

# ADDENDUM to the CA3000 USER MANUAL

## WIRELESS LOCK INTEGRATION GUIDE



**DATE:** 2 AUGUST 2011

**SOFTWARE VERSION AND BUILD:** VERSION 2.8.2.229 AND HIGHER

**DOCUMENT PERTAINS TO:** INSTALLATION AND PROGRAMMING  
ALARM LOCK WIRELESS LOCKS INTO THE  
CONTINENTAL ACCESS CA3000 CONTROL  
SYSTEM

CardAccess 3000 



## FCC WARNING

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

## NOTE

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which the user will be required to correct the interference at his own expense.

Shielded cables must be used with this unit to ensure compliance with the Class A FCC limits.

"This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications."

Le present appareil numerique n'emet pas de bruits radioelectriques dépassant les limites applicables aux appareils numeriques de la class A prescrites dans le Règlement sur le brouillage radioelectriques edicté par le ministere des Communications du Canada.

## DISCLAIMER

Continental Instruments LLC makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Further, Continental Instruments LLC reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Continental Instruments LLC to notify any person of such revision or changes. If possible, always refer to the Continental Access website ([www.cicaccess.com](http://www.cicaccess.com); click **Support**) for the latest documentation, as the released CD may not contain the latest documentation.

**Copyright © 2011 by Continental Instruments LLC.** All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, or stored in a retrieval system, without the prior written permission of Continental Instruments LLC, 355 Bayview Avenue, Amityville, NY 11701. Telephone: 631-842-9400 • FAX: 631-842-9135 • GSA# GS-07F-0039H.

ProxCard® and ProxKey® are trademarks of the HID® Corporation. Microsoft® and Windows® are trademarks of their the Microsoft Corporation. Trilogy® is a registered trademark of Alarm Lock. 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. or Continental Instruments LLC has established in any of its product, feature, or service names or logos.*

This document contains proprietary information of NAPCO Security Technologies. Unauthorized reproduction of any portion of this manual without the written authorization of NAPCO Security Technologies is prohibited. The information in this manual is for informational purposes only. It is subject to change without notice. Companies, names and data used in examples herein are fictitious unless otherwise noted. NAPCO Security Technologies assumes no responsibility for incorrect information this manual may contain.

## A NAPCO SECURITY TECHNOLOGIES COMPANY

Publicly traded on NASDAQ Symbol: NSSC

Visit our websites at

<http://www.cicaccess.com/>

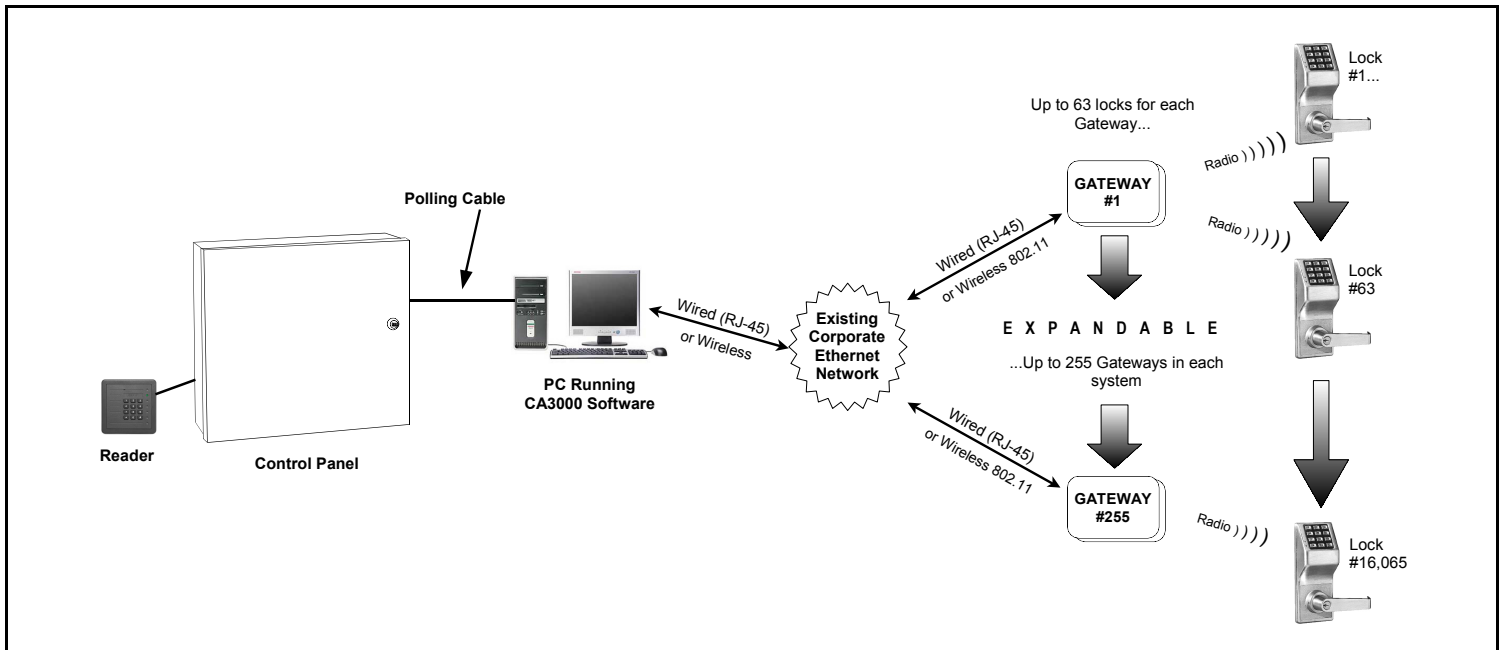
<http://www.napcosecurity.com/>

<http://www.alarmlock.com/>

# Table of Contents

Overview .....	4
Capacity .....	4
Network Security .....	4
How to Use This Manual .....	4
Ordering Information.....	5
CA3000 System Requirements .....	5
Gateway Specifications.....	6
Network Considerations .....	7
Terminology .....	9
Gateway Hardware Installation.....	10
Resetting the Gateway .....	12
Quick Start: Add Gateways and Locks .....	13
Gateways > Discover Gateways .....	19
Gateways > Update Gateway Status .....	20
Gateways > Send Firmware to Gateway .....	21
Gateways > Send Config Table to Gateway.....	22
Gateways > Replace Gateway .....	23
Gateways > Remove Gateway .....	24
Gateways > Configure Network Settings .....	25
Locks > Discover Locks.....	27
Locks > Locate All Locks.....	28
Locks > Display Configured Locks .....	29
Locks > Set Clock on All Locks.....	31
Troubleshooting .....	32
Radio and Television Interference Statement .....	35
Alarm Lock Limited Warranty .....	36

# Overview



## OVERVIEW

Used with the Trilogy Networkx™ series locks and keypads, the CardAccess CA3000 software allows you to upload and download programming features **wirelessly** using a computer network. Use your computer to retrieve events, download badge / time schedules / badge formats and program features into each wireless lock in the system.

CA3000 software is installed on a computer that is connected to a network (either a small Ethernet network or large corporate LAN). 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 Networkx™ series door locks.

To ensure each physical lock is identified correctly by the CA3000 software, 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.

**Note:** Although you can set up the wireless network first and add locks to the doors later, for the sake of convenience it is recommended that you have at least one Networkx™ lock installed on a door before setting up your wireless system. Note that stand-alone individual lock programming at the lock keypad is not supported; in other words, the door lock may only be placed into operation by the use of the CA3000 software. For more information, see the Wireless Lock Hardware Guide (WI1969).

## CAPACITY

In addition, each installed system can contain 255 Gateways--and each Gateway can control up to 63 locks--for a maximum of 16,065 locks allowed. Furthermore, each Continental Networkx lock can contain 3000-4000 badges (depending on configuration).

## 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.

## HOW TO USE THIS MANUAL

**CA3000 software is the basis for wireless lock programming.** For those unfamiliar with using CA3000 software, stop here and review the CA3000 User Manual. It may be helpful to create a "test Account" in CA3000 while walking through the examples presented in this User Guide.

If you are already familiar with CA3000, the transition to working with wireless locks will be straightforward with slight additions in terminology. 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 Wireless Lock Hardware Guide (WI1969) to put the locks into use.
- **To set up the wireless Networkx system** and connect the network to CA3000, go to the "**Network Considerations**" section on page 7.

# Overview (cont'd)

## 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-IM80211** - Hardwired/Wireless 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 Network Locks. Ceiling- or wall-mountable.
  - **Gateway "Wired" AL-IME** - Hardwired Gateway Interface Module, supports up to 63 Network 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-IMEPOE** - Hardwired Gateway Interface Module + POE (Power Over Ethernet), supports up to 63 Network Locks, connects directly to a network using a standard RJ-45 Ethernet cable and POE. Ceiling- or wall-mountable.
  - **Gateway "Plenum Rated POE" AL-IMEPOEP** - Same as above "AL-IMEPOE", with added enclosure protections and installation hardware for mounting above "drop-ceiling" tiles or other locations subject to air pressure changes (HVAC air-filled spaces, etc.).
- Note:** Alarm Lock door lock models not yet converted to the CA3000 system begin with "DL", "PL" or "PDL" (for example "PDL6100". Locks converted to the CA3000 system have the letter "C" added before the "DL", "PL" or "PDL" letters (for example, an Alarm Lock model "PDL6100" becomes a "CPDL6100" when converted for use with CA3000.
- **CPDL6100/26D** - Cylindrical Trilogy® Network™ 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 SCI keyway for manual key override, 4 7/8" ASA Strike (included).
  - **CPL6100** - Cylindrical Trilogy® Network™ 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 SCI keyway for manual key override, 4 7/8" ASA Strike (included).
  - **CETPDNL, CETDLN & CETPLN** - Network™ Wireless standalone access control exit trims for most major manufacturers of exit devices. Ideal for securing exterior doors in schools, hospitals and commercial build-

ings, Trilogy Exit Trims allow audit trail, multi-users and auto lock/unlock capabilities. For the highest security measures, the CETPDNL is outfitted with both PIN and HID Prox technology. Both CETDLN and CETPDNL locks come with a rugged, 12-button metal keypad and a non-handed fully field reversible clutch mechanism to insure long life and durability. Add, delete, change users at the keypad or use CA3000 software to manage your system at the PC with ease. Our Trilogy Exit Trims grant access for up to 2000 users, provide 40,000 event audit trail and 500 lock/unlock scheduled events with time zone support. Also available for purchase is our proximity-only Exit Trim model (ETPLN).

- **WI1674** - CPDL6100 Installation Instructions.
- **WI1676** - CPDL6100 Door Installation Template.

See [www.cicaccess.com](http://www.cicaccess.com) for a complete list of all available standard Trilogy and Network™ series devices and manuals (downloadable in PDF format).

## CA3000 SYSTEM REQUIREMENTS

Minimum Server (1-4 Workstations) Software and Hardware Requirements:

- Processor** - Pentium Dual Core, 2.6GHz (min)
  - Ram** - 2.0 GB Min/ 3GB+ for Win 7 and Win Server 2008
  - Hard Drive** - 300 GB
  - USB Ports** - 4 Min
  - Serial Ports** - Optional - 1 expandable to 64
  - Parallel Ports** - Optional - 1
  - Mouse** - PS2 or USB
  - Monitor** - 17" SVGA (1024x768)
  - CD/DVD ROM** - 48x/16x
  - CDRW/DVDR** - 24x/8x
  - Sound** - Optional but Stand-Alone recommended
  - Network Card** - 100/1000 Mb NIC Ethernet
  - Operating System** - Win XP Pro w/SP3, Win 7 Pro 32/64 bit, Win 2003 Server 32/64 bit, or Win 2008 Server 32/64 bit.
  - Database** - MS SQL 2005/2008 Express or MS SQL Server 2005/2008 for higher performance
  - Backup** - Tape / CD / DVD / Network
  - System Size** - This is the recommended PC server specification for a system with up to four workstations. It can be used for a stand-alone system, a workstation or a CA3000 Server. For high transaction environments some specifications may change.
- Notes:** - (1) If using SQL Express, the database size should not exceed 4GB. (2) Disk drive usage is dependent on the number of transactions kept in backup. (3) Additional RAM will improve performance (4) It is best to perform badge and other integration functions on a workstation, not the server.

# Overview (cont'd)

## GATEWAY SPECIFICATIONS

**Note:** For all Gateway modules, network activity or bandwidth usage does NOT occur until the user operates the CA3000 software to send programming to (or receive log data from) locks.

