Number**. Upon selection, the **Add Lock Serial Number** screen opens, where you can *manually* assign a specific lock by serial number to a Gateway or Expander.

This screen is typically used to assign multiple locks without needing to perform the discovery process. Manually type the serial number of the lock(s) and select their corresponding models from the **Lock Type** pull-down, then click **Add Lock**. Each lock, in succession, will be entered into a Configuration Table. When finished adding locks, you must manually send the Configuration Table to the Gateway by clicking **Gateways** > **Send Config Table to the Gateway**. **Note:** Remember to Link your locks after sending the Configuration Table.



Add Lock Serial Number [H Group]

This screen is typically used when removing a broken Lock from a door (and adding a new Lock), or when moving a Lock from one Gateway to another Gateway. Type all characters of the serial number; do not include dashes or spaces.

Serial Number: 76953C81

Lock Type: PDL6100

Assign To: Exp - 1 (4177A058)

Serial Number

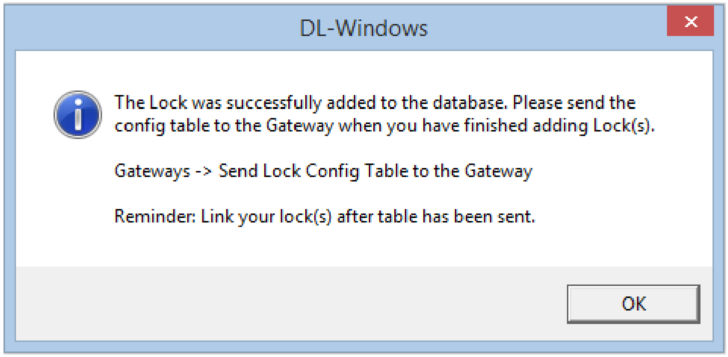
Carefully type the lock's unique 8-character factory serial number located on the lock housing (each Networx lock is identified in DL-Windows by this unique number). Type all characters of the serial number, **do NOT include dashes or spaces**.

Lock Type

Click the **Lock Type** pull-down and select the corresponding wireless lock model ("DL6100", "PDL6100", etc.).

Assign To (not displayed for non-version 2 Gateways)

Manually assign a specific lock serial number(s) to a selected Gateway or Expander (click the pull-down and select the desired Gateway or Expander).



DL-Windows

The Lock was successfully added to the database. Please send the config table to the Gateway when you have finished adding Lock(s).

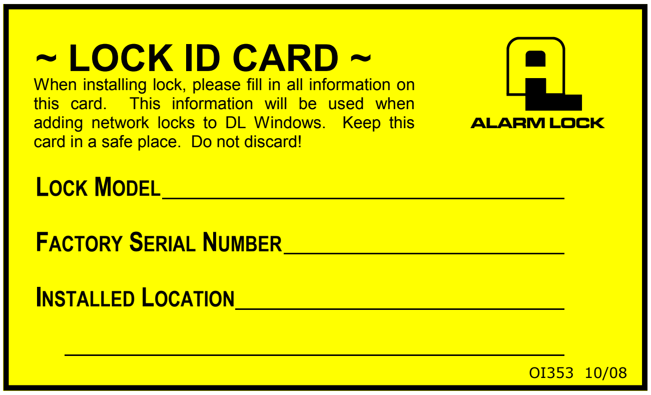
Gateways -> Send Lock Config Table to the Gateway

Reminder: Link your lock(s) after table has been sent.

Add Lock (button)

Click to manually add the lock to the Gateway (**Serial Number** plus **Lock Type**). The following message will display:

TIP We recommend that when installing the lock on the door, a yellow-colored "**LOCK ID CARD**" (see image below) be completed. These yellow cards are a useful way to organize lock information, including lock serial numbers.



~ LOCK ID CARD ~

When installing lock, please fill in all information on this card. This information will be used when adding network locks to DL Windows. Keep this card in a safe place. Do not discard!

LOCK MODEL ______________________________

FACTORY SERIAL NUMBER ______________________

INSTALLED LOCATION _________________________

____

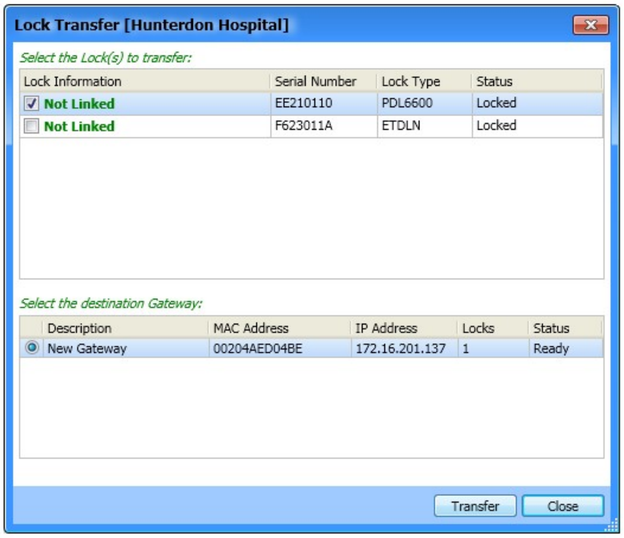
OI353 10/08

Gateway Configuration > Locks > Import Assigned Lock

In the **Gateway Configuration** screen, click to highlight a Gateway, then click **Locks > Import Assigned Lock**. Upon selection, the **Gateway Lock Table** for the Account will be updated with data from the Gateway. Locks that are assigned to the Gateway that are not in the **Gateway Lock Table** (in the DL-Windows database) will be imported / added to the DL-Windows database. Though rare, this feature is typically used when a DL-Windows database has been corrupted, and therefore requires an update from the Gateway.

Gateway Configuration > Locks > Transfer Lock(s) to Another Gateway

In the **Gateway Configuration** screen, click **Locks > Transfer Lock(s) to Another Gateway**. **IMPORTANT:** This option is currently only available during the Discover Locks function when using a USB Gateway (**AL-IME-USB**) and is used to selectively transfer locks *already* assigned to the **USB Gateway** to a Networx Gateway. There are many potential uses for this feature, but it is especially useful in situations where you wish to take advantage of the benefits of both a Networx Gateway and a USB Gateway (**AL-IME-USB**).



Lock Transfer [Hunterdon Hospital]

Select the Lock(s) to transfer:

Lock Information	Serial Number	Lock Type	Status
☑ **Not Linked**	EE210110	PDL6600	Locked
□ **Not Linked**	F623011A	ETDLN	Locked

Select the destination Gateway:

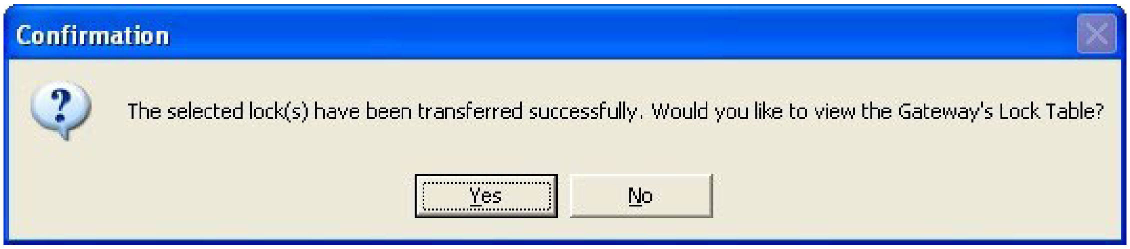
	Description	MAC Address	IP Address	Locks	Status
●	New Gateway	00204AED04BE	172.16.201.137	1	Ready

To transfer locks from the **USB Gateway** to a Networx Gateway:

1. In the top window of the **Lock Transfer** screen, use the checkboxes to select the desired lock(s) you wish to transfer.

2. In the bottom window of the **Lock Transfer** screen, click the radio button to select the "**Destination Gateway**". Only one Gateway can be selected for each operation.

3. Click the **Transfer** button. **Note:** This lock transfer operation may take some time; please be patient!
   A confirmation popup will appear when successful:



Confirmation

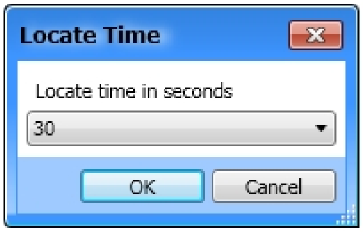
The selected lock(s) have been transferred successfully. Would you like to view the Gateway's Lock Table?

Note that the above popup optionally allows you to verify the results of the transfer operation. Click **Yes** to verify the operation by opening the Gateway's **Lock Table**, or click **No** to close the popup and continue without viewing the **Lock Table**.

For complete migration of all locks on the **USB Gateway** to a new Networx Gateway, select **Gateways** > **Replace Gateway with New One** (for more information about this feature, see page 19).

Gateway Configuration > Locks > Locate ALL Locks on Gateway

In the **Gateway Configuration** screen, click to highlight a specific Gateway in the list, then click **Locks** > **Locate All Locks on Gateway**. Upon selection, the **Locate Time** screen opens (shown below) where you can set the duration of time (in seconds) for all locks assigned to the selected Gateway to beep and flash their red LEDs. This option is typically used when you wish to find all of the physical locks or to confirm the wireless connection is operational. **Note:** Locks may be located even if they are not Linked to a Lock Profile.


Locate Time

Locate time in seconds

30

Locate Time in Seconds
Click the pull-down menu to select the time in seconds. during which all wireless locks assigned to the selected Gateway will beep and flash their red LEDs. Up to 255 seconds (4 minutes 15 seconds) can be selected; default duration is 30 seconds.

OK (button)
Click **OK** and all wireless locks assigned to the selected Gateway will beep and flash their red LEDs for the selected **Locate Time** duration.

Cancel
Click to exit without requesting the locate action.

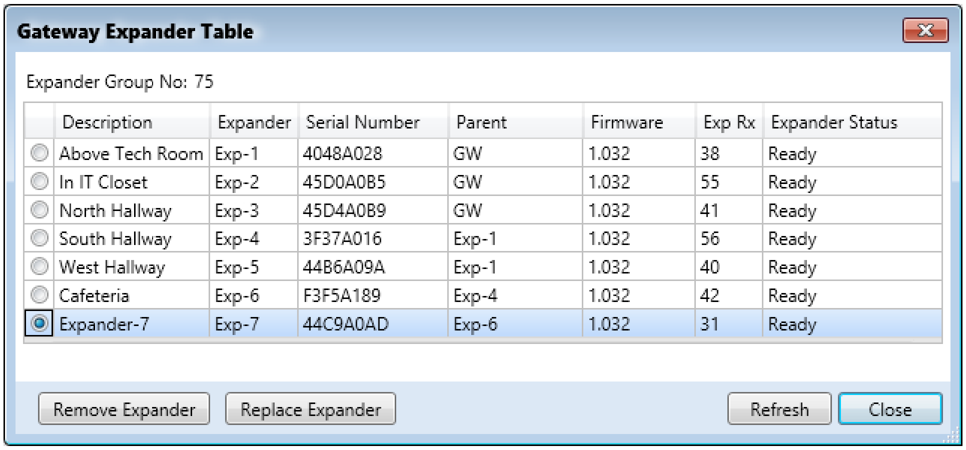
Note: Individual locks may be located (beep and flash their red LEDs) via a right-click option from the Account List area (see "**Locate Lock**" on page 54).

Gateway Configuration > Expanders > Discover New Expander(s)

IMPORTANT: For optimal performance, we recommend reading the documentation accompanying the Expanders for information regarding Expander location guidelines and "Expander Group" dial settings.

After your Gateway has been discovered and added to the Account, up to 7 Expanders may then be discovered and added to a Gateway. With the Expanders powered, their Group dials set identical to the Gateway and mounted within range of the Gateway (or another Expander) click **Gateway Configuration** > **Expanders** > **Discover New Expander(s)**. The procedure is slightly different from discovering locks or Gateways in that the Gateways / Expanders will automatically determine the optimal routing pathways between each other, ensuring optimal signal levels.

Note: Be patient; depending on the number of Expanders in your system, this procedure may take up to several minutes. When complete, the Gateway Expander Table will appear displaying the routing information, status, firmware versions and signal levels of each discovered Expander.


Gateway Expander Table

Expander Group No: 75

	Description	Expander	Serial Number	Parent	Firmware	Exp Rx	Expander Status
○	Above Tech Room	Exp-1	4048A028	GW	1.032	38	Ready
○	In IT Closet	Exp-2	45D0A0B5	GW	1.032	55	Ready
○	North Hallway	Exp-3	45D4A0B9	GW	1.032	41	Ready
○	South Hallway	Exp-4	3F37A016	Exp-1	1.032	56	Ready
○	West Hallway	Exp-5	44B6A09A	Exp-1	1.032	40	Ready
○	Cafeteria	Exp-6	F3F5A189	Exp-4	1.032	42	Ready
●	Expander-7	Exp-7	44C9A0AD	Exp-6	1.032	31	Ready

TIP If an Expander is accidentally reset, **don't worry!** Simply use this **Expanders** > **Discover New Expander(s)** command. This discovery process will reconfigure the reset Expander and add it back to its original location in the Expander Table.

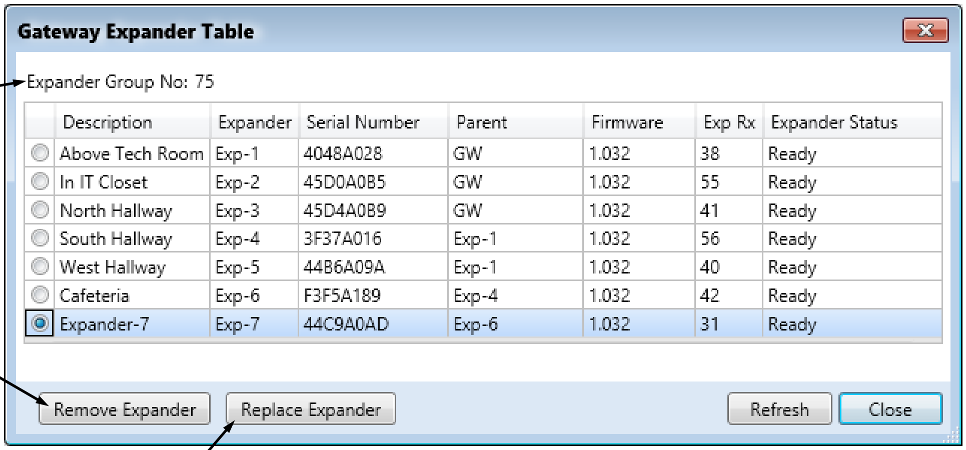
Gateway Configuration > Expanders > View Expander Routing Table

In the **Gateway Configuration** screen, select / highlight the desired Gateway from the list, then click **Expanders** > **View Expander Routing Table** to view information about *added* Expanders. In addition, in this screen, Expanders can be removed or replaced.

