Iris ID

IrisAccess® SoHo User Manual

Ver 1.04.04

June 2010

IrisAccess® SoHo User Manual

Iris ID Systems, Inc. 7 Clarke Drive, Cranbury, New Jersey 08512, USA.

Document Number: IRISIDSOHO-01-0104-0610

Table of Contents

1. Introduction

Since 1997, Iris ID has been the key developer and driver of the commercialization of iris recognition technology. IrisAccess, now in a third generation, is the world's leading deployed iris recognition platform. Found on 6 continents, in thousands of locations, authenticating the identities of millions and millions of persons, more people in more places authenticate with IrisAccess than with all other iris recognition products combined. Through our expertise and Iris ID Advanced Identity Authentication, Iris ID helps add security, convenience, privacy, and productivity to the enterprise operation you wish to improve.

Traditional Notions of Establishing Identity

Historically, identity or authentication conventions were based on things one possessed (a key, a passport, or identity credential), or something one knew (a password, the answer to a question, or a PIN.) This possession or knowledge was generally all that was required to confirm identity or confer privileges. However, these conventions could be compromised - as possession of a token or the requisite knowledge by the wrong individual could, and still does, lead to security breaches.

Biometric Appeal of Iris Recognition

Of all the biometric technologies used for human authentication today, it is generally conceded that iris recognition is the most accurate. Coupling this high confidence authentication with factors like outlier group size, speed, usage/human factors, platform versatility and flexibility for use in identification or verification modes - as well as addressing issues like database size/management and privacy concerns - iris recognition has also shown to be exceedingly versatile and suited for large population applications.

Benefits:

1. The smallest outlier population of all biometrics. Few people can't use the technology, as most individuals have at least one eye. In a few instances even blind persons have used iris recognition successfully, as the technology is iris pattern-dependent, not sight dependent.

2. Iris pattern and structure exhibit long-term stability. Structural formation in the human iris is fixed from about one year in age and remains constant (barring trauma, certain rare diseases, or possible change from special some ophthalmologic surgical procedures) over time. So, once a individual is enrolled, re-enrollment requirements are infrequent. With other biometric technologies, changes in voice timbre, weight, hairstyle, finger or hand size, cuts or even the effect of manual labor can trigger the need for re-enrollment.

3. Ideal for Handling Large Databases. Iris recognition is the only biometric authentication technology designed to work in the 1-n or exhaustive search mode. This makes it ideal for handling applications requiring management of large user groups, such as a National Documentation application might require. Large databases are accommodated without degradation in authentication accuracy. IrisAccess® platforms integrate well with large database back ends like Microsoft SQL and Oracle 9i.

4. Unmatched Search Speed in the one to many search mode is unmatched by any other technology, and is limited not by database size, but by hardware selected for server management. In a UK Government-commissioned study, Iris ID's IrisAccess® platform searched records nearly 20 times faster than the next

fastest technology. Iris ID has developed a high speed matching engine, IrisAccelerator™, designed to deliver 10 million+ matches per second.

5. Versatile for the One to Many, One to One, Wiegand and Token Environments. While initially designed to work in one-to-many search mode, iris recognition works well in 1-1 matching, or verification mode, making the technology ideal for use in multifactor authentication environments where PINs, or tokens like prox or smartcards are used. In a token environment, many privacy issues related to biometric database management are moot, as the user retains control of biometric data – a small template of 512 bytes per iris.

6. Safety and Security Measures In Place. Iris recognition involves nothing more than taking a digital picture of the iris pattern (from video), and recreating an encrypted digital template of that pattern. 512-byte iris templates are encrypted and cannot be re-engineered or reconstituted to produce any sort of visual image. Iris recognition therefore affords high level defense against identity theft, a rapidly growing crime. The imaging process involves no lasers or bright lights and authentication is essentially non-contact.

7. Convenient, Intuitive User Interface. Using the technology is an almost intuitive experience, requiring relatively little cooperation from subjects. Proximity sensors activate the equipment, which incorporates mirror-assisted alignment functionality. Audio auto-positioning prompts, automated image capture, and visual and audio authentication decision-cueing completes the process.

1.1 Product Overview

iData SoHo, an acronym created by Iris ID that stands for Small-Office-Home-Office has been designed specifically to address the needs of that clientele. This IrisAccess®SoHo product is also designed to fit in residential buildings and home locations that demand the very best and most technologically advanced access control based security offerings available.

What is the IrisAccess® SoHo? Iris ID's IrisAccess®SoHo is a packaged product that provides a solution to IRIS recognition equipment in a small, easy to setup, expandable, and manageable product suite. The included Touch screen Panel PC, pre-installed iData SoHo software and iCAM4000 Camera Unit can be used for the purposes of Door Access Control, time and attendance, identification verification and privacy control. Capable of integrating with almost any environment, SoHo has been optimized to function with all the power of similar devices in the Iris ID IRIS platform, but with a simplified setup, smaller size and customizable expansion that lends itself to ultimate convenience for the user.

1.2 Purpose and Audience for this Guide

Read this document before attempting to install, configure, expand, run, or modify the product that has been provided from Iris ID Electronics.

This Guide is intended to be used as a reference for the SoHo product and its accessories. This document includes detailed background on the product technology, setup instruction, iCAM4000 Hardware and software configurations, Panel PC setup, Enrollment processes, additional recommended accessories, Troubleshooting-frequently asked questions, as well as a multitude of configuration options to assist in setup and expansion of this device. It is the most complete reference available once you setup and begin using your IrisAccess® SoHo system.

Much of this guide provides detailed and specific information that was catered for reading by professional installers, access control specialists such as lock-smiths and Alarm System companies. A general level of access control knowledge is recommended when referencing this guide, as well as installing the Iris ID iData SoHo products.

1.3 Reference Materials

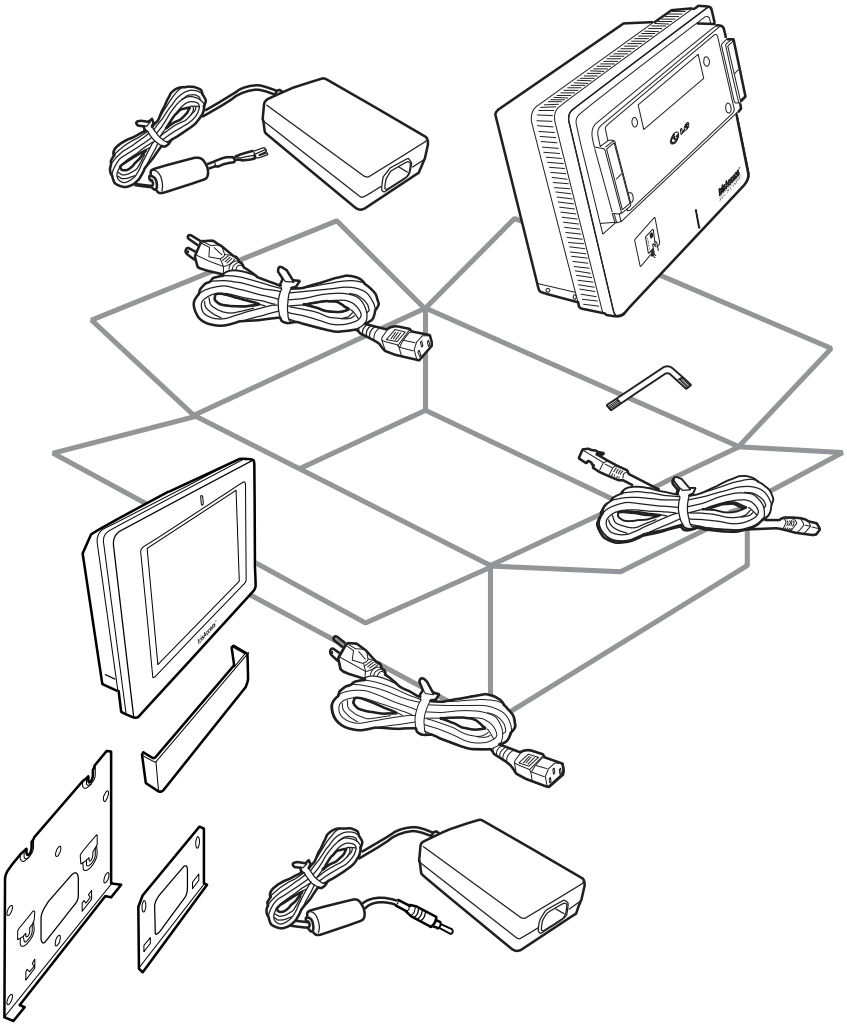
In addition to this guide, your box should contain a "Read Me first – Quick Start Guide" designed to streamline the initial setup of your SoHo product.

Also included with your iCAM4000 is an "iCAM4000 SoHo Hardware Manual". This manual was written to provide specific information on the iCAM4000 camera unit hardware.

** Note: Additional reference, amendments and updated documentation material may become available directly from the http://www.lgiris.com website. Check the site for updated information, frequently asked questions, and tips to be used with your product.*

2. What's In The Box

The IrisAccess® SoHo package should contain the following items



- iCAM4000
- iCAM4000 Power Supply & Power Cord
- iCAM Security Wrench
- Panel PC
- Panel PC Power Supply
- Panel PC Mount
- Documentation CD
- License Key for SoHo (on documentation CD)

** Note: In the event that an item is missing, contact your vendor or Iris ID Electronics U.S.A immediately before continuing any installation.*

Required Equipment (not included)

- Philips Screw Driver
- Ethernet Switch (Ethernet hub is not acceptable)
- Ethernet Wiring (Straight through or cross-over cable)
- Uninterruptible Power Supply
- IBM Compatible PC (for use with initial setup and when using back-office WebAccess administration)

Minimum Computer requirements (for Initial Setup)

- Windows 2000, XP Pro, Server 2003, Vista or Window 7 Operating System
- CD-ROM for software installation
- Ethernet Port (100 Mbps recommended)
- Mouse, SVGA Monitor, Keyboard
- Internet Browser (such as Internet Explorer)

2.1 The iData SoHo Software and Panel PC

About the Software

The iData SoHo software bundled and pre-loaded with your Panel PC is designed to operate using the iCAM4000 series hardware. The iData SoHo which stands for Small Office, Home Office, is an intuitive Iris recognition user interface based system designed to configure the system, manage the user database, monitor system and users activities, and enrolls users. iData SoHo software has been created exclusively for your Panel PC to act as the central HUB of your system. This software is pre-installed with your Panel PC.

** Note: As Firmware and or patch updates to the Panel PC's iData software become available, additional updates to the software may be recommended or required by Iris ID IRIS.*

About the Panel PC

The IrisAccess Panel PC bundled with your purchase is a 7 inch Touch-panel Personal Computer that acts as the enrollment, Manager, and Control Monitor of the system. The system is designed to run off of one Panel PC (or stand-alone computer) without the need for additional computer stations after initial setup has been performed.

Directly from Iris ID, the IrisAccess SoHo Suite in its basic form will provide one iCAM4000 Camera based unit. At least one iCAM4000 is required to operate the system correctly (which has been provided with the IrisAccess SoHo). Additionally, the iData SoHo packaged suite is an expandable system that when configured, the Panel PC is designed to work with up to four iCAM4000 units. (Additional iCAM4000 units sold separately).

Technical Specifications of Panel PC

- Screen Size: 7 inch 16x9 touch screen display
- Resolution: 800x480
- Processor: 1.6 Atom

- Memory: 1GB RAM
- Storage: 2GB Compact Flash Memory Card
- Bus Controllers: USB ports (Two)
- Ethernet port(s): Two Network Interface port input connections (one -active, and one disabled)
- Serial Connection: RS-232 input
- Power: External12V DC in
- External Power cable (included)

Recommended Additional Items

This product does not substitute for an alarm system. Rather, SoHo can be used with an active monitored or passive alarm to achieve additional and added protection. To achieve maximum security benefits from SoHo, it is required that the use of third party equipment be incorporated.

Your Iris ID SoHo product is capable of working with an external card reader for bypass and other door entry access products readily available from 3rd party vendors. Because of this, it is highly recommended that the IrisAccess product be used in conjunction with some of the below items to maximize the effectiveness of access security in a controlled access entry environment.

** Note: The IrisAccess SoHo Suite conforms to generally recognized industry standards and will work with Wiegand based product with GPI/GPO connection configurations available through the iCAM4000.*

- Secure tamper "Latch"
- Access Control Panel
- MAG (magnetic) Lock
- Door Strike
- Egress button, REX switch, motion sensor, or pressure sensor

3. Preparing for Installation

When setting up the IrisAccess SoHo system, configuration of the iCAM4000 Camera unit must be performed first. In order to configure your iCAM4000 the use of a stand-alone computer (not included) is required. Make sure to have an available PC based computer with an installed RJ-45 based Ethernet adapter card, Internet browser, CAT-5 cable, and Network Switch.

** Note: In the event that a network switch is unavailable, the use of a standard Cross-over CAT-5 cable can be used when connecting only 2 devices together. (i.e.: With a PC and 1 iCAM connected together, a crossover cable can be used)*

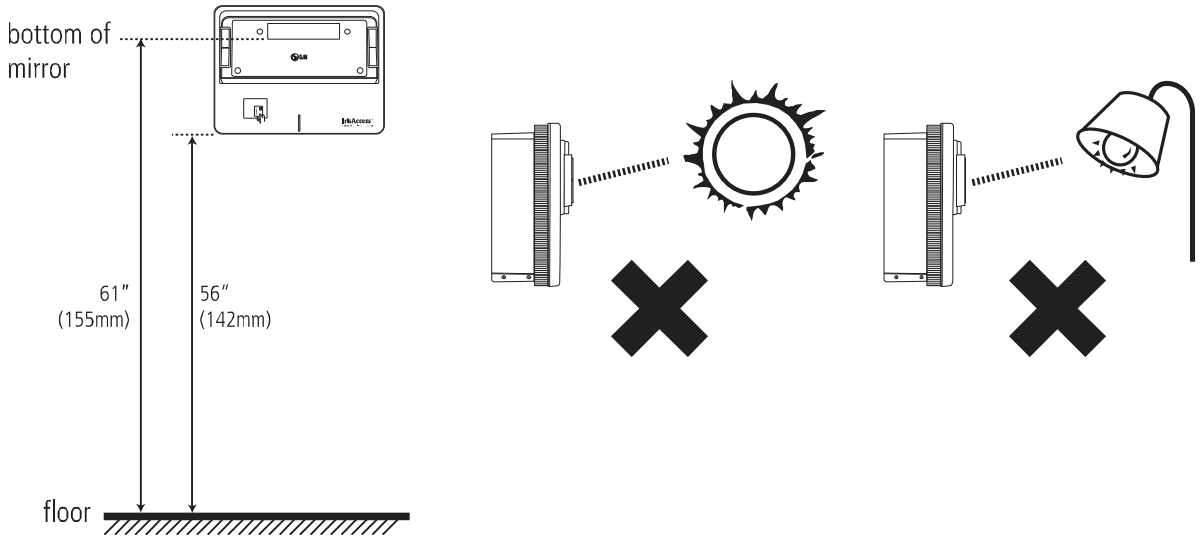
IMPORTANT: REMOVE ITEM CONTENTS FROM PACKAGING. VERIFY ALL EQUIPMENT HAS BEEN INCLUDED WITH YOUR PURCHASE.

3.1 IrisAccess SoHo Installation

This section will take you through the complete installation of your IrisAccess SoHo Product.

Additionally, it is recommended that if possible, more than one person perform the setup installation of the IrisAccess SoHo system. Although much of these processes can be completed without an assistant, you may find that installation will be performed quicker with two individuals.

3.2 Installation Requirements of the iCAM



- The recommended mounting height for the iCAM4000 is 142cm (56 inches) from the floor to the bottom of the unit. This mounting height can be adjusted to accommodate the height of the average user at the installed location.

- High amounts of ambient light must be avoided. Intense light sources such as sunlight or halogen lamps may reduce the image capture performance of the iCAM, this may result in an increased "failure to acquire" rate.
- The iCAM is not weatherproof and must not be exposed to precipitation or extreme temperatures. An enclosure may be used to protect the unit if required. See www.lgiris.com – Support & Service for more information.
- All system components including the Ethernet network must be powered through Uninterruptible Power Supplies (UPS). UPS must provide power line filtering as well as power back-up operation.
- Each IrisAccess™ system component on the Ethernet network system must have a unique manually assigned IP address.

IMPORTANT: IT IS RECOMMENDED THAT THE IRISACCESS SYSTEM BE PLACED ON A PRIVATE NETWORK SEPARATE FROM GENERAL CORPORATE OR PUBLIC ACCESS. SYSTEM PERFORMANCE AND STABILITY MAY BE AFFECTED DEPENDING ON AMOUNT OF GENERAL NETWORK TRAFFIC.