### Model AL-IM80211

("Wireless/Wired" Gateway)

#### Wireless Specifications

Wireless Standards: IEEE 802.11b; 802.11g  
Frequency Range: 2.412 – 2.484 GHz  
Output Power: 14dBm +1.5 dBm/-1.0 dBm  
Maximum Receive Level: -10dBm (with PER < 8%)  
Data Rates with Automatic Fallback: 54Mbps – 1Mbps  
Range: Up to 328 feet indoors  
Modulation Techniques: OFDM, DSSS, CCK, DQPSK, DBPSK, 64 QAM, 16 QAM

#### Network Interface

Interface: Wireless 802.11b, 802.11g and 10/100 Ethernet  
Protocols: TCP/IP, UDP/IP, DHCP

#### Security

IEEE 802.11 - PSK with AES Encryption 128-bit

#### Power Consumption

Average Power Consumption:

- 1300mW (WLAN mode; maximum data rate)
- 300mW (WLAN mode; idle)
- 750mW (Ethernet mode)

Peak Supply Current: 650mA  
Input voltage: 5 - 6 volts AC/DC

#### Environmental

Operating Temp: -20° to 60°C (-4° to 140°F)  
Storage range: -40° to 85°C (-40° to 185°F)

### Model AL-IME

("Wired" Gateway)

#### Network Interface

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

#### Encryption

128-bit AES Rijndael encryption

#### AL Radio Link

900MHz GFSK  
50 Channels  
10mW power output

#### Input Power

Voltage: 5 - 6 volts AC/DC

#### Environmental

Operating Temp: -20° to 60°C (-4° to 140°F)  
Storage: -40° to 85°C (-40° to 185°F)

### Model AL-IMEPOE

("Power Over Ethernet" Gateway)

### Model AL-IMEPOEP

("Plenum Rated POE" Gateway)

#### Network Interface

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

#### Encryption

128-bit AES Rijndael encryption

#### AL Radio Link

900MHz GFSK  
50 Channels  
10mW power output

#### Input Power

POE Voltage: 48 volts DC nominal  
Class 2

#### Environmental

Operating Temp: -20° to 60°C (-4° to 140°F)  
Storage: -40° to 85°C (-40° to 185°F)

#### Compliance

802.3af POE Standard (AL-IMEPOEP only)  
UL 2043: UL Standard for Safety Fire Test for Heat and Visible Smoke Release for Discrete Products and Their Accessories Installed in Air-Handling Spaces

# Network Considerations

This section will help you define the steps required to suit the specific needs of your installation. **Note:** Refer to the **Terminology** section on page 9.

## SUBNETS

Use the following information when installing multiple wireless Networkx Gateways within a corporate Intranet that contains multiple "subnets".

To improve security and processing performance, corporate Intranets are often divided into interconnected but separate segments called "subnets". 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.

*CA3000 can only Discover Gateways when the Gateways are connected to the same subnet to which CA3000 is also connected.*

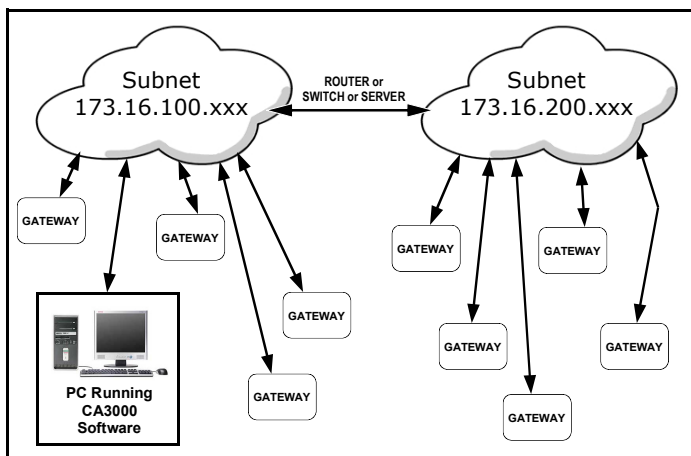
IP addresses are written as four groups of numbers separated by periods; these groups are called "octets". IP addresses can be permanent ("static") or dynamically assigned (by DHCP) when a device, such as a Gateway, is powered.

### Class B Subnets

Some corporate Intranets contain multiple "Class B" subnets; the "Class B" refers to the octet that does not change, if naming each octet from left to right. An example of two "Class B" subnets where the first two octets of each network IP address remain the same are:

- |          |     |    |     |     |
|----------|-----|----|-----|-----|
|          | A   | B  | C   | D   |
| • Subnet | 173 | 16 | 100 | xxx |
| • Subnet | 173 | 16 | 200 | xxx |

In this example, the "A" and "B" octets "173" and "16" are the same within the network. (**Note:** The "xxx" is a way of showing a variable number).



GATEWAYS ON DIFFERENT SUBNETS WITHIN A NETWORK

As shown in the image above, if the computer running CA3000 is connected to the first subnet (173.16.100.xxx), and several Gateways are connected to the second subnet (173.16.200.xxx), CA3000 *will ONLY be able to communicate with the Gateways on the second subnet when:*

- ALL Gateways use only static IP addresses, and

- The network administrator allows for open addressing between the two subnets in the network

The network administrator may decide to use routing tables or may specify blocks of addresses through which the two subnets can freely communicate in both directions. Regardless of the method selected, your network administrator must determine the range of network addresses to assign to the Gateways and to the CA3000 computer. As shown below, three address fields must be obtained from your network administrator: **IP Address**, **Subnet Mask**, and **Default Gateway**.

### Why we recommend using static IP addresses

We recommend using static IP addresses for each Gateway you install because they have the following advantages:

- CA3000 software performs more smoothly because the software does not have to waste time re-locating Gateways that have had their IP addresses changed by DHCP;
- Static IP addresses allow operation across subnets in large corporate networks (such as those that exist between buildings);

### Contact the Network Administrator

If you know that you will install your wireless Networkx system within a large corporate network that includes multiple subnets, we recommend you start by contacting the corporate network administrator and request the following:

- **IP Address** - An address for each Gateway device
- **Subnet Mask** - Filtering data (mask bits) as required by the aforementioned IP Address
- **Default Gateway** - The address of the physical device, such as a router, for the current subnet to which CA3000 will be connected

In addition, inquire about wireless authentication and encryption, as required.

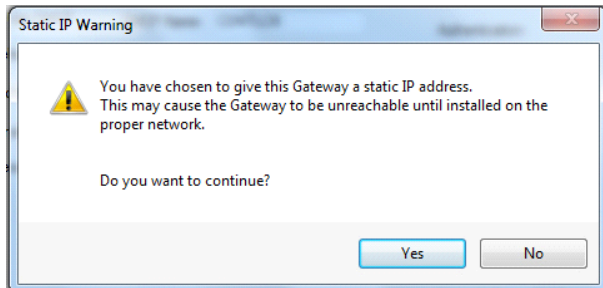
## ASSIGNING STATIC IP ADDRESSES TO GATEWAYS

CA3000 can only Discover Gateways when the Gateways are connected to the same subnet to which CA3000 is also connected. To allow CA3000 residing on one subnet to communicate with Gateways located on a second subnet (with both subnets located within a single network) a typical installation strategy is:

1. Estimate the number of Gateways needed in the installation.
2. Install CA3000 on a PC connected to the first subnet (for example, plug the PC into a wall network outlet the network administrator confirms is wired to the first subnet).
3. Open CA3000 and create a new (or open an existing) Account.

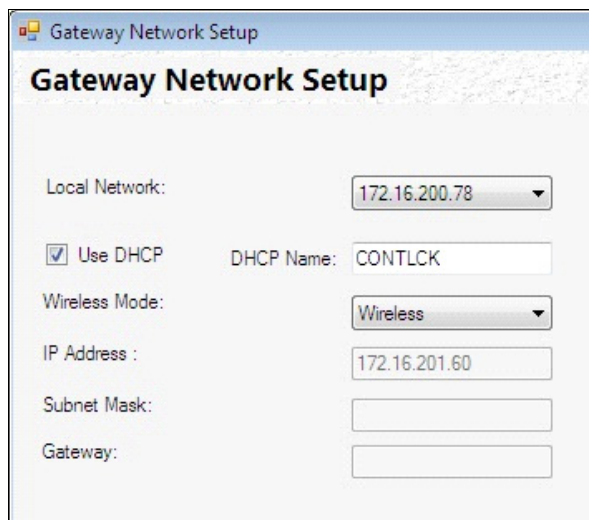
# Network Considerations (cont'd)

4. Power up a Gateway and connect the Gateway to the same (first) subnet to which CA3000 is connected (in the example above, "173.16.100.xxx"). This connection to the first subnet may be through a second network socket in the wall, or to a router (or switch) connected to the same network socket in the wall that the CA3000 PC is also connected.
5. In CA3000, discover and assign the Gateway.
6. In the **Gateway Configuration** screen, click **Tools, Configure Network Settings**. In the **Network Configuration** screen, (shown below) uncheck **Use DHCP**, and a warning popup appears:



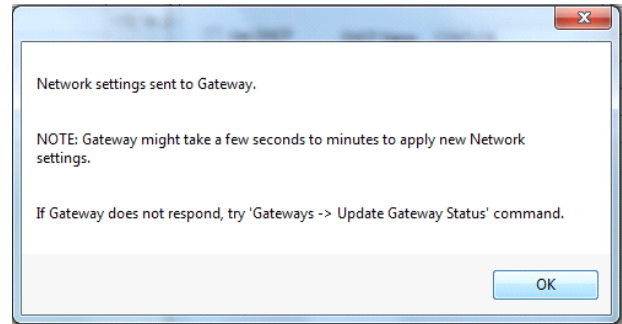
Click **Yes** to close the warning popup. In the **Network Configuration** screen, type the three addresses obtained from your network administrator into the following three fields:

- **IP Address**
- **Subnet Mask**
- **Default Gateway**



(partial screen image shown)

Click **Save Configuration and send to Gateway**. The following popup appears:



As shown in the above popup, the Gateway may take several seconds up apply the new settings. If the Gateway does not respond, click **Gateways, Update Gateway Status** before proceeding. Click **OK** to close the popup.

7. Physically disconnect (unplug) the Gateway from the first subnet, physically relocate and plug the Gateway into the second subnet (in the example above, from "173.16.100.xxx" to "173.16.200.xxx"). Install the Gateways in their final locations.

The remaining tasks are to install your locks on the doors, and have CA3000 Discover them (as outlined in the section **Quick Start: Add Gateways and Locks**):

8. Discover physical locks on the Gateway.
9. Assign (add) discovered locks to the Gateway.



# Terminology

The following words are used throughout this manual to convey specific concepts and/or actions used in the CA3000 software when adding the Trilogy Networx™ series locks .

**Assign** - Add to hardware or specify a relationship. Can be used with badges and locks ("to *assign* badges to specific locks"), or with hardware identification ("the factory *assigns* each lock a unique Serial Number"), or a fixed wireless communication channel between locks and a Gateway ("locks *assigned* to a Gateway").

**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.

**DHCP** (Dynamic Host Configuration Protocol) - Software that automatically assigns IP addresses to devices that are connected to a network. It eliminates having to manually assign fixed IP addresses.

**Discover** - To "discover" Gateways, the system searches for Gateways not yet assigned to an Account; to "discover" locks, the selected Gateway searches for locks not yet assigned to Gateways.

**Download** - See Communicate.

**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.

**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 listed in red colored text on the **Gateway Configuration** screen.

**Lock Config Table** - When a Gateway is "discovered" and added to an Account, CA3000 sends a **Lock Config Table** to the Gateway. This **Lock Config Table** is stored in the Gateway memory, and may or may not contain assigned physical lock data. The table is a database structure that is designed to hold the physical lock data (serial numbers, etc) when physical locks are "assigned" to the Gateway.

**Panel** - A "panel" has two definitions: (1) A wall-mounted microcomputer-based unit to which detection devices, access control and/or alarm system devices are ultimately connected and managed. These devices may include sirens, door contacts, PIR's, credential readers, etc. Control panels may also include an integral digital communicator to allow communication with police, fire or medical personnel. (2) A wireless Networx series door lock.

**Physical** - Same as "**Real**". Tangible, not virtual. See **Virtual**.

**Real** - Same as "**Physical**". Tangible, not virtual. See **Virtual**.

**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.

**Upload** - See Communicate.

**Virtual** - Simulated on a computer.

# Gateway Hardware Installation

## HARDWARE INSTALLATION

For a *minimum* wireless system, you need:

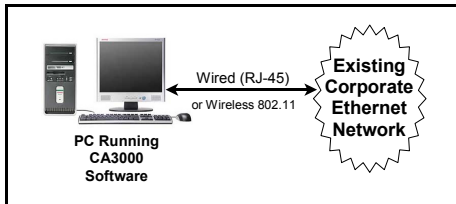
- A laptop or desktop **computer** (to run CA3000)
- A wired or wireless home **router** (to allow connection to a computer network)
- An Alarm Lock **Gateway** module (the intermediary device between the network and the locks)

**Note:** Before proceeding, you should have a working knowledge of CA3000 software. See the CA3000 User Guide for basic information such as how to install and open CA3000, how to create Accounts, how to add badges, etc.