Expander Group No:
Indicates the "Expander Group" dial setting of the selected Gateway.

Remove Expander (button)
In order to maintain proper routing table integrity, Expanders may ONLY be removed from the bottom up.

Using the image at right as an example, "**Expander-7**" must be removed first before removing "**Cafeteria**". **Note:** The **Remove Expander** button is only available for use with the last Expander in the list (will remain "grayed-out" for all other Expanders selected).



Expander Group No: 75

	Description	Expander	Serial Number	Parent	Firmware	Exp Rx	Expander Status
○	Above Tech Room	Exp-1	4048A028	GW	1.032	38	Ready
○	In IT Closet	Exp-2	45D0A0B5	GW	1.032	55	Ready
○	North Hallway	Exp-3	45D4A0B9	GW	1.032	41	Ready
○	South Hallway	Exp-4	3F37A016	Exp-1	1.032	56	Ready
○	West Hallway	Exp-5	44B6A09A	Exp-1	1.032	40	Ready
○	Cafeteria	Exp-6	F3F5A189	Exp-4	1.032	42	Ready
●	Expander-7	Exp-7	44C9A0AD	Exp-6	1.032	31	Ready

Replace Expander (button)
This option is used when an Expander needs to be physically replaced with a new one.
Simply type the serial number of the new Expander into the dialog box that appears and click "**Replace**".

Things to consider:

- The new Expander should be powered up and set with the "Expander Group" number of the old Expander.
- The "parent" does NOT change, therefore the new Expander should be placed in the same location as the Expander being replaced.

Description
Displays name of Expander. Default name is Expander-#. Double-click to manually edit the Expander **Description** (maximum 30 alphanumeric characters).

Expander
Displays the number assigned to the Expander upon addition to the Gateway.

Serial Number
Displays the Expanders factory serial number.

Parent
Displays the Expander or Gateway through which the Expander communicates.

Firmware
Displays the current firmware edition the Expander is running.

Exp Rx (Signal)
Indicates the radio transmission strength, as measured between the Gateway to Expander or Expander to Expander. *A **higher** number indicates **stronger** signal.*

Expander Status
Indicates the last retrieved state of the Expander.

Refresh (button)
Click to retrieve and update the contents of this **Gateway Expander Table** screen.

TIP Even if Expanders have not yet been added, but you wish to know setting of the "Expander Group" dials of the selected Gateway, instead of looking inside the Expander enclosure, simply view the **Gateway Expander Table** screen and view the **Expander Group No:** displayed at the top.

Gateway Configuration > Expanders > Update Expander Firmware

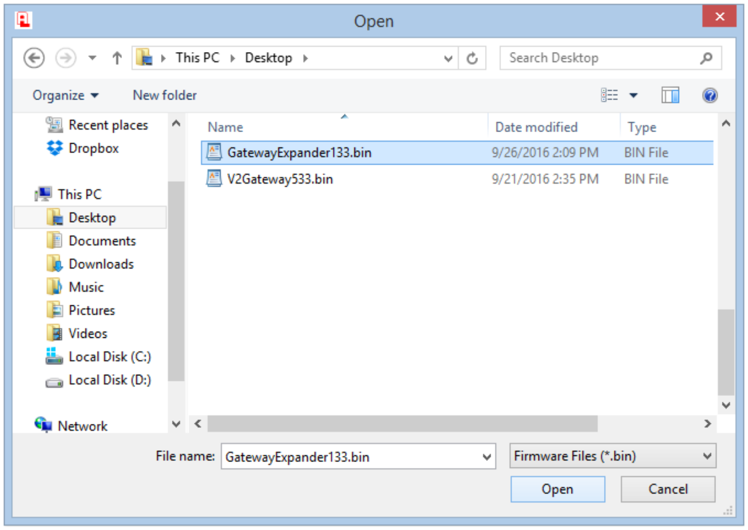
In the **Gateway Configuration** screen, click to highlight a specific Gateway in the list (with the Expanders you wish to update), then click **Expanders** > **Update Expander Firmware**.

Upon selection, the standard Windows **Open** dialog box appears (shown at right), allowing you to browse for the binary ".bin" file containing the Expander firmware.

Select Expander firmware file, then click **Open** to initiate the update process.

DL-Windows will check the integrity of the firmware, will send it to the Gateway, then distribute the file throughout the system (Gateway to Expander and Expander to Expander).

Be patient; the Expander firmware distribution process may take several minutes. Upon completion, the **Gateway Status** screen automatically opens. View the "**Expander(s)**" table at the bottom of the screen to confirm the updated firmware version.



Name	Date modified	Type
GatewayExpander133.bin	9/26/2016 2:09 PM	BIN File
V2Gateway533.bin	9/21/2016 2:35 PM	BIN File

File name: GatewayExpander133.bin

Firmware Files (*.bin)

Gateway Configuration > Expanders > Send Expander Config Table to the Gateway

In the **Gateway Configuration** screen, click to highlight the desired Gateway from the list, then click **Expanders** > **Send Expander Config Table to the Gateway**. This feature is intended to be used in the rare instance that the Expander Routing table becomes corrupted. The Gateway's *added* Expanders will be populated with the Expander Routing Table information stored in the DL-Windows database.

Communicating with Wireless Locks

Networx Communication Overview

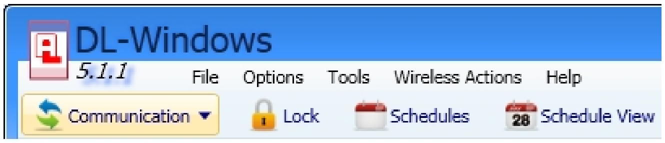
Once your have discovered your Gateways (and/or Expanders) assigned your locks and Linked them to Lock Profiles, there are several methods for sending data to (or receiving data from) wireless locks:

- **Method 1:** Communicate with wireless locks individually using the **Communication** button on the DL-Windows "Main Screen" (or from the **Lock Data** screen);
- **Method 2:** Communicate with multiple wireless locks (one after another) using the **Wireless** screen;
- **Method 3:** Communicate automatically at a specified time using a **Wireless Schedule** screen action.

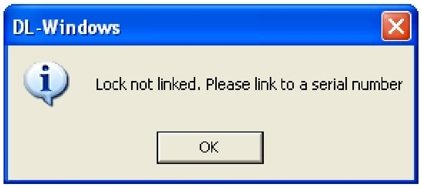
Note: Keypad programming of User Codes, Features, Time Zones, and Schedules is available as a *temporary* convenience to allow the lock to be put into use before installing and configuring a wireless network. *Therefore, all lock programming added via the keypad <u>cannot</u> be retrieved from the lock into DL-Windows.* If you decide to start programming your wireless lock via the keypad, we recommend you keep hardcopy records (in a secure location) of all Users, their User Codes, and any proximity cards that may have been programmed. Keeping complete and accurate records saves time because after the wireless network is set up, any programming added via the keypad must be re-added to DL-Windows and downloaded back to the lock(s).

Method 1:
"Communicate with Selected Networx Lock"

1. In the DL-Windows "Main Screen", click the **Communication** button on the toolbar and select



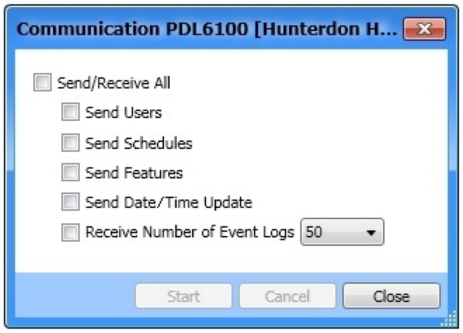
Communicate with Selected Networx Lock.


DL-Windows

Lock not linked. Please link to a serial number

Note: The **Communication** button on the **Lock Data** screen may also be used. In addition, if your lock has not been Linked to a Lock Profile, the following popup appears:

2. If Linked, the following screen appears:


Communication PDL6100 [Hunterdon H...

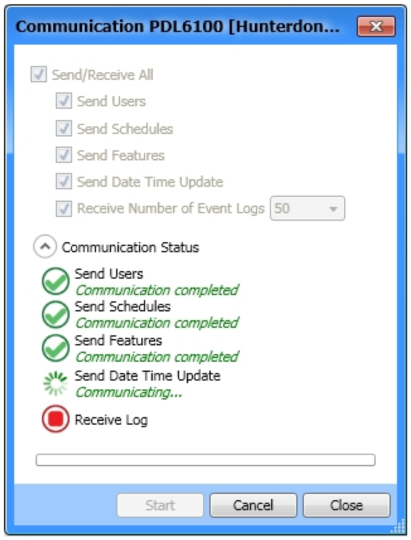
☐ Send/Receive All
☐ Send Users
☐ Send Schedules
☐ Send Features
☐ Send Date/Time Update
☐ Receive Number of Event Logs 50

Any combination of available data may be sent to your lock.

Select any combination of data to send to your wireless lock; a red circle with red square will denote those selections made, though it is recommended to check "**Send/Receive All**".

- **Send/Receive All** - Sends the complete program to (and receives selected number of Event Logs from) the wireless lock.
- **Send Users** - Sends all User Information including User Enable / Disable status, User Codes (PINs), proximity information, Group Assignments and Emergency Users.
- **Send Schedules** - Sends all Schedules (see OI382 for more details).
- **Send Features** - Sends all Features chosen in the **Features** screen (see **Features** section(s) in OI382 for more details).
- **Send Date/Time Update** - Updates the wireless lock with the PCs current date and time.
- **Receive Number of Event Logs (pull-down)** - Receives the selected number of Event Logs from the wireless lock (default = 50; maximum = 40,000).

3. Initiate the communication by clicking the **Start** button. **Note:** Unlike standard non-wireless Trilogy locks, wireless Networx locks do not need to be configured for PC Program Mode (Function 58).


Communication PDL6100 [Hunterdon...

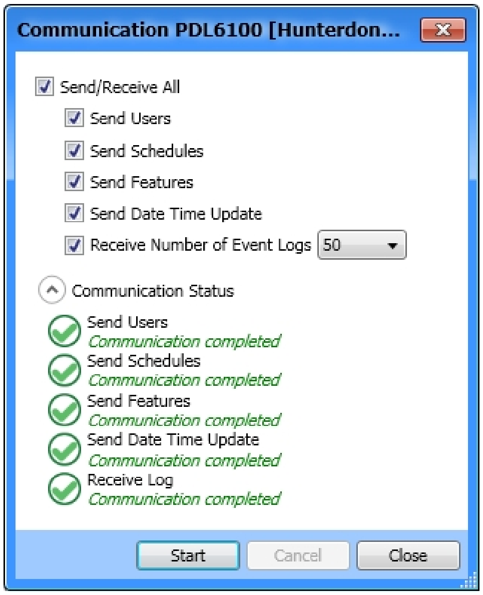
☑ Send/Receive All
☑ Send Users
☑ Send Schedules
☑ Send Features
☑ Send Date Time Update
☑ Receive Number of Event Logs 50

Communication Status

✓ Send Users
Communication completed
✓ Send Schedules
Communication completed
✓ Send Features
Communication completed
Send Date Time Update
Communicating...
● Receive Log

Communicating with Wireless Locks (cont'd)

4. After data transfer has finished, verify all selected options are displayed with a green checkmark and the message "**Communication completed**" appears. **Note:** The **Event Log** screen will automatically appear upon successful communication if **Receive Number of Event Logs** was previously selected:



Communication PDL6100 [Hunterdon...

☑ Send/Receive All
- ☑ Send Users
- ☑ Send Schedules
- ☑ Send Features
- ☑ Send Date Time Update
- ☑ Receive Number of Event Logs 50

Communication Status

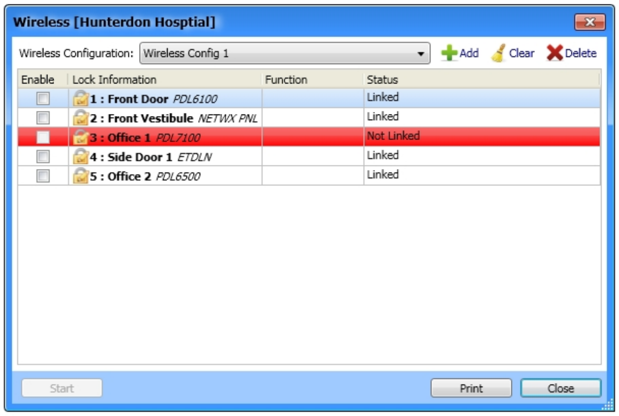
- ✓ Send Users — *Communication completed*
- ✓ Send Schedules — *Communication completed*
- ✓ Send Features — *Communication completed*
- ✓ Send Date Time Update — *Communication completed*
- ✓ Receive Log — *Communication completed*

Note: If data transfer fails, a circle with a red "X" will denote communication error. Verify proper signal levels and check network connections. For more information, see WI2085.

Method 2: Communicate with Multiple Wireless Locks in the Account

1. In the DL-Windows "Main Screen", click the **Wireless** button on the toolbar.

The following screen appears.



Wireless [Hunterdon Hosptial]

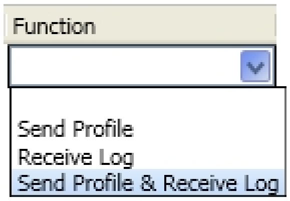
Wireless Configuration: Wireless Config 1

Enable	Lock Information	Function	Status
□	**1 : Front Door** *PDL6100*		Linked
□	**2 : Front Vestibule** *NETWX PNL*		Linked
□	**3 : Office 1** *PDL7100*		Not Linked
□	**4 : Side Door 1** *ETDLN*		Linked
□	**5 : Office 2** *PDL6500*		Linked

Note: See page 40 for detailed explanations of each area of the **Wireless** screen. In addition, if your lock has not been Linked to a Lock Profile, the entire row will be highlighted red, and the **Status** column will indicate "**Not Linked**" The lock *must* be Linked before you can continue to the following steps.

2. For each wireless lock with which you want to communicate, click to add a check to the checkbox in the **Enable** column.

3. For each enabled lock, double-click its empty box in the **Function** column, and click the desired function in the pull-down (as shown in the accompanying image):
   Note: To clear a function, click the blank space above **Send Profile**.