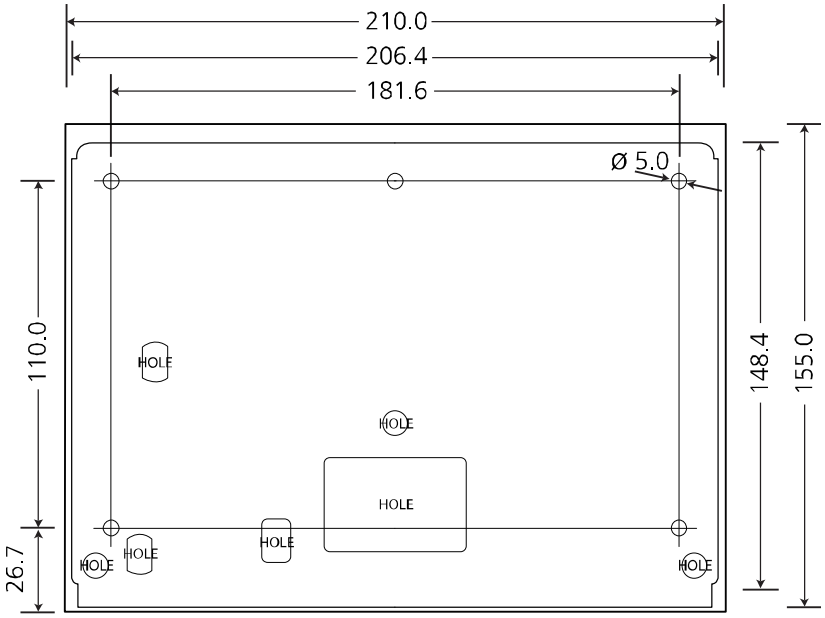
The iCAM4000 requires at least the following wires:

- Ethernet network wiring to connect with the network switch to communicate to IrisAccess Panel PC
- Power (12VDC +/-10% and 2.5Amps MAX)

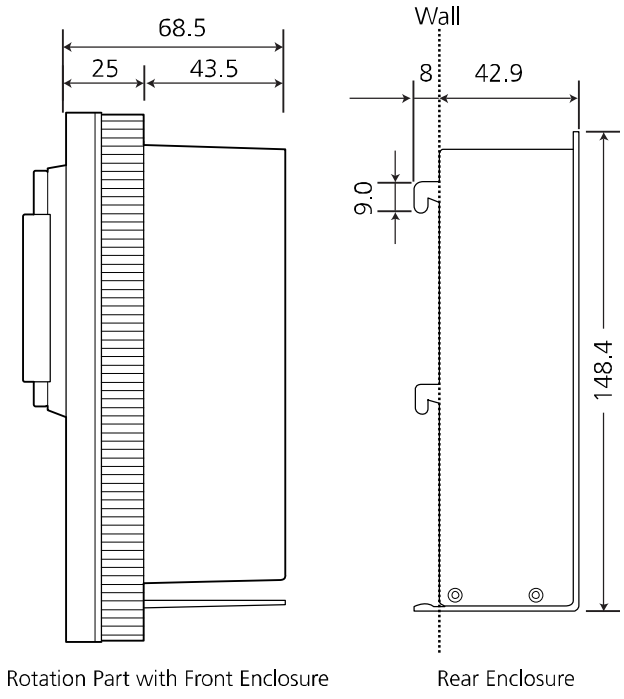
IMPORTANT: IT IS RECOMMENDED TO USE THE POWER ADAPTER SUPPLIED WITH THIS PRODUCT. AN OVER OR UNDER VOLTAGE APPLIED TO THIS PRODUCT MAY CAUSE PERMANENT DAMAGE AND VOID THE WARRANTY

3.3 Getting Started

1. Remove the two security screws (use included security bit wrench) from the bottom of the iCAM.
2. While gently pulling the cover upward on the back plate, pull forward.
3. Position the iCAM back plate on the desired wall near the secured door and mark the holes as the figure below illustrates. The recommended height from the floor to bottom of unit is 142cm (56"), however the installation height can be adjusted depending on average user height.

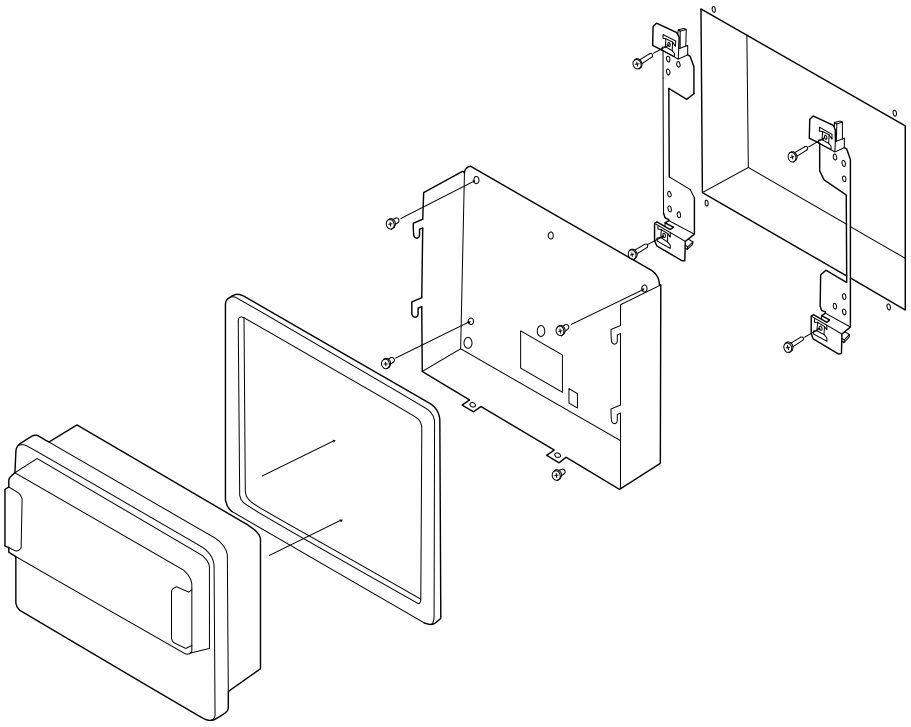


< Dimensions and Screw Holes on the Rear Enclosure (mm unit) >



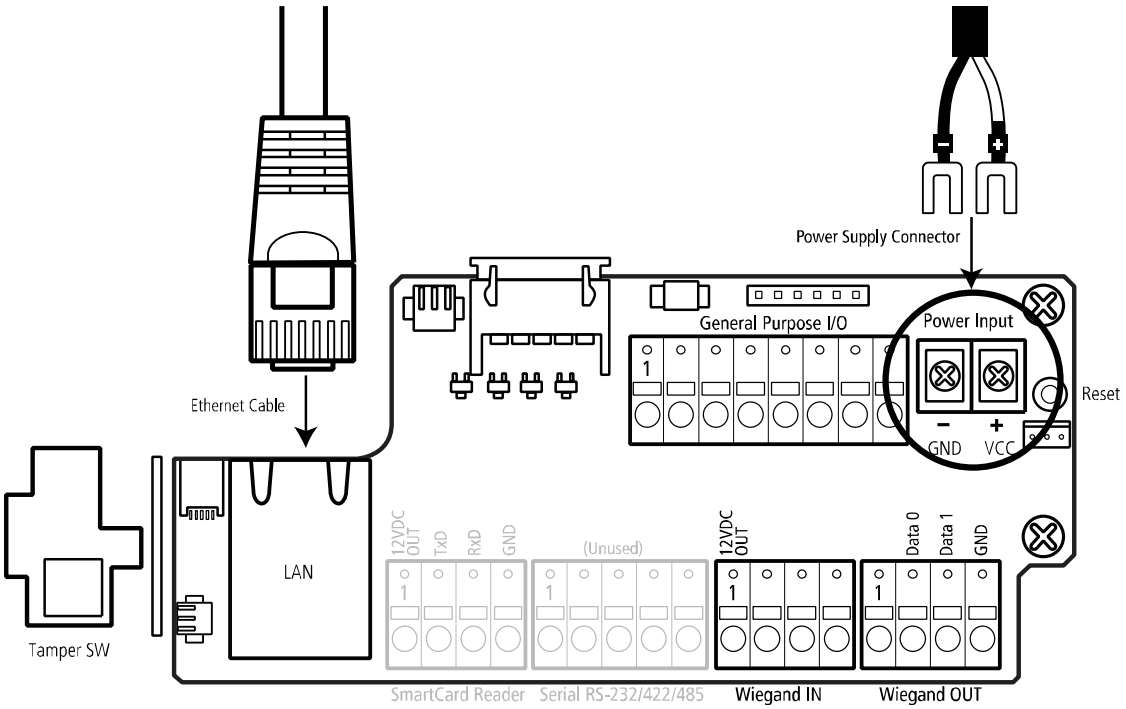
< Dimensions of iCAM4000 (mm unit) >

4. When recessed mounting, leave 6mm (1/4”) of extra space above the marked hole so when mounting the back plate it allows the iCAM to slide down onto the installation plate tabs.



< iCAM Recessed Mounting Diagram >

5. Route the power line, network line, and other necessary cables through the back plate hole.
6. Use the appropriate fasteners for the material in which the iCAM will be mounted, secure the back plate.
7. Attach the wires from the 12VDC power supply to the screw terminal connections. The +12VDC (white wire) power connects to the + (positive) terminal, whereas the 12VDC ground (black wire) connects to the – (negative) terminal.



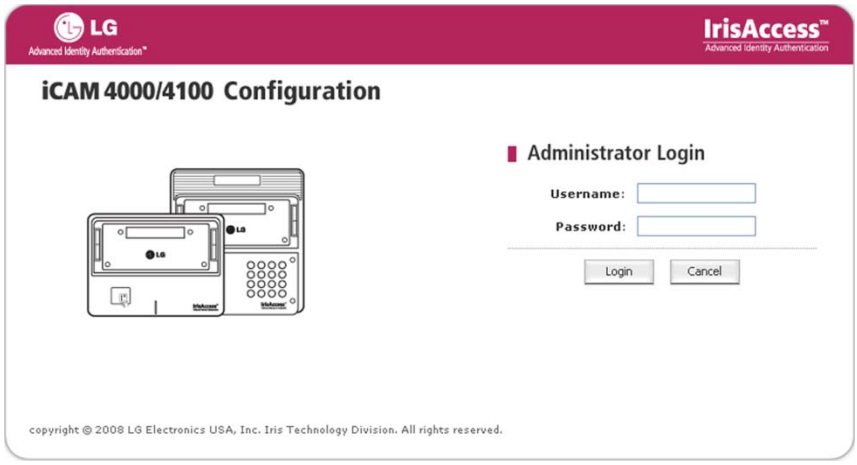
8. Connect the CAT5/RJ45 network wire into the LAN port (CN10) of the iCAM. Make sure that the RJ45 connector locks securely into the LAN port.
9. Wiegand devices such as a card reader may be connected to the iCAM through the Wiegand In connection.
10. Close front cover and gently slide the iCAM downwards over the back plate. Fasten with two security screws on the bottom of the unit.

* Note: The iCAM includes two tamper switches. One switch is located on the rear of the iCAM to detect removal from the wall or enclosure from which it is installed. A second tamper switch is located behind the front plate to detect tampering with the front of the unit. During installation be sure that the rear tamper switch is in a position which can detect unit removal from the wall or enclosure.

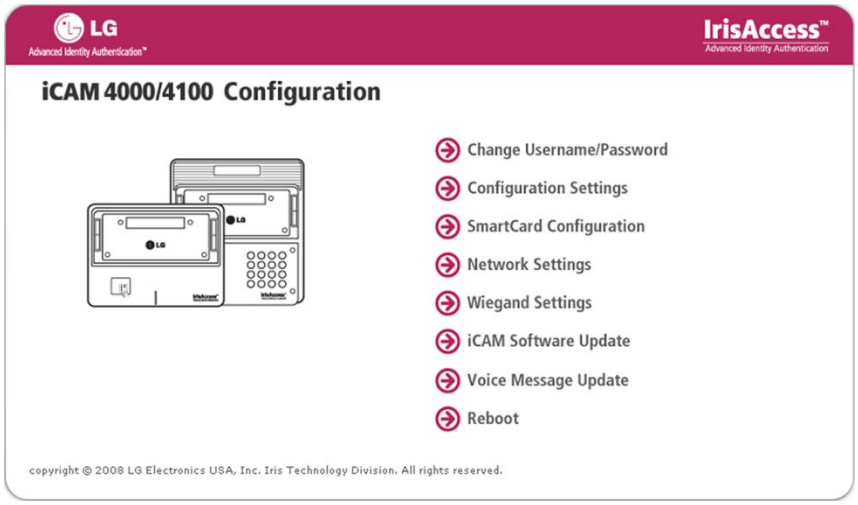
3.4 Configuring the iCAM4000

* Note: The IP Address of each iCAM must be changed individually. Do not connect more than one un-configured iCAM to the network at any one time to avoid IP Address conflicts. Any computer with a web browser which supports graphics (ex. Internet Explorer) can be used to configure the iCAM4000/4100.

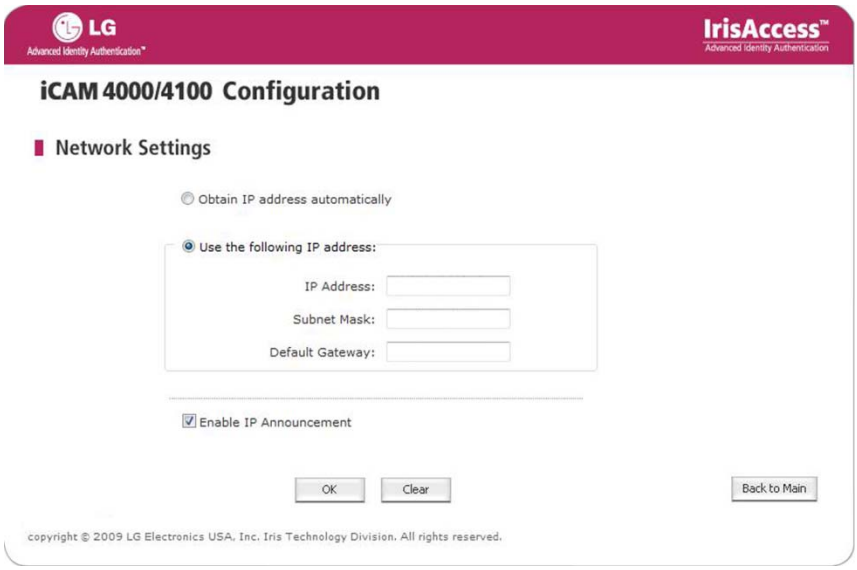
1. Set the computer to the static IP address of 192.168.5.250 - subnet 255.255.255.0
2. Open the web browser and enter http://192.168.5.100 in the address bar then press ENTER. The iCAM login screen will appear.
3. Enter the default Username: iCAM4000 and Password: iris4000 (both are case sensitive).



4. The iCAM Configuration Main Menu will appear.



5. Select Network Settings.



6. Enter the new IP address for the iCAM (default = 192.168.5.100).
7. Enter the new Subnet Mask for the iCAM (default = 255.255.255.0).
8. Enter the new Broadcast Address for the iCAM (default = 192.168.5.255).
9. Enter the new Default Gateway for the iCAM (default = 192.168.5.254).
10. Click OK to save changes and to open network settings verify screen.

** Note: There is a RESET button located on the iCAM4000 interface board. Pressing and holding the RESET button for 3 seconds will reset the iCAM IP Address to the factory default (192.168.5.100).*

- If the new iCAM IP address is still on the same subnet as the computer: after 10 seconds the web browser will resolve to the new IP address and the login screen will appear again.

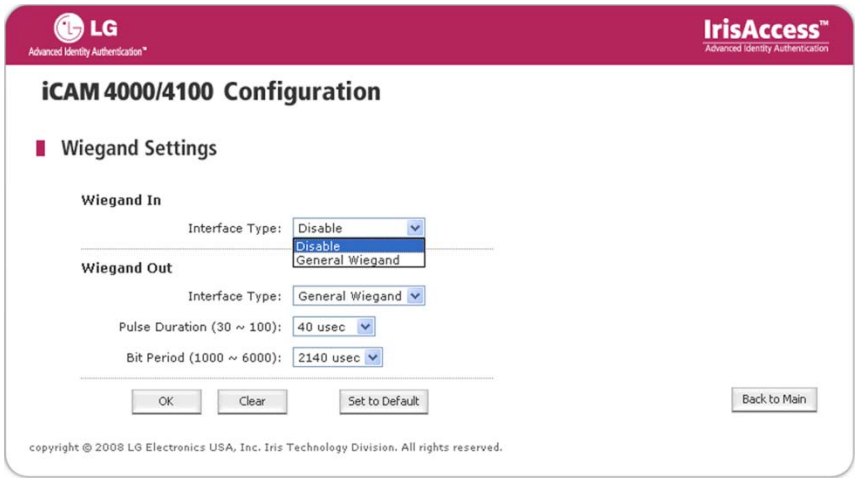
- If the new iCAM IP Address is on a different subnet: the web browser will display the standard "The page cannot be displayed" message.

** Note: Pressing and holding the up tilt button for 10 seconds will cause the iCAM to announce the iCAMs' configured IP Address.*

To test the IP Address change, perform a ping to the new IP Address:

1. Click on Start (in the Windows task bar).
2. Select Run.
3. Type cmd.
4. Press Enter.
5. At the command prompt type: ping <new IP> (ex. ping 192.168.5.120).
6. Close the command prompt window.

Enabling/Disabling of Wiegand IN and OUT from the iCAM:



1. Login to the iCAM4000/4100 configuration screen as shown above (if not already logged in).
2. Select the Wiegand Settings option from the main screen.
3. Select the dropdown box from Wiegand In (as shown above) to either and select Disable to turn off Wiegand input (used for such devices as a card reader), or General Wiegand to Enable the Wiegand Input.
4. Select the dropdown box from the Wiegand Out area on the screen and select Disable to turn off Wiegand output (used for devices such as an Access Control Panel), or General Wiegand to Enable the Wiegand Output.
5. If Wiegand Out is set to be enabled, select the Pulse Duration (30-100 micro-seconds) for purposes of associating the correct time interval which makes up each bit.
6. If Wiegand Out is set to be enabled, select the Bit Period (1000-6000 micro-seconds) for purposes of associating the correct interval between Wiegand bits.

IMPORTANT: BELOW IS LIST OF CARD READER AND ACCESS SYSTEM SETTINGS.