1. **Install the CA3000 software** into your computer as described in the CA3000 User Guide.

2. **Connect your computer to a network**

If you have access to a "large network" such as an existing corporate Ethernet network (such as a LAN), connecting to a network may be as simple as plugging your computer into an RJ-45 wall jack. In this case, you may wish to contact the Ethernet network administrator and inform them as to your plans.

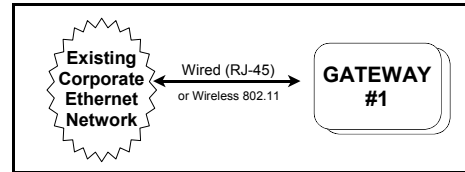


**For the connection between your computer and a large Ethernet network**, most laptops and some desktop computers contain a wireless network card (also called a "wireless network interface controller") to allow for wireless communication between your computer and a this large network. Contact the network administrator for this kind of wireless connection.

For computers *without* a wireless network card, connect the "non-wireless" network card in your computer to the network as follows: Connect one end of the Ethernet cable to the computer network card RJ-45 socket (usually located at the back of your computer); connect the other end of the cable to the RJ-45 socket at a wall jack or a modem that is part of the corporate Ethernet network / LAN. Note that wall jack or modem access points usually need to be configured first by the network administrator before the network will allow a connection.

3. **The Network Connection to the Gateway**

The connection between the network (the router or the existing corporate Ethernet network) and the Gateway device may be either **directly wired** using an Ethernet cable --or--**wirelessly** via 802.11x transmissions, as shown in the illustrations below:



Remember, the Gateway device will eventually be mounted on a wall or in a ceiling; therefore a wired network connection to the Gateway device is relatively straightforward because once you plan the final location of the Gateway and you plan the physical location of the network connection, the only remaining task is to run a wire between these locations.

The instructions for the wired connection are in the next section; for wireless connection instructions, skip to the "**Wireless Network Connection to the Gateway**" section below.

### Wired Network Connection to the Gateway

The double-ended Ethernet cable is used to connect the network **to any of the Gateway models**. Simply plug one end of the Ethernet cable into the network Router or a network wall socket (at any location within the premises) or network modem. Then connect the other end of the Ethernet cable into the Gateway module. Now skip to step 4 below, and read about the importance of selecting a favorable Gateway mounting location and signal strength considerations.

### Wireless Network Connection to the Gateway

*This wireless connection will only work with a "Hardwired/Wireless" Gateway model AL-IM80211.*

To ensure a fixed wireless communication channel exists between the network and the Gateway, you must first **temporarily** connect the network to the Gateway with an Ethernet cable.

**Why?** When the Gateway is first powered, the very first thing the Gateway tries to do is obtain an IP Address--from anywhere. If an installation takes place in a facility that contains several active networks (and/or active routers), there is a possibility that an unknown network (or router) will provide the Gateway with an IP address *outside* the network you want to use.

The solution is to **temporarily** connect the desired network to the Gateway with the double-ended Ethernet cable. This temporary wired connection ensures that all network settings (that you want to use) are sent **DIRECTLY** into the Gateway, thus ensuring that the Gateway device will **ONLY** communicate with that specific router or network.

- 3a. Connect the network to the Gateway with an Ethernet cable. Plug one end of the Ethernet cable into the network Router or a network wall socket (at any location within the premises) or network modem. Connect the other end of the

# Gateway Hardware Installation (cont'd)

cable to the Gateway module.

- 3d. Click on this **"New Gateway 1"** to select this Gateway. Write down the IP Address and MAC Address shown.

IP Address \_\_\_\_\_

MAC Address \_\_\_\_\_

- 3e. Click **Tools, Configure Network Settings**, and the **Network Configuration** screen appears:

## If using DHCP:

- From the **Wireless Mode** pull-down, click **Wireless Only**.
- Type the network name in the **Network Name (SSID)** field. For more information, refer to the setup guide for the router being used.
- From the pull-down, select the appropriate **Network Type** being used, in most cases it will be **Infrastructure**.
- Select the appropriate **Channel Number** for which the router is set. - For more information, refer to the setup guide for the router being used.
- By default, **Wireless Network Security** is disabled. We recommend to use "MAC Address Filtering" for security if your router supports this feature. If **Wireless Network Security** is desired, refer to the router setup for wireless security.

## If NOT using DHCP:

- If you are using Static IP Addresses, refer to the router setup guide for static IP address setup information.

- 3f. Disconnect the Ethernet cable from the network Router (or network wall socket) and also from the Gateway module.

## Gateway ID Card

We recommend that when installing the Gateway, a blue-colored "Gateway ID Card" be completed. Since

Gateways are often installed in ceilings or other hidden locations, their physical locations may be easily forgotten. This ID card may prove very useful when replacing Gateways, or when selecting a Gateway to use to discover locks, or whenever an installed Gateway needs to be physically located.

## 4. Mounting the Gateway module

A Gateway module acts as an interface between a computer network and the Network<sup>TM</sup> wireless locks.

### Gateway Mounting Location

Give careful consideration to the location of the Gateway when planning the layout of the system. Gateways should be mounted in elevated areas (such as drop ceilings), and should be *centrally located* within the separate lock installations. Select a convenient location that allows access to an AC outlet (to plug in the Gateway supply transformer for models AL-IM80211 and AL-IME) and allows access to the RJ-45 Ethernet cable running from the Gateway to the router/network. You can plan for a single Gateway to cover a circle several hundred feet in diameter, greater within open areas without walls. Choose a location as high above ground level as practical (home attic installations are *not* recommended), keeping in mind that metal objects may adversely affect reception. It may be helpful to draw a layout of the system, identifying all proposed Gateway locations and the anticipated door locations. Also include notations indicating construction materials in use. Although wood and wallboard construction will have little effect upon signal strength at the lock, concrete or brick can reduce signal strength by up to 35%, while steel-reinforced concrete or metal lath and plaster can reduce Gateway transmitter strength as much as 90%.

*All Gateway models should be mounted **vertically** on either a wall or ceiling. Horizontal "flat" mounting of the Gateway enclosure should be specifically avoided.*

**Note:** In difficult installations wherein distant Gateways pose reception problems, the use of multiple gateways throughout the premises is recommended.

### First Time Gateway Power Up

We supply a "Class 2" 6V power supply (*never substitute power supplies; use only the supplied unit*) that is wired to the terminal strip located on the Gateway PC board. Wiring is non-polarized, so connect either wire to either of the two terminals.

When the Gateway is first powered, the red light flashes

# Gateway Hardware Installation (cont'd)

slowly (about once every 2 seconds), indicating the unit is looking for a valid IP address (unit may take up to 90 seconds to find a valid address). If the unit finds a valid IP address prior to 90 seconds, the red light flickers.

If the unit does not obtain a valid IP address after 90 seconds, the flashing rate increases to one flash per second, and will attempt to find an IP address later.

The one flash per second flash rate indicates the Gateway is "configured". At this point you can reset the Gateway:

## Reset the Gateway

At this point, the Gateway is mounted and connected to the router (or the network) with the RJ-45 cable. Apply power to the Gateway and the red light flashes slowly, about once every 2 seconds. Before securing the Gateway housing cover, reset the Gateway memory—even if the Gateway has never been used.

"Resetting" the Gateway clears all memory and ensures that any residual voltage or test data existing from the factory is cleared from the unit. Always reset the Gateway for new installations; you can also reset the Gateway anytime after the Gateway is powered. Follow the instructions below for "**Resetting the Gateway**", then secure the Gateway housing cover with the screws provided.

## Resetting the Gateway

Two levels of the reset process exist, a "**Partial**" reset and "**Full**" reset, as follows:

"**Partial Reset**" clears the Gateway's "Lock Config Table"; but if the Gateway was previously programmed for wireless network communication, this reset leaves the Gateway in this "wireless" condition.

- *With power applied to the Gateway, press and hold the "RESET" button and the red light turns on con-*

*tinuously; continue to hold the button and the red light will start to flicker. Release the button and the red light will continue to flicker. The Gateway is now "Partially Reset".*

"**Full Reset**" returns the Gateway to its factory condition, clearing the Gateway's "Lock Config Table" and resets the network selections to its factory default "wired" condition.

- *With power applied to the Gateway, press and hold the "RESET" button and the red light turns on continuously; continue to hold the button and the red light will start to flicker. Release the button and the red light will continue to flicker. Press and hold the "RESET" button again and the red light turns on continuously...continue to hold the button and the red light will start to flicker...continue to hold the button until the red light turns on continuously...then release the button and the red light turns off...after a few seconds the red light will then start to flicker. The Gateway is now "Fully Reset".*

**Note:** Gateway modules are shipped from the factory with Alarm Lock firmware pre-installed, for use within the Alarm Lock Network system. It will therefore be necessary to convert this Gateway firmware to the firmware necessary for CA3000 integration, as detailed in the next section "**Quick Start: Add Gateways and Locks**".



# Quick Start: Add Gateways and Locks

## OVERVIEW

At this point, the CA3000 v2.8 software should be up and running with badges entered and working. Remove the Alarm Lock wireless door lock from its factory packaging, and power the lock as per the specific startup instructions included with the lock (the wireless lock can be physically installed on the door or left uninstalled while powered and configured). The Gateway should be installed at its final location and powered as per the instructions detailed in "**Gateway Hardware Installation**" earlier in this guide.

**Note:** For additional information, see the *CardAccess Quick Start Guide*. Generally, CA3000 "up and running" means the software is fully and successfully installed, the Continental security key entered and accepted, the installation computer restarted and a new password entered and accepted.

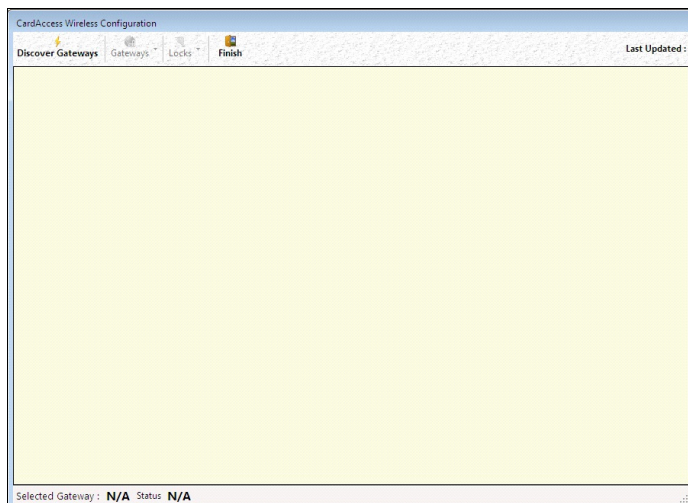
The following is a list of general steps required in CA3000 to add one wireless door lock and one Gateway into the CA3000 system:

1. **Discover Gateways**
2. **Discover Locks**
3. **Add Discovered Lock to the Gateway**

The numbered steps above correspond with the detailed procedures that follow.

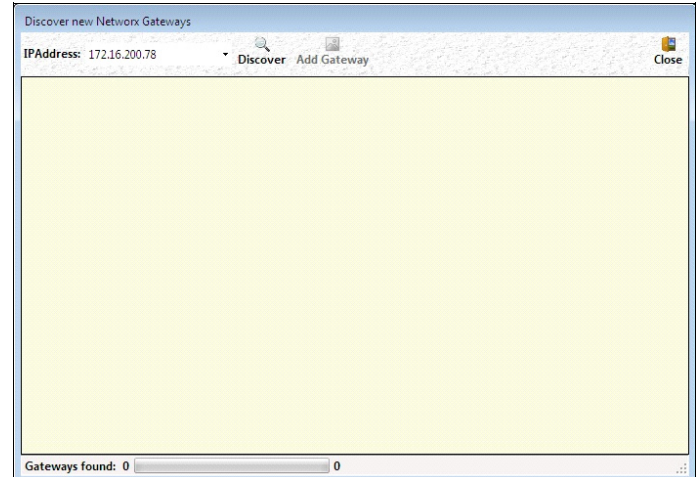
### 1. Discover Gateways

The first step is to search for Gateways not yet "configured" (enrolled into a CA3000 system). In the CardAccess 3000 main screen, click **Configuration**, **Wireless Lock Configuration**. The **CardAccess Wireless Configuration** screen opens.



In the **CardAccess Wireless Configuration** screen,

click the **Discover Gateways** button. The **Discover new Network Gateways** screen opens. Ensure the **IP Address** field displays the IP Address of the network you want to search. The **IP Address** field is also pull-down list, displaying multiple networks to which your computer is connected, if available. Click the **Discover** button to start the Gateway search.



The CA3000 software searches the network for all available Gateway modules not yet "configured" (enrolled into a CA3000 system). While the search is in progress, a splash screen appears (below). Note that similar splash screens appear when the software is performing these kinds of operations.



At the bottom of the **Discover new Network Gateways** screen, the **Gateways found** status bar displays the number of Gateways detected and current percentage progress of the search.