Function

- Send Profile
- Receive Log
- Send Profile & Receive Log

Once function is set, the **Start** button will be enabled. Click **Start** to initiate communication to enabled wireless locks. **Note:** The function set for each lock will be performed; upon completion, the **Status** column for each lock will denote the ending status of the communication (i.e. **Communication completed**").

Method 3: Automatically Communicate with Wireless Locks

This method requires programming in the **Wireless** screen and **Wireless Schedules** screen.

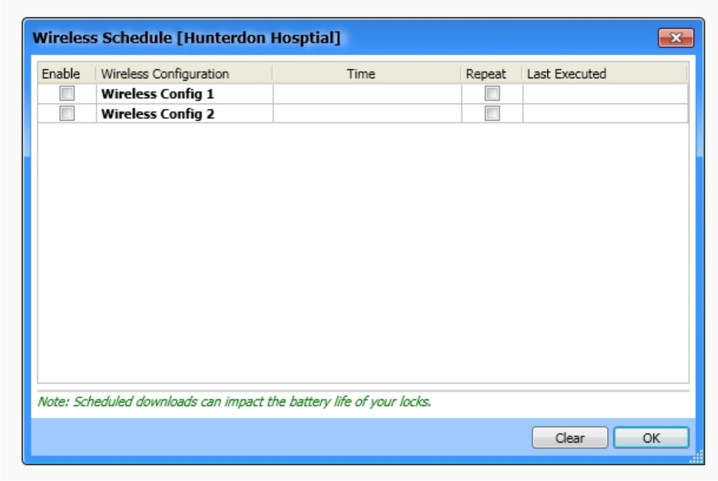
1. In the **Wireless** screen, create a **Wireless Configuration** to be used for your wireless Schedule. For each wireless lock you wish to communicate with via a Schedule, click to add a check to the checkbox in the **Enable** column and select the desired function from the pull-down list.
   Note: Additional **Wireless Configurations** may be added with the "**+ Add**" button. In addition, names are customizable; click **Edit** to rename, then click **Save**.

2. DO NOT click the **Start** button; close the **Wireless** screen. The configuration(s) will be saved, and used in the **Wireless Schedules** screen.

3. In the DL-Windows "Main Screen", click **Wireless Actions** > **Wireless Schedule**. The **Wireless Schedule** screen appears:

N
cu
al
co
Sa

Communicating with Wireless Locks (cont'd)



Wireless Schedule [Hunterdon Hosptial]

Enable	Wireless Configuration	Time	Repeat	Last Executed
□	**Wireless Config 1**		□	
□	**Wireless Config 2**		□	

Note: Scheduled downloads can impact the battery life of your locks.

Note: See page 40 for detailed explanations of each area of the **Wireless Schedule** screen.

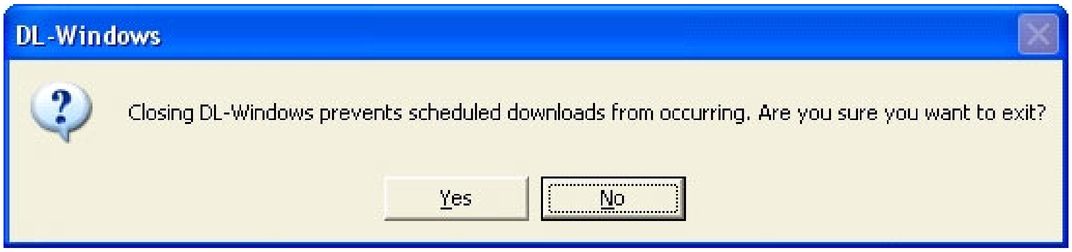
4. Check the **Enable** checkbox for desired wireless configurations. **Note: Wireless Configurations** were pre-programmed in step 1.

5. For each enabled configuration, double-click the empty box in the **Time** column to display the pull-down for **HH / MM / AM PM**. Set desired time to initiate the intended automatic communications.

6. Optional - Check the **Repeat** checkbox to program *daily automatic Schedules*. Automatic wireless communication will be performed every day at the programmed time until the **Repeat** checkbox is unchecked.

7. Click **OK** to save wireless Schedule programming.

   Warning: If you have a Schedule programmed, and DL-Windows is closed, the Schedule will **not** occur. A warning popup appears (shown below) if you try to exit DL-Windows with a schedule programmed:



DL-Windows

Closing DL-Windows prevents scheduled downloads from occurring. Are you sure you want to exit?

"Wireless" Screen - Field and Button Definitions

As described in **Method 2** of the section **Communicating with Wireless Locks** (page 38) , the **Wireless** screen allows communication with *individual* or *multiple* wireless locks. The **Wireless** screen can be configured for various functions, as required. Functions include **Send Profile**, **Receive Log**, and **Send Profile & Receive Log**.

Click the **Wireless** button to access the **Wireless** screen.

Wireless Configuration (pull-down)
Click pull-down to select and display wireless configurations (the selections made in this screen will be saved as a "Wireless Config"). **Note:** Wireless configuration names are customizable; click **Edit** to rename; then click **Save**.

Lock Information
Displays Lock ID, Lock Profile and Lock Type (model) of the wireless lock. **Note:** Non-wireless locks (i.e. PDL3000) will not be displayed in this screen.

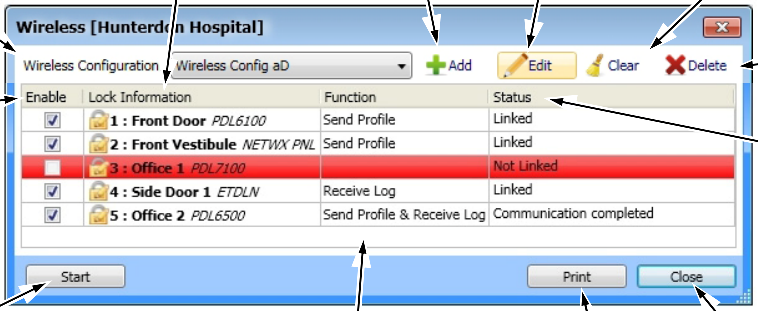
+ Add
Click to add additional Wireless Configurations.

Edit
Click to customize the name of the Wireless Configuration (in the pull-down).

Clear
Click to clear the selected (checked) Wireless Configuration. **Note:** Also clears last-known communication condition (see **Status**).

Delete
Click to remove the selected Wireless Configuration.

Enable
When checked, upon communication, the **Function** programmed for the enabled wireless lock will be performed. See **Right Click Menus** below for programming short cuts available.


Wireless [Hunterdon Hospital]

Wireless Configuration: Wireless Config aD

Enable	Lock Information	Function	Status
☑	1 : Front Door *PDL6100*	Send Profile	Linked
☑	2 : Front Vestibule *NETWX PNL*	Send Profile	Linked
□	3 : Office 1 *PDL7100*		Not Linked
☑	4 : Side Door 1 *ETDLN*	Receive Log	Linked
☑	5 : Office 2 *PDL6500*	Send Profile & Receive Log	Communication completed

Status
Displays current state of the link between the Gateway and the lock ("Linked" or "Not Linked"). **Note:** "Not Linked" locks are highlighted in red. This field also displays the last-known lock communication condition and is updated upon subsequent communications.

Start
Click to initiate communications to all enabled wireless locks.

Close (button)
Click to save settings and exit the screen.

Function (pull down)
Click to display a pull-down and select a function to perform upon communication.

- **Send Profile:** Sends full lock program to the wireless lock (Users, Schedules, Features, time/date).
- **Receive Log:** Retrieves the Event Log (local keypad entries and other lock events) from the wireless lock.
- **Send Profile & Receive Log:** Combines the above two functions.

See **Right Click Menus** below for programming short cuts available.

Print
Click to open a "**Print Preview**" screen, displaying all information in the **Wireless** screen. Click the "**Printer**" icon to send the request to your default printer.

Right Click Menus ☞

Enable (right-click menu)
To save time, right-click the "**Enable**" column; the desired action can be selected as follows:

- **Select All**: Adds a check to enable all (Linked) wireless locks.
- **Unselect All**: Removes a check from all (Linked) wireless locks.
- **Select Highlighted**: Adds a check to the **Enable** checkbox for all highlighted rows.
- **Invert Highlighted**: Removes a check from the **Enable** checkbox for all highlighted rows.

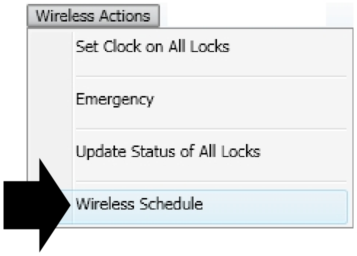
Function (right-click menu)
To save time, right-click the "**Function**" column; the desired action can be selected as follows:

- **Change All to**: "**Receive Log**"; "**Send Profile**"; "**Send Profile & Receive Log**": Selects function for all (Linked) wireless locks.
- **Change Selected**: "**Receive Log**"; "**Send Profile**"; "**Send Profile & Receive Log**": Selects function for all enabled wireless locks.
- **Change Highlighted to…**: "**Receive Log**"; "**Send Profile**"; "**Send Profile & Receive Log**": Selects function for all highlighted wireless locks.

"Wireless Schedule" Screen - Field and Button Definitions

As described in **Method #3** of the section **Communicating with Wireless Locks** (page 38), the **Wireless Schedule** screen allows for automatic scheduled downloading of wireless locks. The Wireless Configuration created in the **Wireless** screen is used to determine which wireless locks (and their respective pre-programmed functions) will automatically download at a pre-designated time. After the scheduled download completes, the **Wireless Schedule** screen automatically opens to allow the **Status** of each download to be verified.

In the DL-Windows "Main Screen", click **Wireless Actions** > **Wireless Schedule**.

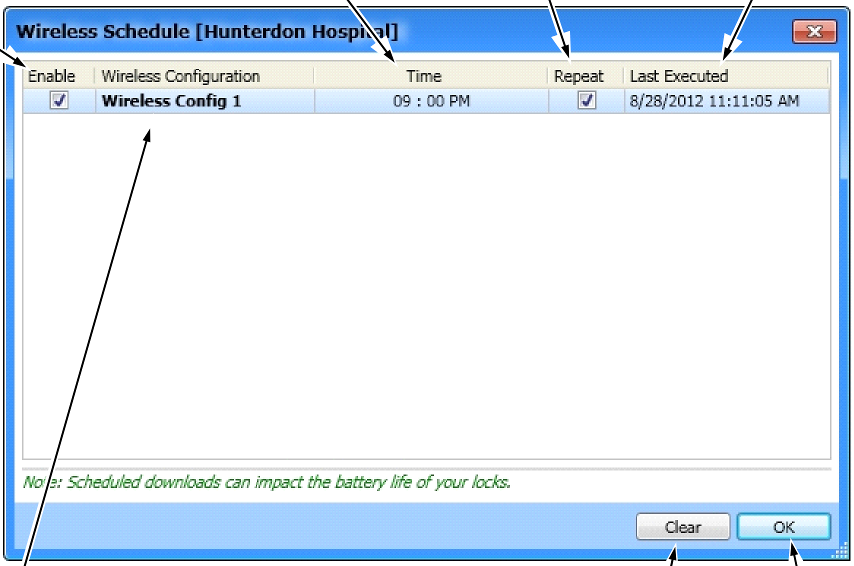


Time
Click to set the start time of the scheduled communications from the pull-downs (HH / MM / AM PM).

Repeat
Click to repeat the scheduled communication every day at the programmed time. Leave unchecked for one-time scheduled communication. **Note:** Daily automatic communication may impact battery life.

Enable
Add a check to enable the Wireless Configuration, thus activating the Schedule.

Last Executed
Displays the date and time the Schedule was last executed.



Enable	Wireless Configuration	Time	Repeat	Last Executed
☑	Wireless Config 1	09 : 00 PM	☑	8/28/2012 11:11:05 AM

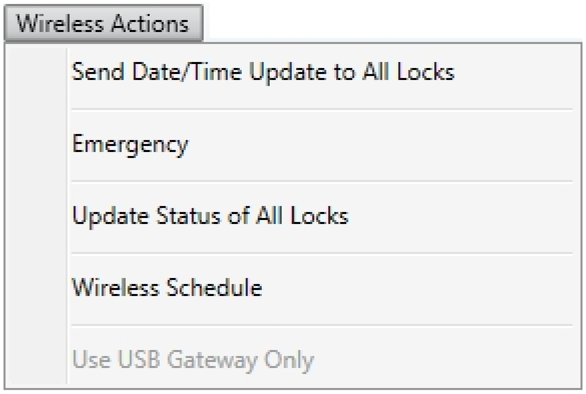
Note: Scheduled downloads can impact the battery life of your locks.

Wireless Configuration
The "Wireless Configuration" created in the **Wireless** screen (enabled locks and pre-set functions).

Clear
Click to uncheck the **Enable** and **Repeat** checkboxes, thus disabling the Schedule.

OK
Click to save the wireless schedule programming and exit.

Wireless Actions Menu



In the DL-Windows "Main Screen", click **Wireless Actions**:

Send Date/Time Update to All Locks
Based upon the current time and date of the PC running DL -Windows, a command is sent to all Gateways (and Expanders) to update all locks with this current date and time. **Note:** Locks not Linked will not receive this update command.

Emergency
Opens the **Emergency Commands** screen. For more information about the **Emergency Commands** screen, see page 43 and page 44.

Update Status of All Locks
A command is sent to all Gateways (and Expanders) in the Account to request the current status for all assigned wireless locks. Status data received from each lock updates each Gateways Lock Table. When the Lock Table of the Gateway is subsequently viewed, the Table displays the information as of the latest update request.
Note: To view the Gateway Lock Table, in the **Gateway Configuration** screen, select Gateway, then click **Locks** > **View Gateway's Lock Table** (see page 30).

Wireless Schedule
Opens the **Wireless Schedule** screen. Used for programming automatic scheduled communication with wireless lock(s). See page 40 for more information.

Use USB Gateway Only
Upon selection, all communications to the Networx locks in the Account are routed through the **USB Gateway** (regardless of the Network Gateway to which the lock may have been assigned). **Note:** The above is denoted by a USB "stick" icon displayed at the bottom of the DL-Windows screen (shown at right).

IMPORTANT: This selection is not available (grayed-out) if version 2 Gateways exist in the Account.