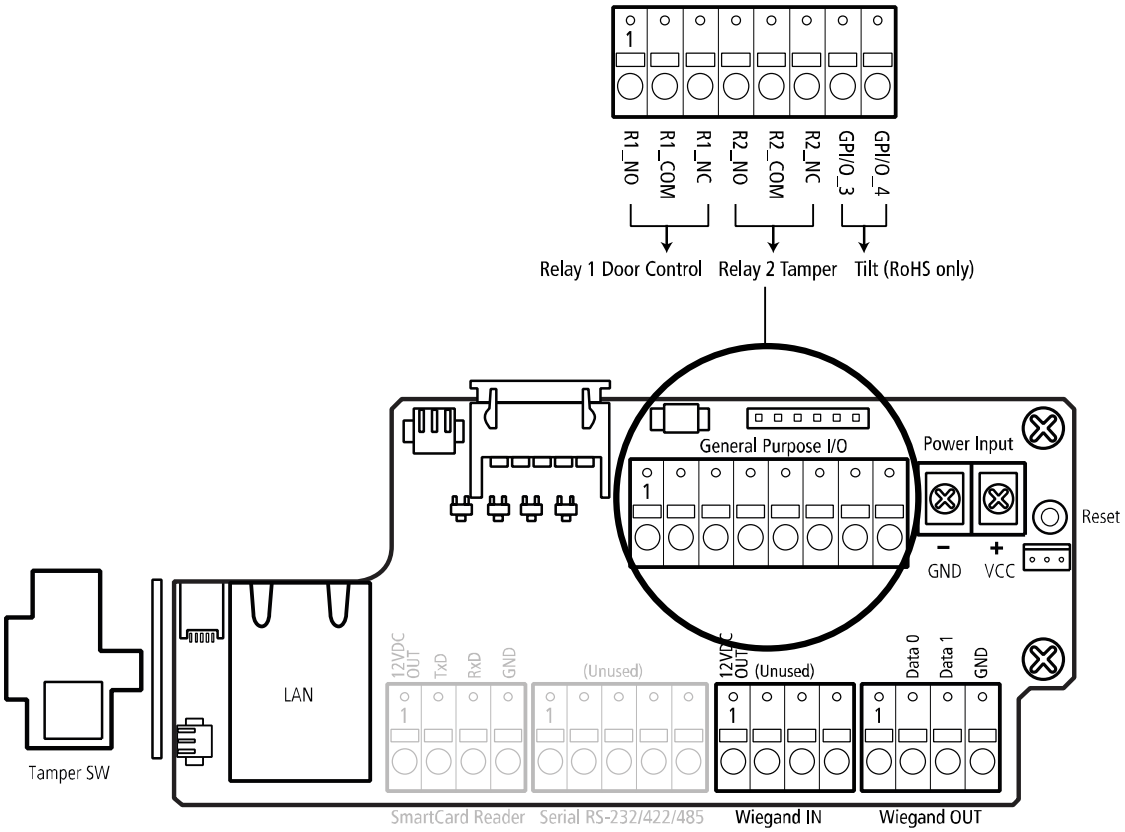
The Wiegand Output from the iCAM emulates the Wiegand Output from a Card Reader. To correctly emulate a card reader output the correct pulse duration and bit period must be properly configured in the iCAM. The chart below lists these values from some common card readers.

Reader Type	**Pulse Duration**	**Bit Period**
HID ProxPoint / ProxPro II	40 uS	2150 uS
Casi Rusco Picture Perfect	40 uS	2000 uS
HID / Banquetec MIFARE	68 uS	1000 uS
HID Dorado	100 uS	1000 uS

Note: *The Total Wiegand Bits, Facility Code, and Vaild Bits are determined by the card or Access system configuration.*

3.5 Detailed Information of Wiegand and GPI/O Connections

General Purpose Input and Output connections are available through the iCAM4000. They allow for additional 3rd party items to be added to the iCAM4000. Because the iCAM has been designed to work with other products, use of the GPI/O can create the ability for customized features specific to the needs of the environment. Examples 3rd party expansion products are listed below.



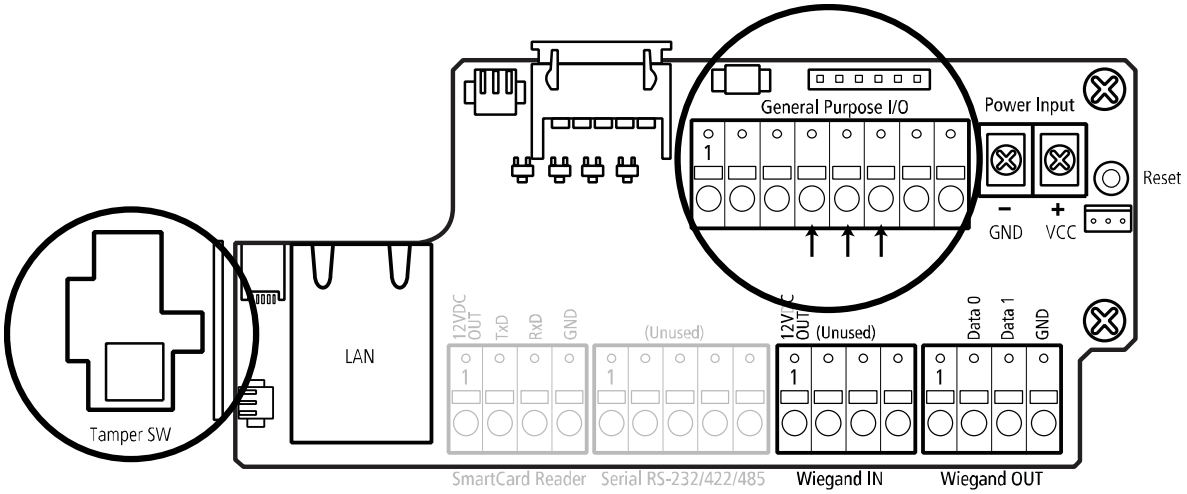
< Location of the General Purpose I/O connectors >

3.5.1 Tamper Switch Operation on the iCAM

The tamper (circled below) switch works on a “change of state”, where as once the iCAM is powered on, the tamper will detect a press or release of the tamper switch.

The tamper alarm at the iCAM is indicated by a single shutter sound, not a continuous beep.

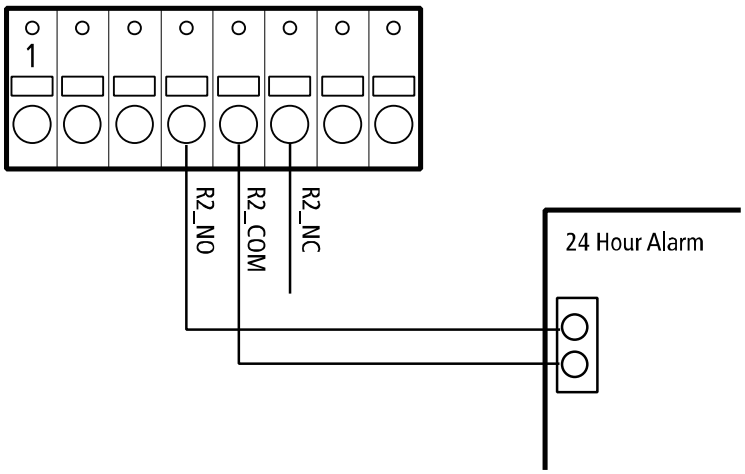
Recognition processes will cease at the iCAM and a message will be sent back to the Iris Server to log the event and process if GPO responses are configured.



<Diagram for use when connecting a Tamper Using the General Purpose Outputs >

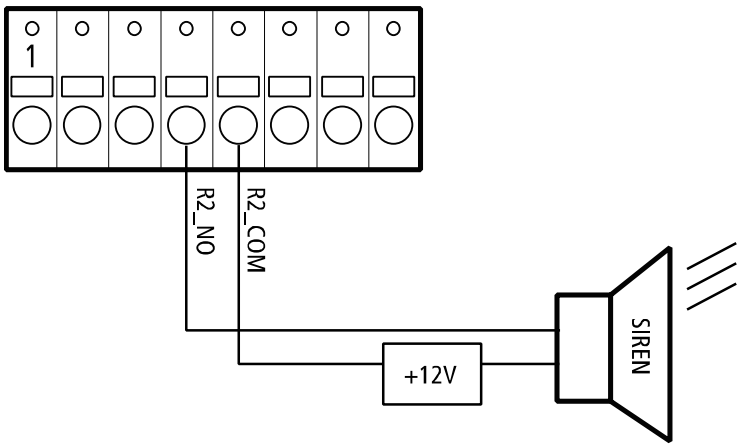
A: 24-Hour Monitored Alarm Zone (Skip if not using a Tamper relay output)

Connecting a tamper relay to either an active 24-hour monitored alarm system, or a passive alarm designed to alert locally can be configured with the iCAM4000 and Panel PC iData SoHo software. In the event that the iCAM is tampered, the alarm will be triggered when configured as illustrated below. Connect from the General Purpose I/O location of your iCAM4000 as circled above with positions R2_COM and R2_NO.



B: External Siren or Audible Device (Skip if not using a Tamper relay output)

Connecting a tamper relay to an audible device such as a siren locally positioned in your environment allows immediate recognizable audible input that the iCAM4000 may be potentially compromised as a change of tamper state has occurred.



3.5.2 iCAM Connection to Door Access Control Devices - Wiring

Magnetic Locking systems and common door strikes are designed to function as security door controls. Such products often require independent external electrical power to control the entrance and exit of a door location. Proper installation of these units is required for proper functionality when used with your iCAM (consult 3rd party documentation for requirements and installation procedures).

A magnetic lock is a simple locking device that consists of an electromagnet and armature plate. By attaching the electromagnet to the door frame and the armature plate to the door, a current passing through the electromagnet attracts the armature plate holding the door shut. Unlike an electric strike a magnetic lock has no interconnecting parts and is therefore not suitable for high security applications because it is possible to bypass the lock by disrupting the power supply.

To remain locked the magnetic lock requires a constant power source. At around 3 watts, the power drain of the lock is typically far less than that of a conventional light bulb (around 60 watts), but it may cause security concerns as the device will become unlocked if the power source is disrupted. In comparison, electric strikes can be designed to remain locked should the power source be disrupted. Nevertheless, this behavior can actually be preferable in terms of emergency situations like fires or severe weather.

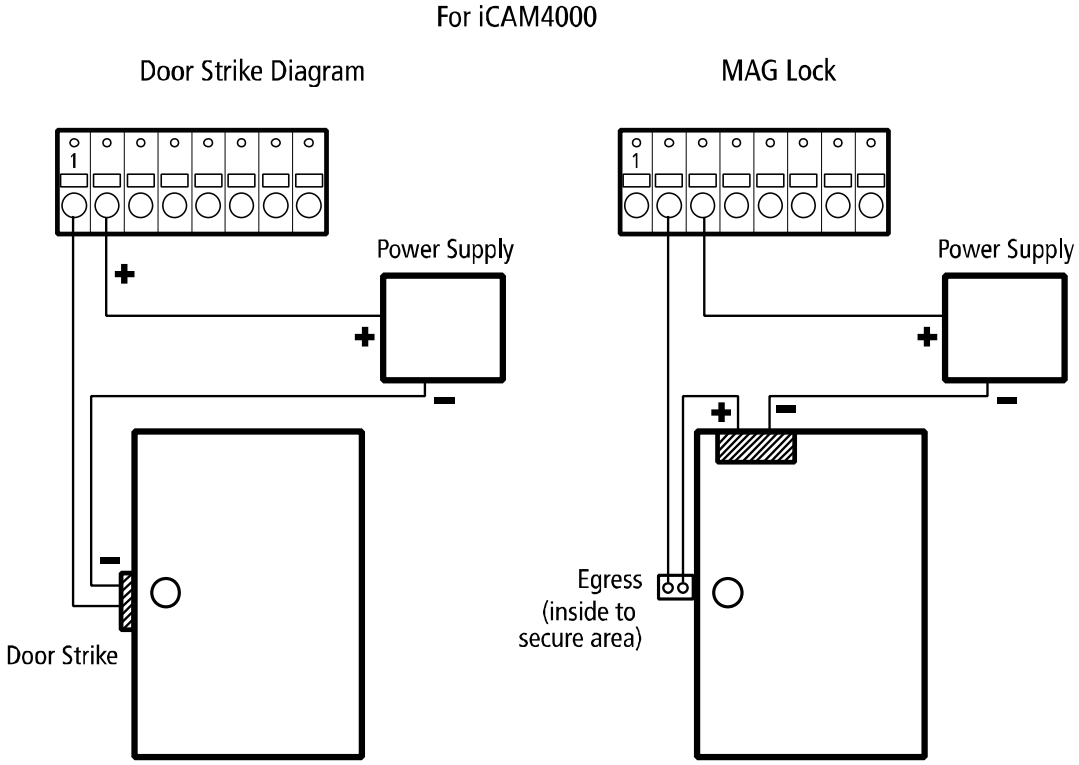
iCAM Connections

The Door-Strike Diagram (to follow) shows an example of the iCAM4000 connected to the Negative wire from the 3rd party external Magnetic door strike's connecting to R1_NC, and the Positive wire from the 3rd Party required external power supply connecting to R1_COM GPIO connectors. (Completing the connection through to the door strike plate is then required as per the instructions provided by your Magnetic lock company provider.)

Disclaimer: Only knowledgeable insured professional installers should attempt to install Magnetic locking systems with use of the iCAM4000.

Consult with your fire Marshall and local town/county code requirements to guarantee adherence to specific local ordinances and restrictions. Iris ID Electronics takes no responsibility for the incorporation of any 3rd party products, nor does it endorse one type of product over another. Iris ID will not be held accountable for installation errors, and subsequent failure, or safety concerns of 3rd party product. Additionally, Iris ID

cannot be held responsible for regulatory issues, and mandated legal requirements applicable to the potential installation of any 3rd party products compatible with the ICAM4000 or otherwise.



< Example of General wiring configuration when connecting to an iCAM >

3.5.3 iCAM External Tilt Control – Wiring (Skip if not using an external tilt control)

When firmware enabled, the GPIO connections on the iCAM can be used to control the tilt position of the camera module. This tilt feature is only available on the RoHS compliant iCAM4000R series of iris cameras.

It is recommended that only momentary switches are used for the tilt control and that the wire length between the switches and iCAM does not exceed 15 meters (50 feet).

External Tilt Switch Operation

The External Tilt Switch allows the iCAM user to remotely control the tilt operation of the iCAM camera module. This feature is useful if the iCAM is installed where the tilt switches on the face of the camera module are inaccessible or inconvenient to the user.

Connection and operation of the External Tilt Switches does not disable or alter the operation of the tilt switches located on the face of the iCAM camera module.

Switch Wiring for the iCAM4000R Series Iris Camera

For instructions on how to access the iCAM4000 interface board connections, refer to the iCAM4000 Hardware Manual for iData SoHo which was included with the iCAM.

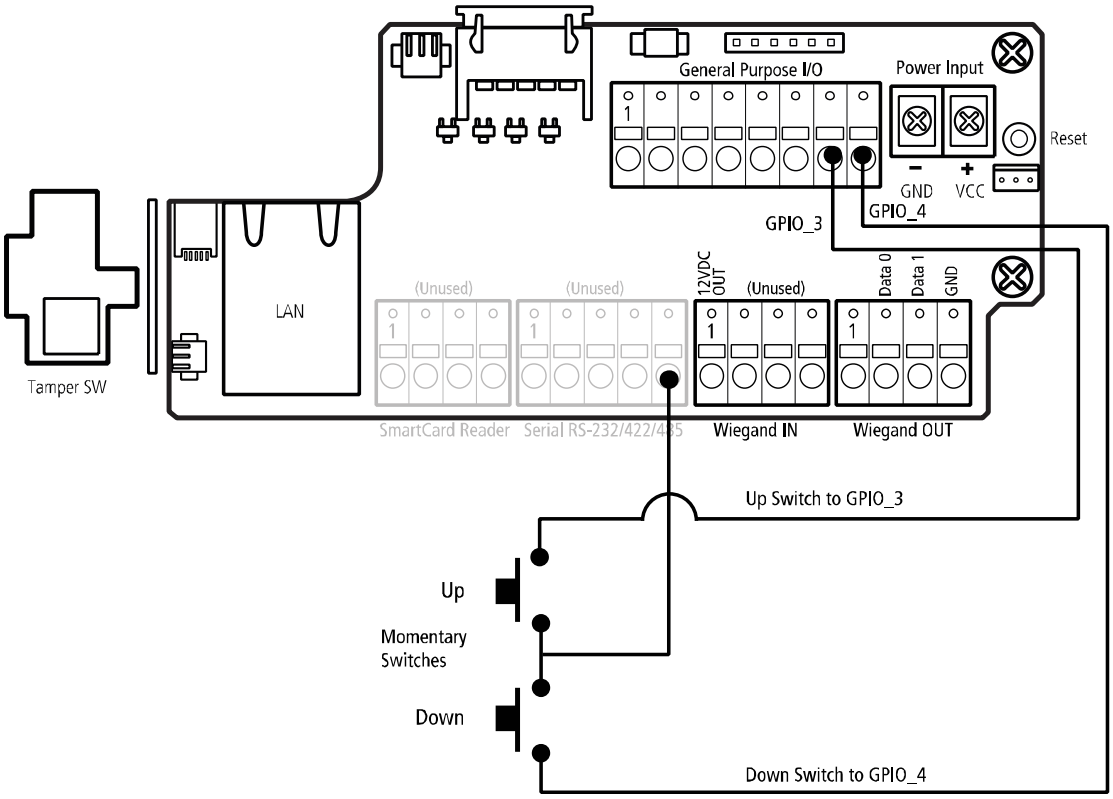
The external tilt switches are to be connected to the GPIO connections located on the interface board inside the iCAM. The GPIO are located on the General Purpose Input /Output port (labeled CN605).

See the interface board and wiring diagram located on next page.

** Note: The PINs on the iCAM4000 interface board are numbered from left to right.*

Up Switch: The up tilt switch is to be wired between the GND (Ground) connection (located at PIN 5 of the Serial RS232/422 port – CN607) and the GPIO3 connection (located at PIN 7 of the General Purpose I/O port (CN605)).

Down Switch: The down tilt switch is to be wired between the GND (Ground) connection (located at PIN 5 of the Serial RS232/422 port – CN607) and the GPIO4 connection (located at PIN 8 of the General Purpose I/O port (CN605)).



