Internet Protocol Access Control

Installation Manual

LiftMaster®

Safety

Safety Symbol and Signal Word Review

When you see these Safety Symbols and Signal Words on the following pages, they will alert you to the possibility of serious injury or death if you do not comply with the warnings that accompany them. The hazard may come from something mechanical or from electric shock. Read the warnings carefully.

When you see this Signal Word on the following pages, it will alert you to the possibility of damage to your property or product if you do not comply with the cautionary statements that accompany it. Read them carefully.

⚠ WARNING

MECHANICAL

⚠ WARNING

ELECTRICAL

CAUTION

⚠⚠ WARNING

To reduce the risk of SEVERE INJURY or DEATH:

- Disconnect power at the fuse box BEFORE proceeding.
- To AVOID damaging gas, power or other underground utility lines, contact underground utility locating companies BEFORE digging.
- ALL electrical connections MUST be made by a qualified individual.
- ALL power and control wiring MUST be run in separate conduit.

To protect against fire and electrocution:

- Disconnect power and battery BEFORE installing or servicing operator.
- NEVER connect a keypad/reader or lock to doors without first consulting the applicable fire code.
- You MUST consult with, and get approval from, local fire officials BEFORE installing locks or devices on ANY doors that may be fire exits.
- Use of egress push buttons may not be legal. Single action exits may be required.
- ALWAYS obtain proper permits and approvals in writing BEFORE installing equipment.

INTRODUCTION

Overview

This product is a network enabled and Internet ready access control solution for community doors and gates that offers a simple and intuitive resident and visitor experience. This product utilizes computer network connections and communication. The notification functionality is a supplementary feature.

The unit is capable of controlling up to two access points. The inputs and outputs are grouped as follows for each access point:

Access Point 1

OUTPUTS

RELAY 1 (Gate/door Operator, Maglock, or Door Strike)
Connect the wires to N.O. or N.C. depending on your product and the COM terminal. Refer to the owner's manual for your product for more information on wiring and proper strike time.

AUX 1 (Alarm, Light, or Camera)
The bypass or activation is controlled by AUX 1 and is triggered by an event related to RELAY 1.

INPUTS

REX 1 (Postal Lock, Exit Request Button (REX), Keyswitch, Passive Infrared Device (PIR))
Connect the wires to the REX 1 terminal block on the peripheral board (COM and SENSE). Refer to the Administrators Manual for relay configuration settings.

INPUT 1 (Door Sensing Device)
Connect the wires to INPUT1 (COM and SENSE).
NOTE: *A door sensing device should provide contact closure when door is closed.*

PASSPORT RECEIVER

READER 1 (PPWR)
The READER 1 input is already is use by the factory installed PPWR receiver.

Access Point 2

OUTPUTS

RELAY 2 (Gate/door Operator, Maglock, or Door Strike)
Connect the wires to N.O. or N.C. depending on your product and the COM terminal. Refer to the owner's manual for your product for more information on wiring and proper strike time.

AUX 2 (Alarm, Light, or Camera)
The bypass or activation is controlled by AUX 2 and is triggered by an event related to RELAY 2.

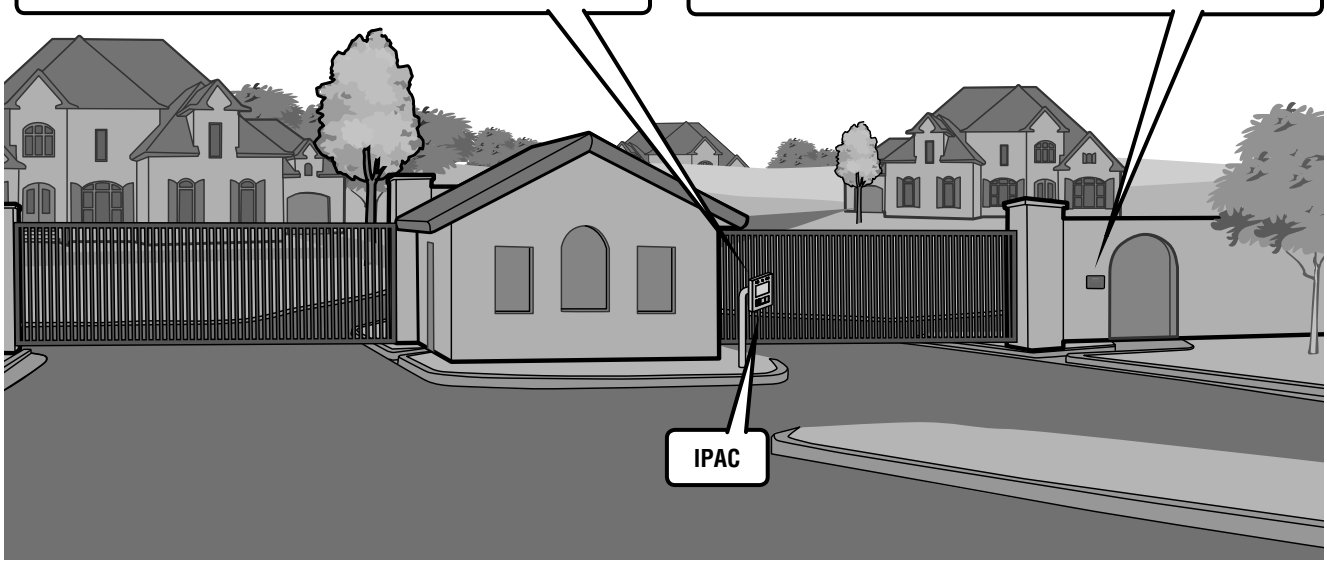
INPUTS

REX 2 (Exit Request Button (REX), Keyswitch, Passive Infrared Device (PIR))
Connect the wires to the REX 2 terminal block on the relay board (COM and SENSE). Refer to the Administrators Manual for relay configuration settings.

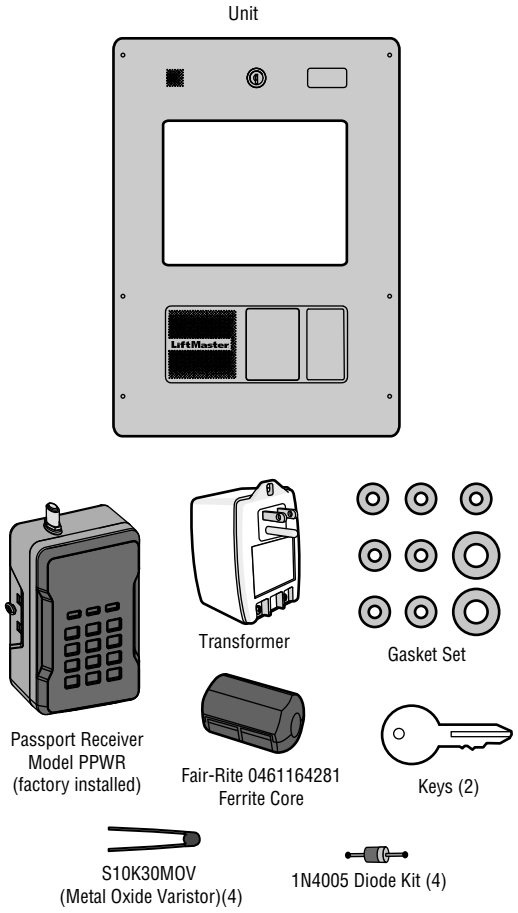
INPUT 2 (Door Sensing Device)
Connect the wires to INPUT2 (COM and SENSE).
NOTE: *A door sensing device should provide contact closure when door is closed.*

WIEGAND

READER 2 (Wiegand Device)
Connect the Wiegand device to the READER 2 input on the relay board. Refer to page 36 and the instructions provided with your Wiegand device for more information.



Carton Inventory



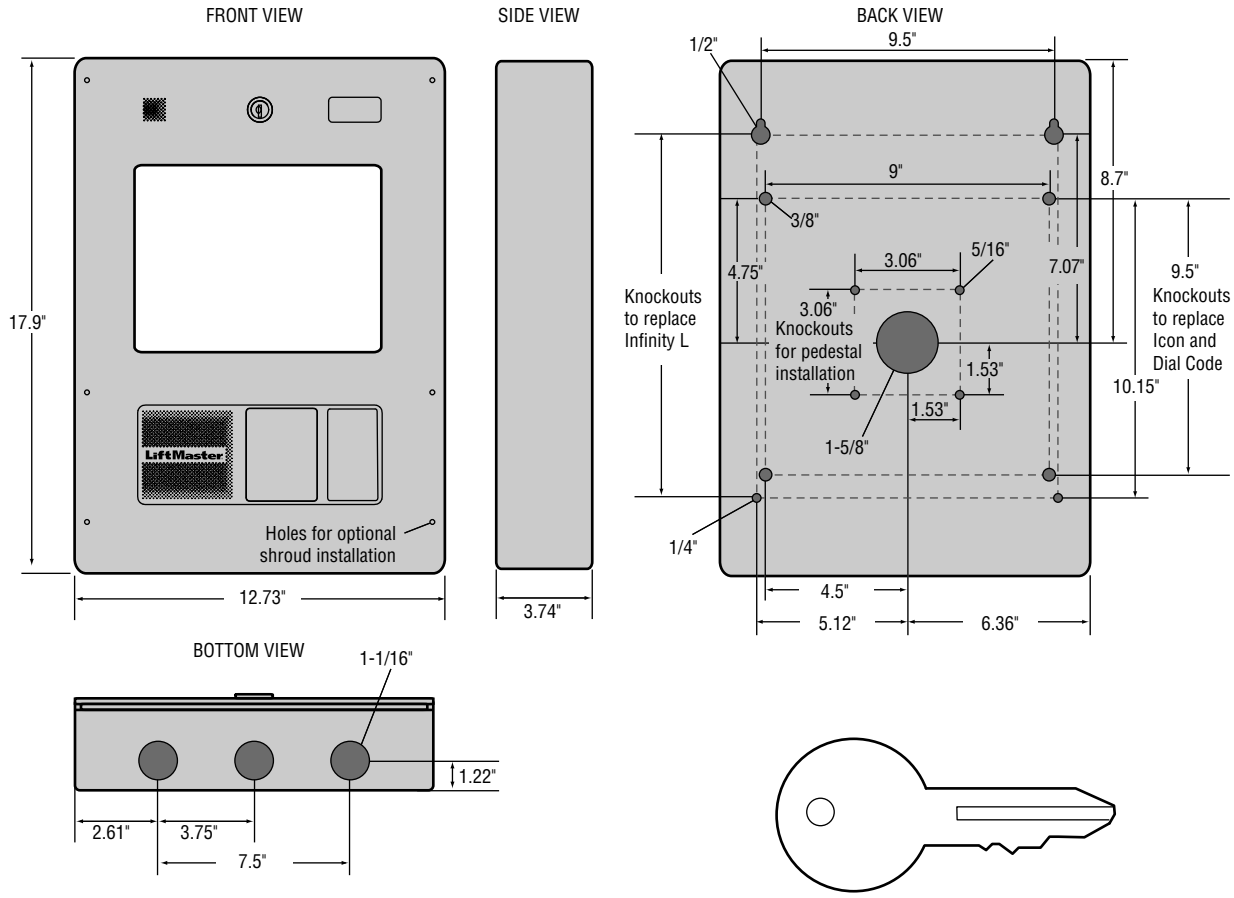
Also included, but not shown:
Antenna Extension Kit Model 86LM
Hardware for Camera Kit
Documentation Packet, Installation Manual and Site Survey

NOTE: *The Spanish version of this manual can be found at http://ipac.liftmaster.com/*

Tools

- Assorted Screwdrivers
- Precision Screwdrivers
- 1/4" Nut Driver
- Multimeter
- Wire Fish Tape
- Bits for Hammer Drill Bits for Drill/Driver
- Drill Screw Bit
- Wire Strippers
- Wire Cutters
- Assorted Pliers
- Flashlight
- Drill/Driver
- RJ45 Crimping Pliers
- Measuring tape
- Work Gloves
- Conduit Bender
- Conduit Cutter/reamer
- Hack Saw
- Center Punch Tool (1" maximum tip length)
- Blue Foam Box included in the packaging as work surface
- Hammer
- 7/64" Drill Bit

Dimensions



System Specifications

System Capacity	User/Tenant Codes: 50000, Events: 50000
Supply Voltage	16Vdc, 2.5A. Ningbo Zhongce ETS-AD0402-W160250, Class 2 (Transformer Input 120Vac, 60Hz, 1.0A)
Operating Current	1.17 Amps - Without Accessories
Surge Suppression	EFT: 2 Kv Power Line, ESD: 15 Kv Hbm / 8Kv Direct / 200V Mm
Unit Operating Temperature Range	- 35°C to 65°C (-31°F to 149°F) - 30°C to 55°C (-22°F to 131°F) Ambient Capability
Enclosure	IP65 Rated
Storage and Shipping Temperature Range	-40°C To 65°C (-40°F to 149°F)
Wiegand Inputs	26Bit, 30Bit, 34 Bit ODD and 34 Bit EVEN, Proximity, 12V, 250mA Power Output (Per Port)
Relay Outputs	Spdt, Maximum Voltage of 30Vdc/ac and Output Current of 3A
Accessory Compatibility	See OPTIONS section (page 38) for Compatible Accessories

Wire Specifications

Use this chart to pull wires in preparation of your installation.