Wait for the status bar to reach and hold at 100% before proceeding (time to reach 100% depends on the network speed). If no Gateways are found, a small popup appears indicating "No Gateways Found" (verify the IP Address is correct, and that the Gateway is powered and connected to the network, and try again).

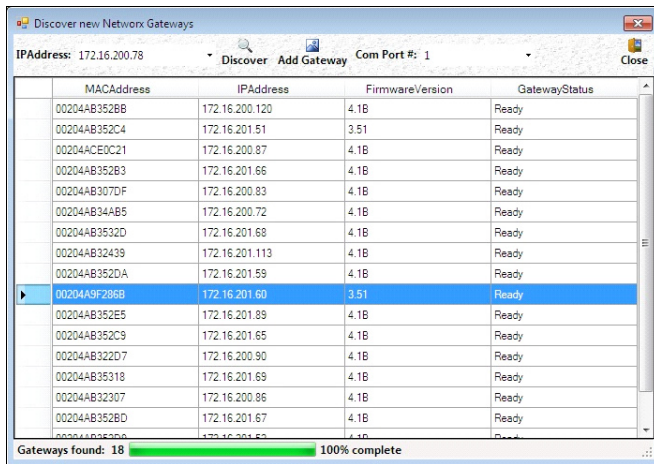
All Gateway modules found are listed in the **Discover new Network Gateways** screen, and each found Gateway module appears listed with the following data columns:

- **MAC Address** - Unique "Media Access Control" number assigned at the factory.
- **IP Address** - Assigned by DHCP to the Gateway module.
- **Firmware Version** - Internal firmware release identification. **Note:** Gateway modules are shipped from

## Quick Start: Add Gateways and Locks (cont'd)

the factory with Alarm Lock firmware pre-installed, for use within the Alarm Lock Networkx system. Therefore this column displays "3.51" to reflect this Alarm Lock Gateway firmware. When the Gateway firmware is compatible with Continental CardAccess 3000 (in the steps below), the Firmware Version will read "4.1B".

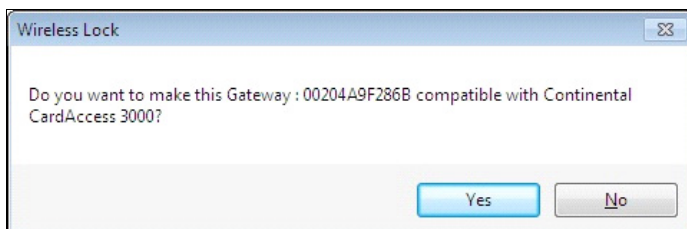
- **Gateway Status** - Condition at the time the module was discovered.



Make note of the new Gateway's unique MAC address located on a square sticker inside the Gateway enclosure (or use the blue **GATEWAY ID CARD**). It has 12 digits, grouped in 6 pairs separated by dashes. Compare the MAC Address listed on the screen to the MAC Address on the sticker to ensure the Gateway you wish to add to the CA3000 system was in fact discovered by the software.

When the Gateway you wish to add is found in the list, click the Gateway to highlight it. Notice the **Com Port #** field at the upper right. Each Gateway added to CA3000 is automatically assigned a COM port, with the first Gateway added to the system assigned to COM port #1 by default. Therefore, the **Com Port #** field displays #1 or the next available COM port. Click to highlight the Gateway and verify the COM port number displayed in the **Com Port #** field. Click the **Add Gateway** button (or just double-click the Gateway).

The following popup appears, requesting to change the selected Gateway firmware to new firmware that is compatible with CA3000:



Re-verify the MAC Address of the Gateway displayed in the popup, then click **Yes** to proceed.

If installing a Gateway for the first time, the **Gateway Password** popup appears:

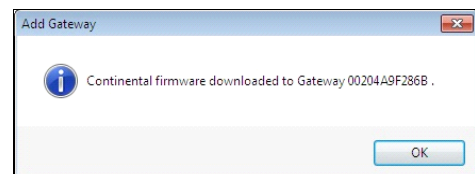


This popup appears because there must be a way for CA3000 to differentiate between separate wireless installations. For example, if a large office building has one company on the 15th floor and another company on the 16th floor, radio signals can overlap from these two separate installations. How does CA3000 prevent this confusion between wireless signals? The answer is to require a unique "Gateway Password" for each Gateway, and to embed that password within the radio transmissions to the locks.

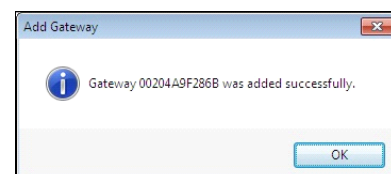
**Important:** Do **NOT** share passwords between Gateways, otherwise the radio signals can become inter-mixed! Be sure you record--in writing--all installation passwords in a safe location; once set, passwords are NOT retrievable from CA3000!

In the **Gateway Password** popup, type a Gateway password exactly 6 characters (no more--no less) in length, then click **OK** to close this popup.

During the download process, the splash screen briefly reads "Adding Gateway...please wait...", then reads "Downloading Firmware...please wait...". When the download is finished, the following popup appears:



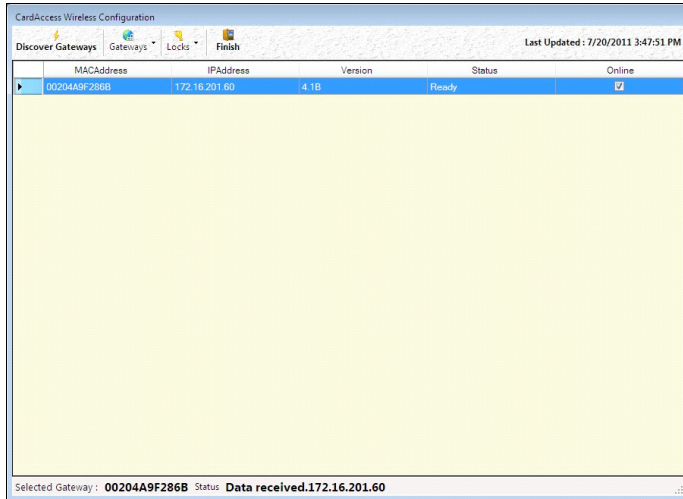
Click **OK** and another popup appears, indicating the process is complete.



# Quick Start: Add Gateways and Locks (cont'd)

Notice that the Gateway just added has been removed from the list in the **Discover new Network Gateways** screen.

If no other Gateways need to be added, close the **Discover new Network Gateways** screen by clicking the **Close** button. The "configured" Gateways enrolled into the CA3000 system are now listed in the **CardAccess Wireless Configuration** screen:



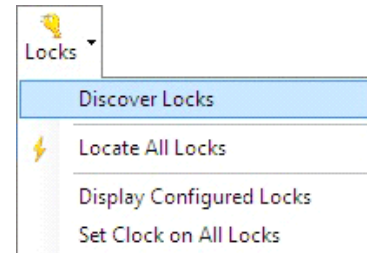
Each configured Gateway module appears listed with the following data columns:

- **MAC Address** - Unique "Media Access Control" number assigned at the factory.
- **IP Address** - Assigned by DHCP to the Gateway module.
- **Version** - Internal firmware release identification.  
**Note:** When the Gateway firmware is compatible with Continental CardAccess 3000, the Firmware Version reads "4.1B".
- **Status** - Indicates the condition of the Gateway module the last time its status was retrieved. Retrieval occurs during several events, including:
  - when manually retrieved (clicking the **Update Status** button in the **Gateway Status** dialog)
  - after making changes to the network settings (click **Gateway, Configure Network Settings**)
  - after discovered locks are configured (assigned) to a Gateway
- **Online** - When the check box is checked, indicates the Gateway module is available for immediate use.

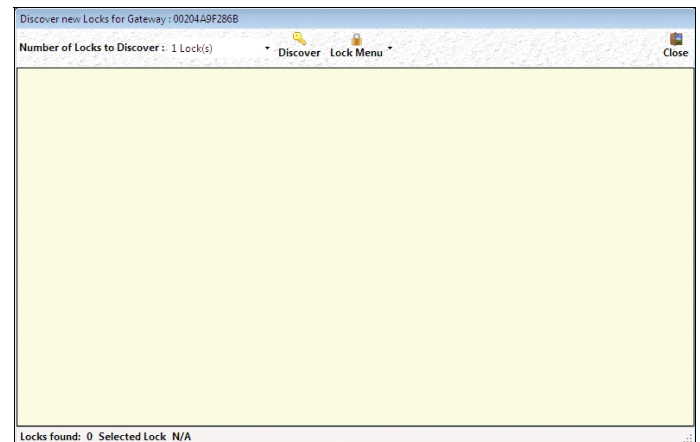
## 2. Discover Locks

In the **CardAccess Wireless Configuration** screen, click to select the Gateway you want to use to discover locks; this will also be the same Gateway to which you want to assign locks. **Note:** The Gateway selected will transmit the discovery request radio signal to all locks in the vicinity, and only those locks within range -- that have not already been assigned to a Gateway -- will respond.

With the Gateway highlighted, click **Locks, Discover Locks**.



The **Discover new Locks for Gateway** screen opens.  
**Note:** If the Gateway does have any locks assigned, double-clicking the Gateway will also open the **Discover new Locks for Gateway** screen.



The maximum search time allowed for each discovery request is 2 minutes. To minimize the search time, this screen allows you to limit the search to a certain quantity of installed locks. In addition, you can manually stop the discovery process at any time by pressing the keyboard **Esc** key.

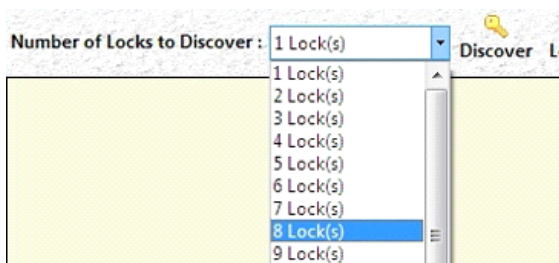
If you know the number of installed locks to be discovered, select that number and the discovery process will stop the moment that selected number of locks are found. If the number of locks selected exceeds the actual number physically installed, the discovery process will continue for either a maximum of 1 minute or until the **Esc** key is pressed.

**Example:** If the number selected is 10, but in fact only 8 locks exist, the system may find all 8 locks, but will keep searching for 10 until either the one minute timeout duration expires or until the **Esc** key is pressed.

**Note:** Only press **Esc** ONCE or additional time will be added to the search.



# Quick Start: Add Gateways and Locks (cont'd)



Click the **Number of Locks to Discover** pull-down list and select a number of locks that you want to detect. Ensuring the physical lock(s) you wish to discover are powered as per the instructions provided with the lock packaging, click the **Discover** button to initiate the search.

The next image displays the results when 8 locks were requested to be discovered ("**Number of Locks to Discover**") and 8 locks were found:

Lock ID	Transmit Signal	Receive Signal	Lock Type
187E4AE0	68	70	PDL6100
3460E074	28	24	Network Control
E49A007E	64	61	PDL6100
E49B007F	30	24	PDL6100
E4A10085	26	19	PDL6100
F7EBCBAA	31	68	CPDL6100
187E4AE0	74	86	PDL6100
DA1A00F4	31	24	PDL6100

The locks listed are only those locks (within range) that have not already been assigned to a Gateway.

The list (shown above in the **Discover new Locks for Gateway** screen) includes the following data columns for each lock:

- **Lock ID** - Each wireless lock is identified by this unique serial number programmed into the lock firmware at the factory.
- **Transmit Signal** - Radio transmission strength from the lock as measured by the Gateway, on a scale of 1-100; the lower the number the weaker the signal.
- **Receive Signal** - Radio transmission strength from the Gateway as measured by the lock, on a scale of 1-100; the lower the number the weaker the signal.
- **Lock Type** - Lock firmware type, as identified by the Gateway. Locks not yet converted to the CA3000 system will be listed as "DL", "PL" or "PDL"; locks converted to the CA3000 system will begin with the letter "C".

**Note:** We recommend that when installing a lock on a door a yellow-colored "**LOCK ID CARD**" be completed;

the information on this card is important and should be saved in a safe location.

