

### **ACU-1**

#### **Overview**

The ACU-1 is a self-contained controller for single door access control. Use the ACU-1 to electrically control passage through a physical barrier such as a door or gate.

The controller monitors contacts and controls actuators via its 2 card reader/keypad interfaces, 4 digital outputs, 4 supervised inputs, and 1 relay output. LED indicators, field wiring terminal blocks, and panel mounting ability are other features of this controller. It functions as part of an Echelon LonWorks® Network using the integral FTT-10 Free Topology communications transceiver.

A Local Database Module (LDM) enables the controller to locally validate access attempts in the case of a loss of network communication.

#### **Features**

- Controls access to one barrier (door or gate)
- Compatible with 26-bit Wiegand card readers
- Interfaces with entry and exit (optional) card readers
- Local storage of card database in case of network failure
- Battery backup of local memory
- On-board relay used to control door strike
- Free access set by schedule or manual override
- Door Propped and Door Forced detection
- Two supervised inputs for additional tamper detection (glass break, etc.)
- Maximum of 500 access cards (system wide)
- Occupancy status tracking to interface with HVAC equipment
- Three door access modes (card only, card + PIN, cipher)
- LONWORKS interface to building automation systems and host products
- Automatic configuration via the LCI
- Alarm/Event reporting

#### **Purpose of This Guide**

The *iWorX ACU-1 Application Manual* provides application information for the ACU-1 Controller.

The reader should understand basic HVAC concepts, intelligent environmental control automation, and basic LONWORKS networking and communications. This Application Manual is written for:

- Users who engineer control logic
- Users who set up hardware configuration
- Users who change hardware or control logic
- Technicians and field engineers



Innovex Technologies  
511 Braddock Avenue  
Turtle Creek, PA 15145  
[www.innovextechnologies.com](http://www.innovextechnologies.com)

iWorX is a trademark of Innovex Technologies  
LON, LONWORKS, & LONMARK are trademarks of Echelon Corporation

## Copyright Notice

This document copyright © 2006, Innovex Technologies. All other intellectual property rights and copyrights related to or arising from these products belong to a third party.

The confidential information contained in this document is provided solely for use by Innovex Technologies employees, licensees, and system owners, and is not to be released to, or reproduced for, anyone else. Neither is it to be used for reproduction of this control system or any of its components.

All specifications are nominal and may change as design improvements occur. Innovex Technologies shall not be liable for damages resulting from misapplication or misuse of its products.

## Applicable Documentation

Part Number	Description	Audience	Purpose
iWorX-ACU-INS-100	iWorX ACU-1 Application Manual	<ul style="list-style-type: none"> <li>– Application Engineers</li> <li>– Installers</li> <li>– Service Personnel</li> <li>– Start-up Technicians</li> </ul>	Provides instructions for setting up and using the iWorX ACU-1 Controller.
iWorX-LCI1-USR-100	iWorX LCI User's Guide	<ul style="list-style-type: none"> <li>– Application Engineers</li> <li>– Installers</li> <li>– Service Personnel</li> <li>– Start-up Technicians</li> <li>– End user</li> </ul>	Provides instructions for setting up and using the iWorX Local Control Interface.
Additional Documentation	<i>LonWorks FTT-10A Free Topology Transceiver User's Guide</i> , published by Echelon Corporation. It provides specifications and user instructions for the FTT-10A Free Topology Transceiver.		

## Application Description

### Overview

The controller monitors and controls access to a single entry barrier through the use of an entrance card reader. An exit card reader may also be used to monitor and control exit access. Supervised inputs are provided for tamper detection.

Entrance (required) and exit (optional) card readers may be used to control door access. The controller supports card readers that use 26-bit Wiegand encoding. Up to 500 access cards are supported system-wide.

An LCI must be used to configure all of the controller's access parameters. You can download a database of cards to the LCI or add the cards by putting the controller into auto-add mode and presenting cards to the reader. A local database of card information provides secure access in case the network communication is lost. The memory containing the local database is maintained by a backup battery.