< The iCAM4000R Interface Board Connections with External Tilt Switch Wiring >

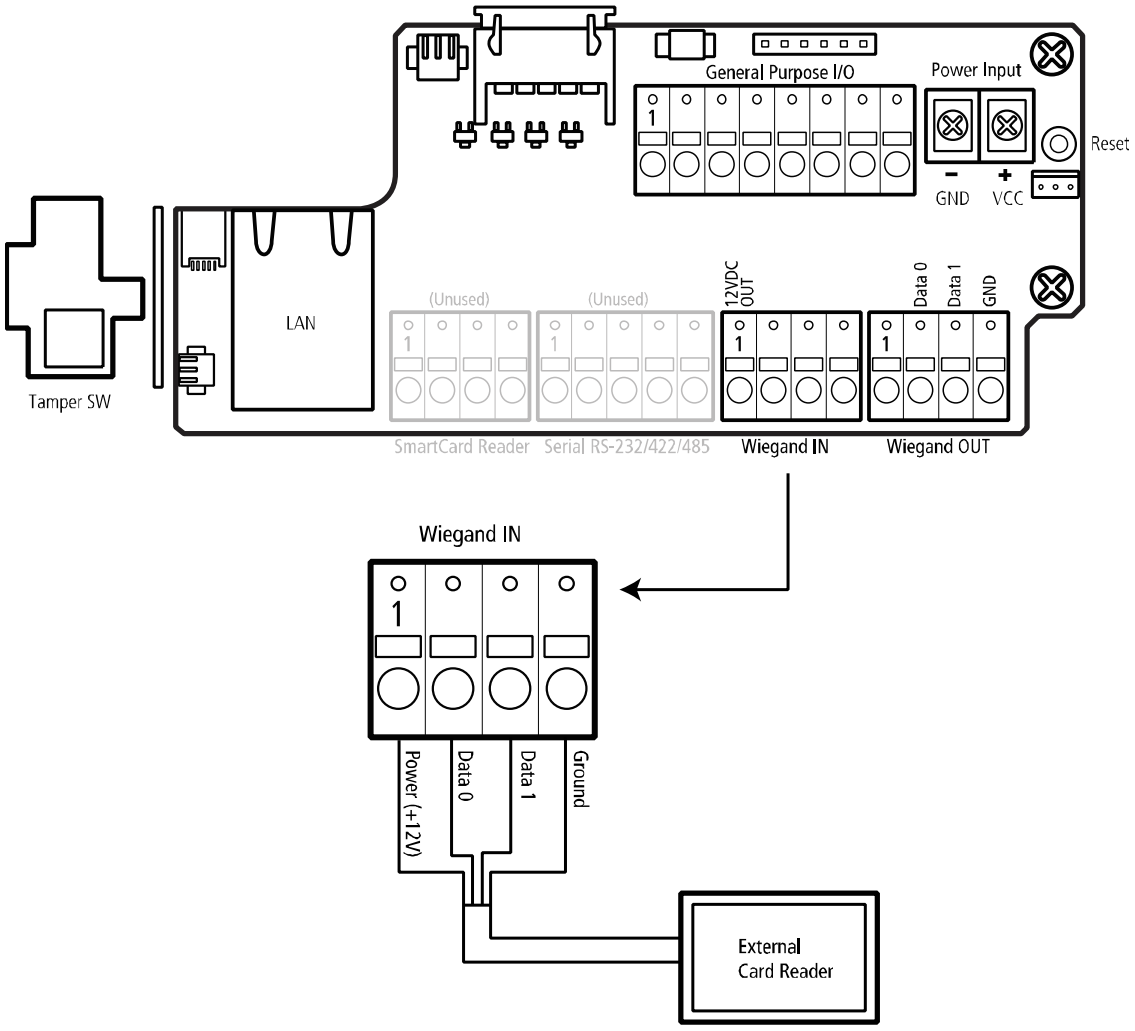
3.5.4 External Card Reader Configuration (Card Bypass)

An external card reader can be used with the iCAM4000 by connecting to the Wiegand Input located in the next diagram.

The iCAM4000 supports standard Wiegand Input formats of 26 bit, 35 bit and Corporate 1000. Input connections for use with external card reader systems can be found on the back of the iCAM. The use of such external card reader systems further promotes security by requiring multiple forms of identification for the user in order to gain verification.

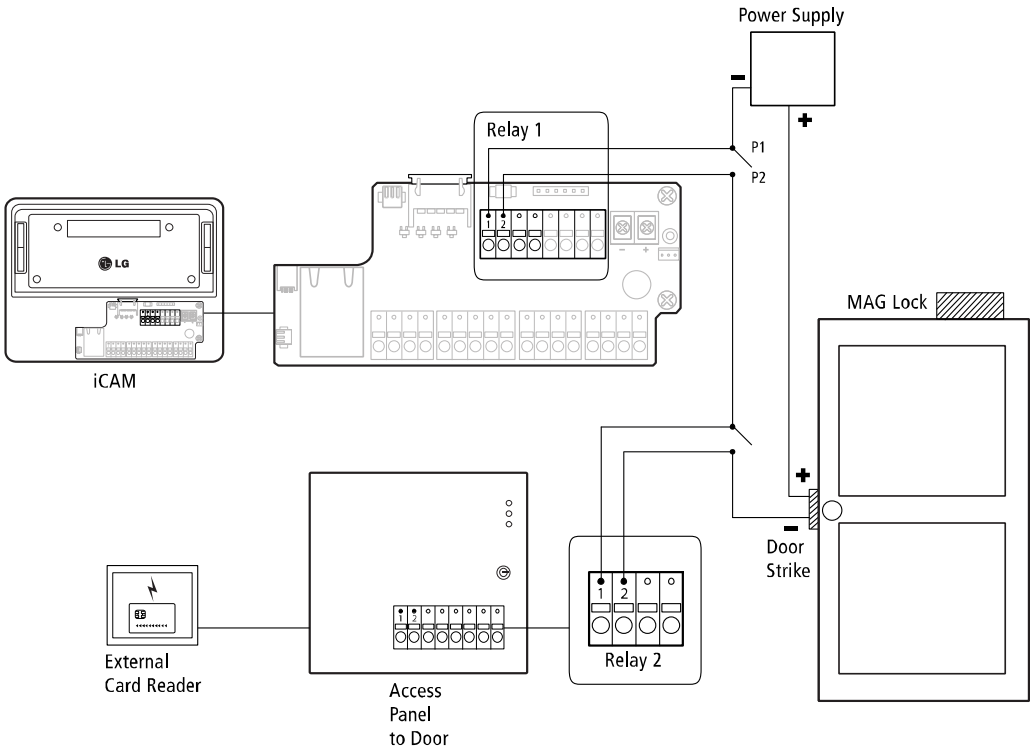
Additional reasons to implement a card reader based system are for convenience to bypass the iris identification at an iCAM unit.

To connect a 3rd party external card reader must connect to the iCAM Wiegand IN connection by connecting to the VCC (Power), D_0 (Data 0), D_1 (Data 1) and GND (ground) locations displayed on the iCAM4000 from your card reader system.

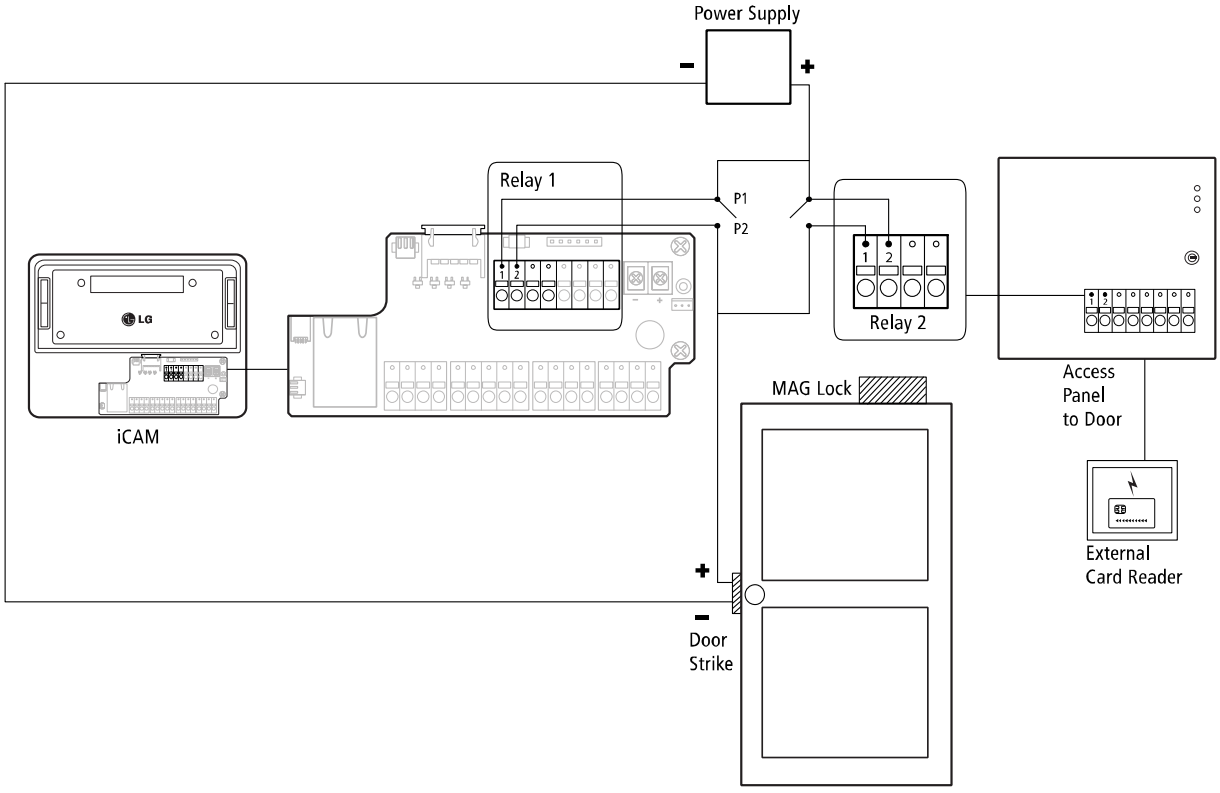


< The iCAM4000R Interface Board Wiegand IN / OUT >

** Note: An External Power supply is required when connecting external devices as needed by 3rd party products.*



< Iris plus Card Configuration Diagram>



< Iris or Card Configuration Diagram>

** Note: P1 = Connector Pin 1, P2 = Connector Pin 2*

3.5.5 Wiegand Output

General Wiegand Information

The Wiegand interface is a de facto wiring and communications standard. It is commonly used to connect a card reader to an electronics entry access control system.

The Wiegand interface uses three wires, one of which is a common ground and two of which are data transmission wires usually called DATA0 and DATA1 but sometimes also labeled Data High and Data Low. When no data is being sent both DATA0 and DATA1 are at the high voltage. When a 0 is sent the Data Low wire (also called DATA0) is at a low voltage while the Data High wire stays at a high voltage. When a 1 is sent Data High is at the low voltage while Data Low stays at the high voltage.

The high voltage level is usually +5VDC to accommodate for long cable runs (most reader manufacturers publish a maximum of 500 feet) from the door readers to the associated access control panel typically located in a secure closet.

Wiegand 26-Bit Format

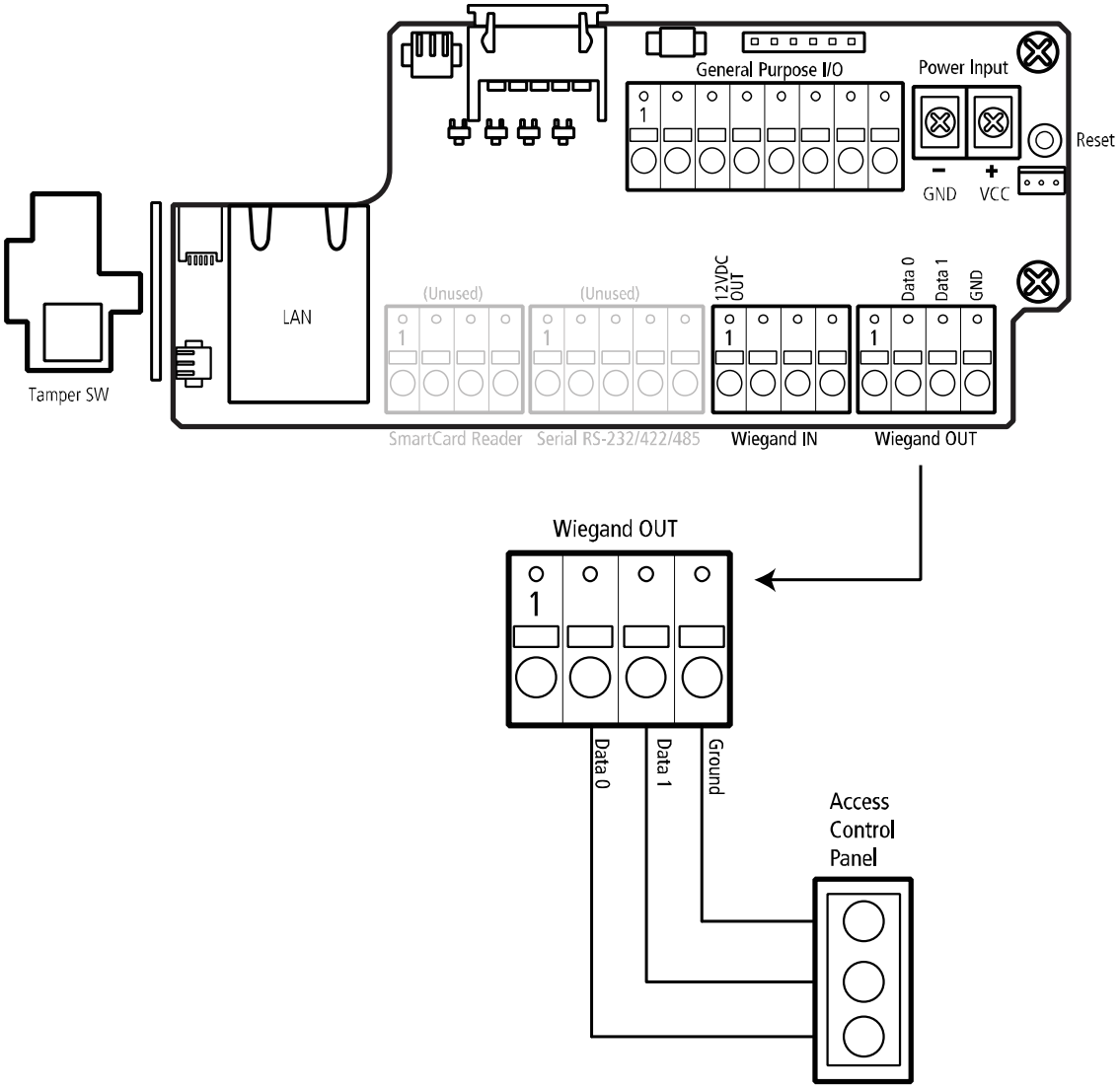
The communications protocol used on a Wiegand interface is known as the Wiegand protocol. The 26-Bit Wiegand format has one 1 parity bit, 8 bits of facility code, 16 bits of ID code, and a stop parity bit for a total of 26 bits. The first parity bit is calculated from the first 12 bits of the code and the trailing parity bit from the last 12 bits (Diagram Shown below). However many inconsistent implementations and extensions to the basic format exist.

Start Parity	Facility Code	Card ID	Stop Parity
P	FFFFFFFF	CCCCCCCCCCCCCCCC	P

< 26-Bit Wiegand Format >

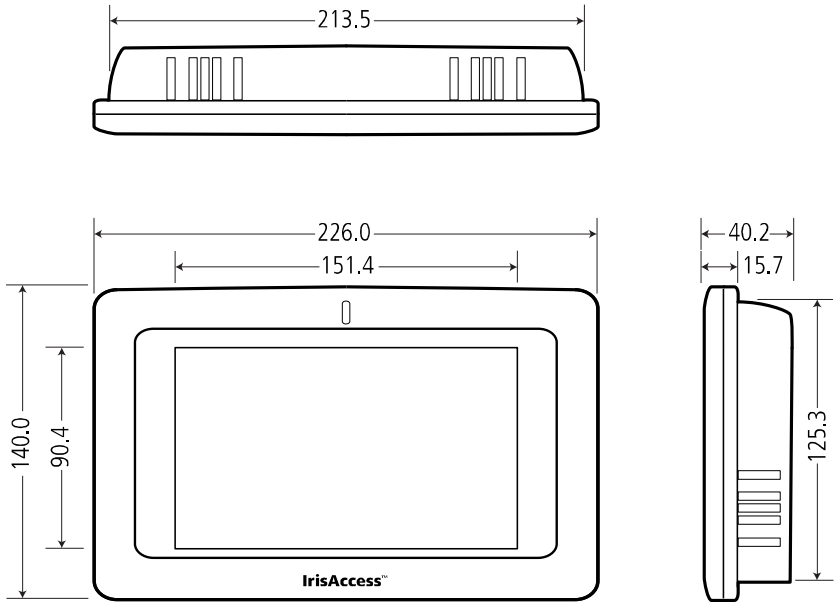
Wiegand Output from iCAM4000

The Wiegand Output from the iCAM4000 Camera unit used with the iData SoHo uses a 26-Bit format only. Any 3rd party device capable of receiving a 26-bit Wiegand stream will be able to communicate with this camera unit once configured. See image below for general wiring of Wiegand Output to an Access Control Panel.

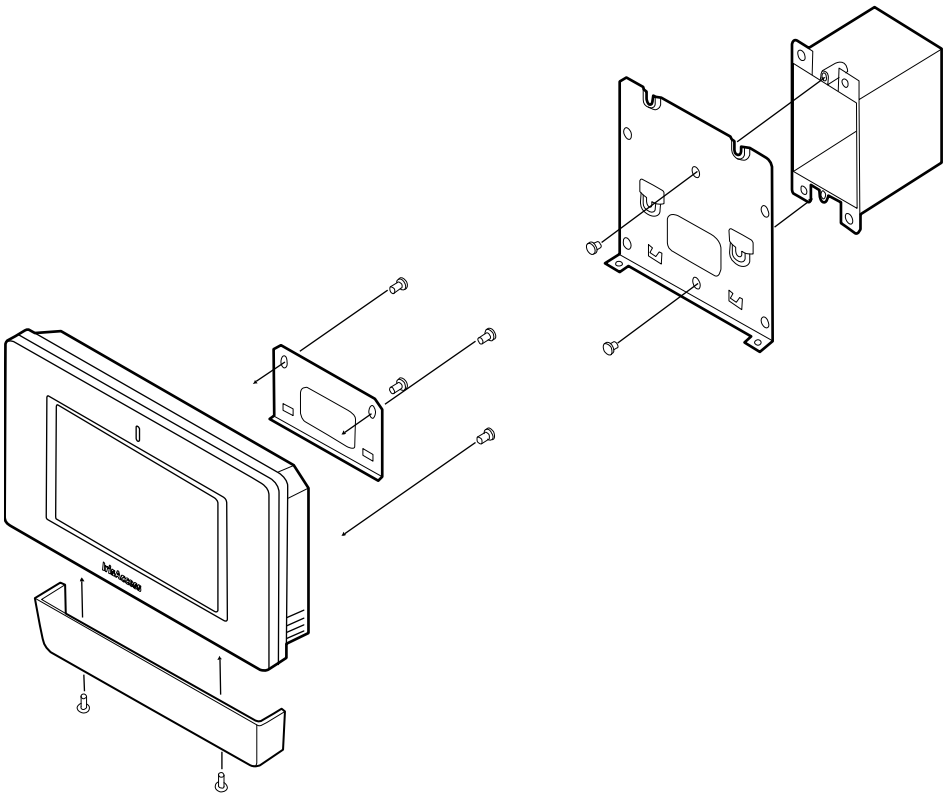


< Wiring for Wiegand Output to Access Control Panel >

3.6 Setting Up the IrisAccess Panel PC



< Panel PC Dimensions in mm unit>

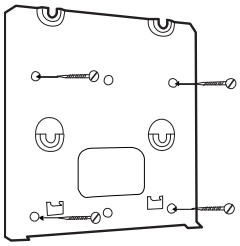


< Panel PC Mounting Bracket Diagram>

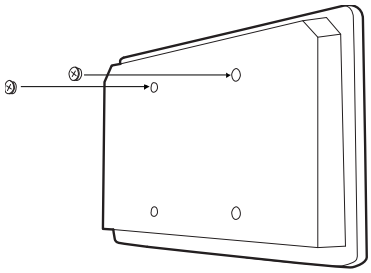
Your IrisAccess Panel PC can be positioned on the wall by mounting the unit with the optional wall mount bracket or by placing the Panel PC on a cradle stand for use on a flat surface area.