### 3. Add Discovered Lock to the Gateway

To add ("assign") the discovered lock serial number ("Lock ID") to the specified Gateway, in the **Discover new Locks for Gateway** screen, click to select and highlight the lock you wish to add. Only one lock may be added at a time. Re-verify the Lock ID displayed matches the lock you wish to add, then click **Lock Menu**, **Add Discovered Lock**. The **Add Lock** dialog appears:

The **Add Lock to Gateway** screen contains several fields, including:

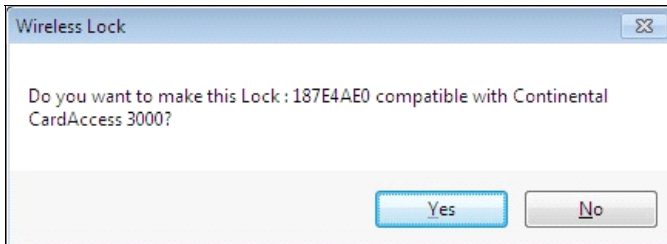
- **Gateway Address** - Unique "Media Access Control" number assigned to the Gateway module at the factory.
- **Panel Name** - User can enter the name of the lock; if you wish, this name can be changed, perhaps to identify the room or door onto which the lock has been installed. Defaults to "Lock" followed by an internally incremented number.
- **Panel #** - Internal identifier for all wireless locks in the system, assigned by the CA3000 software. Must be unique; should not be changed.
- **Lock ID** - Unique serial number programmed into the lock firmware at the factory.
- **Lock Address** - Internal lock number, from 1 through a maximum of 63, assigned by the CA3000 software and is *unique per Gateway*. This number is used by the specified Gateway to communicate with the wire-



## Quick Start: Add Gateways and Locks (cont'd)

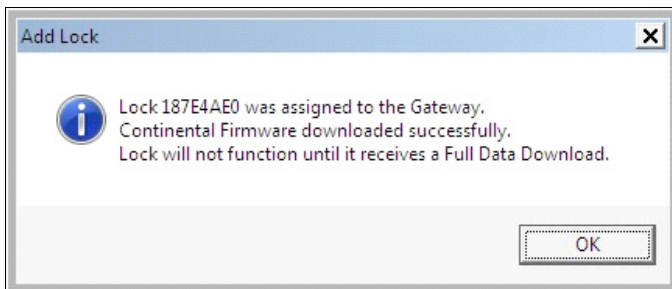
less lock. We recommend this number NOT be manually changed.

To add the lock to the Gateway, click the **Add Lock** button. A confirmation popup appears (shown below), requesting you to confirm that you wish to make the selected lock compatible with CA3000. Click **Yes** to proceed, or **No** to cancel without making changes.



**Note:** When the **Add Lock** button is clicked, the Gateway attempts to "assign" the lock by sending "configuration data" to the selected lock. 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 to communicate ONLY with that Gateway and prevents other Gateways from communicating with the physical lock. Note that this assignment process may take a few minutes.

When the selected lock compatible with CA3000, an informational popup appears:



**Note:** When a lock is converted to be compatible with CA3000 and assigned to a Gateway, the lock contains only limited data. The lock is programmed with a single User Code ("123456") to allow the lock to be unlocked (to avoid a door that cannot be unlocked during its physical installation), and the two "remote release" wires (two white wires) are programmed to be operational. Therefore, if a badge is presented to the lock, the card will not be "read" by the lock, the data will not be sent through the system, nor will events be logged. The lock must have a full data download sent to it before it can interact with the CA3000 system. Therefore, once all badges and schedules (etc.) are added to CA3000, perform a full data download from the CA3000 **Panels** screen.

Notice that the Lock just assigned to the Gateway has

been removed from the list in the **Discover new Locks for Gateway** screen.

Add additional locks (from the list in the **Discover new Locks for Gateway** screen) to the Gateway if desired. If no other locks are to be added, close the **Discover new Locks for Gateway** screen by clicking the **Close** button (located at the top right of the screen). Note that the **Discover new Locks for Gateway** screen must be closed to fully update the Gateway "Status" field and the "Last Updated" date and time in the **CardAccess Wireless Configuration** screen.

At this point, close the **CardAccess Wireless Configuration** screen by clicking the **Finish** button. Note that clicking **Finish** also starts the CardAccess Wireless Lock socket server; please wait while the status of all Gateways and the status of all locks are verified and updated within the CA3000 system. The wireless lock is referred to as a "Panel" within CA3000. Be sure to perform a Full Download using the Panel screen from CA3000 to the physical lock. Please see the CA3000 User Guide for setting up badges, schedules, access groups, time zones, etc.

### ADDITIONAL CA3000 TASKS

#### Create Schedules, Access Groups and Personnel

With the discovered locks now added to the Gateway, at this point other standard tasks must be performed. See the CA3000 User Manual for details. These include the following tasks, such as:

- **Create a Schedule.** Locks can be activated to allow access at the doors by assigning a time Schedule. In the CardAccess main screen, open the **Schedules** screen by clicking on the **Schedules** button or click **Administration, Schedules**.
- **Create an Access Group** by assigning a Schedule to a lock. These Access Groups do not play any role unless they are attached to Personnel. Access Groups are created to control the badge holders' access to specific doors within specific times. When creating an Access Group, a list of all locks and devices in the CardAccess system is available, and these devices can be activated to allow access at the doors by assigning Schedules to these devices. Therefore, when an Access Group (a "Schedule attached to a lock") is assigned to a badge holder, the badge holder is allowed access to the doors included in the Access Group, during the Schedule specified for every lock in the Access Group. The same Access Group can be assigned to other badge holders who have similar access permissions at a door. The CardAccess permits a maximum of 1000 Access Groups (inclusive of Dedicated Access Groups). To create a new Access Group, click **Access, Access Groups** in the CardAccess main screen, then click the **New** button located on the Access Groups screen toolbar.

## Quick Start: Add Gateways and Locks (cont'd)

- **Add Personnel.** The Personnel screen is used to create badge holder records, associate a badge number with a name, set access rules, and attach special attributes to the badge. In the CardAccess menu bar, click **Access, Personnel**.
- **Assign Personnel to an Access Group.** Located within the **Personnel** screen, the **Access Groups** tab allows you to assign Access Group(s) to the selected badge holder. Access Groups determine which doors (at which times) a badge holder can access.
- Set up reader/door control options.

See the CA3000 User Manual for additional tasks.

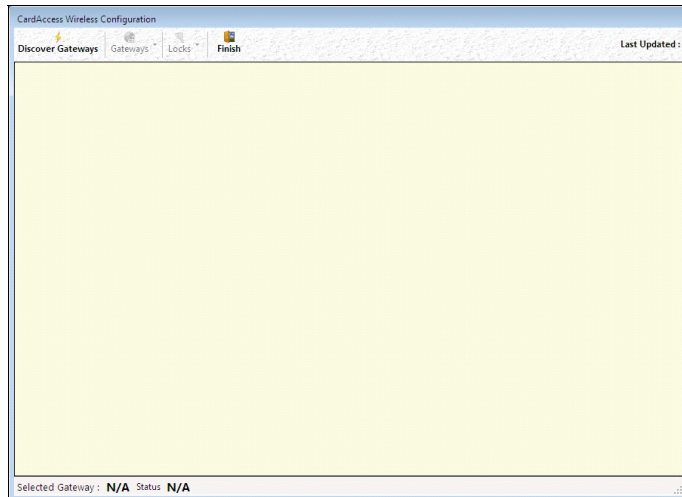
# Gateways > Discover Gateways

The **Discover Gateways** selection is the means of adding a Gateway device to the system. This menu selection causes the software to try to find all Gateway devices on the network. If there are multiple networks, you must first select the network of interest. Only those Gateways not already assigned to a system will be displayed.

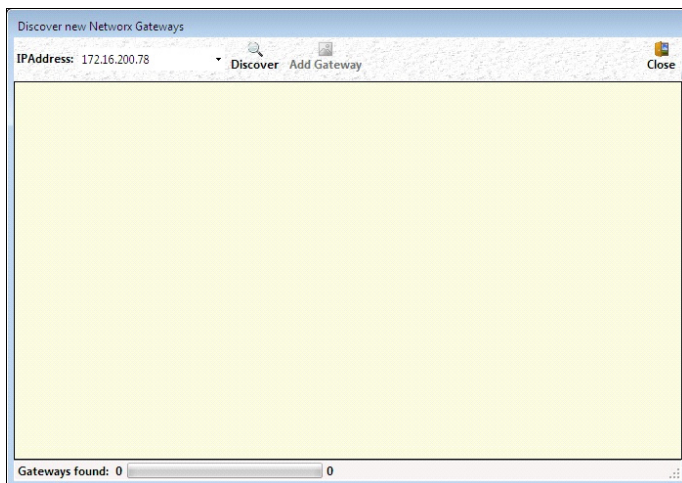
Select this option to discover the Gateways on the network.

**Note:** If Gateways have already been discovered, skip to step 2.

1. The first step is to search for Gateways not yet assigned to the system. In the CardAccess 3000 main screen, click **Configuration, Wireless Lock Configuration**. The **CardAccess Wireless Configuration** screen opens.



2. In the **CardAccess Wireless Configuration** screen, click the **Discover Gateways** button. The **Discover new Network Gateways** screen opens. Ensure the **IP Address** field displays the IP Address of the network you want to search. The **IP Address** field is also pull-down list, displaying multiple networks to which your computer is connected, if available. Click the **Discover** button to start the Gateway search.



The CA3000 software searches the network for all available Gateway modules not yet "configured" (enrolled into a CA3000 system). While the search is in progress, a splash screen appears (below). Note that similar splash screens

appear when the software is performing these kinds of operations.



At the bottom of the **Discover new Network Gateways** screen, the **Gateways found** status bar displays the number of Gateways detected and current percentage progress of the search.



Wait for the status bar to reach and hold at 100% before proceeding (time to reach 100% depends on the network speed). If no Gateways are found, a small popup appears indicating "No Gateways Found" (verify the IP Address is correct, and that the Gateway is powered and connected to the network, and try again).

All Gateway modules found are listed in the **Discover new Network Gateways** screen, and each found Gateway module appears listed with the following data columns:

- **MAC Address** - Unique "Media Access Control" number assigned at the factory.
- **IP Address** - Assigned by DHCP to the Gateway module.
- **Firmware Version** - Internal firmware release identification. **Note:** Gateway modules are shipped from the factory with Alarm Lock firmware pre-installed, for use within the Alarm Lock Networkx system. Therefore this column displays "3.51" to reflect this Alarm Lock Gateway firmware. When the Gateway firmware is compatible with Continental CardAccess 3000 (in the steps below), the Firmware Version will read "4.1B".
- **Gateway Status** - Condition at the time the module was discovered.

MACAddress	IPAddress	FirmwareVersion	GatewayStatus
00204AB352B8	172.16.200.120	4.1B	Ready
00204AB352C4	172.16.201.51	3.51	Ready
00204ACE0C21	172.16.200.87	4.1B	Ready
00204AB352B3	172.16.201.66	4.1B	Ready
00204AB307DF	172.16.200.83	4.1B	Ready
00204AB34AB5	172.16.200.72	4.1B	Ready
00204AB3532D	172.16.201.68	4.1B	Ready
00204AB32439	172.16.201.113	4.1B	Ready
00204AB352DA	172.16.201.59	4.1B	Ready
00204A9F286B	172.16.201.60	3.51	Ready
00204AB352E5	172.16.201.89	4.1B	Ready
00204AB352C9	172.16.201.65	4.1B	Ready
00204AB322D7	172.16.200.90	4.1B	Ready
00204AB35318	172.16.201.69	4.1B	Ready
00204AB32307	172.16.200.86	4.1B	Ready
00204AB352BD	172.16.201.67	4.1B	Ready
00204AB352B0	172.16.201.67	4.1B	Ready
00204AB352B0	172.16.201.67	4.1B	Ready

Gateways found: 18 100% complete

# Gateways > Update Gateway Status

Click **Gateways, Update Gateway Status** to retrieve the current attributes and condition of the Gateways. The **CardAccess Wireless Configuration** screen displays the operational status of the selected Gateway only as of the last update, therefore an update of the Gateway status may be necessary after configuring a Gateway to be wireless or when setting a static IP. **Note:** For new installations, some data may not yet exist, and therefore several fields may be empty.

## MAC Address

Unique "Media Access Control" number assigned at the factory.

## IP Address

Specifies the static IP Address on the TCP/IP network currently assigned by DHCP to the Gateway module. Required for communication.

## Version

Indicates the firmware source code edition currently residing in the Gateway. Internal firmware release identification.

**Note:** When the Gateway firmware is compatible with Continental CardAccess 3000, the Firmware Version reads "4.1B".

## Gateway Status

Indicates the condition of the Gateway module the last time its status was retrieved (displayed in the "**Last Updated**" field located at the top right of this screen). Automatic status retrieval occurs during several events, including:

- when manually retrieved (clicking the **Update Status** button in the **Gateway Status** dialog)
- after making changes to the network settings (click **Gateway, Configure Network Settings**)

- after discovered locks are configured (assigned) to a Gateway

Entries for the **Status** field include:

- **Ready** - The last time its status was retrieved, the Gateway was operational and configured correctly
- **Ready, Lock Error** - An assigned lock had lost its connection to the Gateway at the time the Gateway status was retrieved. If the lock is known to be reconnected to the Gateway, click **Gateways, Update Gateway Status** to refresh this information.