"Emergency Commands" Screen - Field and Button Definitions

The **Emergency Commands** screen allows for sending Emergency Commands ("Emergency Lock Down", "Emergency Passage" and "Return to Normal") to Groups of Gateways in your system, thus sending the command to all locks assigned to those Gateways. **Note:** All added Gateways are automatically placed into "**GROUP A**" by default; Gateways may be moved to another Group via the **Set Emergency Groups** button. In addition, the **Emergency Users List** may also be viewed from this screen.

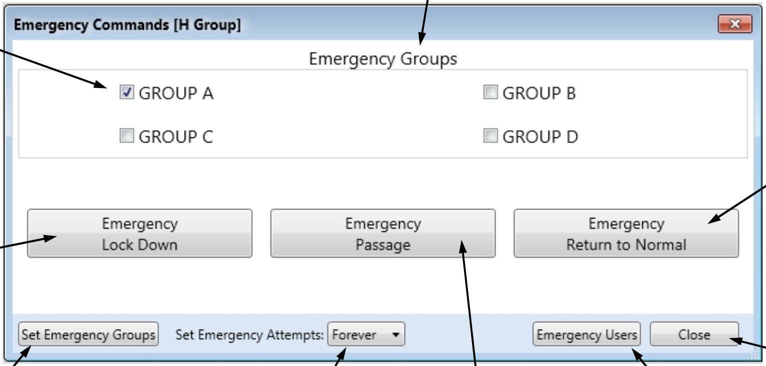
Click the **Emergency** button to access the **Emergency Commands** screen.

The **Emergency Commands** screen may also be accessed in the DL-Windows "Main Screen" by clicking **Wireless Actions** > **Emergency**.

IMPORTANT: Before using the **Emergency Commands** screen, it is important to read the next section regarding how to use Emergency Commands.

Emergency Groups
Select Group of Gateways to receive Emergency commands. **Note:** If only one Gateway exists in the Account, the "**GROUP A**" checkbox will be checked and the other checkboxes will be disabled. **Note:** The description of each Group (e.g. "**GROUP A**") may be changed in the **Set Emergency Groups** screen.

GROUP A
(This Group selected by default).



☑ GROUP A ☐ GROUP B
☐ GROUP C ☐ GROUP D

Set Emergency Attempts: Forever

Emergency Return to Normal
Sends "Return to Normal" command to all Gateway(s) in the selected Group(s).

Emergency Lock Down
Sends "Emergency Lock Down" command to all Gateway(s) in the selected Group(s).

Close
Saves the Emergency Group selections and exits the screen.

Set Emergency Groups (button)
Click to open the **Set Emergency Groups** screen, allowing for Gateway Group assignment and setting the Gateway Group description text.

Emergency Passage
Sends "Emergency Passage" command to all Gateway(s) in the selected Group(s).

Emergency Users (button)
Click to open the **Emergency Users** screen, listing those Users allowed to send Emergency commands.

Set Emergency Attempts
In this pull-down, select the number of Emergency attempts (**Forever**, **1-10**). If an Emergency Command fails or is unable to be verified, this selection determines the number of retry attempts. Default = **Forever** (retry until manual abort).

Using Emergency Commands

Emergency Overview

Three "Emergency Commands" are available in the wireless Trilogy Networx system:

- "**Emergency Lock Down**": Places all assigned locks into an indefinitely locked state
- "**Emergency Passage**": Places all assigned locks into an indefinitely unlocked state
- "**Return to Normal**": Reverts all assigned locks to the state they were in prior to the initiation of the Emergency command

These "Emergency" Commands can be initiated from DL-Windows via the **Emergency Commands** screen, or at any **Networx** wireless lock keypad. For more information regarding issuing Emergency Commands at the keypad, see the programming instructions included with your lock and OI382. **Note:** DL-Windows does *not* need to be running when issuing an Emergency Command at the keypad.

WARNING: NEVER use Emergency Commands to "toggle" Passage Mode, as this will severely impact battery life.

Getting Started

Automatic Gateway Grouping ("Emergency Grouping")

Upon the addition of each Gateway into an Account, the Gateway is automatically placed into an Emergency Group ("**GROUP A**" by default). This is done so that upon the initiation of an Emergency Command, **ALL** Gateways in the Emergency Group (and their assigned locks) will respond to Emergency Commands issued from DL-Windows. In addition, the automatic placement of a new Gateway into an Emergency Group allows for keypad-initiated Emergency Commands, to lock down an entire system from a single wireless lock.

Required Static IP Address

IMPORTANT: To ensure Gateways can respond to Emergency Commands, all Gateways **MUST** be configured with static (unchangeable) IP addresses. For more information about configuring a Gateway with a static IP address, see **Gateway Configuration > Gateways > Configure / Edit Network Settings** (page 22), and WI2085.

WARNING

All Emergency Commands MUST be tested weekly (or daily if necessary) to ensure their correct operation.

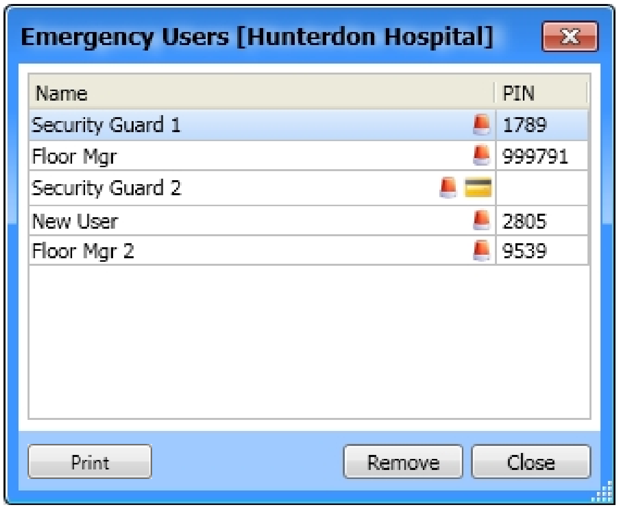
With the addition of each newly added Gateway to an Account, a "**red siren**" symbol appears at the bottom of the DL-Windows "Main Screen" to serve as a reminder that the added Gateway is configured with a changeable IP address (DHCP). This "**red siren**" symbol will remain until all Gateways in the Account are configured with a *static* IP address.

Configure Lock to Accept Emergency Commands

All Networx locks are programmed at the factory to respond to "Local" Emergency Commands (i.e. Lockdown via keyfob or directly from the keypad). However, in order to accept Emergency commands initiated from DL-Windows, a Full Download (which includes required programming from the Features screen) must be completed first. Note: Acceptance of Global and Local Emergency commands are enabled by default for all Networx locks in DL-Windows.
For more information about Local vs Global Emergency Commands, and programming various Emergency features, see OI382.

Who can Initiate Emergency Commands?

- **From DL-Windows:** All Users, Administrators and Operators have access to the **Emergency Commands** screen, and therefore can initiate Emergency Commands to any Gateway (and their assigned locks).
- **From a Networx wireless lock keypad:** Once the Lock Profile has been downloaded to the physical lock, Administrative Users 1 through 11 automatically have the ability to initiate **Emergency Commands** from the keypad. In addition, "non-Admin" Users (12+) may be given the ability to initiate Emergency Commands from the keypad by adding them to the **Emergency Users**


Emergency Users [Hunterdon Hospital]

Name	PIN
Security Guard 1	1789
Floor Mgr	999791
Security Guard 2	
New User	2805
Floor Mgr 2	9539

Using Emergency Commands (cont'd)

list (see next section).

- **From a Wireless Remote Release Keyfob**
  Networx locks have the added ability to accept Emergency Lock Down commands from a Wireless Remote Release (model RR-4BKEYFOB).

Adding Emergency Users

To grant the ability of a "non-Admin" User (12+) to initiate keypad Emergency Commands, in DL-Windows, click the **Global** button to open the **Global Users** screen. Click to highlight User(s) in the **User Name** list, then right-click the User(s); from the menu that appears, select **Lockdown User** > **Add/Remove Emergency User(s)**. In the **Global Users** screen **User List**, a "**red siren**" symbol will display in the **Name** column for those Users who can initiate two of the three Emergency Commands, i.e. **Emergency Lockdown** and **Emergency Passage**; this User cannot initiate the **Emergency Return to Normal** command. In addition, the User(s) will be added to the **Emergency Users** list.

> **TIP** It may be helpful to refer to the **Terminology** section in the DL-Windows User's Guide (OI382) for detailed descriptions of the terms used in this section (i.e. User Code, User Numbers, etc.).

Emergency Users List

The **Emergency Users** list may be accessed from **Global Users > Administrative Users > Emergency Users** or from the **DL-Windows "Main Screen" > Emergency > Emergency Users**. Existing Emergency Users can be removed by selecting the User and clicking the **Remove** button (or from the **Global Users** screen, click to highlight the User(s), then right-click and select from the menu **Add/Remove Emergency User(s)**. The "**red siren**" symbol will be removed.

Emergency Return to Normal (Enable/Disable as Reset Lockdown User)

To enable the **Emergency Return to Normal** command for any Emergency User, open the **Global Users screen**, then select one or more Users from the **User List**. Right-click the selected User(s) select **Lockdown User** > **Enable/Disable as Reset Lockdown User**. The "**Open Door**" icon (shown at right) will appear next to the User's name located in the "Account List" area at the left side of the DL-Windows "Main Screen".

Who has Access during Emergency Lock Down?

After a lock has been placed into the Emergency Lock Down state:

- All Administrative Users (User Numbers 1-11) can still unlock the physical lock.
- All Users added to the **Emergency Users** list (see above) can unlock the physical lock.
  IMPORTANT: Users disabled by a Schedule or by any other means ***cannot*** initiate Emergency Commands, even if they are added to the "**Emergency Users**" list.

To enable access for all Users (including the Master Code) during **Emergency Lock Down**: Click **Features** (for the desired Lock Profile). In the ***Emergency*** tab, un-check the **Users are Disabled During Lock Down** checkbox (default is checked).

Emergency Commands and Expanders

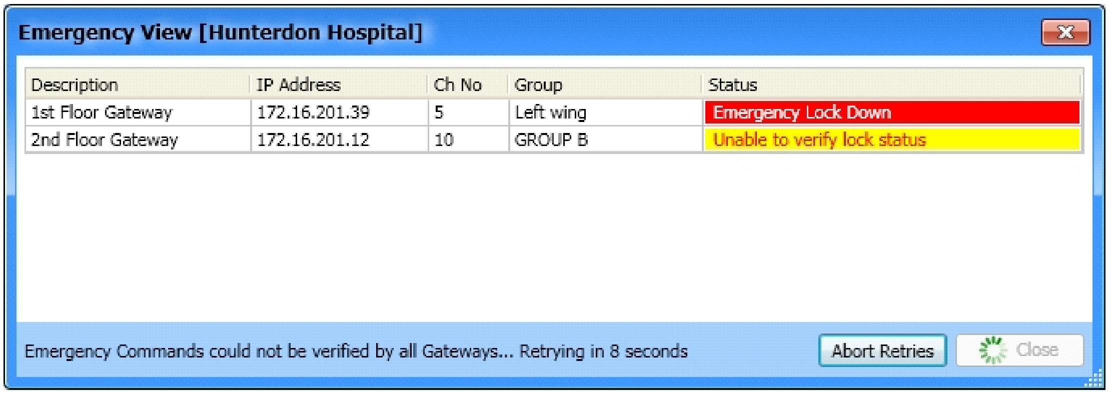
The way in which Emergency Commands are initiated (from DL-Windows or a lock keypad) does not change with the addition of Expanders to your system. However, the total time to complete the Emergency Command does increase with the addition of each Expander.

Emergency > Emergency Lock Down

Selecting **Emergency Lock Down** sends a command to all Gateways (in the selected Gateway Groups) to immediately lock all of their assigned wireless locks, thus securing the protected doors from unwarranted passage. In an Emergency Lock Down state, all Administrative Users (User Numbers 1-11) can still unlock the physical lock. In addition, all Users added to the **Emergency Users** list (see page 45) can unlock the physical lock.

From the **Emergency Commands** screen, click the **Emergency Lock Down** button.

The following **Emergency View** screen appears:



Description	IP Address	Ch No	Group	Status
1st Floor Gateway	172.16.201.39	5	Left wing	Emergency Lock Down
2nd Floor Gateway	172.16.201.12	10	GROUP B	Unable to verify lock status

Emergency Commands could not be verified by all Gateways... Retrying in 8 seconds

Once all locks assigned to the Gateway receive the selected Emergency Command, the status will return "**Emergency Lock Down**" (highlighted red). In the above image, notice how the status of the second Gateway displays "**Unable to verify lock status**" highlighted in yellow. This indicates that one or more locks assigned to the Gateway may not have received the Emergency Command. Therefore, the **Emergency View** screen cannot be closed and the Emergency Command will be re-tried based upon the **Set Emergency Attempts** selection or until the **Abort Retries** button is intentionally clicked.

The following modes will be overridden by an **Emergency Lock Down** Command :

- **Normal** mode ("non-Emergency")
- **Emergency Passage** mode
- **Passage** mode (via keypad Function 45)
- **Scheduled Passage Mode** (via "unlock" Schedule)

Note: Once in **Emergency Lock Down**, the wireless physical lock(s) may be placed in Passage mode manually (using keypad Function 48).

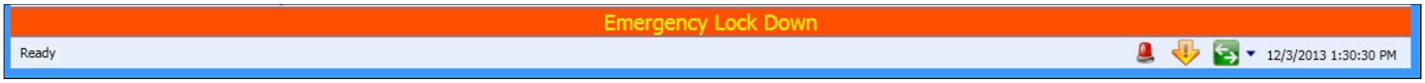
Emergency Lock Down Indication

- **In DL-Windows:** At the bottom of the DL-Windows "Main Screen", a bar will flash from red to yellow with the text "**Emergency Lock Down**" blinking continuously until a subsequent "Return to Normal" command is received (see image at the bottom of this page).
- **At Physical Lock:** Red LED blinks once every two seconds.

IMPORTANT: Threats such as fire emergencies, bomb threats or the release of hazardous substances within a protected premises may require an "Emergency Passage" Command to allow for a facility evacuation.

Other threats such as terrorist attacks, hostile intruder situations, the outdoor release of hazardous substances, tornado emergencies and other life-threatening events, may require an "Emergency Lock Down" - the opposite of a facility evacuation.

It is strongly advised that all facilities develop separate Emergency Lock Down and Emergency Passage procedures appropriate for the specific premises, and these Emergency procedures be frequently practiced and continually refined.