DESCRIPTION OF WIRE RUN	WIRE SPECIFICATION	MAXIMUM RUN DISTANCE
Power Wire	2-Conductor 14 AWG Shielded	Up to 250 Feet
Local Area Network (LAN) CAT 5/6 Network Cable	8-Conductor, 24 AWG Twisted pair	328 feet*
Grounding the Chassis	12 AWG Copper	12 feet
Door Strike	2-Conductor 18-22 AWG Shielded	100 - 250 feet
Magnetic Lock	2-Conductor 18-22 AWG Shielded	50 - 125 feet
Dry Contact Closure (Most Gate Operators)	2-Conductor 18-24 AWG Shielded	500 - 2500 feet
Exit Request (REX) / Auxiliary Open Devices	2-Conductor 18-24 AWG Shielded	250 - 1000 feet
Door Status Sensor	2-Conductor 18-24 AWG Shielded	250 - 1000 feet
Barium Ferrite and Wiegand Readers	5-Conductor 18-22 AWG Shielded	200 - 500 feet
Proximity Readers	5-Conductor 18-22 AWG Shielded	200 - 500 feet
Postal Lock Box	2-Conductor 18-24 AWG Shielded	250 - 1000 feet
CCTV Camera (Optional)	Single Conductor RG-59u Coaxial	1000 feet (Monitor with a .25 volt p-p composite signal sensitivity)

NOTE: *Main power supply and control wiring MUST be run in separate conduits. Conduits must be UL approved for low and high voltage. Refer to the NEC for additional wiring requirements.*

Always provide power from a dedicated source. Plug provided transformer into an outlet wired to its own 10 Amp minimum circuit breaker. This will prevent two problems:

- Other equipment cannot introduce spikes, noise, surges or dips into the power circuit that will affect the system.
- The system's operation will not be affected if any other equipment develops a short circuit across the power line.

**** CAT 5/6 NETWORK CABLE NOTES:***

- *For outdoor distances exceeding 140 feet, a UL497 compliant primary surge protector MUST be installed at the unit.*
- *Distances exceeding 328 feet can be accommodated with additional hardware. Contact Technical Support for more information.*

Model Identification Table

Model	Description
IPAC	IPAC Panel
IPACIPDCC	IPAC 2 Door IPDC - Cloud

INSTALL

1 Site Survey

The unit MUST be configured with the proper network settings to operate. Refer to the ***Site Survey*** and record the settings below.

NETWORK

Internet service provider: _____

IP Address: _____ . _____ . _____ . _____

Netmask: _____ . _____ . _____ . _____

Gateway: _____ . _____ . _____ . _____

Primary DNS: _____ . _____ . _____ . _____

Secondary DNS: _____ . _____ . _____ . _____

Server Port: _____

SIP

SIP service provider: _____

SIP domain: _____

SIP port (usually 6050): _____

SIP username: _____

SIP password: _____

2 Mount the Unit

The unit should not be installed in rain or a wet environment.

1. To protect the screen and faceplate, place the unit face down in the carton.
2. Use a punch tool that is one inch or less to remove knockouts based on your installation requirements.

   IMPORTANT NOTES:
   - *To prevent damage to components DO NOT use a punch tool longer than one inch.*
   - *To prevent damage to latch make sure that door is closed and latch is properly engaged prior to removing knockouts.*
3. Attach the gaskets (provided) to the unit.

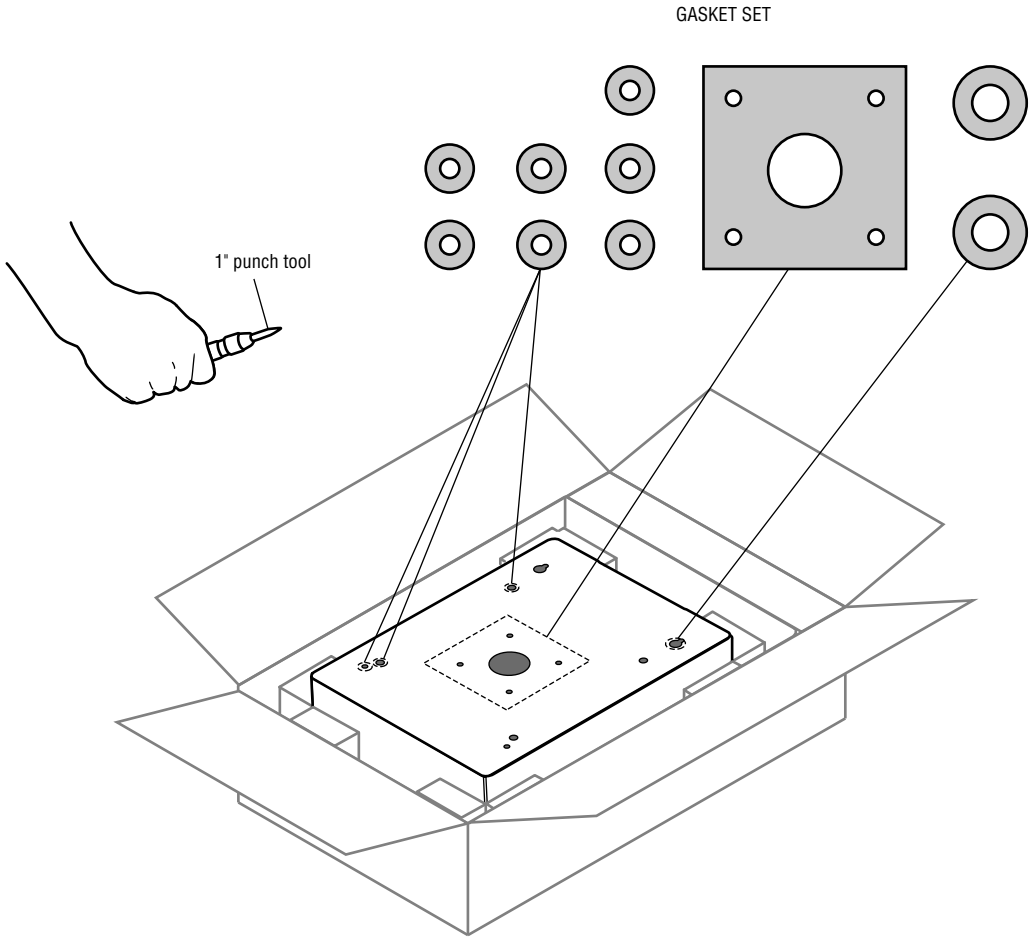
CAUTION

To prevent damage to the access control panel from moisture or water:

- DO NOT install during rain. Internal components MUST be kept free from of water and moisture.
- BEFORE opening the front cover of the access panel, remove ANY accumulated water from the top of the access control panel.

To prevent damage to ANY internal components:

- DO NOT attempt to remove the knockouts with a hammer. Banging on the knockouts may result in shock to the circuit boards, which could cause permanent damage. Use a 1 inch punch tool to remove the knockouts.



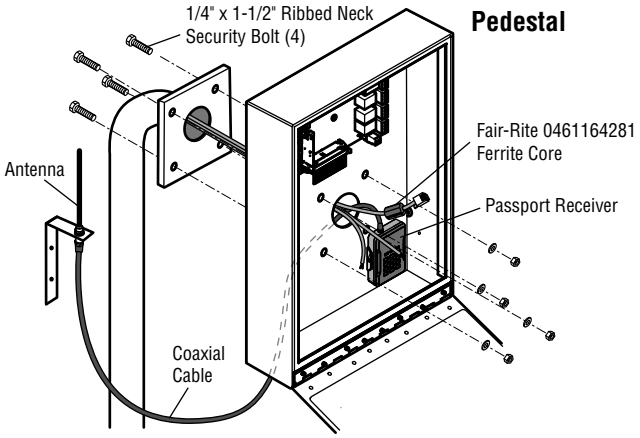
2 Mount the Unit

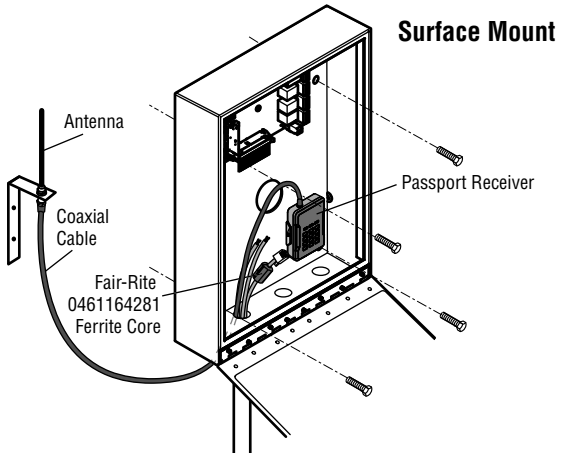
4. Attach the coaxial cable for the antenna to the Passport receiver.
5. Route the coaxial cable through a knockout in the metal enclosure.

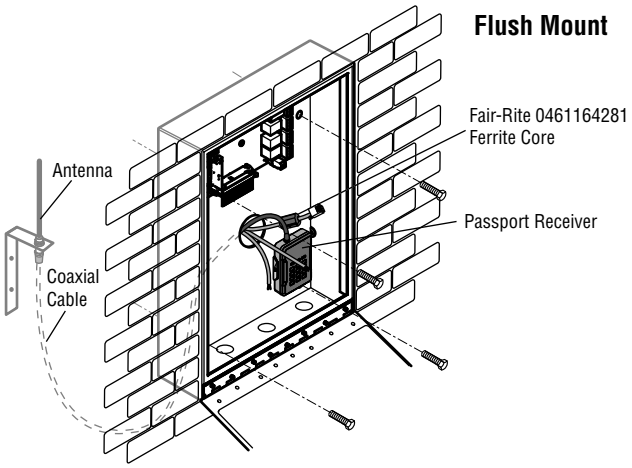
   NOTE: *To maintain the integrity of the metal enclosure use only the existing knockouts, do not drill new holes.*
6. Attach the antenna to the bracket and secure the bracket. To maximize the radio range the antenna must be installed outside of the metal enclosure. Do not place the antenna within the metal enclosure.
7. Insert the wiring. Mount the unit securely to a flat surface or pedestal with appropriate hardware.

   NOTE: *Ensure the cover can fully open to allow access after the installation is complete.*
8. Install ferrite core as shown below.

DO
Make sure the unit is properly sealed to prevent damage to the access control panel from moisture.





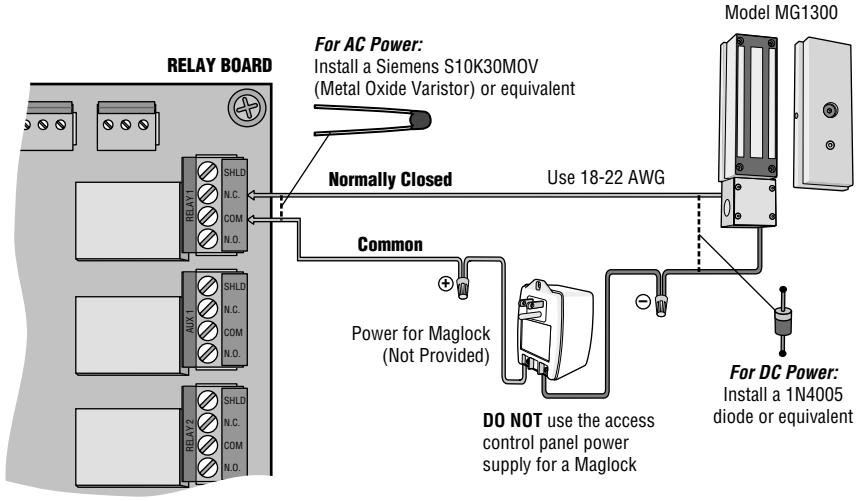


3 Connect Devices

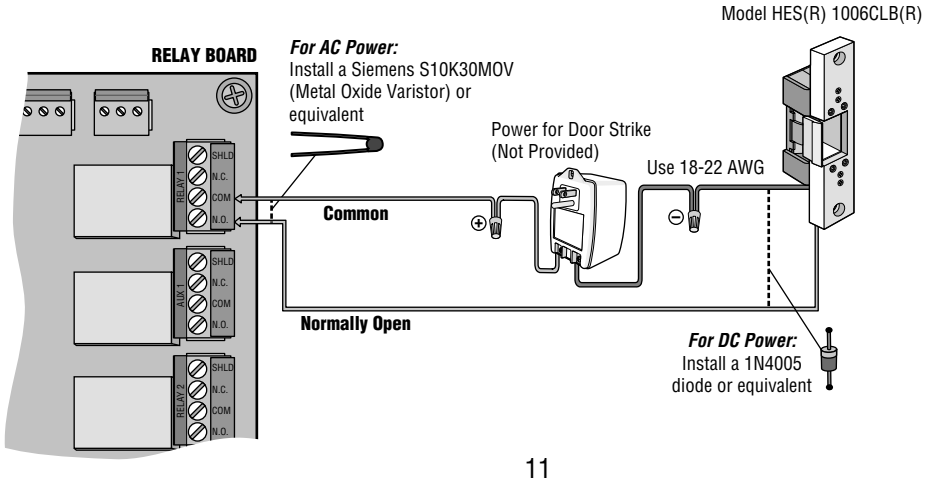
Below are examples of wiring a maglock or door strike. Refer to page 12 for wiring diagram. There is a 3 Amp 24 Volt DC limit on through current for ALL relays.

DO
• Use a separate AC or DC power supply for a maglock or door strike (not provided). • For AC Power: Install a Siemens S10K30MOV (Metal Oxide Varistor or equivalent) across the power connections controlled by the relay. • For DC Power: Install a 1N4005 diode or equivalent.
DO NOT
• DO NOT use the unit power supply for a maglock or door strike. • DO NOT overload the removable terminal block connectors. ONLY one wire per hole. • DO NOT install the system in a fail secure mode (lock devices require power to grant access) unless permitted by the local authority having jurisdiction. Doing so may cause interference with the operation of panic hardware.