It is important to keep the Panel PC in a location that is both safe from unwanted onlookers but also in a location that is convenient to reach as this is a touch panel device.

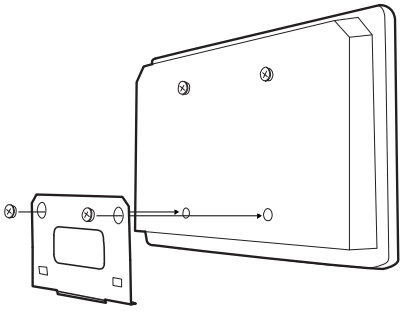
1. Secure the mount plate on the wall using the four included wall screws as shown below.



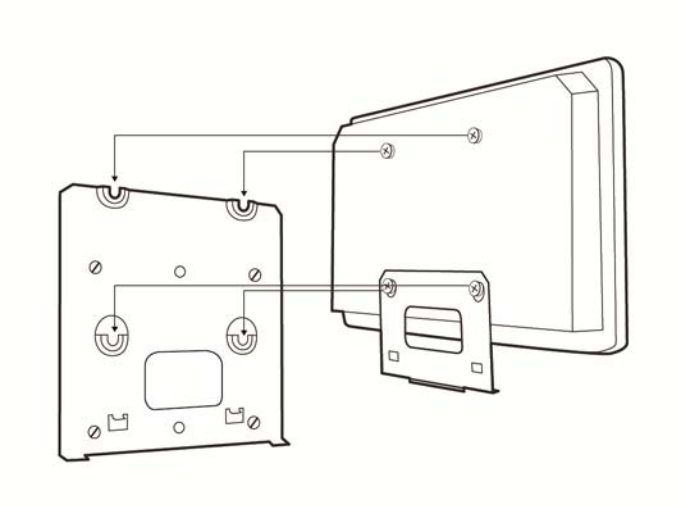
2. Insert the two PC Locking Plate Screws to rear of the Panel PC as shown below.



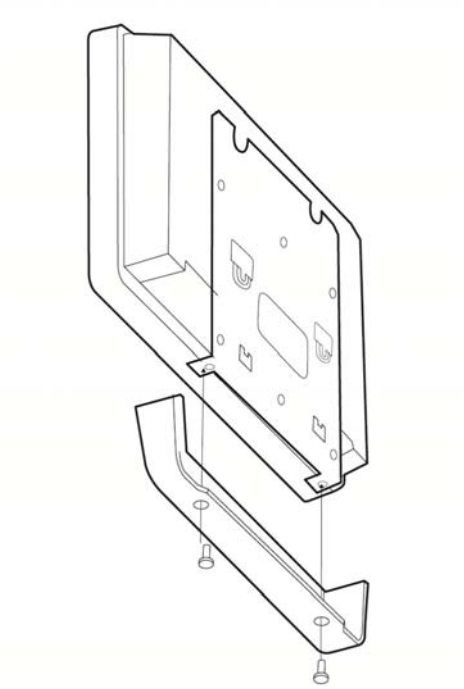
3. Affix locking bracket to the rear of the Panel PC using the two panel screws provided as shown below.



4. Position the Panel PC Wall Plate Screws (already installed in rear panel) to the wall mount plate by sliding the rear of the Panel downwards. Slide Panel down until the screws are securely hooked to the wall plate as shown below.



5. Attach bottom cover to the Panel PC. Use the two provided cover screws to connect the bottom cover securely to the back plate as shown below.

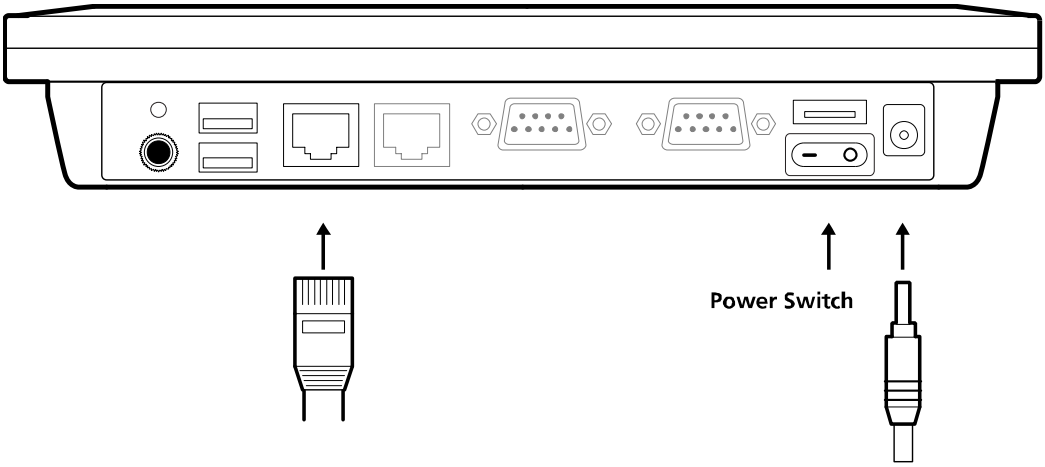


Physical connections and powering ON the Panel PC

The IrisAccess Panel PC has been pre-installed with iData SoHo software and does not require any software installation.

To Power on the Panel PC, plug the external AC adapter into the bottom of the Panel PC. It is recommended that you plug the power connecter into a Universal Power Supply and/or Automatic Voltage Regulator as opposed to directly into a power strip or wall outlet directly.

Press the Power Button on the bottom right of your Panel PC to turn on the device. A green indicator light will appear at the top-center of the Panel PC when powered.



Setup Utility for the IrisAccess Panel PC

The first time you boot the Panel PC you will be prompted to complete the Initial Setup Wizard as described in section 3.7. Select the setup utility to configure the Panel PC.

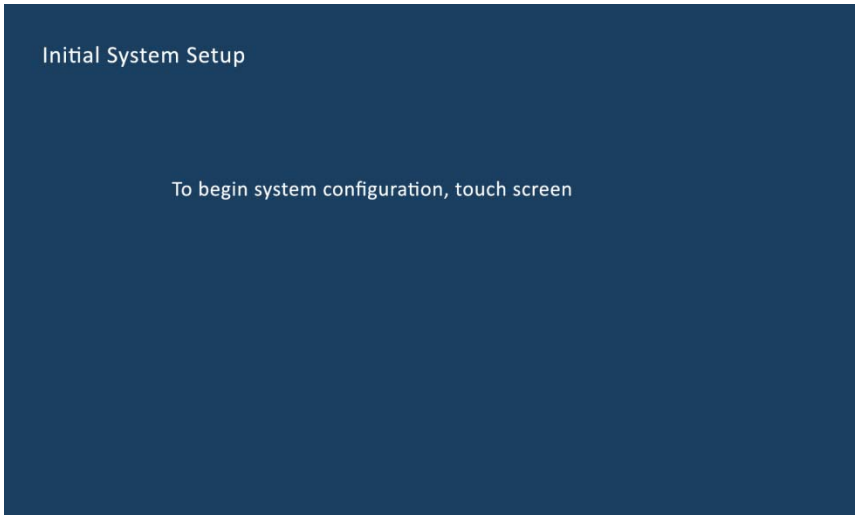
Once the setup wizard has been completed, it will not appear again automatically. Instead, your Panel PC with iData SoHo software will load directly to the Graphical User interface. To access the setup utility after your initial boot-up you can select the option for when the IrisAccess Panel PC is rebooted.

3.7 Configuring the iData SoHo Software on Your Panel PC

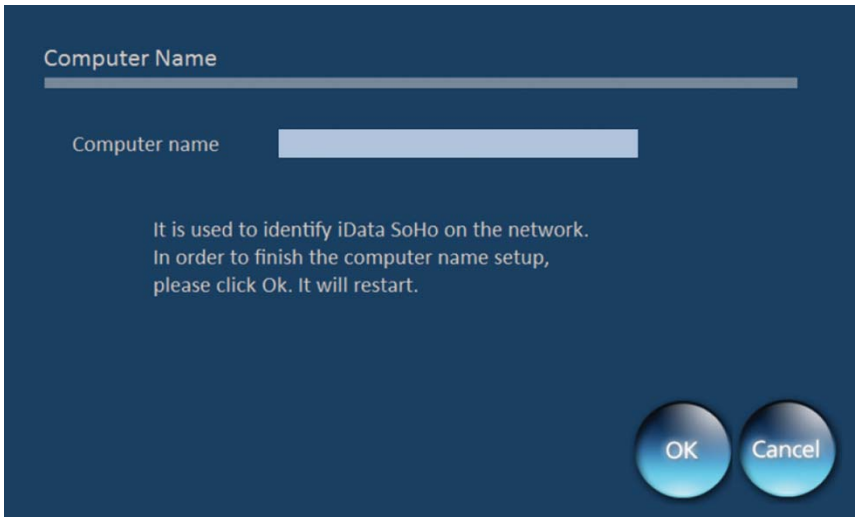
Initial Setup/Settings wizard

** Note: When the Iris Access Panel PC is first turned on, a screen to align the panel will be displayed. Press on the area(s) indicated by the panel to configure alignment.*

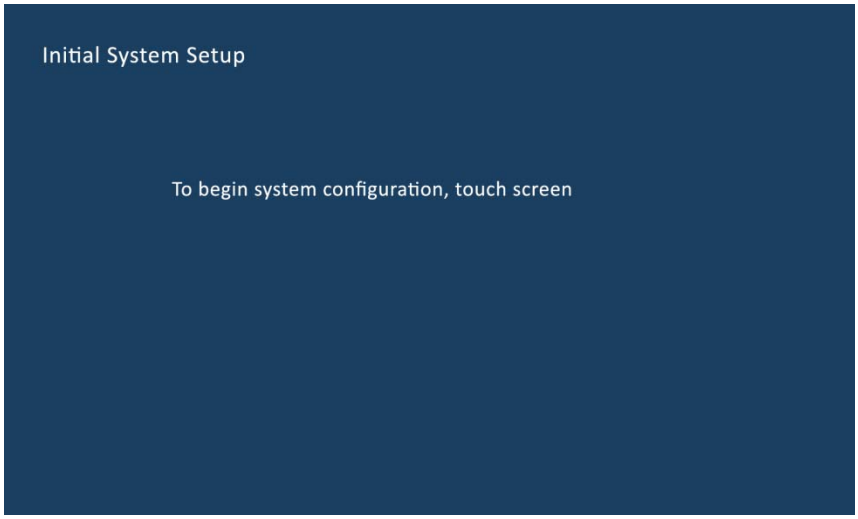
To Begin: Touch the screen as shown below to enter the initial setup utility.



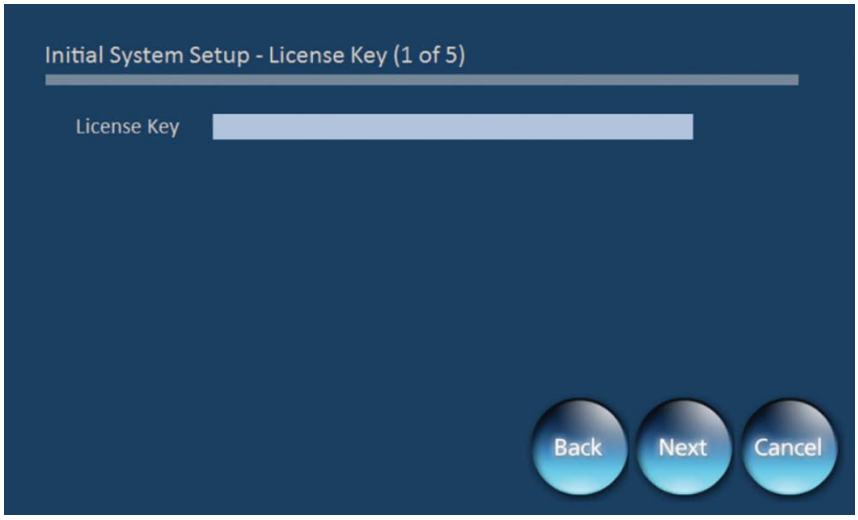
Create computer name: This name is used to identify the IrisAccess Panel PC on the network. After the computer name has been created and the "OK" button is selected the Panel PC will reboot automatically and the initial setup wizard will appear.



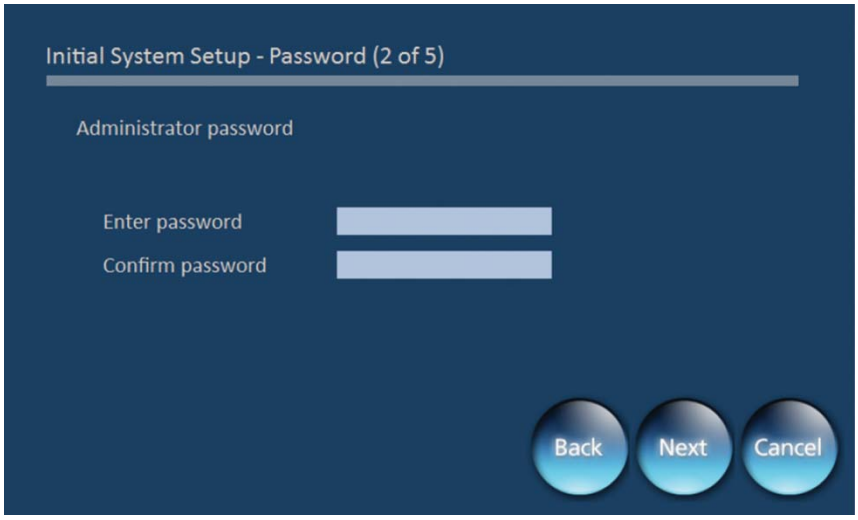
To Begin setup wizard: Touch the screen as shown below to enter the initial setup utility.



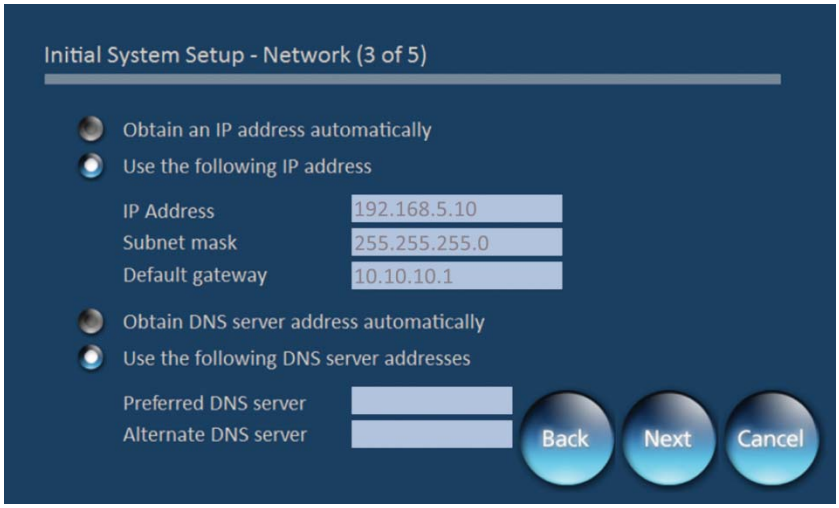
License Key: Enter the Iris ID IRIS iData SoHo software License key provided with your product.



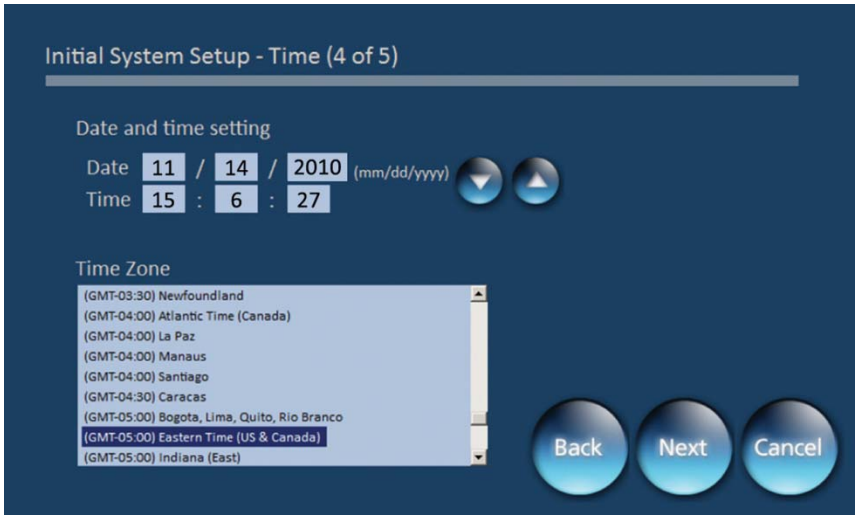
Administrator Password: Enter a 6-12 digit administrator password and confirm password. This will be used to enter the Graphical user interface.