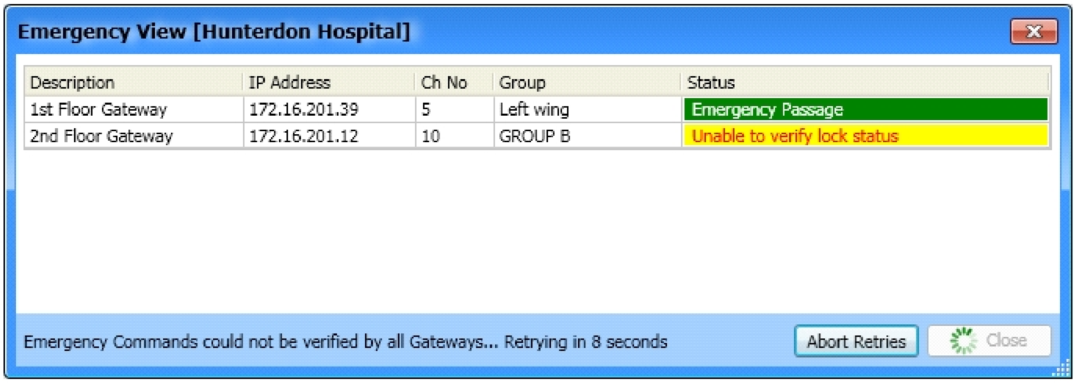

Emergency Lock Down

Emergency > Emergency Passage

Selecting **Emergency Passage** sends a command to all Gateways (in the selected Emergency Groups) to immediately unlock all of their assigned wireless locks, thus un-securing the protected doors to allow passage. In an Emergency Passage state, User credentials are no longer required to allow passage. **Please use caution when using this feature, and consider all implications of un-securing the protected doors.**

From the **Emergency Commands** screen, click the **Emergency Passage** button.

The following **Emergency View** screen appears:



Description	IP Address	Ch No	Group	Status
1st Floor Gateway	172.16.201.39	5	Left wing	Emergency Passage
2nd Floor Gateway	172.16.201.12	10	GROUP B	Unable to verify lock status

Emergency Commands could not be verified by all Gateways... Retrying in 8 seconds

Once all locks assigned to the Gateway receive the selected Emergency Command, the status will return "**Emergency Passage**" (highlighted green). In the above image, notice how the status of the second Gateway displays "**Unable to verify lock status**" highlighted in yellow. This indicates that one or more locks assigned to the Gateway may not have received the Emergency Command. Therefore, the **Emergency View** screen cannot be closed and the Emergency Command will be re-tried based upon the **Set Emergency Attempts** selection or until the **Abort Retries** button is intentionally clicked.

The following modes will be overridden by an **Emergency Passage** Command :

- **Normal** mode ("non-Emergency")
- **Emergency Lock Down** mode
- **Locked** mode (via keypad Function 46)
- **Scheduled Locked Mode** (via "lock" Schedule)

Note: Once in **Emergency Passage**, the wireless physical lock(s) may be placed in Locked mode manually (using keypad Function 49).

For areas that must remain secure, even in an Emergency Passage state, we recommend de-selecting the feature "**Lock Responds to Emergency Commands**" in the **Features** screen.

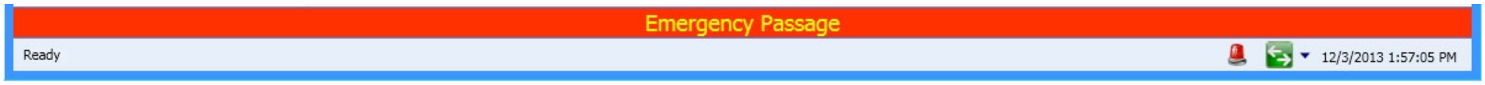
Emergency Passage Indication

- **In DL-Windows:** At the bottom of the DL-Windows "Main Screen", a bar will flash from red to yellow with the text "**Emergency Passage**" blinking continuously until a subsequent "Return to Normal" command is received (see image at the bottom of this page).
- **At Physical Lock:** Red LED blinks once every two seconds.

IMPORTANT: Threats such as fire emergencies, bomb threats or the release of hazardous substances within a protected premises may require an "Emergency Passage" Command to allow for a facility evacuation.

Other threats such as terrorist attacks, hostile intruder situations, the outdoor release of hazardous substances, tornado emergencies and other life-threatening events, may require an "Emergency Lock Down" - the opposite of a facility evacuation.

It is strongly advised that all facilities develop separate Emergency Lock Down and Emergency Passage procedures appropriate for the specific premises, and these Emergency procedures be frequently practiced and continually refined.

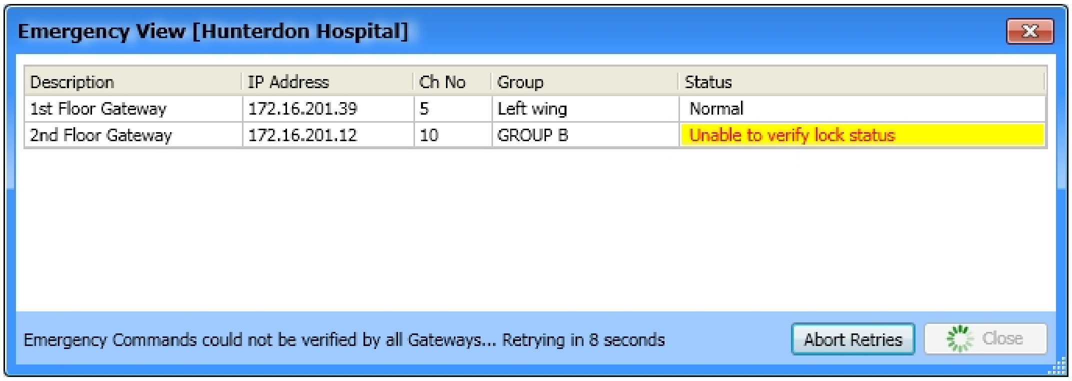


Emergency > Emergency Return to Normal

Selecting **Emergency Return to Normal** sends a command to all Gateways (in the selected Emergency Groups) to immediately revert all assigned locks to the state they were in prior to the initiation of the Emergency command. For example. if the lock was in an unlocked state due to a Schedule, and a subsequent Emergency Lock Down was initiated, the **Emergency Return to Normal** command will revert the lock back to its original unlocked state.

From the **Emergency Commands** screen, click the **Emergency Return to Normal** button.

The following **Emergency View** screen appears:



Emergency View [Hunterdon Hospital]

Description	IP Address	Ch No	Group	Status
1st Floor Gateway	172.16.201.39	5	Left wing	Normal
2nd Floor Gateway	172.16.201.12	10	GROUP B	Unable to verify lock status

Emergency Commands could not be verified by all Gateways... Retrying in 8 seconds

Once all locks assigned to the Gateway receive the selected Emergency Command, the status will return "**Normal**". In the above image, notice how the status of the second Gateway displays "**Unable to verify lock status**" highlighted in yellow. This indicates that one or more locks assigned to the Gateway may not have received the Emergency Command. Therefore, the **Emergency View** screen cannot be closed and the Emergency Command will be re-tried based upon the **Set Emergency Attempts** selection or until the **Abort Retries** button is intentionally clicked.

The following modes will be overridden by an **Emergency Return to Normal** Command :

- **Emergency Lock Down** mode
- **Emergency Passage** mode

WARNING

NEVER use Emergency Commands to "toggle" Passage Mode, as this will severely impact battery life.

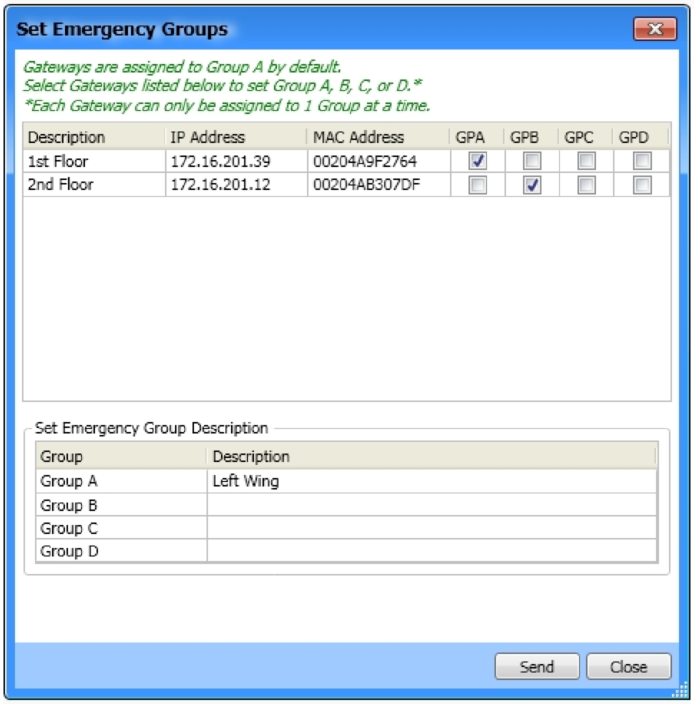
Emergency Commands > Set Emergency Groups

As mentioned in the previous section, each Gateway added to an Account is placed into Emergency "**GROUP A**" by default. This is done to ensure that Gateways will communicate with each other in an Emergency, without the use of DL-Windows (the Emergency initiated via the keypad). **Note:** Access to the **Set Emergency Groups** screen (from the **Emergency Command** screen or from **Gateway Configuration** > **Gateways** menu) is disabled when only one Gateway exists in the Account.

In addition, Emergency Grouping is available to separate Gateways (and therefore their assigned locks) intentionally. For example, to prevent a Gateway whose locks control a secure location from receiving an Emergency Command, place the Gateway into "**GROUP B**"; thus the User may selectively decide via the **Emergency Command** screen, which Group(s) will receive the Emergency Command.

It is also in the **Set Emergency Groups** screen where you may configure the individual description text reflected in the **Emergency Command** screen of the Emergency Group (replacing "**GROUP A**" with another description).

In the **Emergency Command** screen, click the **Set Emergency Groups** button to open the **Set Emergency Groups** screen. The **Set Emergency Groups** screen may also be accessed from **Gateway Configuration** > **Gateways** > **Set Emergency Groups**.



Gateways are assigned to Group A by default.
*Select Gateways listed below to set Group A, B, C, or D.**
**Each Gateway can only be assigned to 1 Group at a time.*

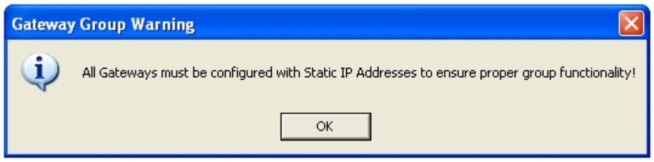
Description	IP Address	MAC Address	GPA	GPB	GPC	GPD
1st Floor	172.16.201.39	00204A9F2764	☑	☐	☐	☐
2nd Floor	172.16.201.12	00204AB307DF	☐	☑	☐	☐

Set Emergency Group Description

Group	Description
Group A	Left Wing
Group B	
Group C	
Group D	

Prerequisite

The following message appears any time the **Set Emergency Groups** screen is accessed:

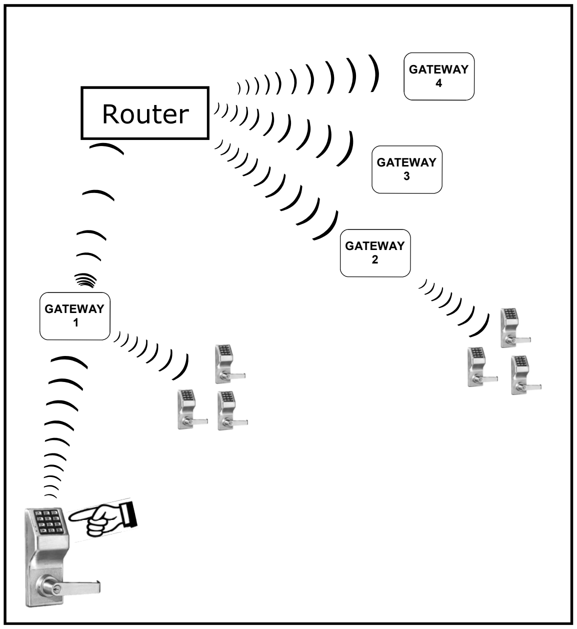


All Gateways must be configured with Static IP Addresses to ensure proper group functionality!

How it Works

When an Emergency Command is initiated from a keypad, the Command is disseminated to all Gateways, and their locks, in the Account. See diagram at right. To allow communication between Gateways, each Gateway must possess the static IP address of every *other* Gateway in the Account. The static IP address "table" is distributed to each Gateway in the Account upon:

- The addition of a new Gateway to the Account
- The removal of a Gateway from the Account
- A manual Emergency Group change

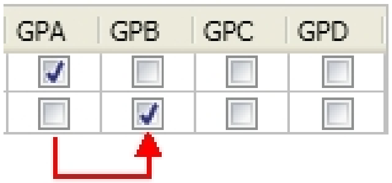


The diagram above illustrates how Emergency Commands are distributed: Initiating an Emergency Command at the lock keypad causes the keypad to send the Emergency Command to its associated Gateway (named "Gateway 1"). "Gateway 1" then sends the Emergency Command to all locks assigned to "Gateway 1". "Gateway 1" then sends the same Emergency Command to each Gateway IP address listed in its static IP address "table" via the Router. With each Gateway receiving the Emergency Command from "Gateway 1", each of these Gateways can then send the Emergency Command to each of its assigned locks. Notice that DL-Windows is not needed to disseminate Emergency Commands and therefore not shown in this diagram.

Emergency Commands > Set Emergency Groups (cont'd)

Setting Emergency Groups

Emergency Group association of any Gateway may be intentionally changed from "**GROUP A**" to another Group (**GPB**, **GPC** or **GPD**). **Note:** A single Gateway can only be assigned to one Emergency Group at a time. To change a Gateway assignment to another Group, click to highlight the desired Gateway, then click the desired Emergency Group checkbox.



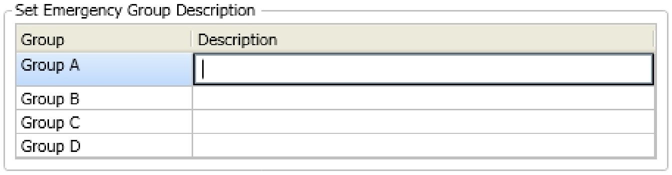
GPA	GPB	GPC	GPD
☑	☐	☐	☐
☐	☑	☐	☐

Note: Every Gateway MUST have an association to an Emergency Group.