One input is dedicated to monitoring the door status, and one is dedicated to monitoring the exit request pushbutton. Two non-dedicated supervised inputs can be used for monitoring other tamper devices such as a glass break detector or a motion sensor.

Digital outputs are provided to control card reader indicators such as LEDs and audible sounders. 5 VDC outputs are provided to power the card readers. If the readers that are used require a different voltage, they must be powered with a separate supply. A relay output is provided to control a barrier locking device such as a door strike or magnetic lock. Both normally open and normally closed contacts are provided to accommodate devices that lock when power is applied or devices that lock when powered off.

Alarms are generated when the controller detects that a door has been propped or when a door has been forced. Alarms are also generated if the two spare supervised inputs have been tampered with.

## Sequence of Operation

### Door Access Modes

A door can be set to allow free access or to require a card, card + PIN, or cipher code for access. Use a schedule to set different access modes for the ON and OFF periods of the schedule. Set the door access mode manually, and it will remain in that mode until you change it or return it to automatic mode.

Use a separate schedule to set a door to allow free access during certain times of the day. The door will allow free access during the ON part of the specified schedule, and will resort to the access mode specified by its normal schedule for the OFF part of the free access schedule. Manually placing a door in or out of free access mode is also supported. Use the LCI to set these parameters for each ACU-1.

### Door Groups

A Door Group defines whether access is permitted or denied to particular doors for the cards in that door group. Define up to 16 different door groups. Door groups can also use schedules to specify when cards are allowed access.

As an example, one door group may be set up to allow engineers access to the building entry doors and the engineering labs. Another door group may be set up for human resources employees that only allows access to the building entry doors.

When defining a door group, all doors in the system are denied access by default. Change the access to permitted for the appropriate doors in this door group.

When deleting a door group, do not delete a door group that is currently being used by some cards. Doing so will remove that door group limitation from those cards, and those cards will be permitted access to all doors.

### Cards

An iWorX system may have a maximum of 500 access cards in its database (kept in the LCI). Add cards to the system through an LCI, or through the LCI's SCS software. To use the LCI, put an ACU-1 in auto add mode, and specify whether the normal access mode will be card only or card + PIN. When the ACU-1 is in auto add mode, present cards to the reader. If you selected card + PIN as the normal access mode, you will need to enter a 4 digit PIN for each card after you present it to the reader. This PIN will be valid system wide at any permitted ACU-1 that requires a PIN, and can be changed at a later date from the LCI. If a door in the system has an exit reader, and the access mode for the door is card + PIN, occupants must use the PIN when exiting the door as well as entering it.

Specifying a door group for a card defines the doors that are accessible by that card. If you designate a default door group on the LCI, all cards will be assigned to that door group when they are added. After the card is added, change a card's door group using the LCI.



You must be sure to take the LCI out of auto-add mode after you are finished adding all cards. Otherwise, any card that is presented to the reader will be added to the database instead of checked to see if access should be granted.

Use the LCI to view the following card attributes:

- Name
- PIN
- Door Group
- Card Number,
- Last Time Used
- Last Door Used

Use the LCI to change the Name, PIN, and door group for a card after it is added to the system. You can also use the LCI to delete cards from the system.

## Local Card Database

The controller keeps a local database of all cards that are permitted access to its door. This enables the door to provide appropriate access even if the ACU-1 loses its network connection. When a card is added to the system through an LCI, it is also added to the local database of the ACU-1 that was used to add the card. When a card is added to the system through the System Configuration Software (SCS) utility, it is automatically added to the local database on the proper ACU-1s.

After a card is added to the system, when it is presented to a reader and granted access to that door by the LCI, it will be added to the local database of that door's ACU-1. If a card is presented to a reader and denied access by the LCI, it will be deleted from that ACU-1's local database if it was previously included.

## Ciphers

An ACU-1 can be set to allow the use of cipher codes rather than cards to grant access. Use the LCI to set up to four 4-digit cipher codes that can be used at any ACU-1 in the system that is in cipher mode. Cipher access can be limited to certain times of the day through the use of schedules.