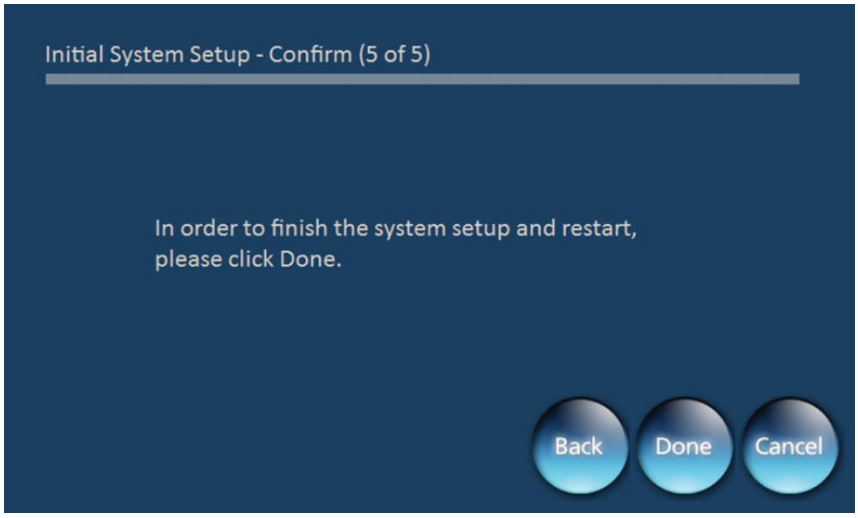
Network: Configure the IP address settings for the Panel PC to either obtain an IP address automatically or specify IP address and DNS settings. (It is often recommended that a static IP address be used when configuring the system as a DHCP server is needed if configuring with automatic addressing).



Time & Date: Set the Date, Time, and Time Zone for the location the Panel will be used.



Confirmation page: Save and confirm your settings by pressing "Done". If you wish to cancel or append any entries made in the initial System Setup Wizard press Cancel or Back. After this screen is completed the system will automatically reboot and load the iData SoHo Graphical software to begin using your product.



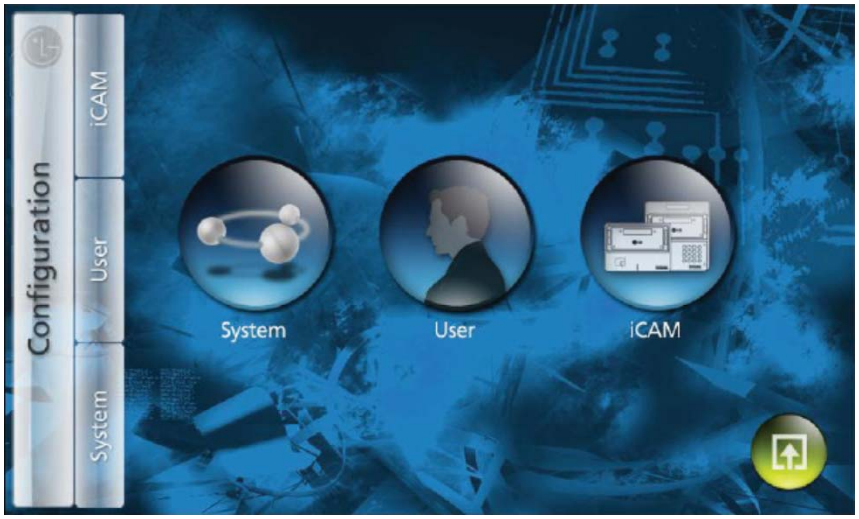
Connecting to an iCAM and setting Up multiple iCAM units

** Note: Tap screen if needed to initiate onscreen keyboard*

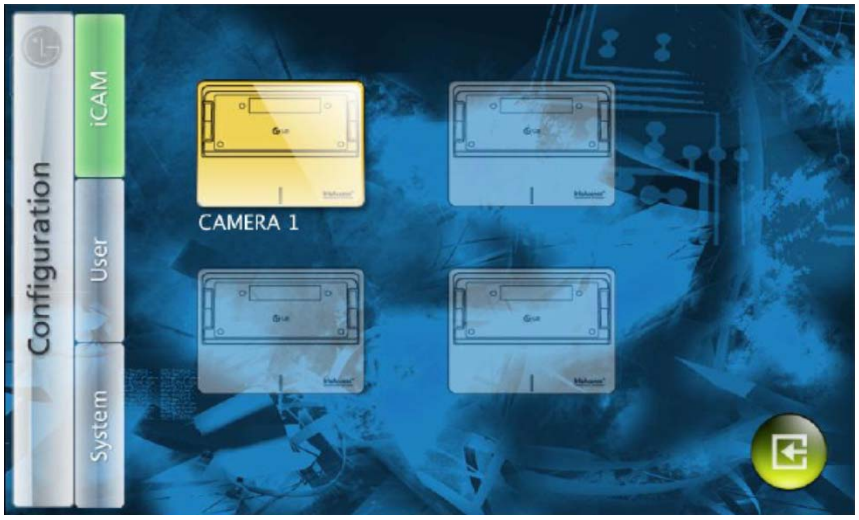
Steps to configure the iData SoHo software with an iCAM:

1. Sign in using administrator account login.
2. Select the Config button.

3. Select iCAM on the Configuration screen



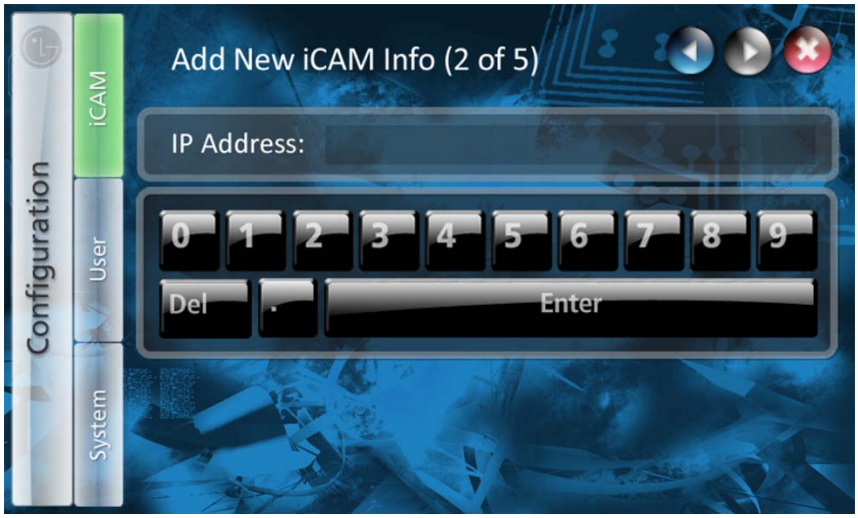
4. Select Grayed out iCAM icon you wish to setup (the first iCAM that you setup also will become the enrollment station iCAM that will be used when enrolling users in the system).



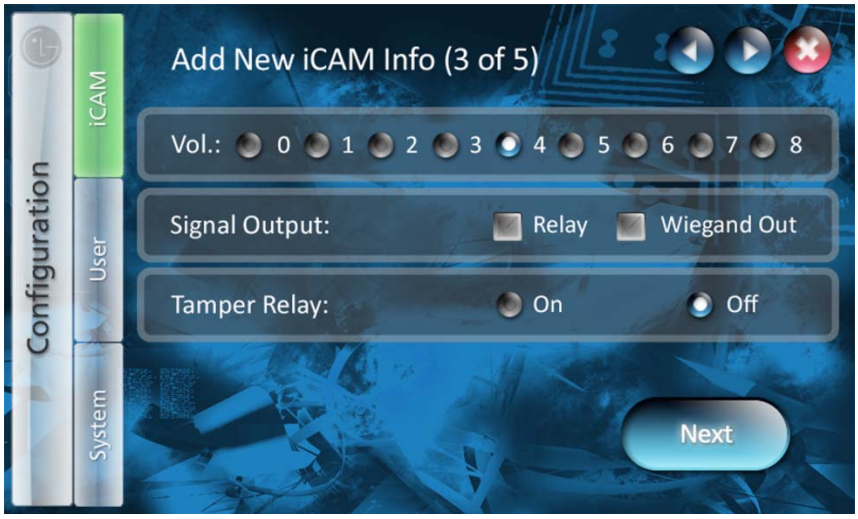
* Note: The iCAM selected for enrollment can be modified from the back-office WebConfig utility after initial setup has completed.

5. From the Add New iCAM information (1 of 5) screen insert a Name then press the right arrow.

6. From the Add New iCAM information (2 of 5) screen enter the IP address of the iCAM4000 that you wish to have work with your iData SoHo (iCAM4000 should already have been configured with a unique Static or Dynamic IP address).



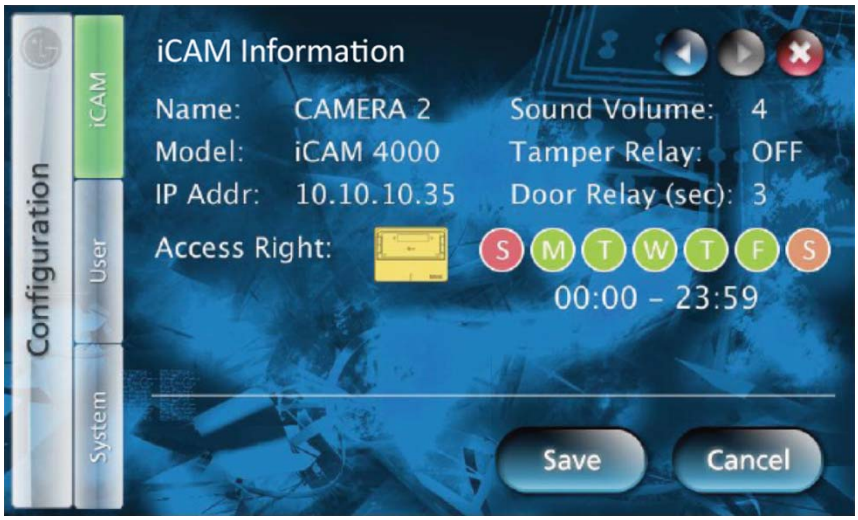
7. From the Add New iCAM information (3 of 5) screen select the volume level from 0 (Mute) to 8 (High). Then select the Signal Output that will be used for this iCAM as *Relay* and/or *Wiegand as needed* . Select *On* or *Off* for the tamper relay which will either enable or disable the tamper switches embedded in the front and back of your iCAM. Then press Next or the Right Arrow.



8. From the Add New iCAM information (4 of 5) screen Select Door Relay time (in seconds) and press Next or the Right Arrow.

9. From the Add New iCAM information (5 of 5) screen select the Enable Radial Button to activate the iCAM communication with the IrisAccess Panel PC. Select the Upper Purple Modify button to select the Days that you wish to have the Camera Enabled as Default and press Set. To configure the Time select the lower Purple Radial box that says Modify to set the daily time range default that the iCAM unit will allow users to be authorized into the system and press the right Arrow or Enter. (Time Clock works on 24-hour time only)

10. When ready select Next to finish (or the back arrow to perform additional changes if needed.



** Note: In the event that the Panel PC is unable to locate the iCAM. Verify you have entered the right IP address for the iCAM. If the issue still persists check all your local network hardware and software settings.*

3.8 Enrolling Users into the System

Enrolling a user into the IrisAccess iData SoHo system is a streamlined process requiring the use of the Panel PC and an enrollment iCAM. By default, the enrollment iCAM is the first iCAM camera unit that you configured when setting up your iData SoHo based Panel PC. Therefore, unless a user already modified settings, camera 1 will be the enrollment station.

When enrolling a user, an administrator or operator will need to be at the panel PC to start the enrollment screen process while the enrolling user is at the enrollment iCAM. The user being enrolled will hear announcement prompts to center their eyes in the mirror, or present a card to a card reader so that an image or card data can be obtained by the system. Audible instruction from the iCAM unit will follow as needed until the system has acquired the needed information from the enrollee.

Once an image has been acquired successfully, the IrisAccess Panel PC will display 5 images on the screen. 1 is of the Face capture image, and 4 additional images are of the Iris Capture images. Once satisfied with the facial image, it is crucial to pay detailed attention to the green bars under all four iris images. These green bars are called Quality Image capture bars and are intended for use specifically during the enrollment process. Attempt to achieve an enrollment with Quality Image Capture bars as close to the full maximum limit as possible.

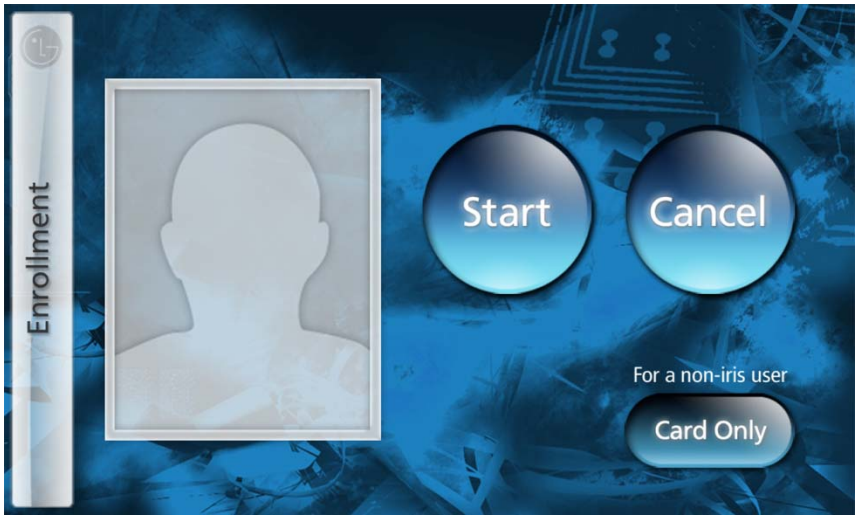
** Note: The better the iris image capture that is obtained during enrollment, the better the accuracy and speed of the IrisAccess SoHo System will be. If finding difficultly enrolling a user such as iris not accepted, cannot acquire image, or receiving poor green Quality Image Capture bar strength please retry the enrollment process with that user while verifying that they do not have any eye coverings impeding the process.*

Additionally, although an enrollment image can often be acquired successfully while someone is wearing glasses, contact lenses, and sun-glasses; for best practice enrollment purposes it is recommended that the user remove any eye coverings in order to achieve a higher quality Iris Image capture.

Steps for standard Iris User enrollment:

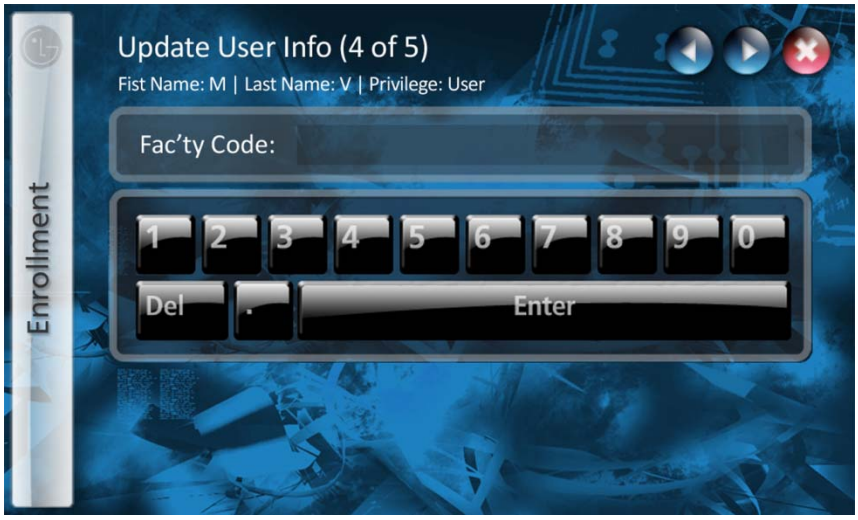
1. Sign in using administrator account login.
2. Press Enroll on Panel PC.

3. Press Start.



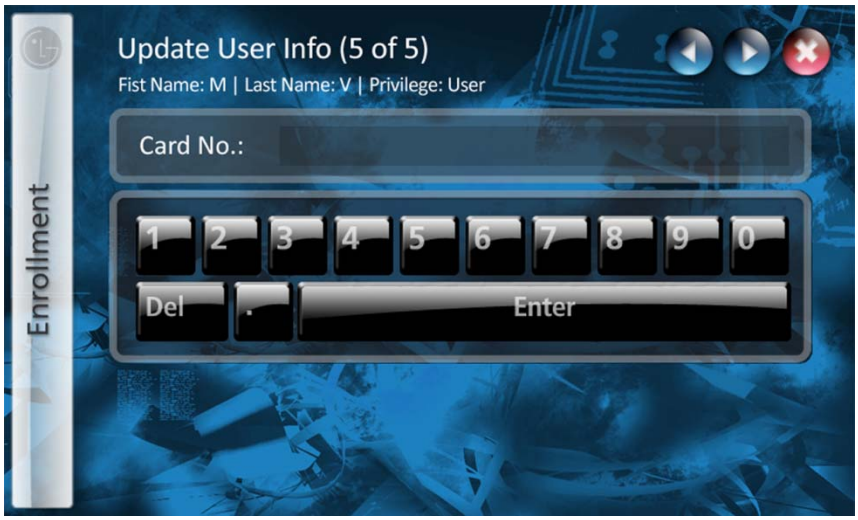
4. Center eyes in front of the enrollment iCAM4000 for image capture.
5. Select Okay or Retry on Panel PC. (Make sure the Green Quality bars under each Iris Image are as close to full as possible.)
6. Enter First name of User and select the forward arrow.
7. Enter Last name of user and select the forward arrow.
8. Select Gender and rights Privileges (Operator or User) and select the forward arrow if not using Wiegand Output with an Access Control Panel.
9. If an Access control Panel is used - Select the *Edit Wiegand Output* button from the panel PC.

10. Enter the Facility code (maximum number allowed is 255) and press the forward arrow.



* Note: *A Facility Code is a unique ID for the facility, and the group of cards issued. (Also known as site code) This Facility Code field is required for identification purposes when Wiegand Output is selected as enabled in an iCAM configured with the iData SoHo Panel PC.*

11. Enter the Card Number (maximum number is 65535) and press the right arrow.



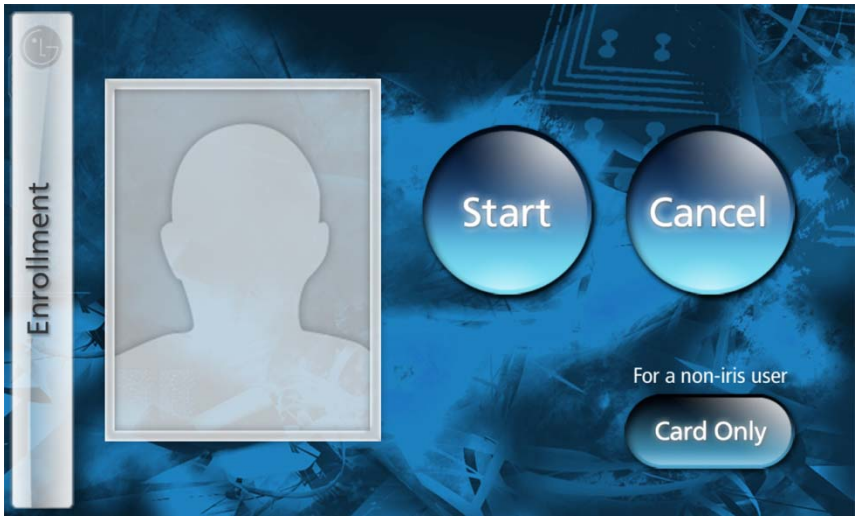
12. Confirm the User Information Summary and select the Next (or back arrow if changes need to be made)
13. Re-verify User information and select Access Right to assign right access privileges for what iCAM door units and day/time allowances are required.
14. Select Back Arrow when complete and then Done to finish the user enrollment.