## Online

When the check box is checked, indicates the Gateway module is available for immediate use. **Note:** If **Online** is unchecked, Gateway will be unreachable; the Status field will be blank/empty, and the firmware Version field will display a zero ("0").

The screenshot shows the 'CardAccess Wireless Configuration' window. At the top, there are tabs: 'Discover Gateways', 'Gateways', 'Locks', and 'Finish'. The 'Gateways' tab is selected. On the right, it says 'Last Updated : 7/25/2011 3:21:36 PM'. Below the tabs is a table with the following columns: 'MACAddress', 'IPAddress', 'Version', 'Status', and 'Online'. There is one row of data:

MACAddress	IPAddress	Version	Status	Online
00204A9F286B	172.16.201.60	4.1B	Ready	<input checked="" type="checkbox"/>

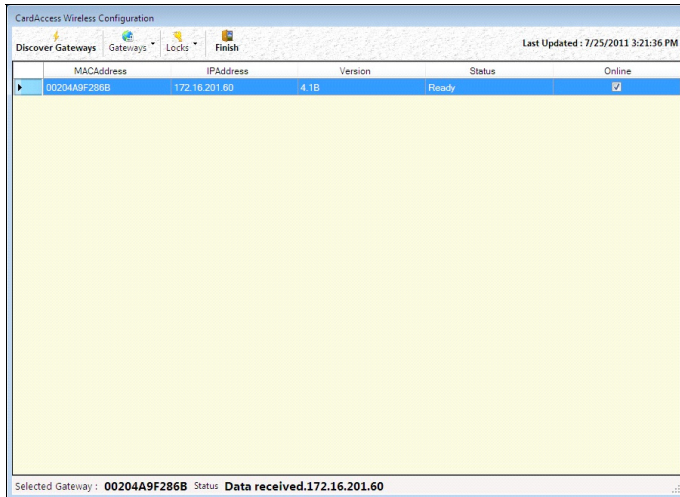
Below the table, it says 'Selected Gateway : 00204A9F286B Status Data received.172.16.201.60'.



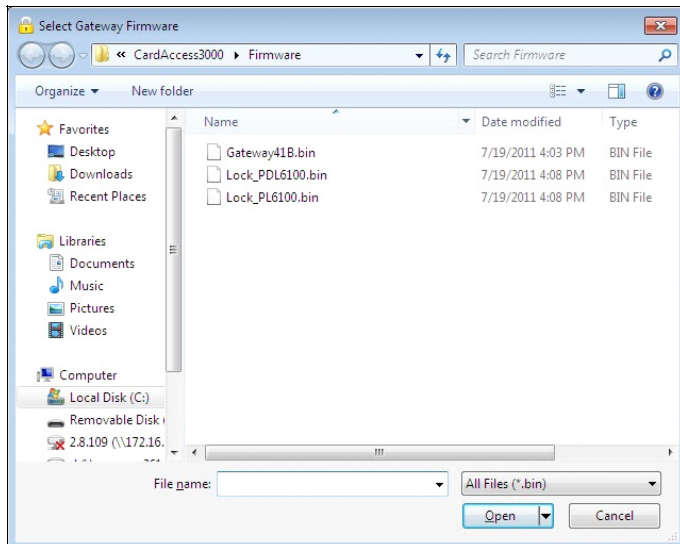
# Gateways > Send Firmware to Gateway

This menu selection updates the Gateway firmware.

1. In the **CardAccess Wireless Configuration** screen, click to highlight a specific Gateway in the list, then click **Gateways, Send Firmware to Gateway**.



The **Select Gateway Firmware** dialog opens:



2. Select the firmware binary (.bin) file (usually named Gatewayxxx.bin) to send to the Gateway. We recommend that all firmware files, including both Gateway files and wireless lock files, reside in a folder named **Firmware** located within the CA3000 software folder.
3. When the firmware transfer is complete, an information popup appears, indicating "**Gateway firmware was downloaded successfully**".

## Gateways > Send Config Table to Gateway

**Send Config Table to Gateway** results in the CA3000 software sending the Lock configuration information to the Gateway (for example, used if the Gateway crashes or is physically replaced).

In the **CardAccess Wireless Configuration** screen, click to highlight a specific Gateway in the list, then click **Gateways, Send Config Table to Gateway**.

A configuration table is sent to the Gateway automatically when a Gateway is "replaced" (see page 23). However, in the event the Gateway loses its configuration data (for example when "reset"), this **Gateways > Send Config Table to Gateway** menu selection allows you to manually re-send the lock configuration table stored in the CA3000 database to the Gateway.

# Gateways > Replace Gateway

This option is used when a configured Gateway device (discovered on the network, assigned to a CA3000 account and operational with physical locks assigned) becomes faulty and needs to be physically replaced.

**Replace Gateway** Allows you to swap an existing Gateway with a new one. The lock "Config Table" (see page 22) and Gateway Password (see page 14) are then automatically sent to the new Gateway.

In the **CardAccess Wireless Configuration** screen, click to highlight a specific Gateway in the list, then click **Gateways, Replace Gateway**.

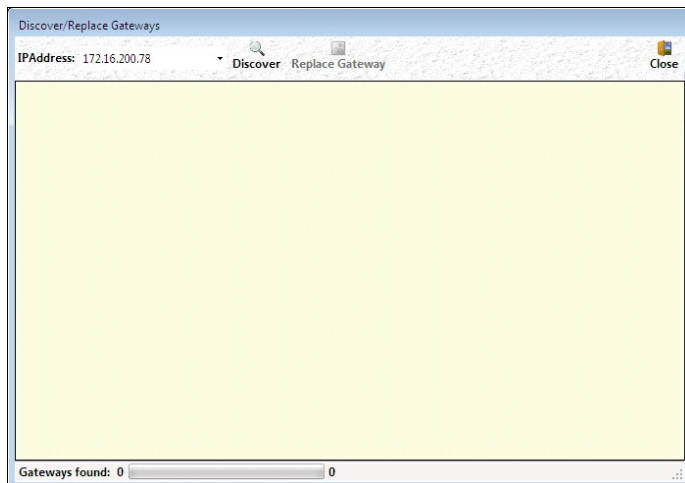
To replace an existing Gateway device, proceed as follows:

1. Physically replace the Gateway device by disconnecting the power wires and the RJ-45 plug from the old device and reconnecting all wires to the new device. Remember to press the "**RESET**" button on the new Gateway PC board to clear the Gateway memory (turn to page 12 and follow the section "**Resetting the Gateway**" instructions for a "**Full Reset**").

**IMPORTANT:** Be sure to remove power from the old Gateway.

Within CA3000, proceed as follows:

2. In the **CardAccess Wireless Configuration** screen, click to highlight the specific Gateway that you wish to replace, then click **Gateways, Replace Gateway**. The following **Discover/Replace Gateways** screen appears:

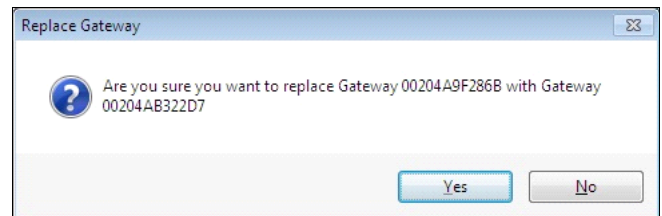


The **Discover/Replace Gateways** screen allows you to search for the new "replacement" Gateway connected to the system in step 1 above.

3. In the **Discover/Replace Gateways** screen, ensure the **IP Address** field displays the IP Address of the network you want to search. The **IP Address** field is also pull-down list, displaying multiple networks to which your computer is connected, if available. Click the **Discover** button to start the Gateway search. Wait for the status bar to reach and hold at 100% before proceeding (time to reach 100% depends on the network speed). If no Gateways are found, a small popup

appears indicating "No Gateways Found" (verify the IP Address is correct, and that the Gateway is powered and connected to the network, and try again).

4. If the system finds the newly installed Gateway, the new Gateway will appear in the **Discover/Replace Gateways** screen, indicating the MAC address, IP address, firmware version and Gateway status of the newly installed Gateway device (for a definition of each field, see each definition in the section "**Adding Gateways and Wireless Locks**" on page 15).
5. Click to highlight and select the Gateway listed, then click **Replace Gateway**. A confirmation popup appears:



Click **Yes** to proceed. The system will automatically replace the old Gateway with the new Gateway by copying all needed information (lock table, Gateway Password, etc.) into the new Gateway device, then adding the new Gateway to the CA3000 system.

Click **Close** to exit the **Discover/Replace Gateways** screen.

6. In the **CardAccess Configured Locks** screen, verify that the locks previously listed within the old Gateway now reside in the replacement Gateway.

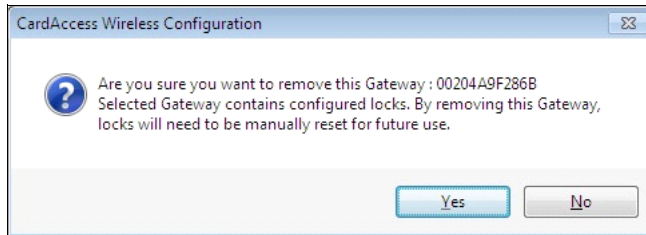
## Gateways > Remove Gateway

This option causes the Gateway to be reset (removing the communication channels between the Gateway and any configured locks), and deletes the Gateway from the CA3000 database.

In the **CardAccess Wireless Configuration** screen, click to highlight a specific Gateway in the list, then click **Gateways, Remove Gateway**.

To remove an existing Gateway device, proceed as follows within the CA3000 software:

1. In the **CardAccess Wireless Configuration** screen, click to highlight the specific Gateway that you wish to replace, then click **Gateways, Remove Gateway**. The following warning popup appears:



Read the popup carefully to ensure the MAC address of the Gateway displayed in the popup matches the Gateway you intend to remove (check the blue **GATEWAY ID CARD**). Click **Yes** to continue with the removal process or click **No** to exit without performing changes.

**Note:** This popup will appear differently if no locks are assigned to the Gateway; the last two sentences will not be included as they are not needed.

If the Gateway is able to communicate with its assigned lock(s), the Gateway will send an "un-assignment" command, to allow the lock(s) to be ready for re-discovery and re-assignment to another Gateway. If you are removing a Gateway because it is unresponsive, note that its assigned lock(s) may likely not receive this "un-assignment" command, the lock(s) will not function correctly--therefore, we highly recommend all locks previously assigned to the removed Gateway be manually reset (see WI1969 for instructions).

In addition, if the system is able to communicate with the Gateway, the Gateway will also be "unassigned" (clears its lock table, Gateway Password and assignment) allowing the Gateway to be ready for re-discovery and re-assignment. This process is performed automatically, avoiding the need to physically reset the Gateway manually (by pressing the **"RESET"** button on the PC board).

2. When the Gateway is successfully removed, an informational popup will appear, indicating "The [MAC Address] Gateway was removed successfully". Click **OK** to close the popup.



# Gateways > Configure Network Settings

The **Gateway Network Setup** dialog displays the various networking attributes required for the selected Gateway to work correctly within the current network. See your network administrator for more information if needed.

**Note:** For wireless security, because the communications between the network and the Gateway conform to the AES (Advanced Encryption Standard), we recommend leaving the system unsecure, but to use MAC address filtering within the router software (if your router supports MAC Address filtering). Using this kind of security is easier to setup and more secure than using the security protocols (encryption methods) shown within this screen.

**Note:** As shown in the two images below, this dialog appears in two sizes: If **"Wired"** is selected in the **Wireless Mode** field, the dialog is smaller, and expands if **"Wireless"** is selected (requires the use of the Gateway model AL-IM80211).

## Local Network

This field is also a pull-down list, displaying multiple networks (if available) to which your computer is connected. Ensure this field displays the IP address of the network to which you want to assign and configure your Gateway.

## Use DHCP

**Use DHCP** (Dynamic Host Configuration Protocol) is enabled by default. When checked and **Save Configuration** is clicked, CA3000 allows the selected Gateway to accept the dynamic assignment of an IP address by the TCP/IP network. **Use DHCP** (checked by default) removes the need to manually assign a static (fixed) IP address to the Gateway. Uncheck **Use DHCP** to allow the manual assignment of a static IP address to the selected Gateway (a warning popup appears warning that the Gateway may be unreachable until it is installed on the correct network or is manually defaulted). See your network administrator for additional information.

## DHCP Name

To aid in locating the Gateway on the network, specify a name to describe the domain name (host name) of the corresponding IP Address assigned to the selected Gateway. The DHCP name entered here will be used for the DNS configuration.

## 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** fields located in this screen become active and available for selection.

## IP Address

If the **Use DHCP** (see above) is unchecked, this field allows the IP address to be manually assigned to the selected Gateway.