After making selections, click the **Send** button, and the new Group associations will be distributed to the Gateways.

Setting Emergency Group Descriptions

The default Emergency Group names ("**GROUP A**", "**GROUP B**", etc.) may be changed as desired. The new Emergency Group name will then be reflected in the **Emergency Command** screen. To modify the name, in the **Set Emergency Groups** screen, double-click in the **Description** field of the desired Group, and type the new Emergency Group description name (maximum 16 characters).



Set Emergency Group Description

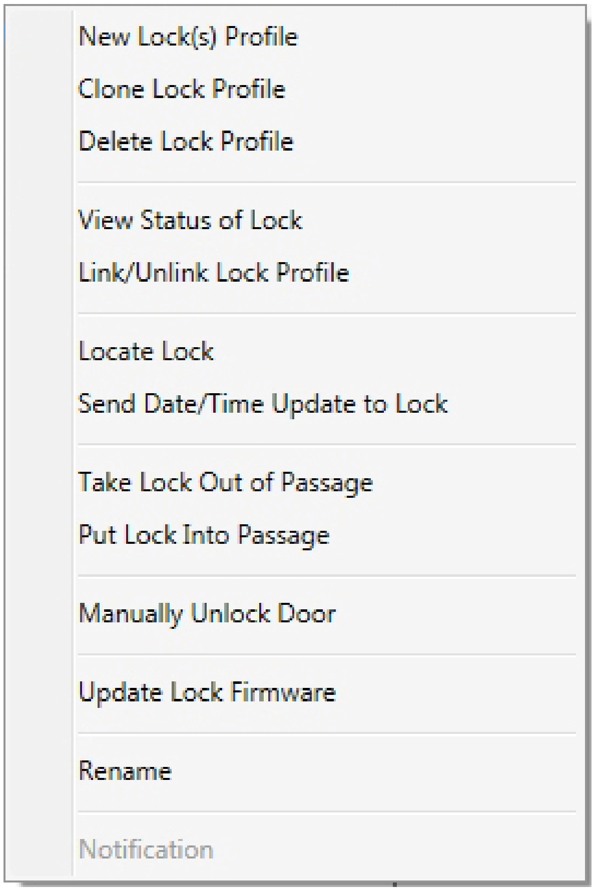
Group	Description
Group A	|
Group B	
Group C	
Group D	

When finished making changes to the Emergency Group descriptions, click **Close** to save and exit the screen (description changes do not require the use of the **Send** button).

Networx Lock Right-Click Profile Menu

For wireless locks, additional options are available for Networx Lock Profiles. In the Account List area, click the Account, then click the small "+" sign next to the "**blue file cabinet**" icon, and all Lock Profiles in the Account appear. Click the desired Lock Profile (denoted by the "**padlock**" icon) then right-click to display the right-click menu shown below.

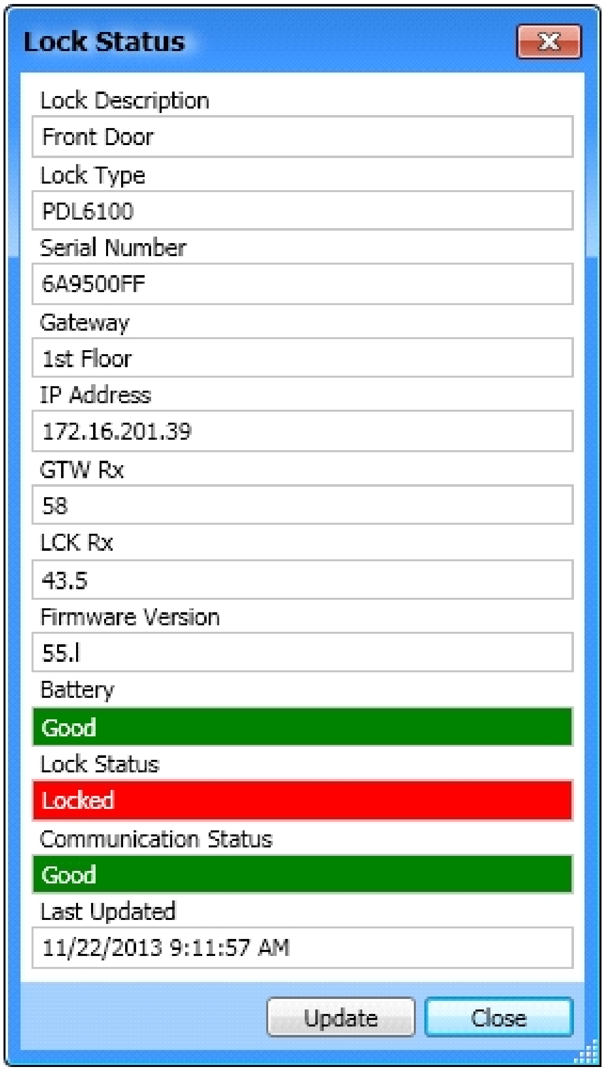
Note: The first three items listed (plus "**Rename**") in this right-click menu (shown below) are items that also exist for non-wireless locks. For information regarding these menu items, see OI382.



- **New Lock(s) Profile** (see OI382)
- **Clone Lock Profile** (see OI382)
- **Delete Lock Profile** (see OI382)
- **View Status of Lock** (page 52)
- **Link/Unlink Lock Profile** (page 53)
- **Locate Lock** (page 54)
- **Send Date/Time Update to Lock** (page 54)
- **Take Lock Out of Passage** (page 54)
- **Put Lock Into Passage** (page 55)
- **Manually Unlock Door** (page 55)
- **Update Lock Firmware** (page 56)
- **Rename** (see OI382)
- **Notification** (page 56)

Right-Click Menu > View Status of Lock

In the Account List area, click to highlight a Lock Profile, then right-click and select **View Status of Lock** from the menu that appears. Upon selection, the **Lock Status** is updated and retrieved, and displays various attributes of the selected lock. **Note:** Lock must be Linked to a Lock Profile in order to view the **Lock Status** screen.



Lock Status

Lock Description: Front Door

Lock Type: PDL6100

Serial Number: 6A9500FF

Gateway: 1st Floor

IP Address: 172.16.201.39

GTW Rx: 58

LCK Rx: 43.5

Firmware Version: 55.I

Battery: Good

Lock Status: Locked

Communication Status: Good

Last Updated: 11/22/2013 9:11:57 AM

Lock Description
Displays the name of the selected Lock Profile.

Lock Type
Specifies the model of the Trilogy Networx™ series locking device, such as "PDL6100", "DL6100" or "PL6100".

Serial Number
Displays the lock's unique serial number assigned and programmed into the lock firmware at the factory. Each Networx lock is identified in the system by this unique serial number.

Gateway
Displays the name of the Gateway to which the selected physical lock is assigned. **Note:** Lock Assignment to an *added* Expander is not displayed here. To view the Expander to which the lock is assigned, click **Gateway Configuration** > **Locks** > **View Gateway's Lock Table**.

IP Address
Displays the IP address of the Gateway to which the physical lock is assigned.

GTW Rx
Indicates the radio transmission strength, as measured between the Gateway / Expander to the physical lock. A **higher** number indicates **stronger** signal.

LCK Rx
Indicates the radio transmission strength, as measured between the physical lock to the Gateway / Expander. A **higher** number indicates **stronger** signal.

Firmware Version
Indicates firmware source code edition of the selected physical lock.

Battery
Displays the status of the battery powering the physical lock. If battery status cannot be retrieved, "**Unknown**" will be displayed.

Lock Status
Indicates the latest condition of the physical lock (i.e. "Locked", "Passage", etc.). If status is unknown or unable to be retrieved, "Communication Error" will be displayed.

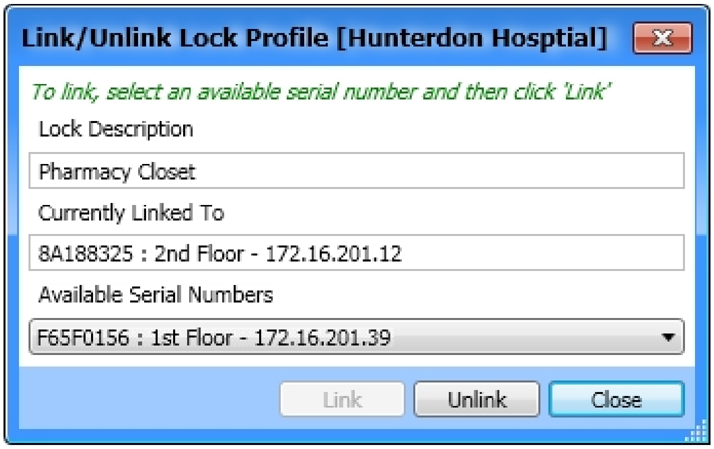
Communication Status
Indicates the integrity of the communication link between the physical lock and the Gateway / Expander. If status is unknown or unable to be retrieved, "Communication Error" will be displayed.

Last Updated
Displays the date and time of the latest lock status update.

Update (button)
Click to request an updated lock status from the physical lock. All fields will be refreshed upon lock status retrieval.

Right-Click Menu > Link/Unlink Lock Profile

In the Account List area, click to highlight a Lock Profile, then right-click and select **Link/Unlink Lock Profile** from the menu that appears. Upon selection, a condensed version of the **Link/Unlink Lock Profile** screen appears. For detailed information about Linking physical locks to Lock Profiles, see "**LINKING PROCEDURE**" on the bottom of page 17.



Link/Unlink Lock Profile [Hunterdon Hosptial]

To link, select an available serial number and then click 'Link'

Lock Description: Pharmacy Closet

Currently Linked To: 8A188325 : 2nd Floor - 172.16.201.12

Available Serial Numbers: F65F0156 : 1st Floor - 172.16.201.39

Lock Description
Displays the name of the selected Lock Profile.

Currently Linked To
Displays the physical lock's serial number, the Gateway Description, and the Gateway's IP address to which the physical lock is currently Linked. **Note:** The information in this field is only displayed when the physical lock is Linked to a Lock Profile.

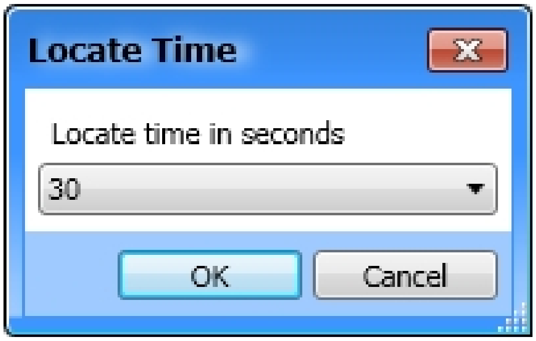
Available Serial Numbers
This pull-down list displays the lock serial numbers of all physical locks of the same lock model (Lock Type) discovered by all Gateways in the current Account. Each lock serial number is unique and assigned to the physical lock at the factory.

Link (button)
Click this button to "Link" the selected Lock Profile (**Lock Description** field) with the selected physical lock serial number (from the **Available Serial Numbers** pull-down list).

Unlink (button)
Click this button to remove the Link between the physical lock and the Lock Profile. Note that after the Link is removed, the physical lock serial number previously displayed in the **Currently Linked to** field is then displayed in the **Available Serial Numbers** pull-down list ready for Linking.

Right-Click Menu > Locate Lock

In the Account List area, click to highlight a Lock Profile, then right-click and select **Locate Lock** from the menu that appears. Upon selection, the **Locate Time** screen appears where you can set the duration of time (in seconds) for the selected lock to beep and flash its red LEDs. This option is typically used when you wish to find the physical lock or to confirm the wireless connection is operational. **Note:** The physical lock may be located even if it is not Linked to a Lock Profile.



Locate time in seconds: 30

Locate time in seconds
Click the pull-down menu to set the duration of time (in seconds) for the selected lock to beep and flash its red LEDs. Up to 255 seconds (4 minutes 15 seconds) can be selected; default duration is 30 seconds.

OK (button)
Click **OK** and the physical lock will beep and flash its red LEDs for the selected duration.

Cancel
Click to exit without requesting the locate Action.

Note: All locks on a Gateway (and/or Expander) may be sent the locate command (**Gateway Configuration** > **Locks** > **Locate ALL Locks on Gateway**). For more information, see page 34.

Right-Click Menu > Send Date/Time Update to Lock

In the Account List area, click to highlight a Lock Profile, then right-click and select **Send Date/Time Update to Lock** from the menu that appears. Upon selection, a command is sent to the physical lock to update the date and time based upon the current time and date settings of the PC running DL-Windows.

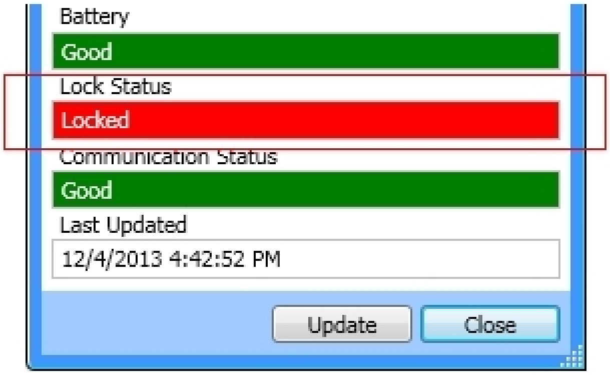
Right-Click Menu > Take Lock Out of Passage

In the Account List area, click to highlight a Lock Profile, then right-click and select **Take Lock Out of Passage** from the menu that appears. Upon selection, a command is sent to the physical lock to change its state to "locked" ("secured"). The **Lock Status** screen will automatically appear, displaying the updated **Lock Status** ("Locked").

TIP: For more information about Passage Mode and "Passage", see OI382.

IMPORTANT: If the selected physical lock is in an Emergency state (**Emergency Passage** or **Emergency Lock Down**), this **Take Lock Out of Passage** menu item will be ignored if selected. Lock must be taken out of its Emergency state (**Emergency Return to Normal**) before it will accept this menu command.

For more information about Emergency Commands, see page 43 and page 44.