* Note: If an enrollee is given Operator Rights they will be able to access the Panel PC and make setting changes, modifications, and enroll other individuals. However, only the administrator account is able to change the Panel PC administrator password information.

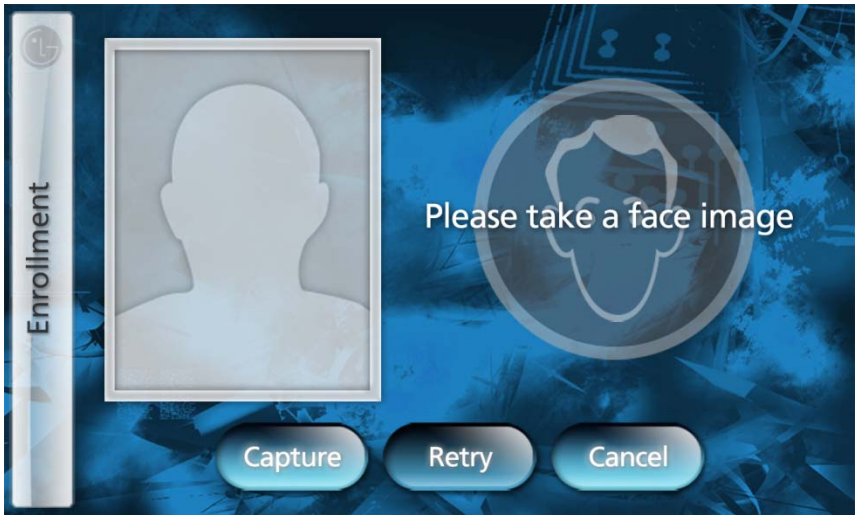
Steps for Smart Card User Enrollment:

1. Sign in using administrator account login.
2. Press Enroll on Panel PC.

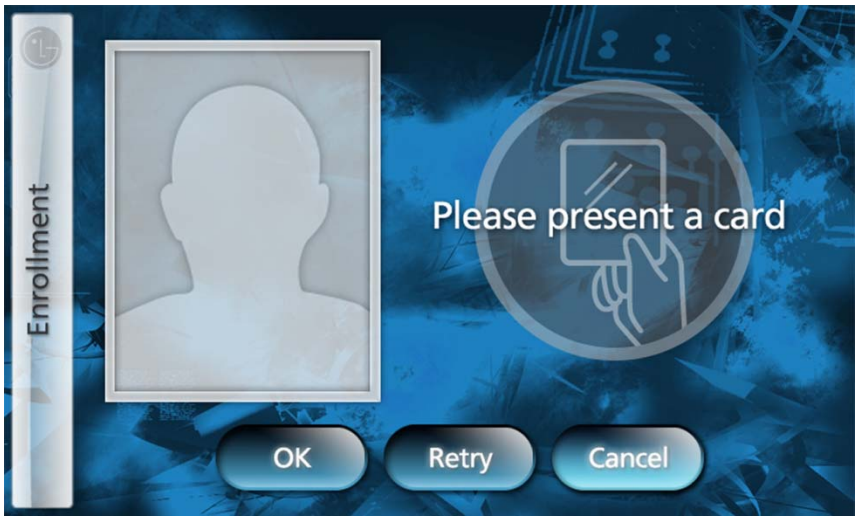
3. Press Card Only (for non-iris user).



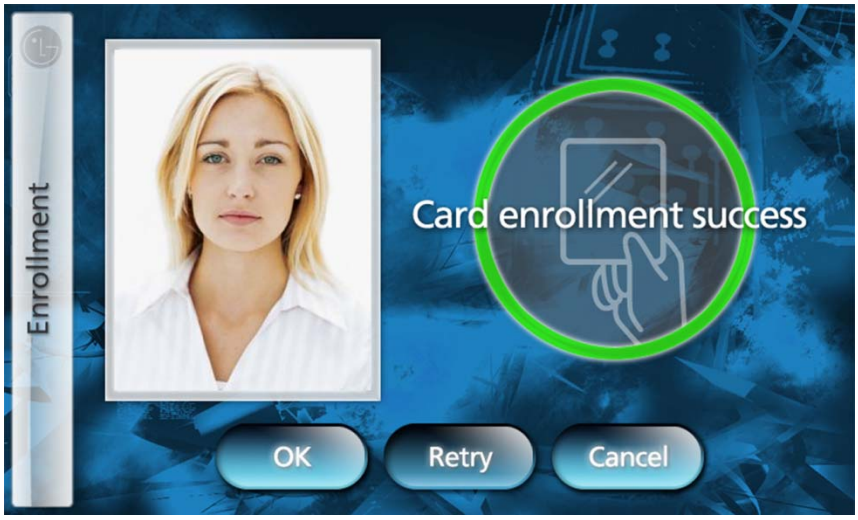
4. Take face image of user being enrolled by pressing Capture and Okay to accept image.



5. Present the Card to the Card Reader when audibly prompted by the iCAM.



6. Press Okay on the Panel PC when Card enrollment success appears to continue.



7. Enter First name of User and select the forward arrow.
8. Enter Last name of user and select the forward arrow.
9. Select Gender and rights Privileges for User and select the forward arrow.
10. Confirm the User Information Summary and select the Next (or back arrow if changes need to be made).
11. Re-verify User information and select Access Right to assign right access privileges for what iCAM door units and day/time allowances are required.
12. Select Back Arrow when complete and then Done to finish the user enrollment.

** Note: For advanced configuration options, utilize the web-access utility to append user enrollment information, and edit and upload features. Refer to the Web-access utility section of this guide for more details.*

3.9 Assigning and Editing Rights Access Data to a User

By default, an enrolled user of your IrisAccess iData SoHo software will be given general permissions to the iCAM door units already configured on your system. When the permission settings for a iCAM unit are created, all enrolled users will be defaulted with the permission set of those iCAM units.

To assign specific rights Access to an enrolled user can be performed by modifying that user's information from the IrisAccess Panel PC or through the back office Web-configuration utility.

Steps for editing User Rights Access:

1. Sign in using administrator account login.
2. Select Config on the iData SoHo software.
3. Select User.
4. Search for the person you wish to edit user information settings and press NEXT.
5. Select either the Access Rights, Edit Info, or Delete buttons to modify settings.

4. Understanding the User Interface

The iData graphical user interface application found on the SoHo Panel PC is divided up into sections by intuitive ergonomic function.

Walking through the Interface: Becoming familiar with the user interface requires little more than reviewing the simple options and menus that are displayed on the screen. Below you will find some of the Graphical screens often used with the iData SoHo Software along with the general function that is has been designed for.

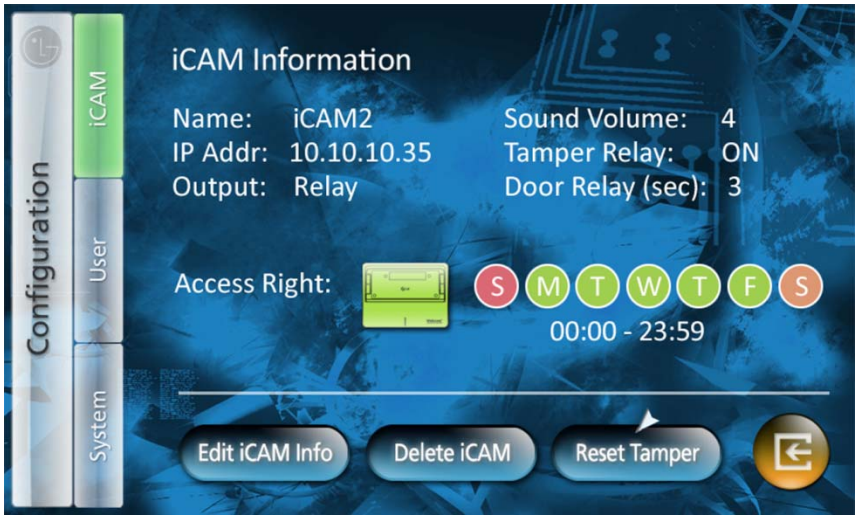
Default Screen: Displays the Date, time and software version on Panel PC.

iCAM Disconnection icons: Default Screen Indicating iCAM communication error on one or more iCAM units. These disconnected camera units are represented by the icons shown in Red at the Bottom Right corner of the Default Main screen. Grayed out icons represent iCAM units not enabled. These icon images only appear if the Panel PC is not able to establish communication with one or more iCAM's.

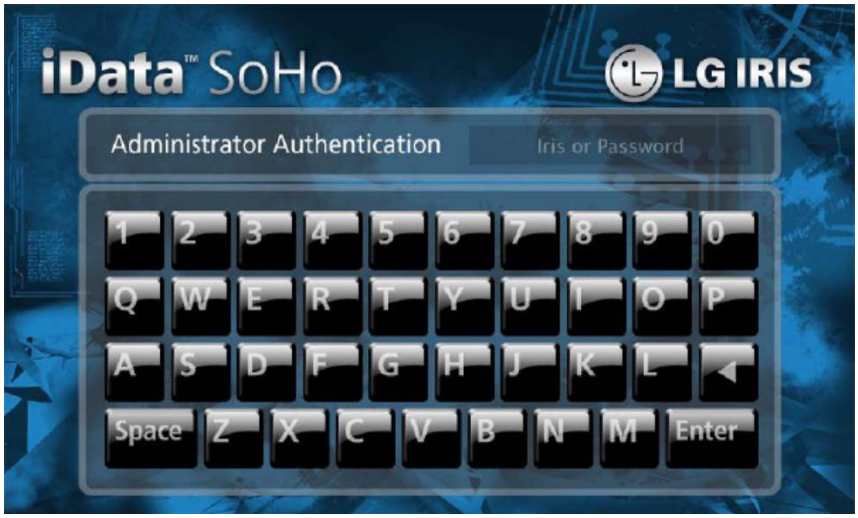
iCAM Tamper icons: Panel PC Default Screen Indicating the iCAM tamper has been triggered on one or more iCAM units. These tamper alarmed camera units are represented by the icons shown in Yellow at the Bottom

Right corner of the Default Main screen. Grayed out icons represent iCAM units not enabled. These icon images only appear if the Panel PC is not able to establish communication with one or more iCAM's.

iCAM Tamper RESET: Pressing the Reset tamper button from iCAM information screen of the specific camera units that require a tamper reset restores functionality to the camera unit after a tamper alarm wqas trigged from an iCAM (Note: Make sure that the camera unit(s) tamper switch has been set back to the proper position prior to attempting to reset the tamper through the panel PC). After you login to the Panel PC, this function can be found from the Config > iCAM interface after the specific camera units is selected.

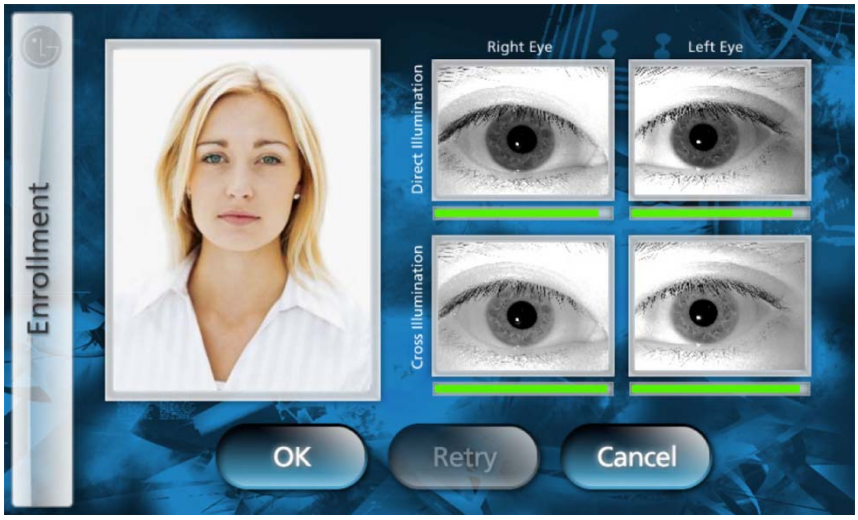


Password Authentication Screen: Displays (touch based) Keyboard to type password credentials and enter software.



Main Menu: The Main Graphical User interface Screen from which all other screens can be accessed from.

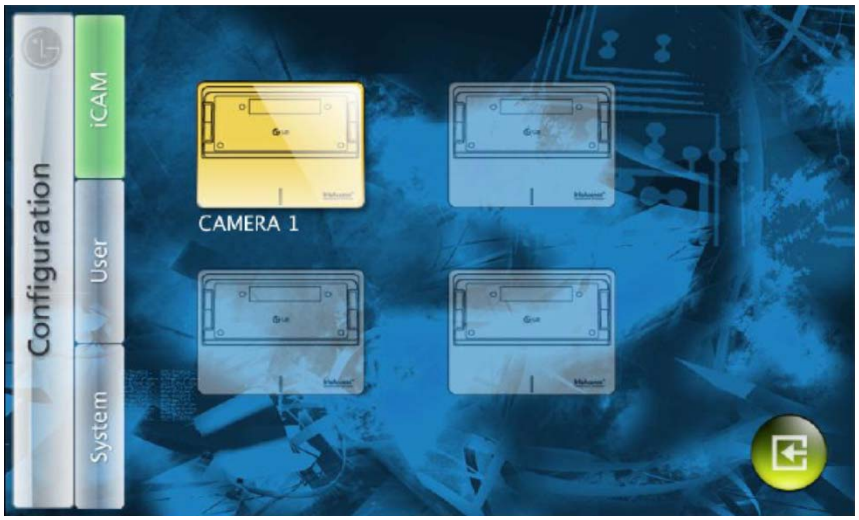
Enrollment Screen: An area that authorized user or administrator can, when logged in, enroll new users into the iData SoHo Software Database. If using an external card reader with Wiegand input to an iCAM, selecting "Card Only" during enrollment allows the user to bypass iris identification and present card only as an option of convenience (optional).



Report Screen: Allows authorized users and administrators the ability to perform a simple queries to the database system without having to use the Web-Access Back-office interface from a stand-alone PC. Enabling the ability to search by persons name, or to specify a date range to gather a listing of reporting information that will be displayed on the screen.

User Configuration: Designed to allow an administrator or authorized user the ability to change user data relating to Access Rights, Edit general information such as first and/or last name, as well as rights access privileges within the system without having to use the Web-Access utility.

iCAM Configuration Screen: Created to allow an authorized user or administrator the ability to add, delete or modify iCAM information directly from the IrisAccess Panel PC.



DHCP IP address Information: When Dynamic IP addressing is enabled for the Panel PC, you modify the settings and/or locate the assigned IP address that the Panel was given by your DHCP Server by logging into the panel as Administrator or a user with Operator rights privileges and going to: Config > System > IP address. The IP address is displayed at the bottom left of the Screen.

4.1 iData SoHo WebAccess Interface

Your SoHo Panel PC is designed to work intuitively when in front of the Panel PC. Although a multitude of configurations and options are available through this interface, an iData SoHo Web access interface utility for administrative use is available.

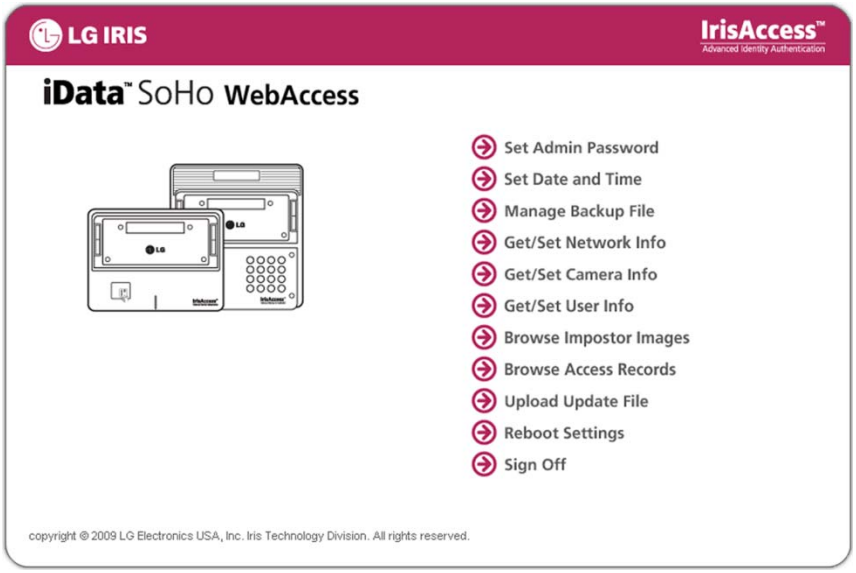
The iData Web Access Interface for your SoHo panel PC is accessible directly through an internet browser that is connected to the same network as your SoHo system.

Accessing the WebAccess Interface: From a PC with an internet browser connected to the network (that the IrisAccess Panel is on), type the IP address of the panel PC. For example, if the IP address of a panel PC was 192.168.5.250 you would access the WebAccess interface by typing http://192.168.5.250 from an internet browser.

IMPORTANT: THE SYSTEM IS CASE SENSITIVE WHEN ENTERING IN YOUR LOGIN CREDENTIALS. BY DEFAULT ALL PASSWORD LETTERS ARE UPPER-CASE.

To login, the User ID required when prompted is Administrator. The Password is the same password that you have created when originally setting up the Panel PC out of the box (upper-case letters needed).

Once you have connected to the iData Web Interface of the Panel PC, a wide variety of in depth setting configurations, information, and options become available to further resource your system.