Maglock



Door Strike

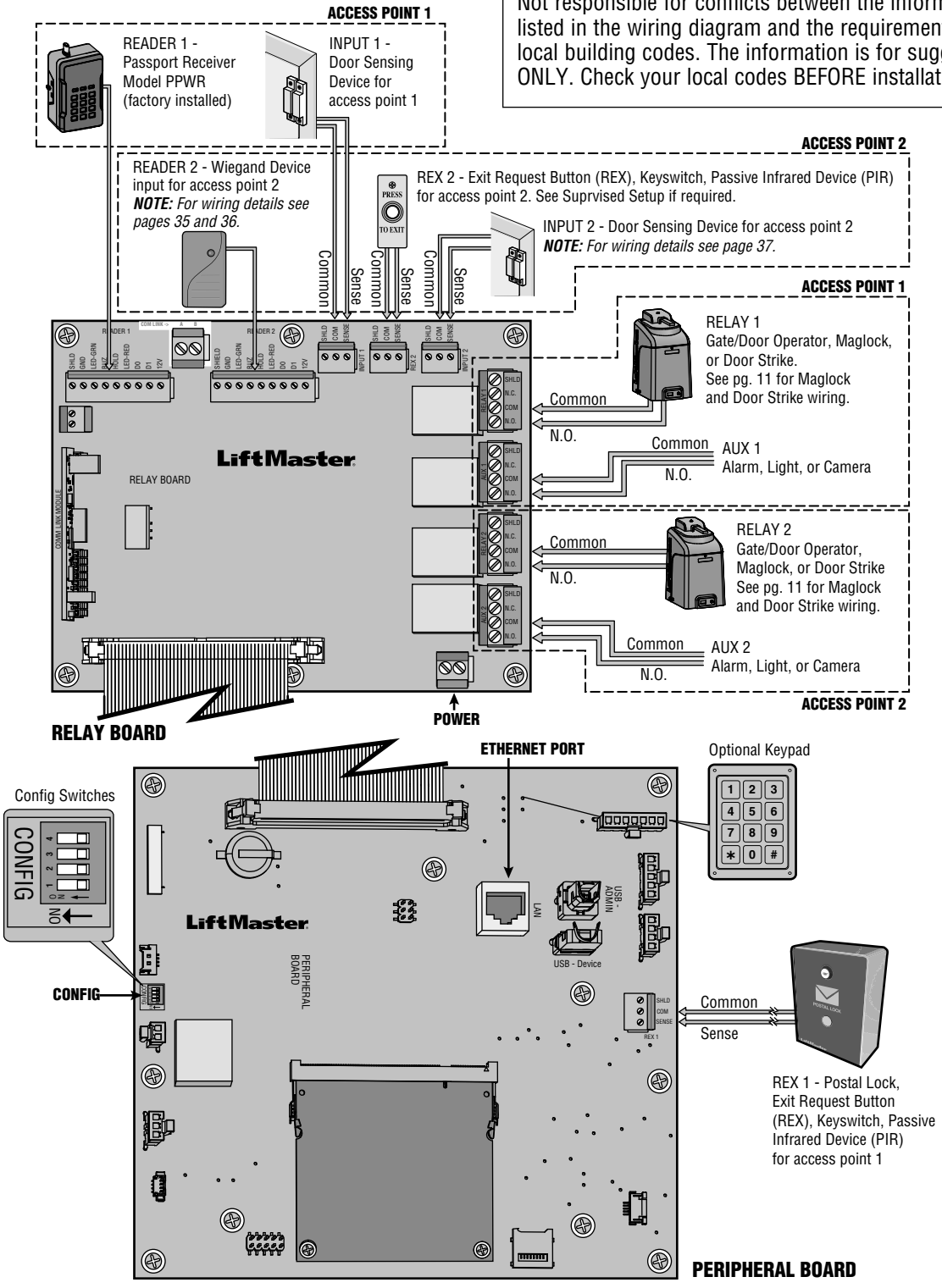


3 Connect Devices

Wiring Diagram

CAUTION

Not responsible for conflicts between the information listed in the wiring diagram and the requirements of your local building codes. The information is for suggested use ONLY. Check your local codes BEFORE installation.



4 Install the Ground

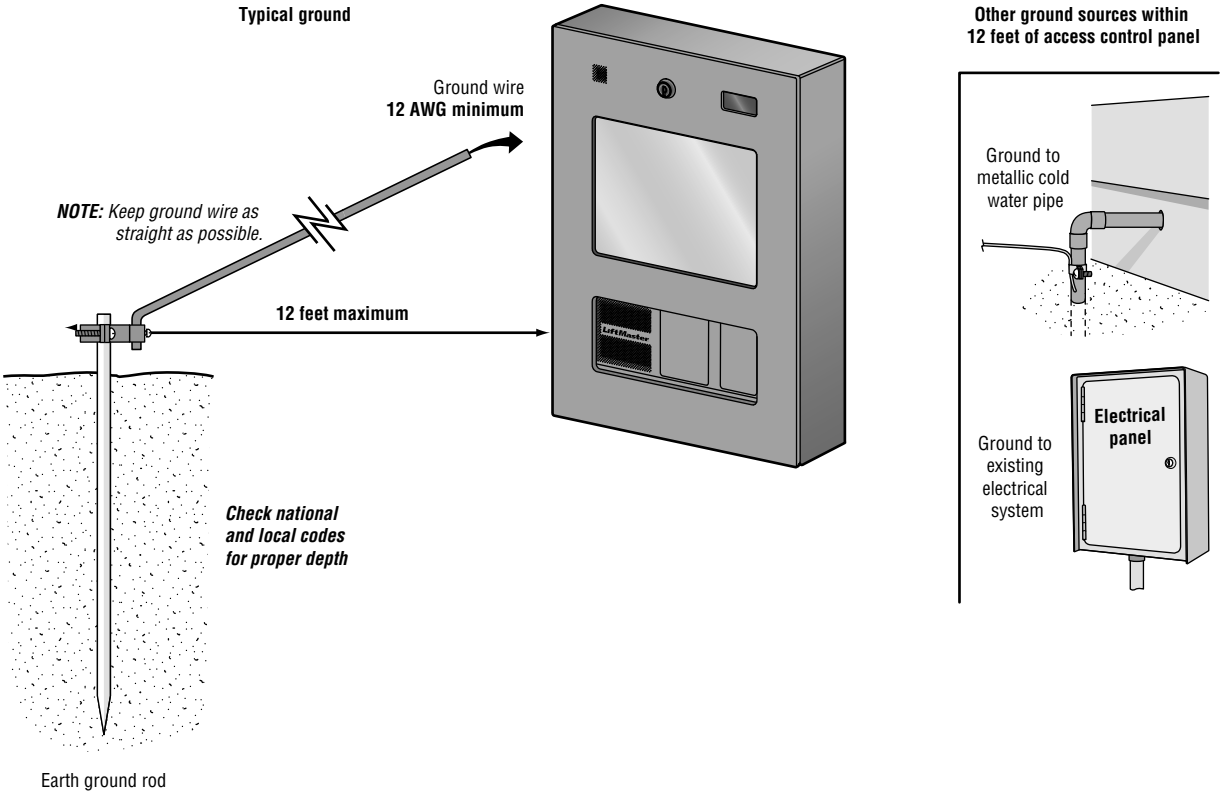
1. Connect the ground wire (12 AWG or larger) to the unit ground lug.
2. Run the wire from unit to suitable earth ground.

NOTE: *Shield connections on boards should not be connected to ground lug.*

IMPORTANT: An earth ground rod is strongly recommended and should be no further than 12 feet from the unit and use a minimum of 12 gauge wire in most cases. The type and length of earth ground rods vary by region. Contact the building inspector's office in the municipality where you plan to install the unit for correct grounding materials and installation procedures.

CAUTION

To AVOID damaging gas, power or other underground utility lines, contact underground utility locating companies BEFORE digging.



5 Connect Power

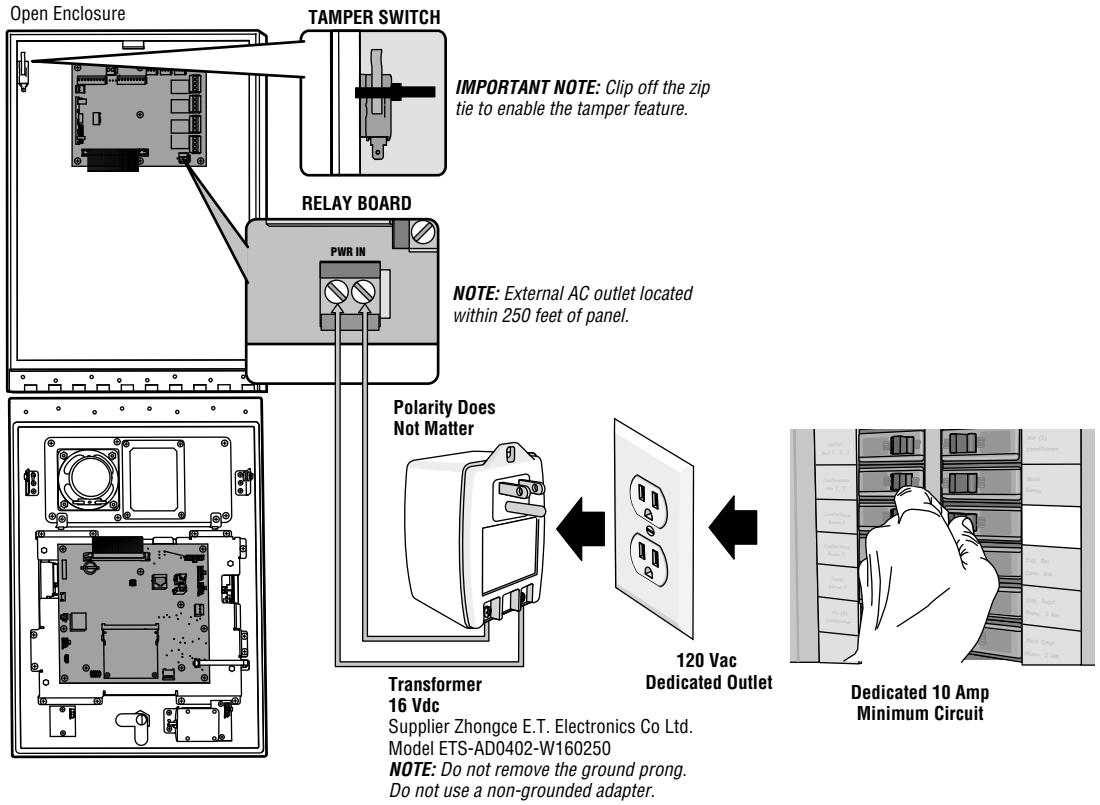
The outlet for the unit MUST be an external dedicated 120 Vac outlet located within 250 feet cable run of the unit. This outlet should be wired back to its own 10 Amp minimum circuit breaker.

1. Connect 18 AWG wire (minimum gauge) to the screw terminals on the transformer.
2. Remove the PWR IN terminal block from the relay board.
3. Connect the transformer wires to the PWR IN terminal block, then reattach the terminal block to the relay board.
4. Plug the transformer into a 120 Vac outlet after all connections have been made. Any other type of outlet will damage the system.

   NOTE: *The green LED on the peripheral board will blink and the green LED on the relay board will light solid when powered up. The unit will display the LiftMaster logo while booting up. When boot up is complete, the user interface will appear.*

CAUTION

- DO NOT use ANY power supply other than those supplied with your access control panel.
- DO NOT power electronic strikes and latches with the same power supply used to power the access control panel; doing so will cause DAMAGE to the access control panel. Use ONLY a UL listed burglar alarm or access control system to power electronic strikes and latches.
- DO NOT connect the power supply to a switched outlet or otherwise controlled AC outlet.
- DO NOT connect the power supply to the 120 Vac outlet until ALL wiring is completed.
- Install the transient noise suppression device (MOV) supplied with the access control panel for AC powered devices and Diode for DC powered devices.



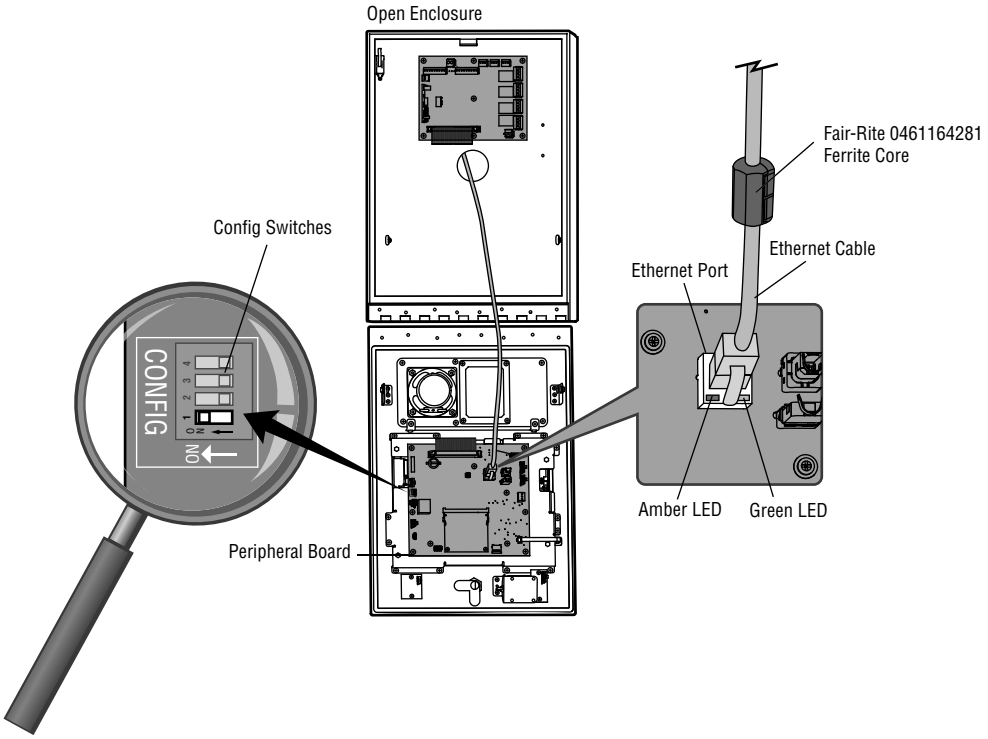
6 Connect Ethernet

The Local Area Network (LAN) port is a 10/100 ethernet interface with an RJ45 jack for connecting the PERIPHERAL BOARD to a LAN in order for it to gain connectivity to the Internet. Use a straight, (i.e., non-crossover) cable to connect this port to a local hub, switch or router. Connect the peripheral board to a LAN functionality is a supplementary feature.