## Subnet Mask

The screenshot shows the 'Gateway Network Setup' dialog box. The 'Local Network' dropdown is set to '172.16.200.78'. The 'Use DHCP' checkbox is checked, and the 'DHCP Name' is 'CONTCLK'. The 'Wireless Mode' dropdown is set to 'Wired'. The 'IP Address' is '172.16.201.60'. The 'Subnet Mask' and 'Gateway' fields are empty. At the bottom are 'Save Settings' and 'Cancel' buttons.

The screenshot shows the 'Gateway Network Setup' dialog box with the 'Wireless Network Configuration' section expanded. The 'Local Network' dropdown is set to '172.16.200.78'. The 'Use DHCP' checkbox is checked, and the 'DHCP Name' is 'CONTCLK'. The 'Wireless Mode' dropdown is set to 'Wireless'. The 'IP Address' is '172.16.201.60'. The 'Subnet Mask' and 'Gateway' fields are empty. The 'Security Type' is 'None', 'Authentication' is 'Open/None', 'Encryption' is '64 Bits', 'Key Type' is 'Hex', 'Key' and 'Retype Key' are empty. The 'Network Name (SSID)' is empty, 'Network Type' is 'Infrastructure', and 'Channel Number' is 'Channel 1'. At the bottom are 'Save Settings' and 'Cancel' buttons.

To improve performance, network administrators determine how best to divide their network. Create more hosts and fewer subnets or more subnets and fewer hosts? 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). **Use DHCP** (see above) must be unchecked before data can be entered into this field. This information must be obtained from your network administrator.

## 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. **Use DHCP** (see above) must be unchecked before typing the IP address. This information must be obtained from your network administrator.

## Security Type

For the selected Gateway, 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 as follows:

- **WEP** (Wired Equivalent Privacy) The WEP encryption method was designed to provide wireless networks with the "equivalent" security available in traditional wired "landline" networks.

# Gateways > Configure Network Settings (cont'd)

- **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** 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 this screen.

## Authentication

Verifies the origin of transmitted data.

For the selected Gateway, 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 DL-Windows.
- **Shared:** Requires a shared symmetric numeric code (encryption "key") for all data transmissions between DL-Windows and the Gateway.

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

- **Pre-Shared Key (PSK):** Requires a numeric code (encryption "key") *previously shared* between CA3000 and the Gateway using a secure channel for all data transmissions.

## 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 WEP 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 WEP 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 CA3000, the Gateways and the locks. The key "type" can be a password, a passphrase, or a hexadecimal string like '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.

## Network Name (SSID)

The Gateway module acts as an interface between a computer network and the Network™ wireless locks. Of the two Gateway models available ("Wired" or "Wireless/Wired"), the "Wireless/Wired" Gateway model supports connection to a network using the 802.11 standard. This field allows you to specify the SSID (Service Set Identifier) name assigned to the wireless Wi-Fi (802.11) network. All "Wireless/Wired" 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. In addition, the **Wireless Mode** pull-down menu in this screen must be set to **Wireless Only** for this field to become active.

## Network Type

Click this 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. Contact your network administrator for more information.

## Channel Number

Click this 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. Contact your network administrator for more information.

## Save Settings

Click **Save Configuration** to save your settings and close the screen, or click **Cancel** to exit without saving. **Note:** Changes made to the **Gateway Network Setup** dialog may require several seconds for the data to be sent to the Gateway and all assigned locks. **Note:** If a popup appears indicating the "Gateway is not found" or if the status is otherwise not updated successfully, click **Gateways, Update Gateway Status** to refresh the data.

# Locks > Discover Locks

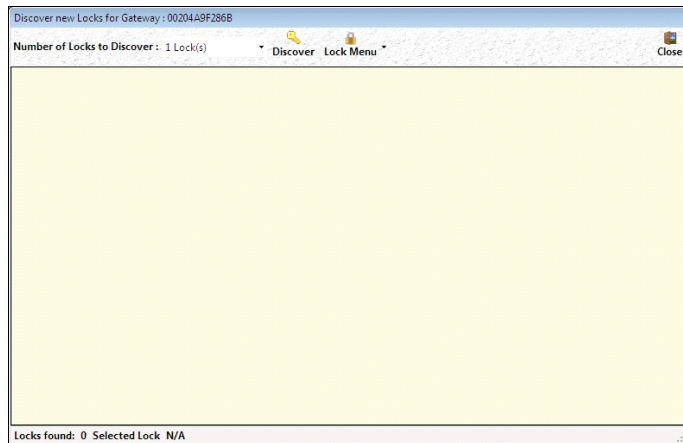
With a Gateway or Gateways added to the **CardAccess Wireless Configuration** screen, click to select the Gateway you want to use to discover locks, then click **Locks, Discover Locks** to find wireless locks within range to add to the system.

## Discover Locks

In the **CardAccess Wireless Configuration** screen, click to select the Gateway you want to use to discover locks; this will also be the same Gateway to which you want to assign locks. **Note:** The Gateway selected will transmit the discovery request radio signal to all locks in the vicinity, and only those locks within range -- that have not already been assigned to a Gateway -- will respond.

With the Gateway highlighted, click **Locks, Discover Locks**.

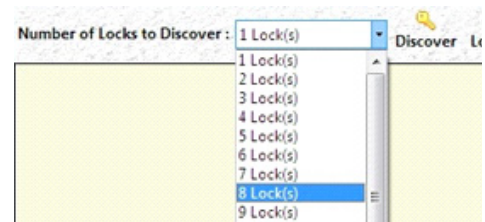
The **Discover new Locks for Gateway** screen opens. **Note:** If the Gateway does have any locks assigned, double-clicking the Gateway will also open the **Discover new Locks for Gateway** screen.



The maximum search time allowed for each discovery request is 1 minute. To minimize the search time, this screen allows you to limit the search to a certain quantity of installed locks. In addition, you can manually stop the discovery process at any time by pressing the keyboard **Esc** key. If you know the number of installed locks to be discovered, select that number and the discovery process will stop the moment that selected number of locks are found. If the number of locks selected exceeds the actual number physically installed, the discovery process will continue for either a maximum of 1 minute or until the **Esc** key is pressed.

**Example:** If the number selected is 10, but in fact only 8 locks exist, the system may find all 8 locks, but will keep searching for 10 until either the one minute timeout duration expires or until the **Esc** key is pressed.

**Note:** Only press **Esc** ONCE or additional time will be added to the search.



Click the **Number of Locks to Discover** pull-down list and select a number of locks that you want to detect. Ensuring the physical lock(s) you wish to discover are powered as per the instructions provided with the lock packaging, click the **Discover** button to initiate the search.

The next image displays the results when 8 locks were requested to be discovered ("Number of Locks to Discover") and 8 locks were found:

Lock ID	Transmit Signal	Receive Signal	Lock Type
187E4AE0	68	70	PDL6100
3460E074	28	24	Network Control
E49A007E	64	61	PDL6100
E49B007F	30	24	PDL6100
E4A10085	26	19	PDL6100
F7E9CBAA	31	68	CPDL6100
187E4AE0	74	86	PDL6100
DA1A00F4	31	24	PDL6100

The locks listed are only those locks (within range) that have not already been assigned to a Gateway.

The list (shown above in the **Discover new Locks for Gateway** screen) includes data columns for each lock (see page 16 for details):

**Note:** We recommend that when installing a lock on a door a yellow-colored "**LOCK ID CARD**" be completed; the information on this card is important and should be saved in a safe location.

~ 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 \_\_\_\_\_

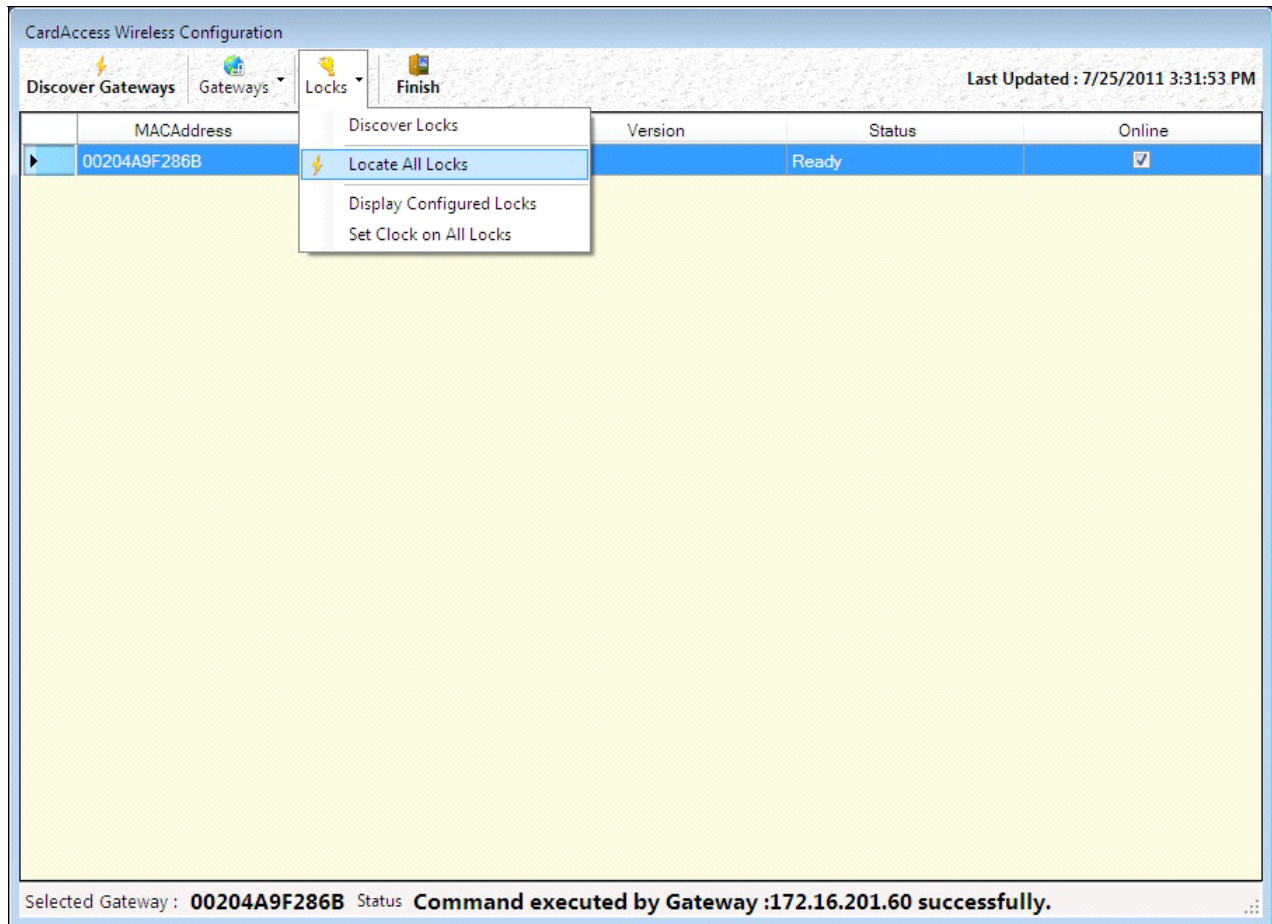
INSTALLED LOCATION \_\_\_\_\_

01353 10/08

# Locks > Locate All Locks

This global option requests all wireless locks assigned to the selected Gateway to beep and flash their red LED's; used when you wish to find the physical locks or to confirm the wireless connection is operational.

In the **CardAccess Wireless Configuration** screen, click to highlight a specific Gateway in the list, then click **Locks, Locate All Locks**.



The default "Locate Time" duration is 30 seconds.

All wireless locks assigned to the selected Gateway will beep and flash their red LED's for the default duration, **all at the same time**.



# Locks > Display Configured Locks

This option allows you to display the current status of all assigned locks for the selected Gateway. Also known as the "Lock Table", this useful dialog allows for several tasks to be performed (detailed below) as well as the ability to verify as operational each connection between the selected Gateway and its assigned locks.

In the **CardAccess Wireless Configuration** screen, click to highlight a specific Gateway in the list, then click **Locks, Display Configured Locks**. **Note:** If the Gateway does have locks assigned, double-clicking the Gateway in the **CardAccess Wireless Configuration** screen will open the screen shown below.

Lock Id	Lock Type	Lock Name	Transmit Signal	Receive Signal	Firmware Version	Lock Status
187E4AE0	CPDL6100	Lock 2	72	82	1.60	Low Battery, Doo...

Notice how the MAC Address of the selected Gateway is incorporated within the title bar of this dialog, thus the title bar text reads "**CardAccess Configured Locks for [MAC Address of the Gateway]**".

## Locate Function

Similar to the menu option **Locks, Locate All Locks**, the above dialog allows you to select a *specific* lock to locate. Click to highlight a specific lock in the table, select a duration in the **Locate Time** pull-down menu (choices are 10 seconds by default, 20 seconds, 30 seconds, 1, 2, 3 or 4 minutes), then click the **Locate Lock** button. The selected lock will beep and flash its red LED for the duration selected.