Battery
Good
Lock Status
Locked
Communication Status
Good
Last Updated
12/4/2013 4:42:52 PM

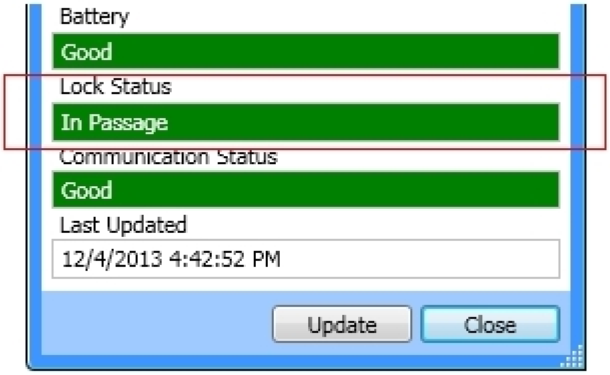
Right-Click Menu > Put Lock Into Passage

In the Account List area, click to highlight a Lock Profile, then right-click and select **Put Lock Into Passage** from the menu that appears. Upon selection, a command is sent to the physical lock to change its state to "unlocked" ("unsecured"). The **Lock Status** screen will automatically appear, displaying the updated **Lock Status** ("In Passage").

TIP: For more information about Passage Mode and "Passage", see OI382.

IMPORTANT: If the selected physical lock is in an Emergency state (**Emergency Passage** or **Emergency Lock Down**), this **Put Lock Into Passage** menu item will be ignored if selected. Lock must be taken out of its Emergency state (**Emergency Return to Normal**) before it will accept this menu command.

For more information about Emergency Commands, see page 43 and page 44.

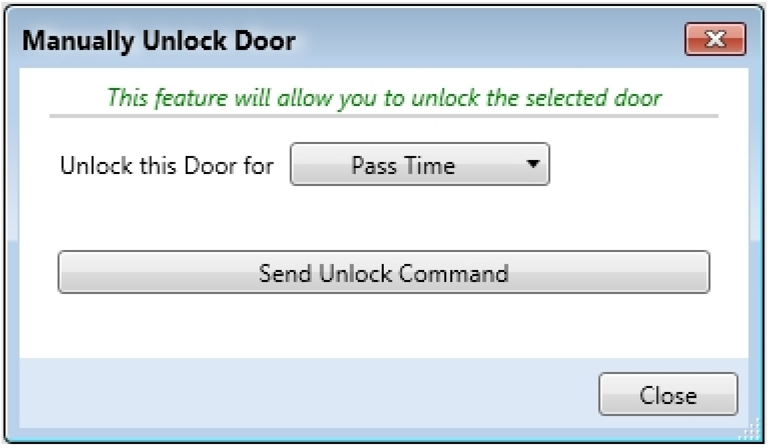


Battery
Good
Lock Status
In Passage
Communication Status
Good
Last Updated
12/4/2013 4:42:52 PM

Right-Click Menu > Manually Unlock Door

In the Account List area, click to highlight a Lock Profile, then right-click and select **Manually Unlock Door** from the menu that appears. Upon selection, the **Manually Unlock Door** dialog box appears (shown below), allowing you to unlock the selected door lock for the "**Pass Time**" or for the duration selected. **Note:** Unlocking the lock is also known as placing the lock into "Passage Mode"). The **Pass Time** is the duration the physical lock remains unlocked after a valid credential allows access to be granted. When the **Pass Time** expires, the physical lock will re-lock automatically). When the duration is selected from the pull-down, click **Send Unlock Command** to initiate the timed unlock event.

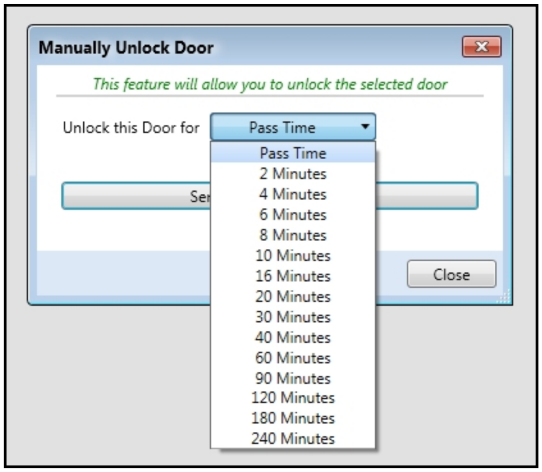
WARNING: Certain keypad-entered programming Functions may have the ability to override manually initiated timed unlock events such as this DL-Windows feature **Manually Unlock Door**. Therefore, understand and be aware of the existence of all keypad-entered (i.e. non-DL-Windows) programming Functions, if they exist. For additional details, consult the Programming Instructions included with your door lock.



Manually Unlock Door

This feature will allow you to unlock the selected door

Unlock this Door for: Pass Time



Manually Unlock Door

This feature will allow you to unlock the selected door

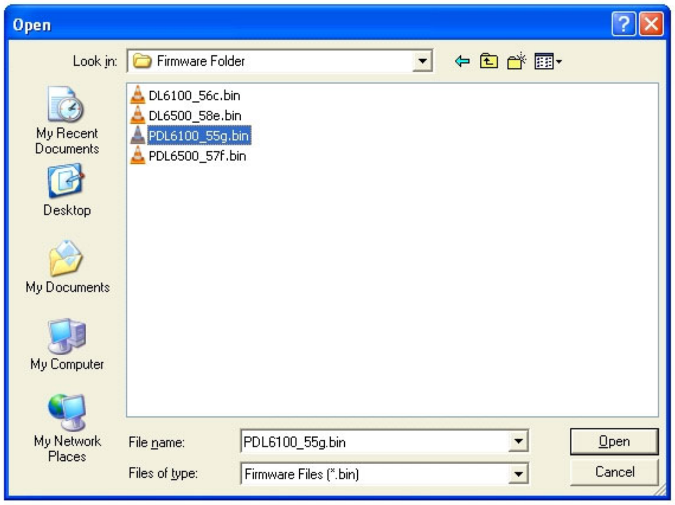
Unlock this Door for: Pass Time

Right-Click Menu > Update Lock Firmware

In the Account List area, click to highlight a Lock Profile, then right-click and select **Update Lock Firmware** from the menu that appears. Upon selection, the standard Windows **Open** dialog box appears (shown below), allowing you to browse for the binary ".bin" file containing the lock firmware update.

Select the lock firmware file based on correct Lock Type (model), then click **Open** to initiate the update process.

The system will check the integrity of the firmware, burn it into the physical lock memory, and reboot the lock. Upon completion, the **Lock Status** screen will automatically open. In the **Firmware Version** field (shown below), verify the updated firmware version of the physical lock. **Note:** Though not always necessary, it is recommended to send a full download to the lock ("**Send Profile**"). **Note:** The total time to complete a lock firmware download increases with the addition of each Expander.

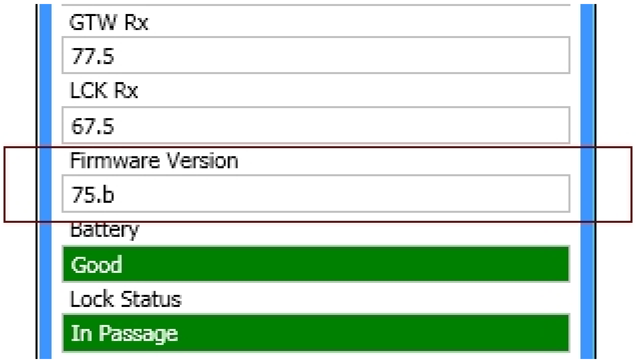


Look in: Firmware Folder

DL6100_56c.bin
DL6500_58e.bin
PDL6100_55g.bin
PDL6500_57f.bin

File name: PDL6100_55g.bin

Files of type: Firmware Files (*.bin)



GTW Rx
77.5

LCK Rx
67.5

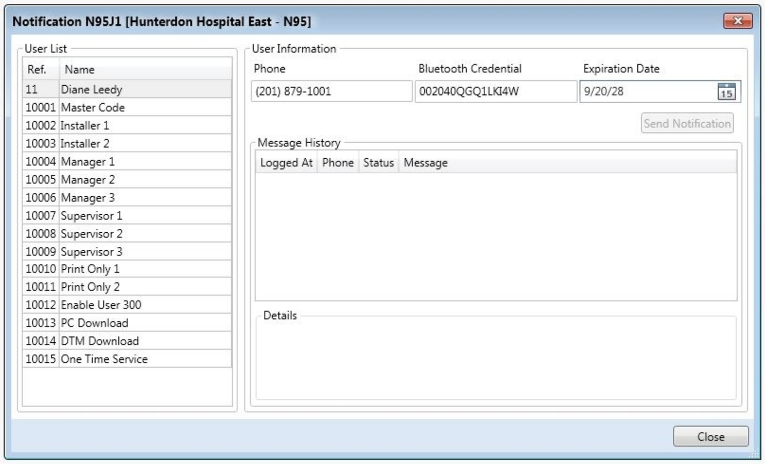
Firmware Version
75.b

Battery
Good

Lock Status
In Passage

Right-Click Menu > Notification

The **Notification** screen, shown below, is used to enroll a mobile device as a Bluetooth user credential. The iLock app, installed in the mobile device, is then used to lock and unlock the door. In the Account List area, click to highlight a Lock Profile, then right-click and select **Notification** from the menu that appears. Upon selection, the **Notification** dialog box appears (shown below), allowing you to send an SMS text message to the telephone number specified in the **Phone** field.
In the **Notification** screen, click to select a User from the **User List** (left side). Select an **Expiration Date**, if desired (see below). When finished, click **Send Notification** button; the notification should be received within a few minutes.
Note: The specified **Expiration Date** specified will disable the Bluetooth credential at midnight on that date (i.e. one second after 11:59:59 PM, at the end of the date selected). This DL-Windows selection is not applicable to locally added Bluetooth smart devices (using the iLock app). The text message received at the mobile device will read, "Alarm Lock: Share Bluetooth Credential", and will include a link that must be tapped and approved to complete the connection process.



Notification N95J1 [Hunterdon Hospital East - N95]

User List

Ref.	Name
11	Diane Leedy
10001	Master Code
10002	Installer 1
10003	Installer 2
10004	Manager 1
10005	Manager 2
10006	Manager 3
10007	Supervisor 1
10008	Supervisor 2
10009	Supervisor 3
10010	Print Only 1
10011	Print Only 2
10012	Enable User 300
10013	PC Download
10014	DTM Download
10015	One Time Service

User Information

Phone	Bluetooth Credential	Expiration Date
(201) 879-1001	002040QGQ1LKI4W	9/20/28

Message History

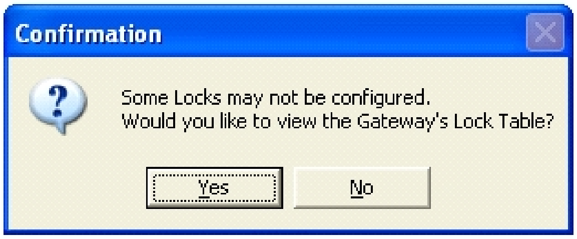
Logged At	Phone	Status	Message

Details

TROUBLESHOOTING

LOCK ASSIGNMENT FAILURE

I discovered the lock successfully but after making the selection and selecting "Assign Lock", the following message appeared:



Confirmation

Some Locks may not be configured.
Would you like to view the Gateway's Lock Table?

This message appears after several configuration attempts by the Gateway (and/or Expander). This indicates the physical lock did not successfully receive the configuration data (internal lock designation, a specific radio channel and security data), and therefore is unable to be assigned to the Gateway/Expander.

When this message appears, perform of the following:

1. Click **Yes** to first view the locks that were not configured / assigned (by viewing the **Gateway Lock Table**).
2. In the **Gateway lock Table**, click the **Re-Configure Unassigned Locks** button to re-send the Config Table to the Gateway thus attempting re-configuration of all unassigned locks in the table.

   --or--

   In the **Gateway Configuration** screen, click **Gateways** > **Send Config Table to the Gateway**. This will also attempt to re-configure the lock(s) that failed the initial assignment attempts. See page 21 for more information regarding the use of this feature.

LOCK DISCOVERY FAILURE

I am trying to discover a Networx lock, but DL-Windows can't find it.

If no locks are found after a discovery attempt:

1. Verify that the lock is reset ("defaulted"). See the programming instructions that came with your lock for reset procedure.
2. Verify the lock is installed within an acceptable radio range of the Gateway. Refer to WI2085 for information about installation and range.
   - Test range with the Networx Signal Meter tool (part AL-NSM).
3. Verify the Gateway has been mounted and physically installed as described in the instructions included with the unit.
4. In the **Gateway Configuration** screen, try increasing the **Number of Locks to Discover** (from the pull-down).

EXPANDER DISCOVERY FAILURE

I am trying to discover Expander(s), but DL-Windows can't find it.

If no Expanders are found after a discovery attempt:

1. Verify that the Expander is reset ("defaulted"). See the instructions that came with the Expander for reset procedure.
2. Verify the Expander is installed within an acceptable range of the Gateway.
   - Test range with the Networx Signal Meter tool (part AL-NSM).
3. Verify the Expander has been mounted and physically installed as described in the instructions included with the unit.
4. Verify "Expander Group" dials are identical to the Gateway to which you wish to add the Expander(s).

EXISTING LOCK COMMUNICATION FAILURE

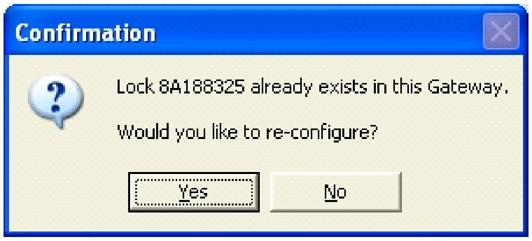
I am no longer able to communicate with an existing Networx lock. It was working just fine, now it does not work!

Before attempting to re-establish communication, consider the following:

1. Has something changed to affect the communication?
   - Is something blocking the radio signal from the Gateway to the lock?
   - Check the radio signal from the Gateway using the Networx Signal Meter tool (part AL-NSM). Is the signal strength very weak?
2. Is the lock still functioning? Find the physical lock and attempt to unlock by entering a working User Code. Are the key-presses even causing beeping sounds?

After verifying above, if the signal strength to that lock has always been strong and suddenly it is non-existent, the lock may have an internal failure. To reestablish a connection with the lock, perform the following steps:

1. Reset ("Default") the lock (see the programming instructions that came with the lock for the reset procedure).
2. Re-discover the lock. Upon assignment, the following message will display:


Confirmation

Lock 8A188325 already exists in this Gateway.

Would you like to re-configure?

This message appears because the lock was never removed from the Gateway table, therefore the lock is simply re-configured (received configuration data, including its internal lock designation, a specific radio channel and security data).

Note: Re-Linking the lock is not required.