1. Connect an ethernet cable from your LAN to the LAN port on the peripheral board. When connected properly, the green and amber LED on the ethernet port will light/flicker. If the green LED is not lit, check the connections on the unit and the ethernet hub.

Switch to Programming Mode

1. Set CONFIG switch #1 on the peripheral board to ON. Factory default settings is OFF (all four switches).
2. Close and lock the faceplate.



CONNECT

NOTE: *The instructions contained in the following sections are ONLY for IPAC Stand-Alone applications. Connectivity and setup information for IPAC Cloud applications can be found in the quickstart guide available online at http://ipac.liftmaster.com/*

1 Bring Unit Online

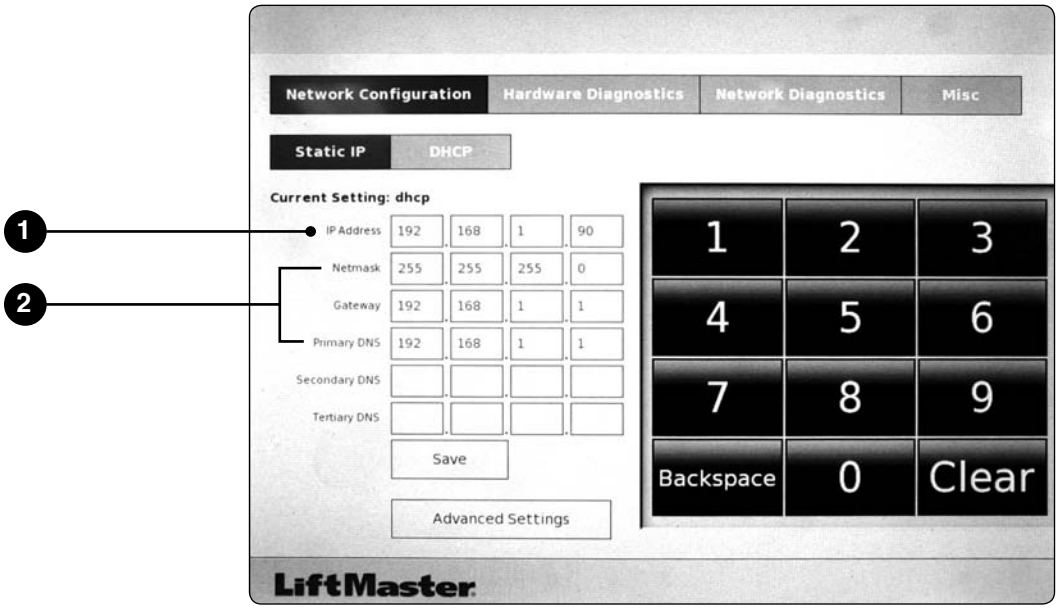
Enter Network Settings

The unit must have a known IP address if it is to be accessed from other machines on the network. The most convenient way to achieve this is to set a Static IP Address appropriate for the local network. Refer to the ***Site Survey*** for your installation site or contact your LAN administrator for the corresponding settings. Configure network settings functionality is a supplementary feature.

1. Enter the IP Address assigned by the local network administrator (refer to the ***Site Survey***).

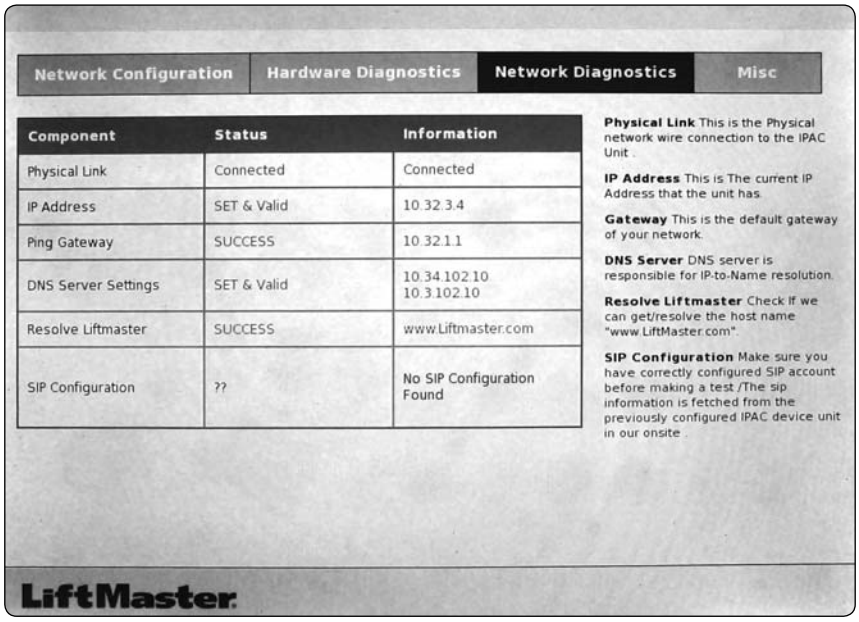
   IMPORTANT: *The use of DHCP is not recommended because the assigned IP address could be inadvertently changed by the LAN router/switch.*

2. Enter network settings for **Netmask, Gateway**, and at least one **DNS Server**.
3. Press **Save**.



2 Network Diagnostics

1. Press the **Network Diagnostics** button to see the status of the network connections. The SIP service will be setup by the property.
2. Open faceplate on unit and set CONFIG Switch #1 to OFF to exit programming mode.

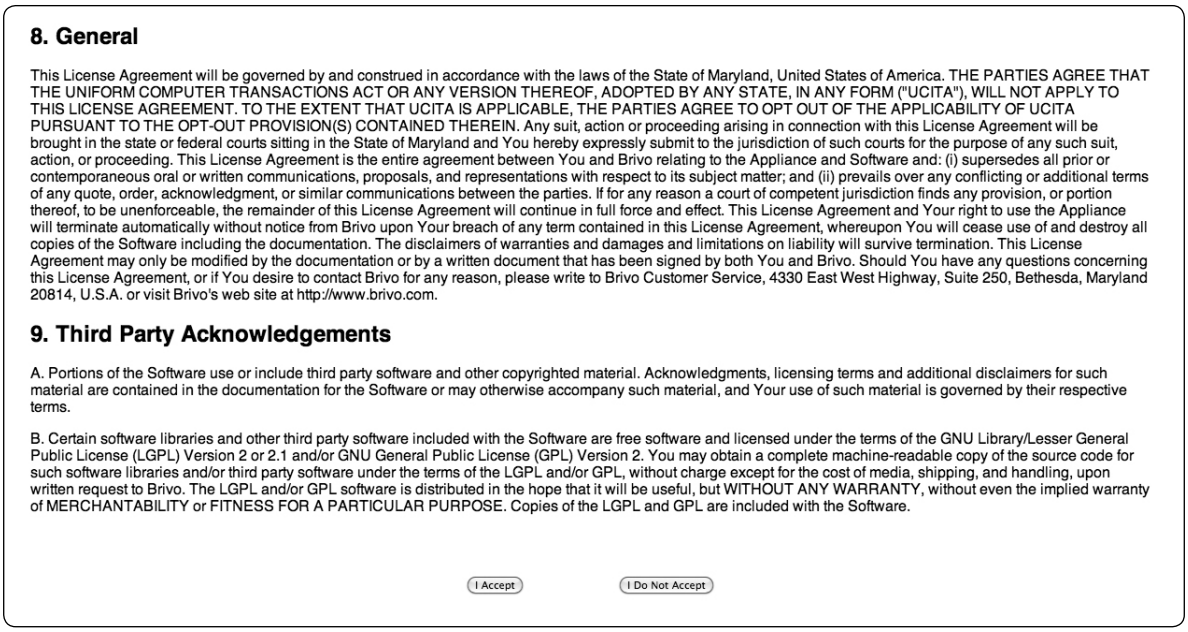


SETUP

1 User Agreement

LiftMaster Access Control Management (ACM) software enables administration of the unit system and is accessible through a web browser from any computer on the local network.

1. In the address bar of your web browser, enter the IP address assigned to the unit.
2. Upon initial connection, the end user license agreement will be displayed. Property management MUST be present to review and provide agreement to terms and conditions.
3. Click **I Accept**. The Log In page displays.
4. Log in with the default **Username** “admin” and do not enter a **Password**. Click **Login**. The Welcome page displays.



8. General

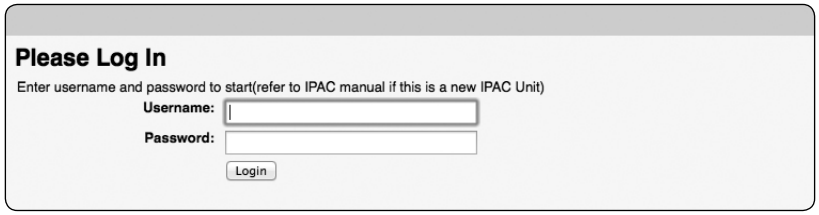
This License Agreement will be governed by and construed in accordance with the laws of the State of Maryland, United States of America. THE PARTIES AGREE THAT THE UNIFORM COMPUTER TRANSACTIONS ACT OR ANY VERSION THEREOF, ADOPTED BY ANY STATE, IN ANY FORM ("UCITA"), WILL NOT APPLY TO THIS LICENSE AGREEMENT. TO THE EXTENT THAT UCITA IS APPLICABLE, THE PARTIES AGREE TO OPT OUT OF THE APPLICABILITY OF UCITA PURSUANT TO THE OPT-OUT PROVISION(S) CONTAINED THEREIN. Any suit, action or proceeding arising in connection with this License Agreement will be brought in the state or federal courts sitting in the State of Maryland and You hereby expressly submit to the jurisdiction of such courts for the purpose of any such suit, action, or proceeding. This License Agreement is the entire agreement between You and Brivo relating to the Appliance and Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. If for any reason a court of competent jurisdiction finds any provision, or portion thereof, to be unenforceable, the remainder of this License Agreement will continue in full force and effect. This License Agreement and Your right to use the Appliance will terminate automatically without notice from Brivo upon Your breach of any term contained in this License Agreement, whereupon You will cease use of and destroy all copies of the Software including the documentation. The disclaimers of warranties and damages and limitations on liability will survive termination. This License Agreement may only be modified by the documentation or by a written document that has been signed by both You and Brivo. Should You have any questions concerning this License Agreement, or if You desire to contact Brivo for any reason, please write to Brivo Customer Service, 4330 East West Highway, Suite 250, Bethesda, Maryland 20814, U.S.A. or visit Brivo's web site at http://www.brivo.com.

9. Third Party Acknowledgements

A. Portions of the Software use or include third party software and other copyrighted material. Acknowledgments, licensing terms and additional disclaimers for such material are contained in the documentation for the Software or may otherwise accompany such material, and Your use of such material is governed by their respective terms.

B. Certain software libraries and other third party software included with the Software are free software and licensed under the terms of the GNU Library/Lesser General Public License (LGPL) Version 2 or 2.1 and/or GNU General Public License (GPL) Version 2. You may obtain a complete machine-readable copy of the source code for such software libraries and/or third party software under the terms of the LGPL and/or GPL, without charge except for the cost of media, shipping, and handling, upon written request to Brivo. The LGPL and/or GPL software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY, without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. Copies of the LGPL and GPL are included with the Software.