## Refresh Function

When clicked, the Gateway requests a status of all locks, in real time, and sends the results into the table. Refreshing the lock data may take some time, depending on the number of locks (up to 63) assigned to the selected Gateway. **Note:** The "Refresh" function can also be initiated by simply double-clicking anywhere within the above dialog.

## Data Columns

The attributes of each assigned lock are displayed in data columns, as follows:

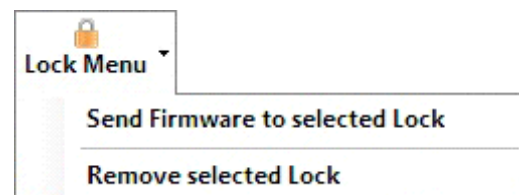
- **Lock ID** - Each wireless lock is identified by this unique serial number programmed into the lock firmware at the factory.
- **Lock Type** - Lock firmware type, as identified by the Gateway. Locks not yet converted to the CA3000 system will be listed as "DL", "PL" or "PDL"; locks converted to the CA3000 system will begin with the letter "C".

- **Lock Name** - Text entered in the **Panel Name** field in the **Add Lock** dialog (when adding a discovered lock to a Gateway).
- **Transmit Signal** - Radio transmission strength from the lock as measured by the Gateway, on a scale of 1-100; the lower the number the weaker the signal.
- **Receive Signal** - Radio transmission strength from the Gateway as measured by the lock, on a scale of 1-100; the lower the number the weaker the signal.
- **Firmware Version** - The Alarm Lock or Continental Instruments internal firmware release identification.
- **Lock Status** - Indicates the condition of the lock the last time its condition was retrieved. Retrieval occurs when this screen is opened or by clicking the **Refresh** button.

The **Lock Status** field descriptions are:

- **Door Secure** - Door locked (secured) and closed
- **Bypass** - Door unlocked/unsecured (in "passage")
- **Not Responding** - Communication failure between the lock and the Gateway (displayed in red colored text)
- **Free Access** - Indefinite "passage" mode where the door is unsecured
- **Low Battery; [current lock state]** - If the voltage of the batteries drops below a certain threshold (varies with model), a **Low Battery** indication will appear, followed by a semi-colon and one of the other four field descriptions ("Door Secure", "Bypass", etc.)

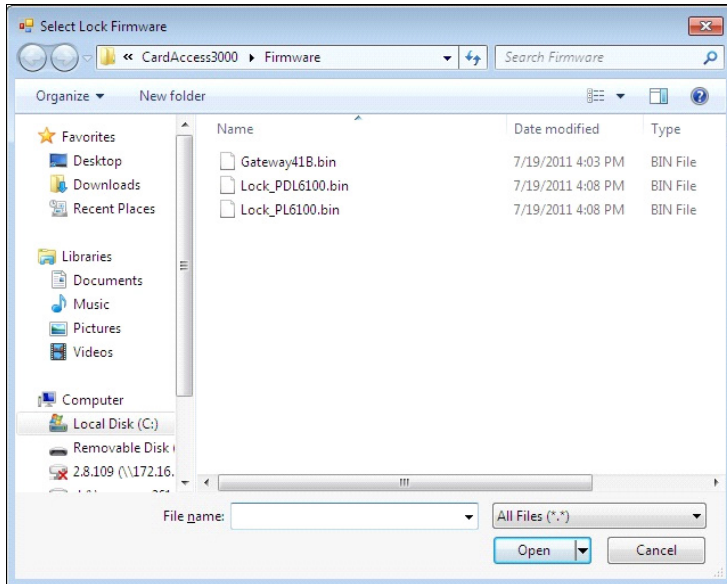
## Lock Menu Pull-Down



Two options are available:

- **Send Firmware to selected Lock** - When new lock firmware is available, install the firmware into the selected lock by clicking this menu option to open the **Select Lock Firmware** dialog, then click to select the firmware binary (.bin) file (usually named Lock\_[model].bin) to send to the lock. We recommend that all firmware files, including both Gateway files and wireless lock files, reside in a folder named **Firmware** located within the CA3000 software folder. Click to highlight the .bin file for the specific lock model, then click the **Open** button, and a confirmation popup appears:

# Locks > Display Configured Locks (cont'd)



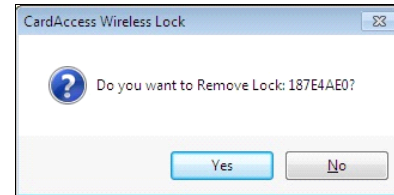
Click **Yes** to continue or **No** to cancel without making changes. The download process may take several seconds. When complete, the lock sounds 3 beeps and a **Download Lock Firmware** popup appears, indicating that the lock firmware download process completed successfully, and that the lock will not function until it receives a Full Data Download. Click **OK** to close the popup.

If a badge is presented to the lock at this time, the card will not be "read" by the lock, the data will not be sent through the system, nor will events be logged. The lock must have a full data download sent to it before it can interact with the CA3000 system. Therefore, once all badges and schedules (etc.) are added to CA3000, perform a full data download from the CA3000 **Panels** screen. **Note:** If firmware is downloaded from the CA3000 **Panels** screen, the system will perform a Full Data Download automatically.

- **Remove selected Lock** - Removes an assigned lock from the selected Gateway while retaining other memory data (such as badges, schedules, etc.).

## Removing a Responsive Lock

If the Gateway is able to communicate with an assigned lock (such as a lock that indicates anything other than **"Not Responding"** in the **Lock Status** field), the Gateway sends an "un-assignment" command to allow the lock to be ready for re-discovery and re-assignment to another Gateway. A confirmation popup appears:



Click **Yes** to proceed with the removal process or **No** to exit without performing changes. When finished, a popup appears indicating "The lock was successfully removed" (click **OK** to close). The un-assigned lock can now be re-discovered and re-assigned to another Gateway. **Note:** Although now un-assigned, the lock still retains its memory, including (but not limited to) badge and schedule information. To clear all memory from the lock, the lock must be manually reset before using it again (see WI1969 for instructions).

## Removing an Unresponsive Lock

If you are removing a lock because it is indicating **"Not Responding"** in the **Lock Status** field, the **Remove Lock** popup reads:

*"Lock did not respond to normal removal, it was removed from the Gateway, but you will need to reset the lock to use it again."*

This popup warns that unresponsive locks are unlikely to receive the "un-assignment" command and although the Gateway records the lock as being un-assigned, the lock will remain in its faulty state. Therefore, an unresponsive lock that has been un-assigned from a Gateway must be manually reset before using it again (see WI1969 for instructions).

When finished, a confirmation popup will appear indicating the lock was "successfully removed". The un-assigned lock can now be re-discovered and re-assigned to another Gateway. **Note:** Although now un-assigned, the lock still retains its memory, including (but not limited to) badge and schedule information. Manually reset the lock to fully clear its memory before using it again (see WI1969 for instructions).

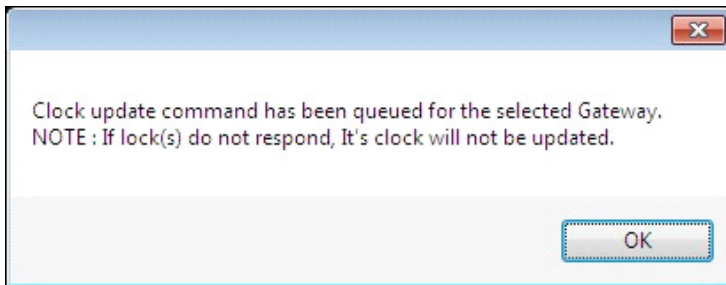
## Close Button

Click **Close** to exit the screen and return to the **CardAccess Wireless Configuration** screen.

## Locks > Set Clock on All Locks

In the **CardAccess Wireless Configuration** screen, click **Locks, Set Clock on All Locks** to retrieve the current time and date from the computer running CA3000 for distribution to all Gateways and all physical wireless locks in the current Account.

In the **CardAccess Wireless Configuration** screen, click **Locks, Set Clock on All Locks** and the following popup appears:



Click **OK** to close the popup.

## LOCK STATUS "NOT RESPONDING"

*I had a lock that was working perfectly but now the "Lock Status" column reads "Not Responding". What do I do?*

In this case, the Gateway is unable to communicate with the lock. First verify a few basic details:

1. Has something changed to affect communications? Is the lock still on the door? Did someone remove the door for some kind of maintenance? Has furniture been moved around and now there is something that is blocking the radio signal to the Gateway?
2. Is the lock still functioning? Find the physical lock and attempt to unlock by entering a working badge. Are the lock key-presses causing beeping sounds? Check the battery voltage and battery connections.
3. Determine if the distance between the lock and the Gateway is greater than 75 to 100 feet. A new Gateway module may need to be installed, discovered and added.
4. Take the lock off the door, bring the lock physically closer to a Gateway and try to re-discover the lock.
5. If the signal strength to that lock has always been strong and suddenly it is non-existent, the lock may have an internal failure and has lost its configuration data. In this case, CA3000 still has the correct lock configuration data, therefore simply try re-discovering the lock:

In the **CardAccess Wireless Configuration** screen, click to select the Gateway you want to use to re-discover the lock (the same Gateway to which you want to re-assign the lock). With the Gateway highlighted, click **Locks, Discover Locks**. The **Discover new Locks for Gateway** screen opens. Click the **Number of Locks to Discover** pull-down list and select "1" (or more). Ensure the physical lock you wish to re-discover is powered (as per the instructions provided with the lock packaging), click the **Discover** button to initiate the search. Check the yellow "Lock ID Card" to verify the "Lock ID" number that appears in the **Discover new Locks for Gateway** screen matches the "Lock ID" of the lock you are trying to re-discover. Click to select and highlight the lock you wish to add then click **Lock Menu, Add Discovered Lock**. The **Add Lock** dialog appears; click the **Add Lock** button. A confirmation popup appears requesting you to confirm that you wish to make the selected lock compatible with CA3000. Click **Yes** to proceed. Close the **CardAccess Wireless Configuration** screen by clicking the **Finish** button. Note that clicking **Finish** also starts the CardAccess Wireless Lock socket server; please wait while the status of all Gateways and the status of all locks are verified and updated within the CA3000 system. Re-check lock operation.

## COMPUTER CRASH!

*My computer running CA3000 just crashed! I had a working system, complete with wireless locks, Gateways and a computer running CA3000--but that computer no longer works! What do I do?*

Although the Gateways and wireless locks may still be up and running, if the CA3000 database cannot be recovered, all locks and all Gateways must be reset, re-discovered, re-configured and re-assigned. Follow the "Resetting the Gateway" instructions on page 12 and "**Quick Start: Add Gateways and Locks**" instructions on page 13.

## BATTERY REPLACEMENT PROBLEMS

*I just replaced the lock batteries--but I accidentally lost the lock programming! What do I do?*

It is actually very difficult to lose the lock programming when replacing batteries. To erase the programming, you need to disconnect the batteries, then reconnect the batteries and press and hold the "AL" keypad button for several seconds (something that would not normally happen when replacing the batteries).

However, if you replace the batteries correctly (without pressing the "AL" key) but the lock does not startup correctly, there is an internal lock attribute named "Bad Startup / No Data", where the lock will sound 3 beeps / 3 red flashes when the batteries are connected. If this "Bad Startup / No Data" condition occurs, the lock will automatically send a signal to the Gateway requesting an automatic data download request. Re-discover the lock and re-configure (continue with step 3 "**Add Discovered Lock to the Gateway**" on page 16).

## RESET GATEWAY ISSUES

*How do I reset the Gateway and what effect will it have on my system?*

Turn to page 12 and follow the "**Resetting the Gateway**" instructions for a "**Partial Reset**" or "**Full Reset**".

Although the Gateway is reset, CA3000 still retains the Gateway data. Therefore, open the CardAccess 3000 main screen, click **Configuration, Wireless Lock Configuration** to open the **CardAccess Wireless Configuration** screen. Click to highlight the specific Gateway in the list, then click **Gateways, Send Config Table to Gateway**.

## GATEWAY "OFFLINE"

*How do I re-establish communication with a "lost" Gateway?*



## TROUBLESHOOTING (cont'd)

If the Gateway is "Offline" (the "Online" checkbox is unchecked in the **CardAccess Wireless Configuration** screen, check all physical Gateway connections, then click **Gateways, Update Gateway Status**. Check with your network systems administrator to verify the IP Address is correct and that network activity is OK. If there is no change, follow the steps in the above "**RESET GATEWAY ISSUES**" where the Gateway is physically reset and the CA3000 Gateway data is resent (through the network) to the Gateway.

*This page intentionally left blank*

## **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.

# ALARM LOCK LIMITED WARRANTY

ALARM LOCK SYSTEMS, INC. (ALARM LOCK) warrants its products to be free from manufacturing defects in materials and workmanship for 24 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.

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.

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 canceled. 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 allege 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.