3. Download the Lock Profile to resume normal lock operation.

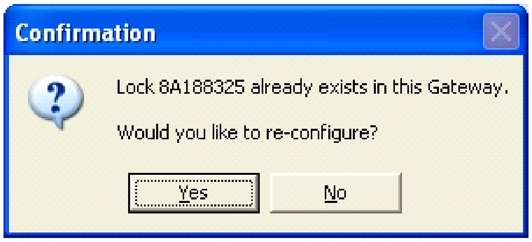
WIRELESS LOCK MEMORY FAILURE

My Schedules no longer function and/or my User Codes no longer unlock the door.

It is difficult to lose the lock programming. For example, when replacing batteries, to erase the entire program, you actually need to disconnect the batteries and press and hold a keypad button for several seconds.

However, upon disconnecting the batteries, if a key is accidentally pressed, the lock may lose its time / date information. In this case, simply turn to page 54 and follow the procedure for the "**Right-Click Menu > Send Date/Time Update to Lock**".

If upon disconnecting the batteries, you accidentally hold down a key for several seconds and indeed lose the lock programming, the solution is to re-discover the lock and re-download the program. See section "**Discovering / Assigning Wireless Locks**" on page 15. **Note:** Keep in mind that although this physical lock has lost its programming, both DL-Windows and the Gateway still consider the state of the physical lock as unchanged (still powered up, assigned and in operation). The following popup will appear upon attempted re-assignment of the lock.


Confirmation

Lock 8A188325 already exists in this Gateway.

Would you like to re-configure?

Note: Re-Linking the lock is not required.

GATEWAY HIGHLIGHTED RED (UNREACHABLE)

How do I re-establish communication with a Gateway that is highlighted in red (unreachable)?

A working Gateway (discovered on the network, added to an Account and operational) is highlighted blue in the **Gateway Configuration** screen. When a working Gateway has subsequently lost communication with the network, the Gateway is highlighted red in the **Gateway Configuration** screen.

To re-establish a connection to the Gateway, click to select the red highlighted Gateway in the list, then click **Gateways** > **Relocate Gateways (Displayed in red)**. See page 28 for detailed information about re-establishing a connection.

GATEWAY HIGHLIGHTED BLUE BUT ACTING "UNREACHABLE"

My Gateway looks OK (highlighted blue) but seems to be unreachable because I keep receiving "Fail to Communicate" messages.

Normally, a working Gateway (discovered on the network, added to an Account and operational) is highlighted blue in the **Gateway Configuration** screen. However, if "**Prevent Gateway Status Check on Gateway Screen Open**" is checked in the **Options** screen, even "unreachable" Gateways would be highlighted blue. In other words, the status that appears could be wrong or misleading.

Simply uncheck the "**Prevent Gateway Status Check on Gateway Screen Open**" option in the **Options** screen, re-open the **Gateway Configuration** screen, and if necessary click **Gateways** > **Relocate Gateways (Displayed in red)**. See page 28 for detailed information about re-establishing a connection.

COMPUTER CRASH!

My computer running DL-Windows just crashed! I had a working system, complete with wireless locks, Gateways and a computer running DL-Windows--but that computer no longer works! What do I do?

The Gateways and wireless locks are still up and running, and therefore they still hold the configuration data (its internal lock designation, a specific radio channel and security data) necessary to get your system working. The data may be retrieved from the Gateways using a new copy of DL-Windows on a new PC (assuming you are in possession of the Security Password). Refer to page 26, **Gateway Configuration > Gateways > Import Gateway and Assigned Lock(s)** to rebuild your database.

Glossary

ACCESS = Entry into a restricted area.

ASSIGN = Add to hardware or specify a relationship. Can be used with User Codes and locks ("to *assign* User Codes to specific locks"), or with hardware identification ("the factory *assigns* each lock a unique serial number"), or a fixaed wireless communication channel between locks and a Gateway ("locks *assigned* to a Gateway").

AUDIT TRAIL = A record of DL-Windows actions (not keypad entries). Located in the File pull- down menu, Audit Trail actions include: **Logged At** (date/time); **Location** (Lock Profile name); **Action**; **Operator**; **Description**. The Audit Trail is primarily intended to track the identity of the person who logged into DL-Windows and the actions they performed; compare with the **EVENT LOG**.

CLOCK

- **REAL TIME CLOCK** = An accurate built-in clock that allows date/time stamping of events. The clock can be slowed or speeded up to fine tune long term accuracy to within three minutes per year.

CODE = Numeric sequence of numbers (such as: 1234) entered at the keypad. If Star-Enter-Key is required, must be followed by a [*] key.

COM PORT = A computer serial communications port used to communicate with the Lock and/or Data Transfer Module.

COMMUNICATE = To send or receive a transmission. To avoid the directionally confusing terms of "download" and "upload", the word "communicate" is used in this guide.

CONFIGURE = To "assign" (add) discovered physical locks to a Gateway (by sending the "Lock Config Table" to the selected Gateway). Configuring ensures a fixed wireless communication channel exists between selected physical locks and a selected Gateway.
The **Gateway Configuration** screen allows you to select a Gateway and allow that Gateway to discover physical locks; these physical locks can then be assigned to that selected Gateway. When the **Use Selected Locks** button is clicked (in the "**DISCOVERED LOCKS**" **POPUP**), the Gateway sends "configuration data" to the selected locks. This "configuration data" contains items (such as an internal lock designation, a specific radio channel and security data) that are all embedded in what is called a "Lock Config Table". This "configuration data" instructs the physical lock(s) to communicate ONLY with that Gateway and prevents other Gateways from communicating with the physical lock(s).
In short, the Gateway tries to "configure" the selected physical locks by assigning the selected physical locks to the Gateway.

CREDENTIAL = A generic word used to indicate a PIN number pressed into a lock keypad, or a proximity card or proximity keyfob.

DATA TRANSFER MODULE = A device that permits transfer of program / data between a computer and the lock.

DATE = Month, Day and Year entered as MMDDYY.

DAY OF WEEK = Sunday through Saturday.

DEFAULT = "Default" settings are the original settings that were set at the factory; in other words, it is the lock's original factory condition when the lock was first taken out of its box. The default settings are permanently encoded within the lock's fixed memory, and when the lock is first started, or when power is removed and re-applied, the original factory default settings are re-loaded and take effect.

DELETE = Used interchangeably with "Remove". User Codes (PINs) and proximity credentials can exist (occupy a User Number) within the lock programming, but are removed when "deleted" (thus the entry of a non-existent PIN does *not* allow access). Similarly, when used with DL-Windows Operators and Administrators, "delete" describes an Operator or Administrator who's **Name**, **Full Name**, **Type** and **Password** was removed from DL-Windows.

DHCP (Dynamic Host Configuration Protocol) = Automatic assignment of IP addresses to devices that are connected to a network. It eliminates having to manually assign fixed IP addresses.

DISABLE = User Codes (PINs) and proximity credentials can exist (occupy a User Number) within the lock programming, but can be rendered inoperative via Schedule, download or keypad programming (PIN entry does not allow access). Similarly, when used with DL-Windows Operators and Administrators, "disable" describes an Operator or Administrator who's **Name**, **Full Name**, **Type** and **Password** exist within DL-Windows but is rendered inoperative. Contrast with "enable," which means active and operational.

DISCOVER = To "discover" Gateways, the system searches for Gateways not yet added to an Account; to "discover" locks, the selected Gateway searches for locks not yet assigned to Gateways.

Glossary (cont'd)

DOWNLOAD = See **COMMUNICATE**.

EMERGENCY COMMANDS = For use only with the Trilogy Networx wireless network, wireless commands can be sent to all wireless locking devices in an Account during a crisis or other urgent situation: "**Emergency Lock Down**", to lock all doors in the Account; "**Emergency Passage**", to unlock all doors in the Account; and **Emergency Return to Normal"**, to revert all assigned locks to the state they were in prior to the initiation of the Emergency command.

EMERGENCY GROUP = Upon the addition of each Gateway into an Account, the Gateway is automatically placed into an Emergency Group ("**GROUP A**" by default). This is done so that upon the initiation of an Emergency Command, **ALL** Gateways in the Emergency Group (and their assigned locks) will respond to Emergency Commands issued from DL-Windows. In addition, the automatic placement of a new Gateway into an Emergency Group allows for keypad-initiated Emergency Commands to lock down an entire system from a single wireless lock.

ENABLE = See **DISABLE**

ERASE = See **DELETE**

EVENT LOG = Records local keypad entries; the Audit Trail records DL-Windows actions. See AUDIT TRAIL, above.

EVENTS = Recorded lock activity.

FIRMWARE = The software programming that runs internally within the physical lock and Gateway circuitry, containing the instructions that these devices use to perform their various functions. Firmware can be updated, if necessary.

FUNCTION (also called **Programming Functions**) = The numbers used to program lock features (enabling/ disabling Users, User Groups, Passage Mode, Schedules, etc.).

GROUP = See **EMERGENCY GROUP**

GTW Rx = Indicates the radio transmission strength, as measured between the Gateway to the physical lock. A **higher** number indicates **stronger** signal.

GUARD TOUR = A *Guard Tour Code* is used to log the movement of a security guard as he or she makes rounds from one assigned guard tour station to the next. A *Guard Tour Code* is used to log the movement of a security guard as he or she makes rounds from one assigned guard tour station to the next. Entering the User 299 code provides precise verification and accountability of a guard's movements by logging the location with a time/date stamp in the Event Log.

IMPORT = When the Account information stored in DL-Windows is lost (such as with a stolen laptop)--AND--the DL-Windows backup files are either non-existent, inadequate or lost, the "Import" options can be used to rebuild an existing wireless system using the data stored inside the onboard memory of the installed Gateway device(s).

IP ADDRESS = The IP (Internet Protocol) address is a unique address of a device (such as a computer or a Gateway) connected to a TCP/IP corporate Intranet. IP addresses are written as four groups of numbers separated by periods; these groups are called "octets". IP addresses can be permanent ("static") or dynamically assigned (by DHCP) when a device, such as a Gateway, is powered.

KEYPAD = 10-numeric keys, * and special 🔒 key.

KEYPAD PROGRAMMING = Ability to program the lock through the keypad.

KEYPRESS = Pressing a button on the lock's keypad.

LCK Rx = Indicates the radio transmission strength, as measured between the physical lock to the Gateway. A **higher** number indicates **stronger** signal.

LINK = In DL-Windows, the word "Link" is used to describe the specific action of associating a Lock Profile to the serial number of the physical lock installed on the door.

LOCATE =

- **With physical lock(s),** the Locate command causes the physical lock to "beep" and flash its LED (helpful when you wish to find the physical lock or confirm the lock's wireless connection is operational).
- **When used with a Gateway**, refers to re-discovering a "lost" Gateway device on the network. Used when an operational Gateway has lost its network connection, and appears highlighted red in the **Gateway Configuration** screen.

LOCK = A generic word used to indicate one of the many Alarm Lock locking devices that can be purchased, including devices such as the DK series keypads that trigger other locking devices.

LOCK CONFIG TABLE = When a Gateway is "discovered" and added to an Account, DL-Windows sends a **Lock Config Table** which contains the assigned (or unassigned) lock data stored in the

Glossary (cont'd)

Gateway memory. The table is a database structure that is designed to hold all physical lock data (serial numbers, etc.).

LOCK PROFILE = See **PROFILE**

LOCK ID = Identification of each door with a specific number--or in other words, a number representing an individual lock within an Account.

LOCK TYPE = Specifies the model of the Alarm Lock locking device, such as "PDL6100", "DL6100" or "PL6100".

LOG = Records local keypad entries; the Audit Trail records DL-Windows actions. See AUDIT TRAIL, above.

PASSAGE = Allow anyone to pass through the door without a User Code or proximity credential (door is unlocked).

PHYSICAL = Same as "**Real**". Tangible, not virtual. See **VIRTUAL**.

PROFILE = "**Lock Profiles"** may also be called "Lock Programs" or "Virtual Locks". A lock "Profile" can be thought of as a "virtual" lock, created within DL-Windows, that contains all of the instructions that a "real" ("physical") lock uses to perform its various functions. Use DL-Windows to create a lock "Profile" on your computer, then transfer and store the "Profile" in the memory of the "real" lock. The lock "Profile" is essentially a computer database file that maintains User Codes, Features, Time Zones and Schedules. When creating these virtual lock Profiles, you are also designing the entire virtual system--conceptualizing which doors will have which locks, adding User names and allowing or restricting access to the virtual locks by the various Users in the Account.

PROXIMITY CREDENTIAL = See **CREDENTIAL**

PROGRAM MODE = A mode allowing program/data to be entered through the keypad. Only specific Users can program a lock manually, by entering their USER CODE, followed by the 🔒 key. To exit program mode, hold any key until repeated beeps are heard.

PROXIMITY CARDS = See **CREDENTIAL**.

REAL = Same as "**Physical**". Tangible, not virtual. See **VIRTUAL**.

SCHEDULE = A programmed operation (enable / disable, lock / unlock, etc.) on a specific day (Sunday through Saturday) and time.

SUBNET (SUBNETwork) = To improve security and processing performance, network administrators often divide their corporate Intranets into interconnected but separate segments called "subnets". Subnets also allow multiple users to access the Intranet with the same subnet address. A router is typically used to allow network traffic to pass between subnets.

SUBNET MASK = The IP protocol makes use of a Subnet Mask to more efficiently route packets to their correct network destinations. When a Gateway receives a data packet, the Subnet Mask indicates how many bits of the packet's destination address are to be used for routing and which bits are to be "masked" (ignored). The Subnet Mask can be thought of as a "filter" that allows the system to ignore unnecessary information, thus increasing efficiency. This information must be obtained from your network administrator.

TIME = Hours and Minutes in the HHMM format.

TIME/DATE STAMP = A recorded date and time that an event occurred.

TIMEOUT = Immediate operation for a specified number of hours.

TYPE = See **LOCK TYPE**.

UPLOAD = See **COMMUNICATE**.

USER = A person that has their personal information typed into the **Global Users** screen, and is assigned a User Code (PIN) or proximity credential (where applicable). This User is then added to (enabled within) Lock Profiles, as necessary.

VIRTUAL = Simulated on a computer. DL-Windows allows you to create a "Lock Profile" that can be thought of as a "virtual" lock, created within DL-Windows, that contains all of the data that a "real" (physical) lock uses to perform its various functions. When creating these "virtual" lock Profiles, you are also designing the entire "virtual" system--conceptualizing which doors will have which locks, adding User Names and allowing or restricting access to the virtual locks by the various Users in the Account. Later, you will "Link" these lock Profiles with the real locks installed on the doors.

Notes

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.