I Accept I Do Not Accept



Please Log In

Enter username and password to start(refer to IPAC manual if this is a new IPAC Unit)

Username:

Password:

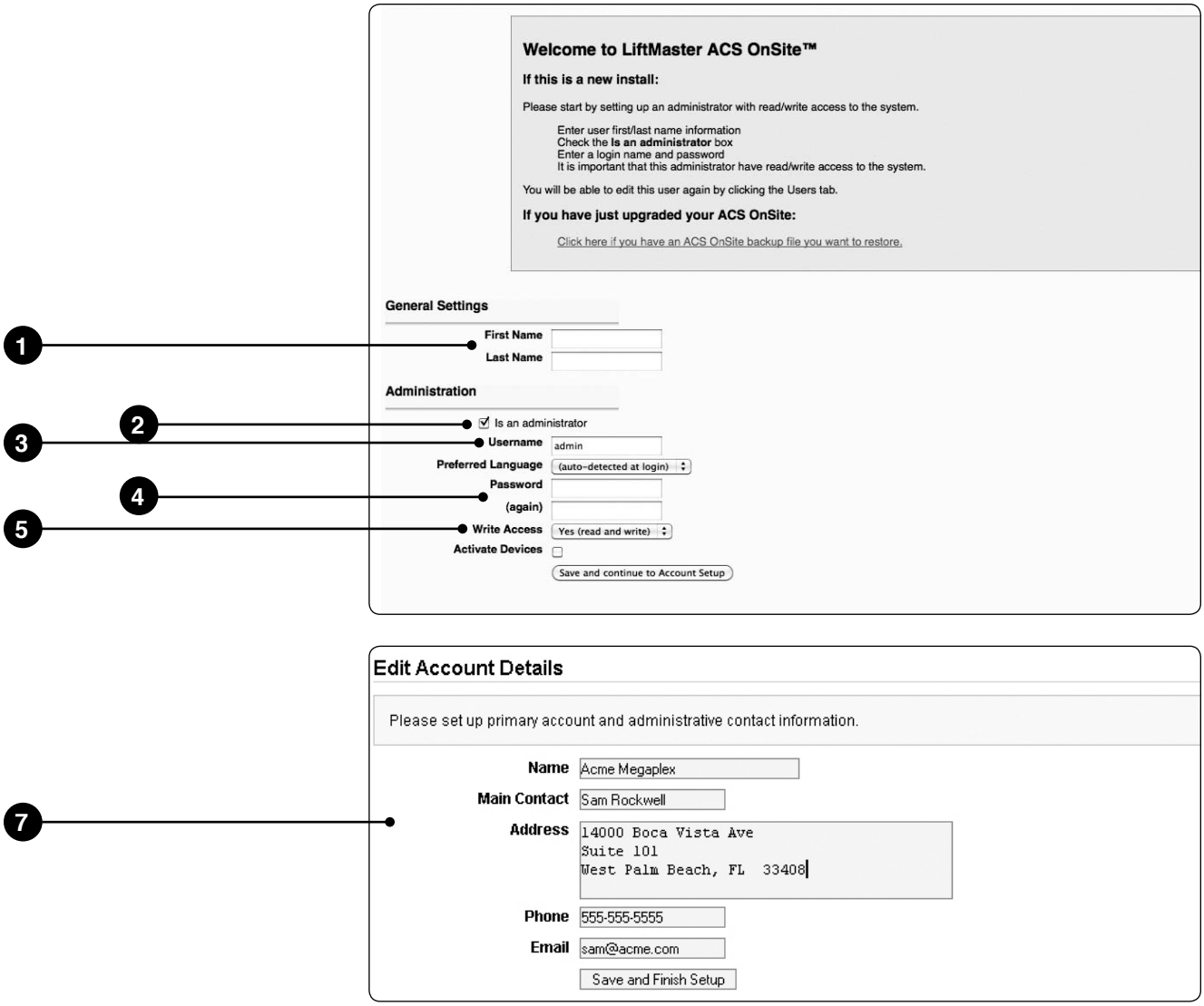
Login

2 Account Setup

Set Up the Administrator Account

The first thing you need to do after logging in is set a password and a few other account details to get started.

1. Enter the **First Name** and **Last Name** of the account administrator.
2. Make sure the **Is an Administrator** box is checked.
3. The default username is “admin”. You may want to change the username of the account administrator for security reasons.
4. Enter a password for the account administrator. Re-enter the exact same password in the **(again)** field.
5. The **Write Access** field defaults to Yes (read and write). Do not change.
6. Click **Save and continue to Account Setup**. The Edit Account Details page displays.
7. Enter the contact information in the fields, and then click **Save and Finish Setup**.



CONFIGURE

1 Configure Hardware (Door Board)

The unit consists of one door board used to manage the doors and devices defined for an account. By configuring the hardware (door board) you tell the unit what type of sensing and request-to-exit devices are connected to the door board.

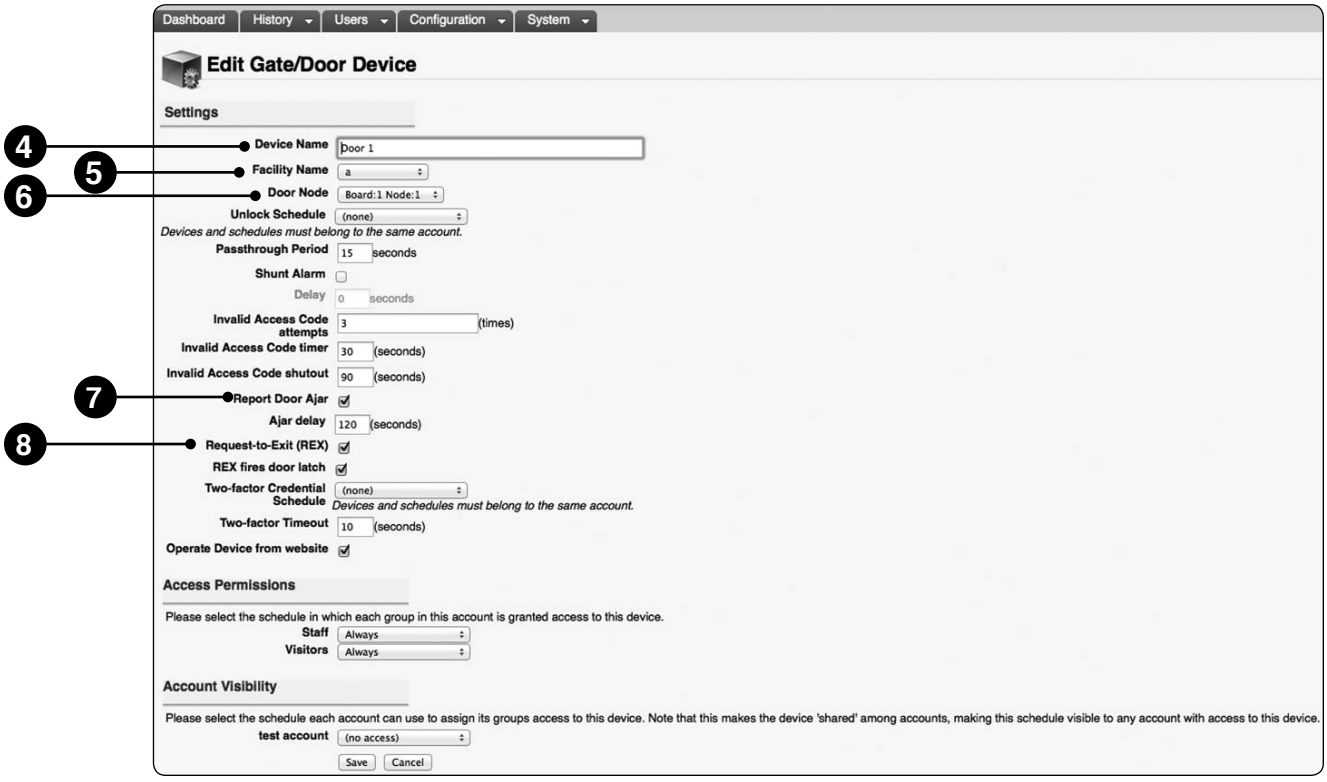
1. Click the **Configuration** tab > Click **Hardware** > Click **Hardware** on the sidebar menu.
2. Click **Door Board** > click the **Edit** Button. The Edit Board Details page displays.

   Modify the settings for REX1, INPUT 1, REX2 and INPUT 2 to match the actual devices that are wired to these connections:
3. In the **EOL** field, click **Yes** or **No** to indicate if the input point is wired for end-of-line supervision.
   NOTE: *For wiring information refer to section "Optional Door Sensor Wiring" on page 37.*
4. In the **Default State** field, click **Open** to indicate that the input point is normally open, or **Closed** to indicate that it is normally closed.
5. Click the **Save** button.

2 Configure Device (Doors)

By configuring devices, you tell the unit what hardware connections are available. Once a door is properly wired to the unit, you must configure the door using the unit interface so it can be used.

1. Click the **Configuration** tab > Click **Hardware** > Click **Devices** on the sidebar menu.
2. Click **Create New Device** button.
3. Select **Door** as the Device Type > Click **Next**. The Edit Device page displays.
4. Enter a **Device Name** for the door.
5. **Facility Name** is a required field for all device types and identifies the account responsible for the device. The default value in the drop-down list is the current account.
6. Select the **Door Node** to which the door is wired.
7. If the door is wired with a closure switch, you may also want to leave the **Report Door Ajar** box checked. This feature controls how long a door can be left propped or held open before it is considered a security risk, causing the event to be recorded in the Activity Log. The default setting is checked.
8. If the door has a motion sensor or request-to-exit button, make sure the **Request-to-Exit** box is checked. With a REX switch, if the door is opened without a credential or a request to exit, the Activity Log records a Door Forced Open event and an optional email notification is sent. The default setting is checked.



2 Configure Device (Doors)

(Continued)

The following settings are not required. Set as needed.

9. The **Unlock Schedule** drop-down list is used to indicate the schedule period during which the door should be left unlocked. (Click the Help button in the upper right corner of ACS Onsite software.)
10. In the **Passthrough Period** field, enter the maximum length of time (1-999 seconds) the door should remain unlocked after a user presents his or her credentials and is authenticated or presses a Request-to-Exit switch. For example, if this value is set to 15, the user has 15 seconds to pass through the door before it automatically re-locks. The default setting is 10.
11. Check the **Shunt Alarm** box if the door is connected to an alarm system that should be shunted (temporarily disabled) for a specified period of time after the Passthrough period has expired. The shunt time is in addition to the Passthrough period. For example, if **Passthrough Period** is set to 10 seconds, and Shunt Alarm Delay is 1 second, the alarm will engage only if the door remains in an open state for more than 11 seconds after the user is authenticated.
12. When the **Shunt Alarm** box is checked, enter the length of time (1-9 seconds) the alarm system should be shunted In the **Delay** field. The default and strongly recommended setting is 1.
13. In the **Invalid Access Code attempts** field, indicate the maximum number of consecutive invalid access codes that can be entered in the door's keypad (1-10) before it is considered a security risk and the keypad freezes. The default setting is 3.
14. In the **Invalid Access Code timer** field, specify the amount of time (1-99 seconds) allowed for each attempted access code entry. For example, if this field is set to 30, and Invalid Access Code attempts is set to 3, a person would have 90 seconds total (30 seconds per attempt) to enter a valid access code before the keypad freezes. The default is 30.
15. The **Invalid Access Code shutout** field lets you set the length of time (1-999 seconds) the keypad should remain frozen if the maximum number of invalid access codes or the access codes timer is exceeded. The default setting is 90.

2 Configure Device (Doors)

(Continued)

16. If the Door Ajar feature is enabled, use the **Ajar delay** field to indicate the maximum length of time (1-999 seconds) the door can be left ajar without causing a security violation. The default setting is 120.
17. Check the **REX fires door latch** field to indicate that the REX switch causes the door to unlock. The default is checked.
18. On the **Two Factor Credential Schedule** drop-down list, click the schedule during which you want this door to require two credentials. During the selected time period, users with privileges at this door will need to scan a security credential and enter a PIN to gain access.
19. In the **Two Factor Timeout** field, enter the amount of time (1-99 seconds) the user will have to present both credentials. If the user takes more than the allotted time, access will be denied. The default setting is 10.
20. When the **Operate Device from website** option is checked, system devices configured with an output behavior of Pulse, Latch or Unlatch will be monitored and controllable from the Dashboard page.
21. The **Access Permissions** section of the page displays only when a Door or Valid Credential Input device is being configured, and lists all user groups currently defined for the owner account. Two groups are defined automatically when the System Account is first created: “Staff” and “Visitors.” For each group, select the schedule according to which the group has access to this door or Valid Credential device.
22. Click **Save**.

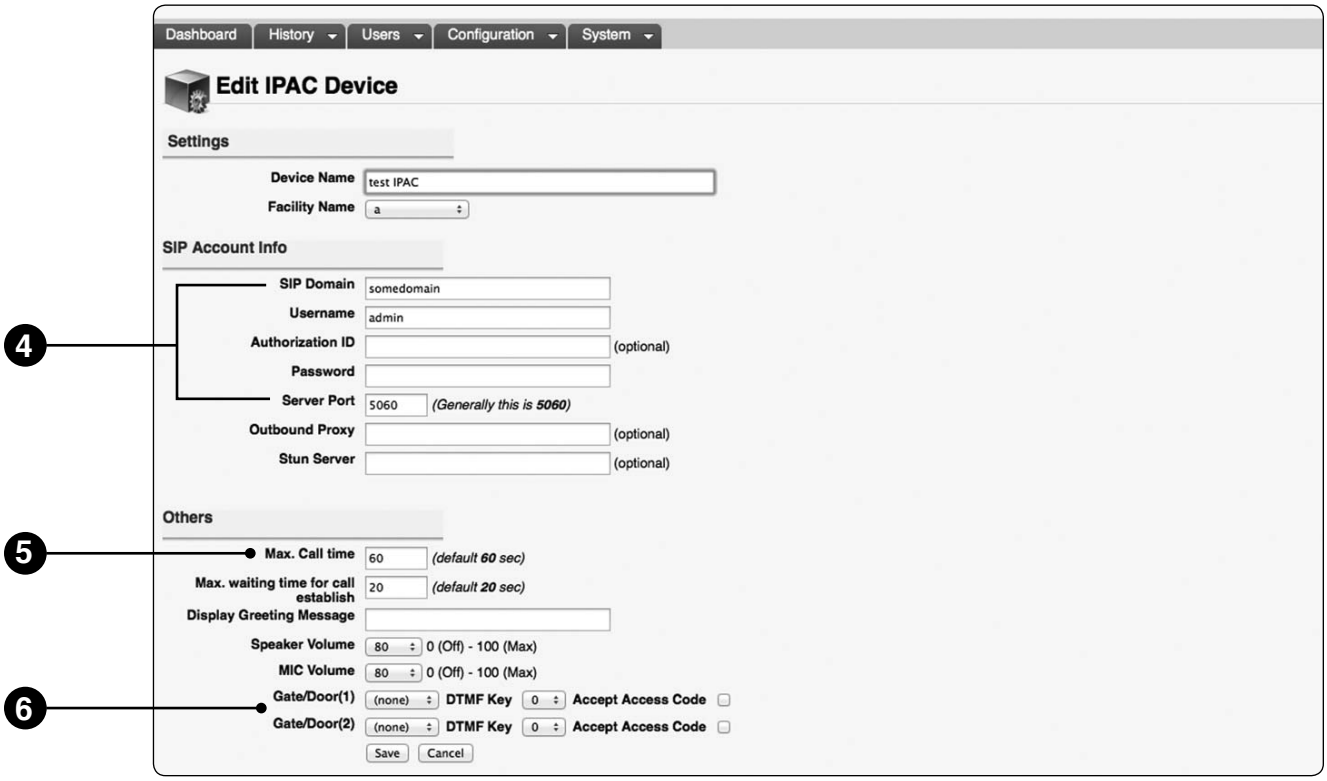
3 Configure Unit

To configure the unit for voice, you must first configure the internet based telephone service SIP (Session Initiation Protocol) provider.