## Alarms and Events

The controller will detect certain alarm conditions and send them to the LCI. Before this can occur, you must use the LCI to configure the controller.

### Controller Identification

You need to press the controller's service pin to allow the LCI to identify it. The controller must be configured by the LCI to allow you to use the LCI to set the controller's network variables. You need to press the service pin after the controller is installed and the LCI is active on the network.

### Supervised Input Alarms

The controller monitors the status of the supervised inputs and generates alarms for the following events:

- Detection of a Door Propped condition (Door Propped alarm)
- Detection of a Door Forced condition (Door Forced alarm)
- Detection of general supervised input tampering (Input #3 Tamper, Input #4 Tamper)

## Troubleshooting

### Diagnostic LEDs

The base board contains 7 LED indicators designated DS1 through DS4, and DS6 through DS8. These indicators can aid in troubleshooting problems with equipment operation. Note that the indicators are designated from left to right, DS7, DS4, DS6, DS1, DS2 DS3, and DS8.

**Table 1: Diagnostic LEDs**

LED	Indication
DS1 (green)	Illuminated while 5VDC power is present on the base board
DS2 (yellow)	Illuminated while a signal is detected from the FTT-10A network (receive data)
DS3 (yellow)	Illuminated while the controller is transmitting data onto the FTT-10A network (transmit data).
DS4 (yellow)	Illuminates briefly when the controller receives a LonTalk "wink" message from a device on the FTT-10A network
DS6 (red)	Illuminated while Relay 2 is on
DS7 (yellow)	Illuminates briefly when the controller sends a LonTalk "service pin" message. The controller sends a service pin message when momentary switch SW2 on the base board is pressed
DS8 (yellow)	Illuminates briefly when the microprocessor is reset. The microprocessor can be reset by pressing momentary switch SW1 on the base board



Resetting the controller will cause it to unlatch any active outputs. These outputs will return to their appropriate state once the controller completes its reset sequence.

## Troubleshooting Tips

### **Controller is not running and DS1 LED is not illuminated.**

No power to controller. Verify the voltage on the controller's power connector.

### **How do I reset the controller?**

The controller can be reset by the LCI, or you can depress the reset button on the ACU-1 base module. Refer to the LCI documentation for more information on resetting the controller using the LCI.

### **The door strike relay will not come on.**

Ensure that the relay has been wired correctly.

### **When a valid card is swiped, access is not granted.**

Verify the following at the LCI:

1. Is the card permitted at this door?
2. Is this still a valid card?

### **Every card swiped is granted to the door, even cards that have never been added to the system.**

The ACU-1 is in Auto Add Card mode. Change the Auto Add feature to "No".

### **An externally powered card reader is wired correctly but not working properly.**

Be sure that your external power supply common is tied to the common (-) on the card reader terminal block of the ACU-1.

## Network and Configuration Variables

This section describes all of the Network and Configuration Variables used in the controller.

**Table 2: ACU-1 Inputs**

LCI Variable Name	Range	Default Value	Description
Door Relay	On/Off	Off	Turns door strike on/off
Open Door	On/Off	Off	Opens the door as if the exit pushbutton was activated

The following output variables are read only and cannot be changed.

**Table 3: ACU-1 Outputs**

LCI Variable Name	Range	Description
Exit Button	On/Off	Shows state of exit pushbutton input
Door Monitor	On/Off	Shows state of door monitor input
Door Relay	On/Off	Shows state of door relay
Door Forced	On/Off	Shows On if door forced condition occurred
Door Propped	On/Off	Shows On if door propped condition occurred

The following are configuration variables.

**Table 4: ACU-1 Configuration Variables**

LCI Variable Name	Range	Default Value	Description
Access Time	0-255 seconds	10 seconds	Time that the door relay output remains in the unlocked state after access is granted. The door relay is switched to the locked state after this time expires, or the door has been detected to have been opened.
Shunt Time	0-255 seconds	10 seconds	Time after the door is opened until a Door Propped alarm is generated if the door is not detected as having been closed
Unlock Time	0-255 seconds	10 seconds	Amount of time that the locking control output remains on after access is granted and the door is opened.