1. Click the **Configuration** tab > Click **Hardware** > Click **Devices** on the sidebar menu.
2. Click **Create New Device** button.
3. Select **IPAC Device** as the Device Type > Click **Next**. The Edit Device page displays.
4. Enter SIP service provider configuration settings (refer to the for your installation site):
   - **SIP Domain**
   - **User name**
   - **Password**
   - **Server Port** (typically 5060)
5. Configure the call time settings.
6. Select a device for **Gate/Door (1)** and **(2)** and **DTMF key** to activate. Check the **Accept Access Code** field to allow users to activate the door with their assigned PIN.

   The rest of the settings are not required. Set as needed.
7. Click **Save**.

   Refer to the administrator's manual for complete information about credentials, users and tenants.



4 Add Credentials

Credentials are the Weigand cards or Passport remote controls that allow users to identify themselves at the unit.

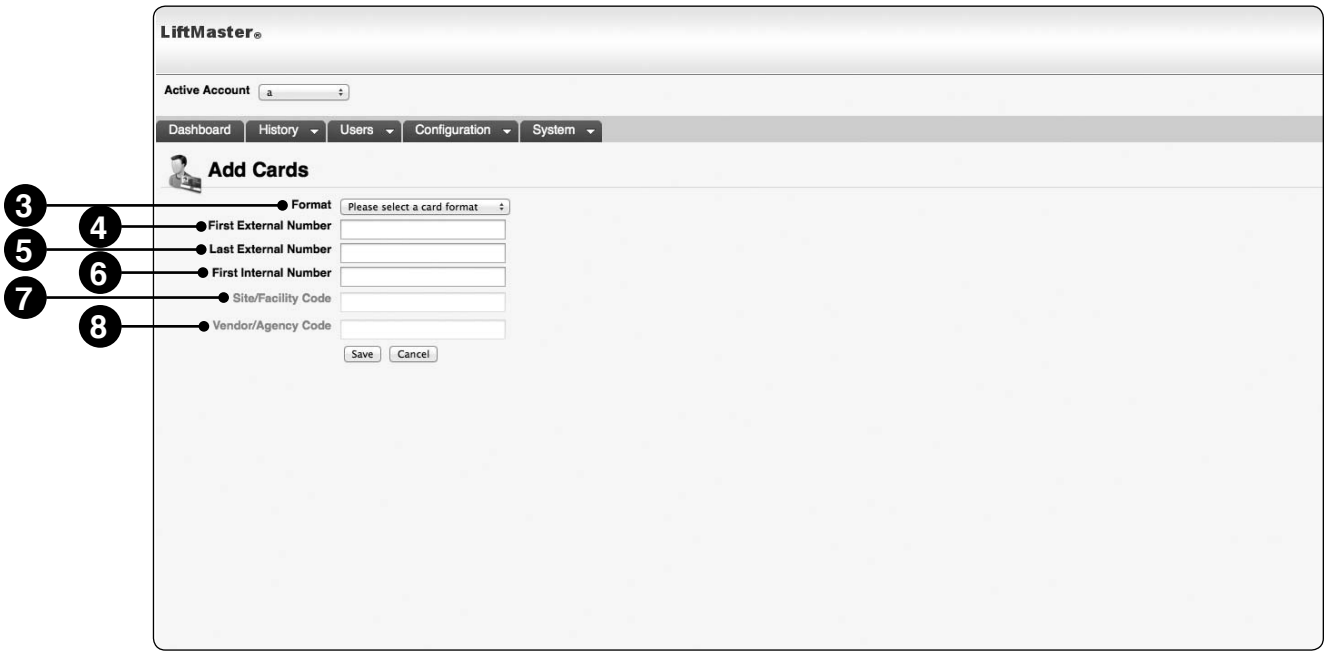
NOTES: *• The included Passport receiver should be left in pass through mode. This is the default setting from the factory. This setting will pass all Passport transmitter facility codes and ID's to the IPAC and the IPAC will validate and allow access as needed.*

• The steps for adding Passport remote controls is based on the factory default settings of the Passport receiver (pass thru, 26 bit Weigand).

1. Click the **Users** tab > Click **Credential Cards**.
2. Click the **Add Credentials** button. The Add Cards page displays.
3. Select the appropriate **Credential Format** from the list (for Passport remote controls select 26 bit standard Weigand).
4. Enter the **First External Number**. The external number is the number printed on the card or Passport remote control. (For a Passport remote control enter the ID number in line with 26 bits.)

   NOTE: *The internal control number and external number are often the same, in which case you only need to enter the external number.*
5. Enter a **Last External Number**. A card is added for each number in the range defined by the first and last external numbers inclusively.
6. For Weigand cards only, enter the **First Internal Number**. The internal number is part of the credential's embedded value. First Internal Number is a required field only if the internal number is different from the external number.
7. Enter the **Site/Facility Code** if provided by the credential manufacturer. Not all credential formats have facility codes. In those cases enter 0 for the facility code. (For a Passport remote control enter the FC number in line with 26 bits.)
8. For Weigand cards only, enter the **Vendor/Agency Code** if one came from the credential manufacturer. Not all credential formats have vendor/agency codes. In those cases, the Vendor/Agency Code field will remain grayed out.

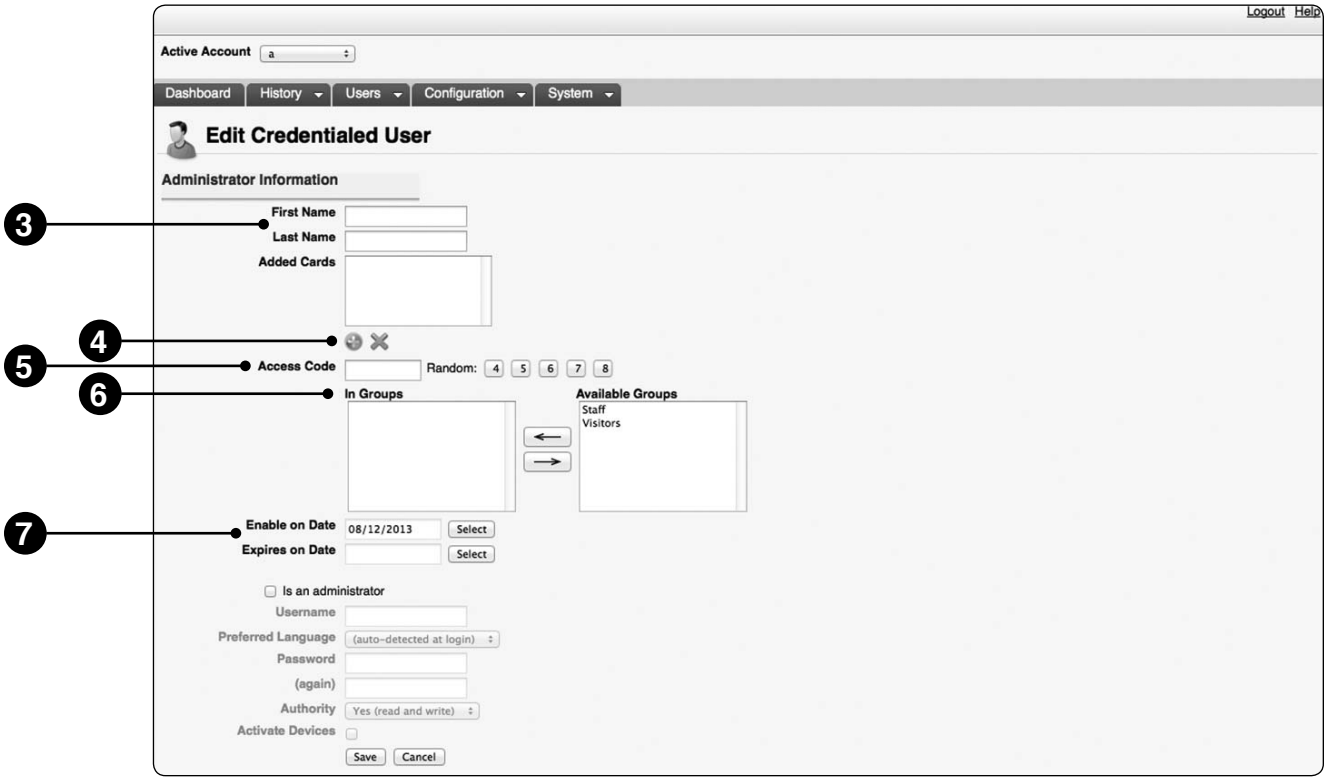
   NOTE: *The maximum number of Weigand cards you can add at one time is 100.*
9. Click **Save**.



5 Add Users

A user is any person who requires access to one or more controlled access points at the facility. A user has a unique card or PIN that enables entry and exit. A user can belong to one or more user groups. Users can be assigned to up to 16 groups at a time. The user inherits access permissions from the groups to which he or she belongs. For users who belong to multiple groups, their access permissions are cumulative.

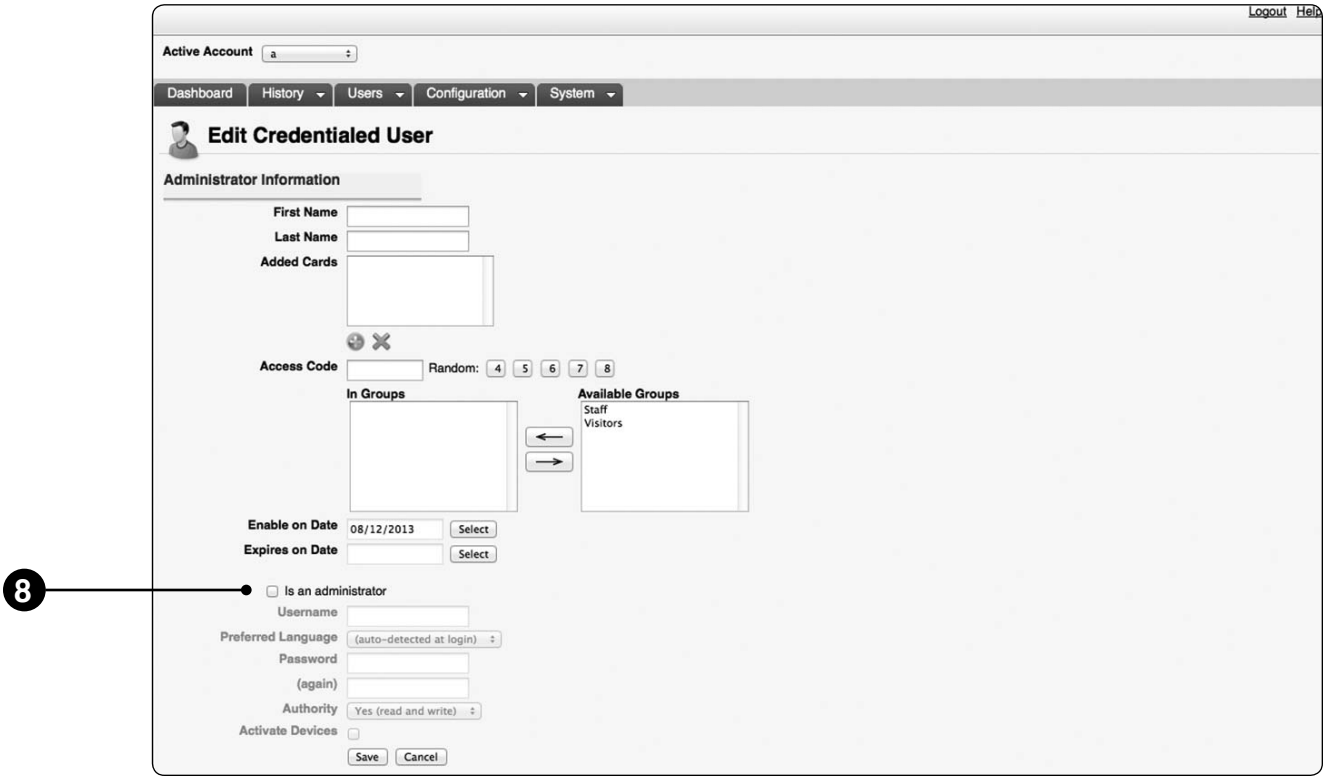
1. Click the **Users** tab > Click **Credentialed Users**.
2. Click the **Create New User** button. The Edit User page displays.
3. Enter the **First Name** and **Last Name**. These fields are required.
4. To assign a card click on the **+** button under the **Added Cards** field and select a card from the popup menu.
5. If your doors have keypads, enter a 4- to 8-digit number in the **Access Code** field, or click one of the number buttons to generate a random PIN with 4, 5, 6, 7 or 8 digits.
6. To assign a user to a group, select the desired group from the **Available Groups** list on the right and click the left arrow (←). The group name displays in the **In Groups** list. To remove a user from a group, select the group from the **In Groups** list and click the right arrow (→).
7. The **Enable on Date** defaults to today's date. Change the date if the user's access permissions should take effect on a later date. The **Expire on Date** field is empty by default. Enter a date for user's access permissions to expire.



5 Add Users

(Continued)

8. If you want the user to be able to log into ACS Onsite, click the box for **Is an administrator**. When you do so, the six associated fields displayed below it become active:
   - **Username**. Enter the name the Administrator will use to log into the system. The username must be 32 or fewer characters long, and can be changed at any time.
   - **Preferred Language**. Select a preferred language from the drop-down list.
   - **Password**. Enter a password for the Administrator. Re-enter the exact same password in the **(again)** field. Both of these fields are required when creating administrative permissions for a user, or when changing the password. Otherwise they are optional fields.
   - **Write Access**. This field defaults to No (read-only), allowing the Administrator to view all data associated with his/her account, but not to manipulate that data in any way. You can also choose Yes, to give the user read/write access.
   - **Activate Devices**. This check box option is used to define if an Administrator is authorized to use the command button controls on the Dashboard page. If checked, an Administrator can control devices configured with an output behavior of Pulse, Latch or Unlatch from the Dashboard page. If unchecked, an Administrator is not given the option of controlling devices from the Dashboard page.
9. Click **Save**.

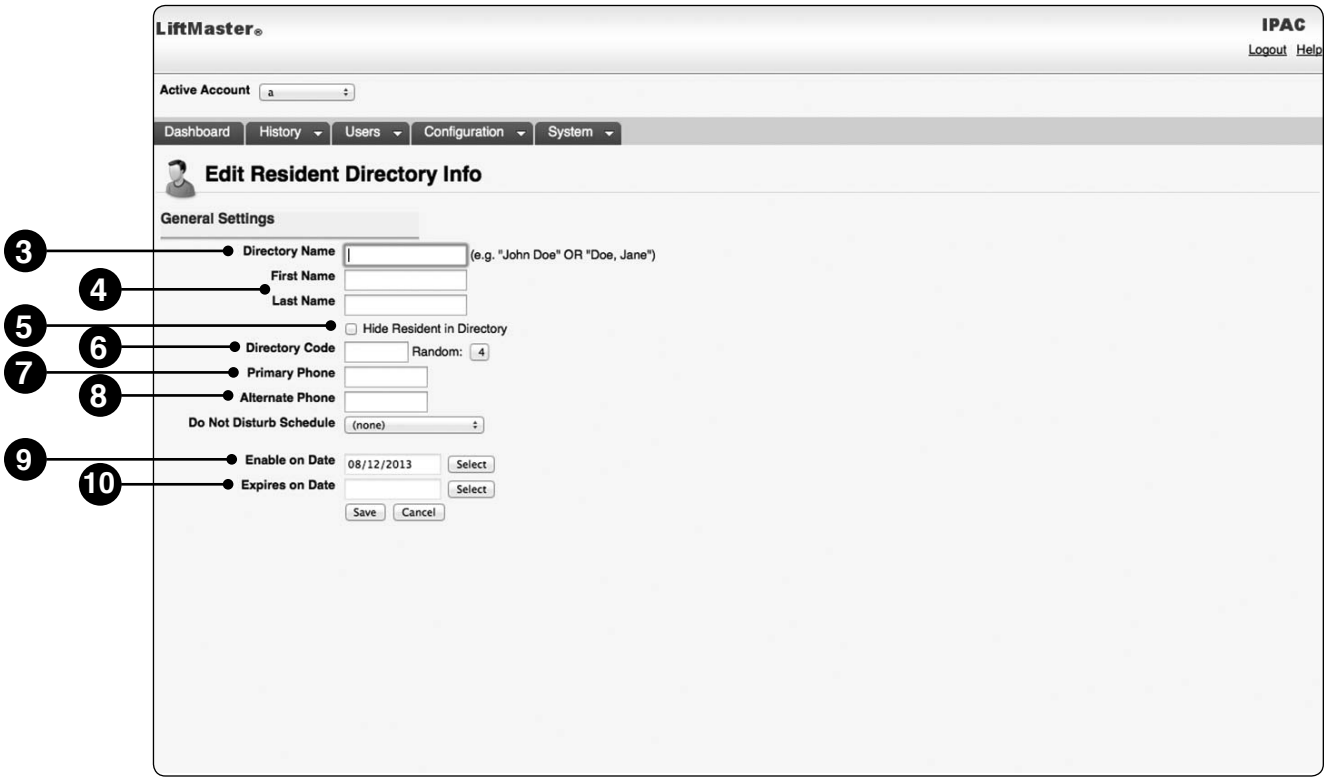


6 Add Residents

The Create Residents function allows the administrator to program names and associated telephone numbers. When users approach the unit they can scroll or search for residents in the directory. Once a resident is found the user may call and establish a telephone communications session with the resident. The resident has the option to grant or deny access by pressing digits on the telephone.

1. Click the **Users** tab > Click **Resident Directory Info**.
2. Click the **Create New Resident** button. The Edit Resident page displays.
3. In the **Directory Name** field, enter the text to be displayed in the directory for this Resident. This value is usually the Last Name and First initial of the Resident.
4. Enter the resident's **First Name** and **Last Name**.
5. If you would like to hide the Resident from the directory display, click on the check box **Hide in Resident Directory**.
6. In the **Directory Code** field select a 4-digit number to assign to this Resident. A random 4-digit number may be assigned by clicking on Random [4].
7. In the **Primary Phone** field, enter the primary telephone number used to contact this Resident.
8. If an alternate telephone number is desired (i.e. – Cellular or office), enter it in the **Alternate Phone** field.
9. Enter the date this Resident is to become effective in the **Enable on Date** field. This value is usually the date of entry.
10. If an expiration date is required, enter into the **Expires on Date** field. This value is usually blank (does not expire).
11. Click **Save**.

IMPORTANT NOTE: *In either stand-alone or server based installations, we suggest periodic backups of your IPAC data.*



VALIDATE

1 Validate Setup

Test a Directory Search

1. Press **Directory** on the unit touch screen.
2. Press the name field and then use the keyboard on the touch screen to enter a name.
3. Press **Search**.

Test a Directory Code

4. Press **Directory Code** on the unit touch screen.
5. Use the keypad on the touch screen to enter a tenant's directory code.
6. Press  .

Test an Access Code

7. Press **Access Code** on the unit touch screen.
8. Use the keypad on the touch screen to enter an access code.
9. Press **Enter**.

OPTIONS

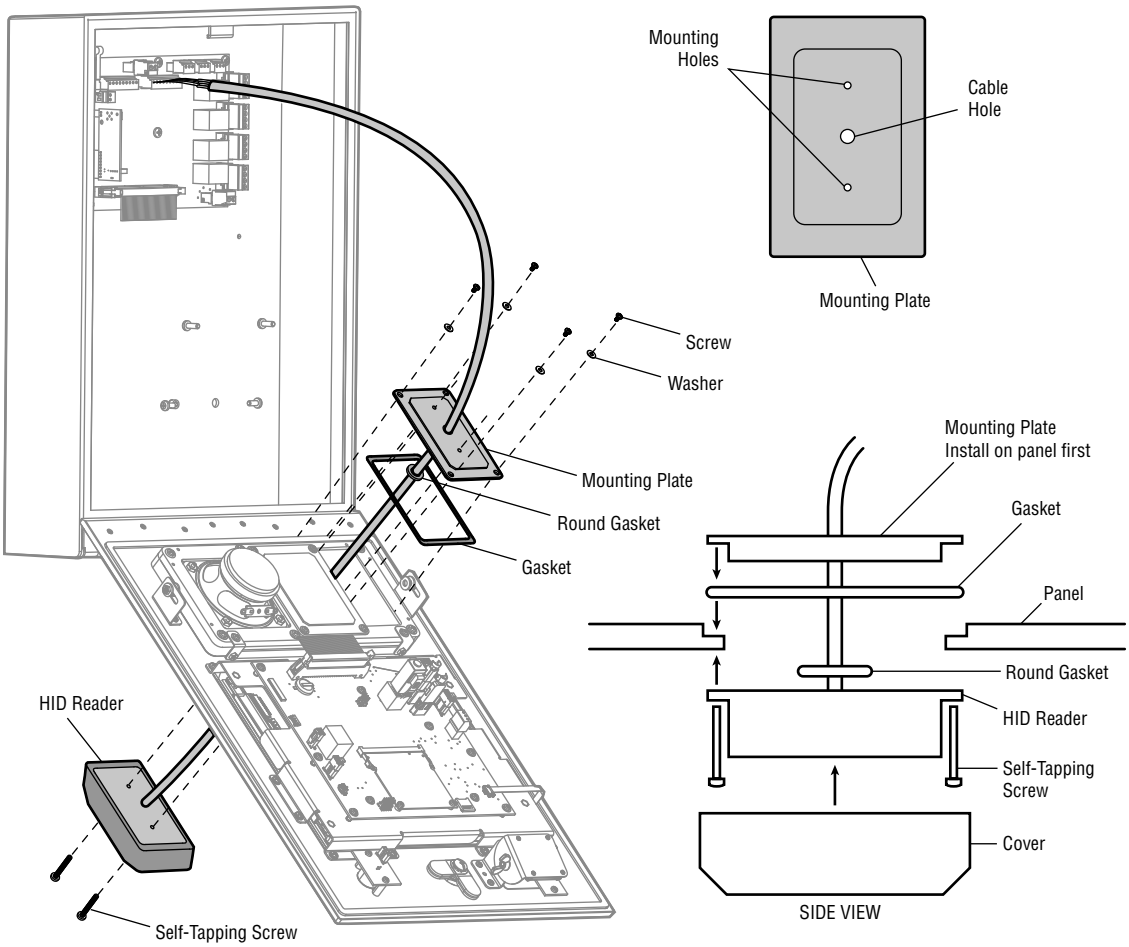
Wiegand Card Reader (optional accessory)

The unit is designed specifically for the model SN7000178 card reader to be mounted on the faceplate.

1. Remove the reader mounting plate from the unit (4 screws and 4 washers).
2. Remove the gasket and save for reinstallation.
3. Use a bench vise with soft jaws to hold the mounting plate.
4. Drill cable hole with a 5/16" drill bit.
5. Drill two outer mounting holes with a 7/64" drill bit.
6. Make the threads using the self-tapping screws provided with the HID reader.

   NOTE: *Thread screw and remove. Clean the mounting hole thoroughly until the entire thread is made.*
7. Remove the screws.
8. Reinstall the gasket and mounting plate onto unit.
9. Use a round gasket (provided) and position it around the center cable hole.
10. Install reader and secure with the two screws.
11. Break the screws at the inside using pliers (hold and rock back and forth until it breaks). Add silicon.

See page 36 for proper wiring instructions.

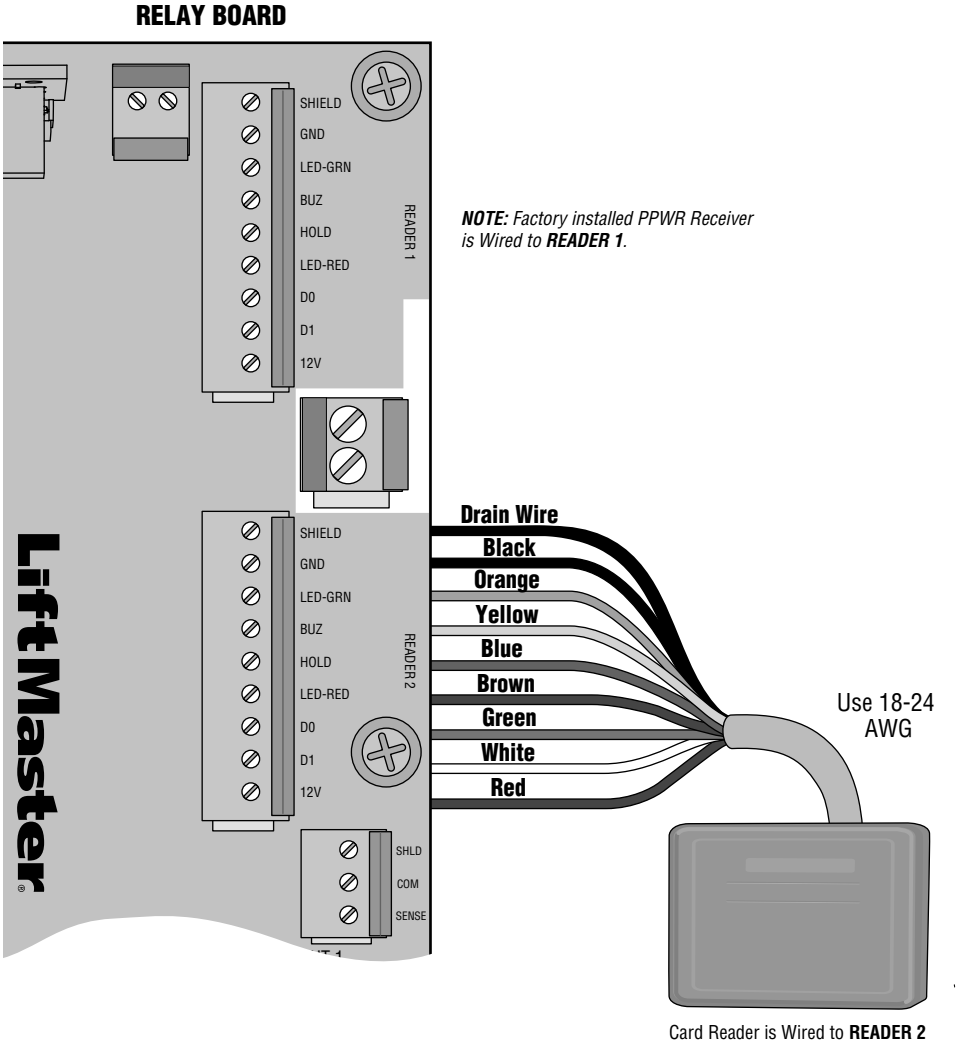


Wire Wiegand Card Reader/Keypad

Connect the Wiegand device to READER input 2. Insulate any unused wires from the unit to prevent a short. (Refer to instructions supplied with your Wiegand device for more information.)

Example of Wiring

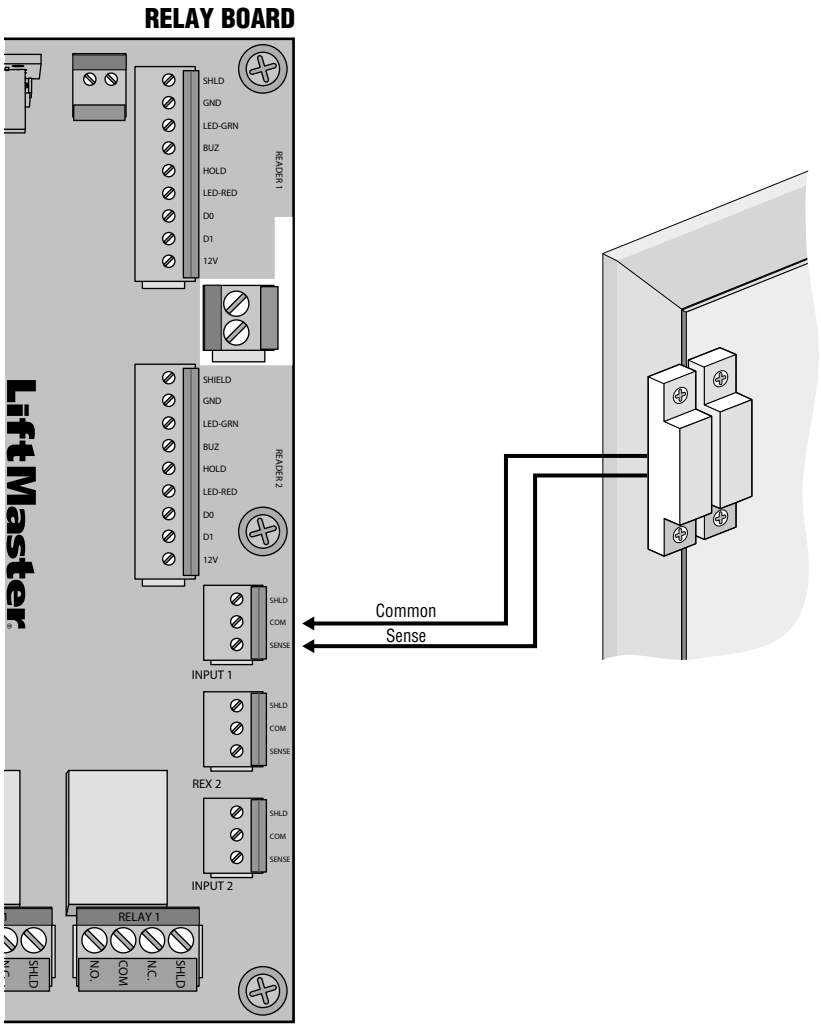
WIEGAND	RELAY BOARD
Shield	SHLD
Black	GND
Orange	LED-GRN
Yellow	BUZ
Blue	HOLD
Brown	LED-RED
Green	D0
White	D1
Red	12V
Purple	Not Used



NOTE: *Factory installed PPWR Receiver is Wired to* ***READER 1***.

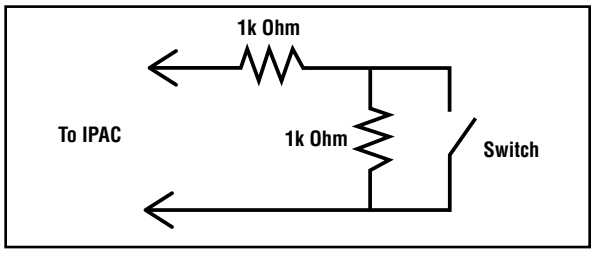
Wire Door Sensor

Connect the door sensor to INPUT 1 or 2.



Optional Door Sensor Wiring

The unit supports supervised inputs. A network of 1k Ohm (10% tolerance) resistors wired at point of contact switch can be used in conjunction with the software EOL (End of Line) configuration. See page 22 for software configuration.



Regular Maintenance Service Kits

ITEM	PART NUMBER
IPAC Hardware Parts Kit:	**IPACHWK**
Box mount gasket sheet	
HID insert with gasket, fasteners	
Key lock with cam, 2 keys, hardware	
Camera bracket, fasteners	
Lanyard, brackets and fasteners	

ITEM	PART NUMBER
IPAC Electric Parts Kit:	**IPACELK**
Tamper switch, cable fasteners	
Transformer	
Ribbon cable	

Repair Parts

ITEM	PART NUMBER
NOTE: PERFORMING FIELD REPAIRS WITH ANY OF THE FOLLOWING PARTS VOIDS ANY OUTSTANDING WARRANTY.	
Touchscreen Kit	IPACTSK
IPAC LCD frame with interconnect kit	IPACLCDK
IPAC peripheral PCB kit	IPACPCBK
IPAC relay/IO board kit	IPACIOK
IPAC microphone board kit	IPACMBK
IPAC light sensor and camera window kit	IPACLSBK
IPAC speaker kit	IPACSK
IPAC LED frontlight kit	IPACLEDK
IPAC hinge kit	IPACHK

Accessories

ITEM	PART NUMBER
IPAC Paintable Faceplate + Shroud Kit	IPACTRK
IPAC Retrofit Trim Ring	IPACRTR
IPAC Keypad	IPACKEY
IPAC Postal Lock Box	IPACPLB
HID ProxPoint Plus Mini Card Reader	SN7000178
IPAC Panel Camera kit	IPACCAMK
Raw Camera	002B0896
Transformer	023B0587
Passport 3-Button Visor Remote Control MAX	PPV3M
Passport 3-Button Mini Remote Control MAX	PPK3M
Passport 3-Button Mini Proximity Remote Control MAX	PPK3PHM
Passport Lite 1-Button Visor Remote	PPLV1-X*
Passport Lite 1-Button Key Chain Remote	PPLK1-X*
Passport Lite 1-Button Mini Proximity Remote	PPLK1PH-X*

* Available in 10 and 100 packs, replace X with 10 or 100

Configuration Sheet

Record device information and configuration settings below.

HARDWARE

DOOR BOARD	End Of Line Resistors Yes or No	Default State Normally Open or Normally Closed
REX 1		
INPUT 1		
REX 2		
INPUT 2		
Notes:		

DEVICE CONFIGURATION

DEVICE	DOOR NAME:			
WIEGAND	Reader 1			
INPUT	REX 1	INPUT 1		
OUTPUTS	Relay 1		Aux 1	
	N.O.	N.C.	N.O.	N.C.
	Notes:			

DEVICE	DOOR NAME:			
WIEGAND	Reader 2			
INPUT	REX 2	INPUT 2		
OUTPUTS	Relay 2		Aux 2	
	N.O.	N.C.	N.O.	N.C.
	Notes:			

UNIT:
Login:
Password:
NOTE: *Any user of the system is subject to the terms outlined in the product EULA.*
Notes:

Legal Disclaimers

Federal Communications Commission (FCC) Compliancy

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 or 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. 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:

- Increase the distance between the equipment and receiver.
- Connect the equipment to a circuit other than the one to which the receiver is connected.
- Consult the dealer for help.

Canada-Underwriters Laboratories (C-UL) Compliancy

For C-UL Listed applications, the unit shall be installed in accordance with Part 1 of the Canadian Electrical Code.

Documentation Disclaimer and Restrictions

Information in this document is subject to change without notice and does not represent a commitment on the part of LiftMaster. For the most up-to-date information, visit www.LiftMaster.com.

This document and the data herein shall not be duplicated, used or disclosed to others for procurement or manufacturing, except as authorized with the written permission of LiftMaster. The information contained within this document or within the product itself is considered the exclusive property of LiftMaster. All information in this document or within the hardware and software product themselves is protected by the copyright and/or other intellectual property laws of the United States.

UL 294 Access Control Unit Level 1

NOTICE: To comply with FCC and/or Industry Canada (IC) rules, adjustment or modifications of this digital device are prohibited. THERE ARE NO USER SERVICEABLE PARTS. Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules and IC License-Exempt RSS Standard(s). Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This Class B digital apparatus complies with Canadian ICES-003.

AVIS : Les règles de la FCC et/ou d'Industrie Canada (IC) interdisent tout ajustement ou toute modification de ce récepteur. IL N'EXISTE AUCUNE PIÈCE SUSCEPTIBLE D'ÊTRE ENTRETENUE PAR L'UTILISATEUR. Tout changement ou toute modification non expressément approuvé par la partie responsable de la conformité peut avoir pour résultat d'annuler l'autorité de l'utilisateur de faire fonctionner l'équipement.

Ce dispositif est conforme à la partie 15 des règles de FCC et des normes Permis-Exemptes d'IC RSS. Son utilisation est assujettie aux deux conditions suivantes : (1) ce dispositif ne peut causer des interférences nuisibles, et (2) ce dispositif doit accepter toute interférence reçue, y compris une interférence pouvant causer un fonctionnement non souhaité.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Limited Warranty

LiftMaster, Inc. (“Seller”) warrants to the first purchaser of this product, for the structure in which this product is originally installed, that it is free from defect in materials and/or workmanship for a period of two years from the date of purchase. The proper operation of this product is dependent on your compliance with the instructions regarding installation, operation, maintenance and testing. Failure to comply strictly with those instructions will void this limited warranty in its entirety.

If, during the limited warranty period, this product appears to contain a defect covered by this limited warranty, call 1-800-528-2806 before dismantling this product in order to obtain authorization and instructions for returning defective product. Products returned to Seller for warranty replacement, which upon receipt by Seller are confirmed to be defective and covered by this limited warranty, will be repaired, replaced with new or factory rebuilt parts, or credited into customer account, at Seller’s sole option. You are responsible for any costs incurred in removing and/or reinstalling the product or any component.

THIS LIMITED WARRANTY IS IN LIEU OF ANY OTHER WARRANTIES, WHETHER ORAL, WRITTEN, STATUTORY, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR OTHERWISE, AND OF ANY OTHER OBLIGATIONS OR LIABILITY ON SELLER’S PART. IN SO FAR AS SUCH WARRANTIES CANNOT BE DISCLAIMED, SELLER LIMITS THE DURATION AND REMEDIES OF SUCH WARRANTIES TO THE DURATION OF THIS LIMITED WARRANTY AND, AT SELLER’S OPTION, THE REPAIR, REPLACEMENT, OR CREDIT INTO CUSTOMER ACCOUNT AS DESCRIBED HEREIN.

THIS LIMITED WARRANTY DOES NOT COVER NON-DEFECT DAMAGE, DAMAGE CAUSED BY IMPROPER INSTALLATION, OPERATION OR CARE (INCLUDING, BUT NOT LIMITED TO ABUSE, MISUSE, FAILURE TO PROVIDE REASONABLE AND NECESSARY MAINTENANCE, UNAUTHORIZED REPAIRS OR ANY ALTERATIONS TO THIS PRODUCT), LABOR CHARGES FOR REINSTALLING A REPLACED UNIT, PROBLEMS RELATED TO INTERFERENCE, OR REPLACEMENT OF BATTERIES.

EXCEPT AS EXPRESSLY PROVIDED IN THIS LIMITED WARRANTY AND TO THE MAXIMUM EXTENT PERMITTED BY LAW, UNDER NO CIRCUMSTANCES SHALL SELLER BE LIABLE FOR DIRECT, CONSEQUENTIAL, INCIDENTAL OR SPECIAL DAMAGES ARISING IN CONNECTION WITH THE USE, OR THE INABILITY TO USE, THIS PRODUCT. IN NO EVENT SHALL SELLER’S LIABILITY, INCLUDING, WITHOUT LIMITATION, LIABILITY FOR BREACH OF WARRANTY, BREACH OF CONTRACT, NEGLIGENCE OR STRICT LIABILITY, EXCEED THE COST OF THE PRODUCT COVERED HEREBY. NO PERSON IS AUTHORIZED TO ASSUME FOR US ANY OTHER LIABILITY IN CONNECTION WITH THE SALE OF THIS PRODUCT OR MODIFY, EXTEND OR ADD TO THIS LIMITED WARRANTY.

Some states and provinces do not allow the exclusion or limitation of consequential, incidental or special damages, so the above limitation or exclusion may not apply to you. This limited warranty gives you specific legal rights, and you may also have other rights which vary from state to state and province to province.