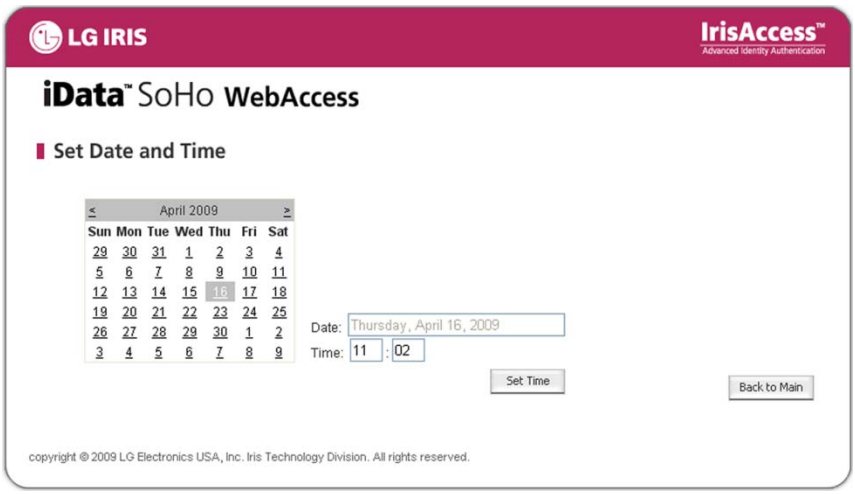


iData Web Options: Once you have accessed the Back Office of the Panel PC, configurations such as date and time settings, changing of administrator password, creating and restoring backup files, Getting network settings, User information, browsing of access records, and managing custom images, are available for you to help further utilize and configure your SoHo system.

Below you will find a breakdown of the available options currently available when using the iData Web interface.

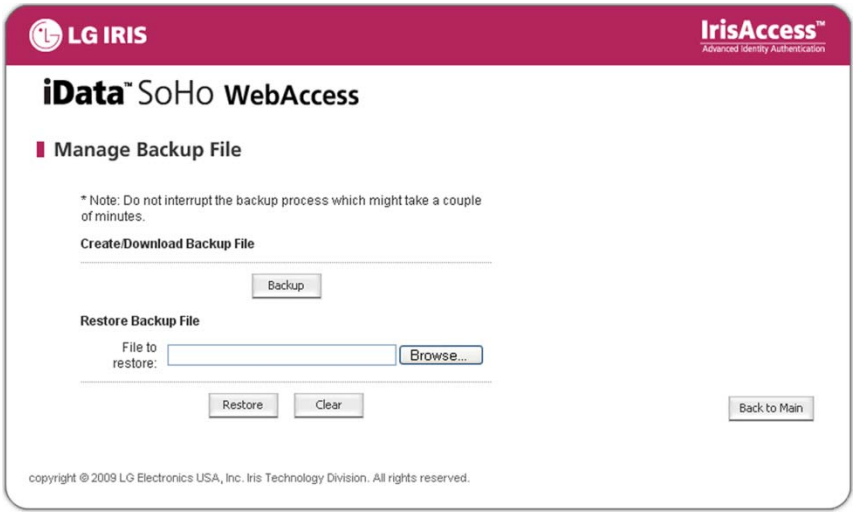
Change Username/Password: Provides the administrator or rights authorized user the ability to change Username and Password settings currently existing in the system.

Set Date and Time: Provides the administrator or rights authorized user the ability to change the Date and Time of the System.



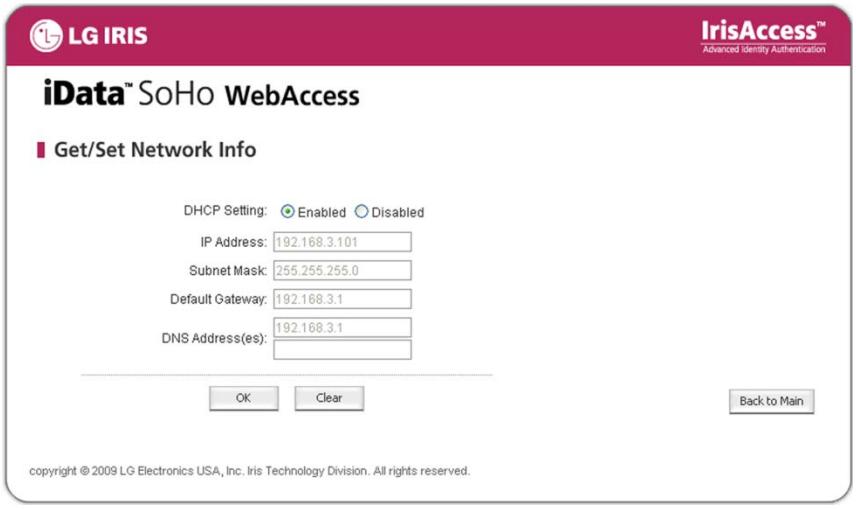
Create Backup File: Provides the administrator or rights authorized user the ability to backup the database of enrolled users and access log data. Note: Do not disrupt the backup process while running as this process can take several minutes.

Manage Backup File: Provides the administrator or rights authorized user/operator the ability to manage the database of enrolled users and access log data. From this screen you can create and/or restore a backup file already created by the iData SoHo WebAccess.



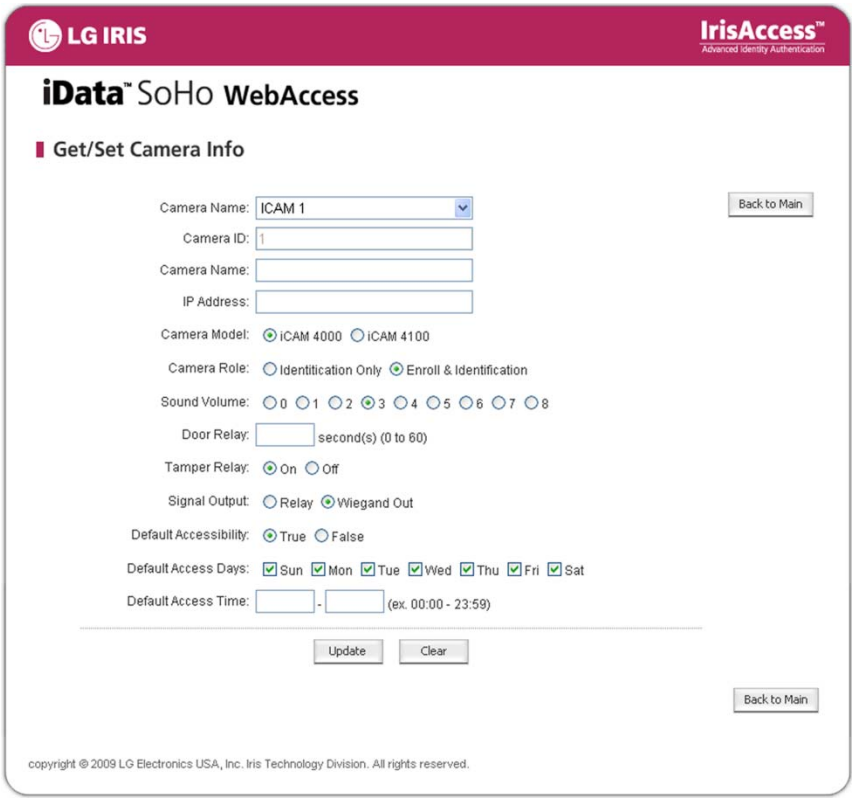
Restore Backup File: Provides the administrator or rights authorized user the ability to restore a backup file already created by the iData SoHo WebAccess.

Get/Set Network Info: Provides the administrator or rights authorized user the ability to get detailed information on the IP settings of the SoHo Panel PC connected on the network. From this location you can set IP address information and network protocol based information.

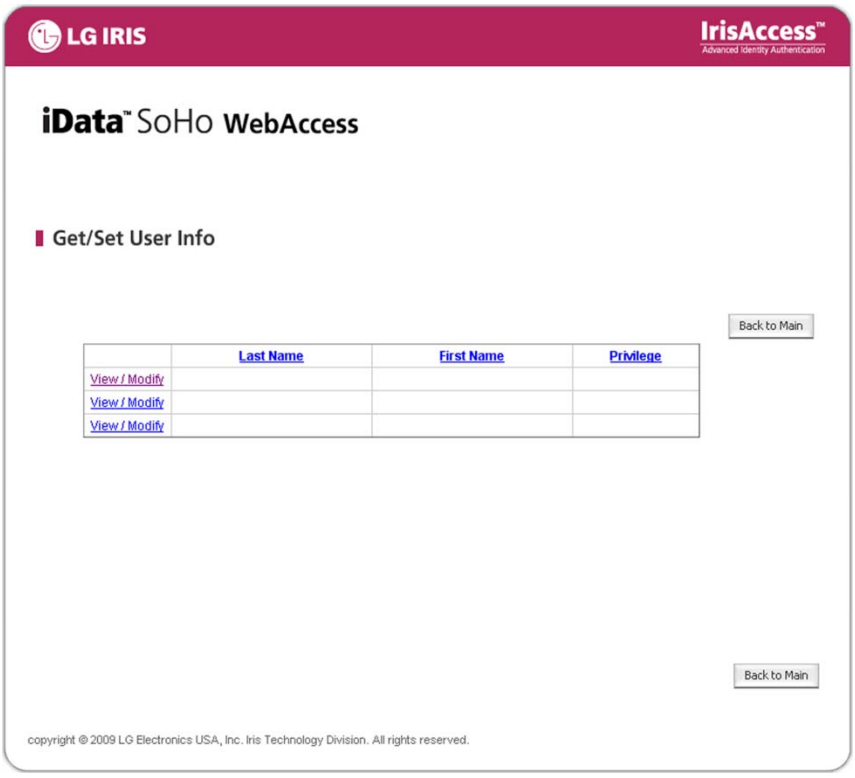


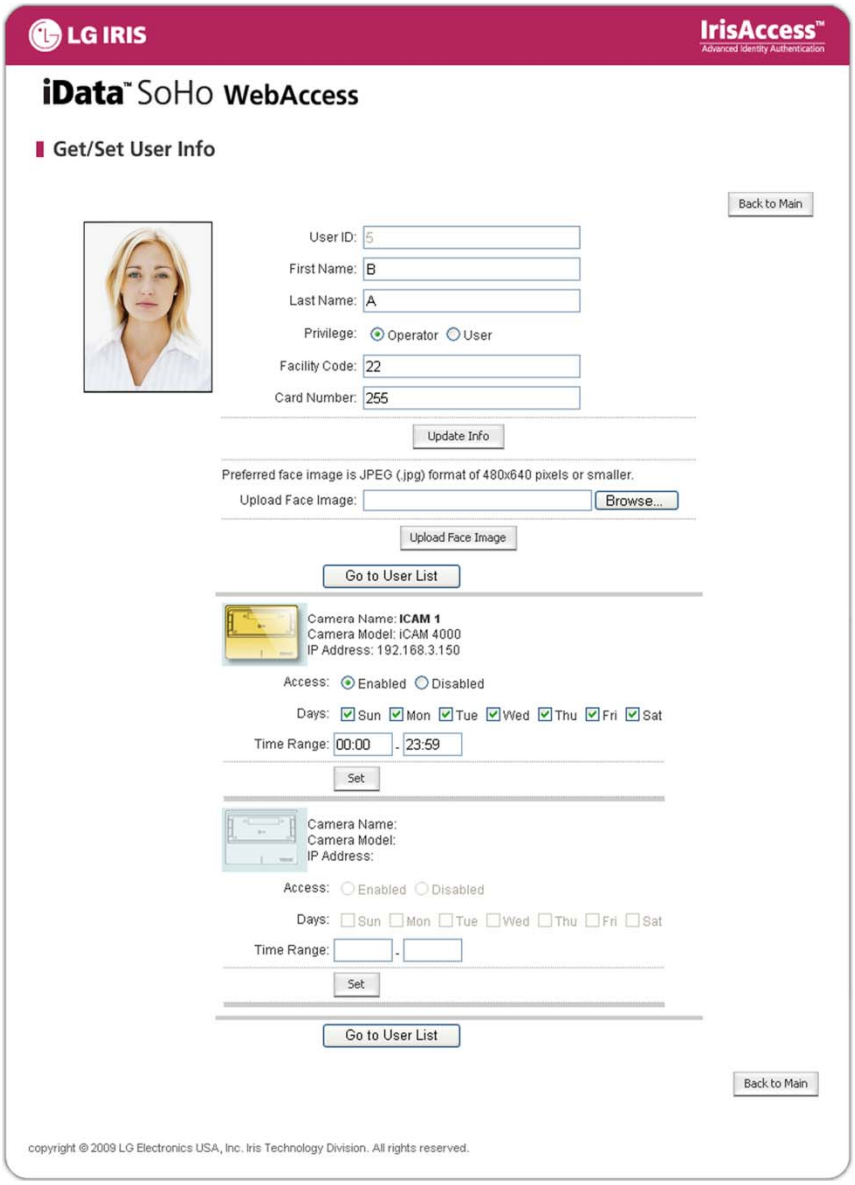
Get/Set Camera Info: Provides the administrator or rights authorized user the ability to enter iCAM4000 Camera data into the system after the initial configuration settings of the iCAM have been performed. From

this location you can also modify detailed information related to identification such as camera role, sound volume, Door Relay timing (when applicable), Tamper relay, and access time configuration.

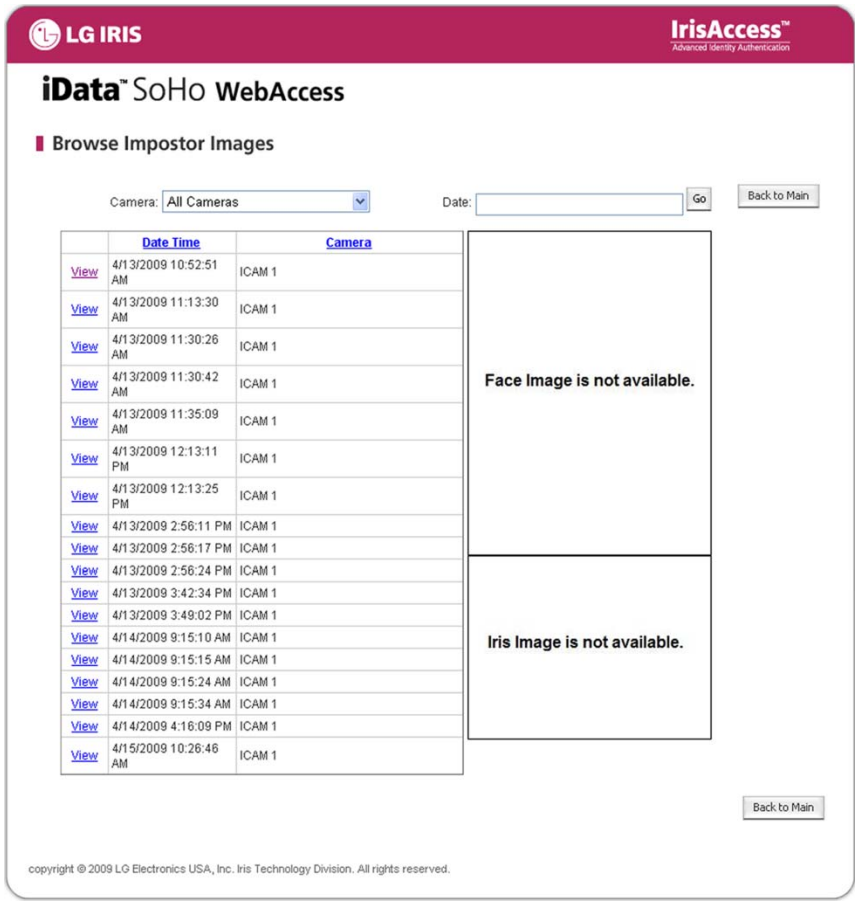


Get/Set User Info: Provides the administrator or rights authorized user the ability to create or modify specific customer information, access rights, and details specific to the enrolled user. From this location you can specify exactly what right access an enrolled user will be provided.

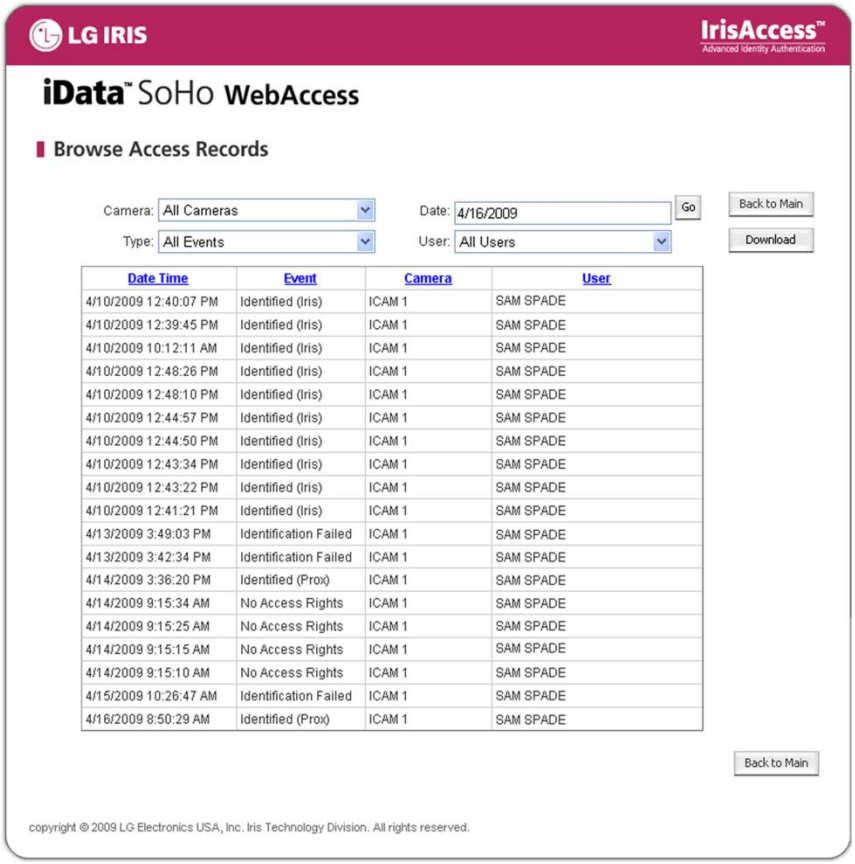

LG IRIS
IrisAccess
Advanced Identity Authentication
iData SoHo WebAccess
Get/Set User Info
Back to Main
Last Name
First Name
Privilege
View / Modify
View / Modify
View / Modify
Back to Main
copyright © 2009 LG Electronics USA, Inc. Iris Technology Division. All rights reserved.



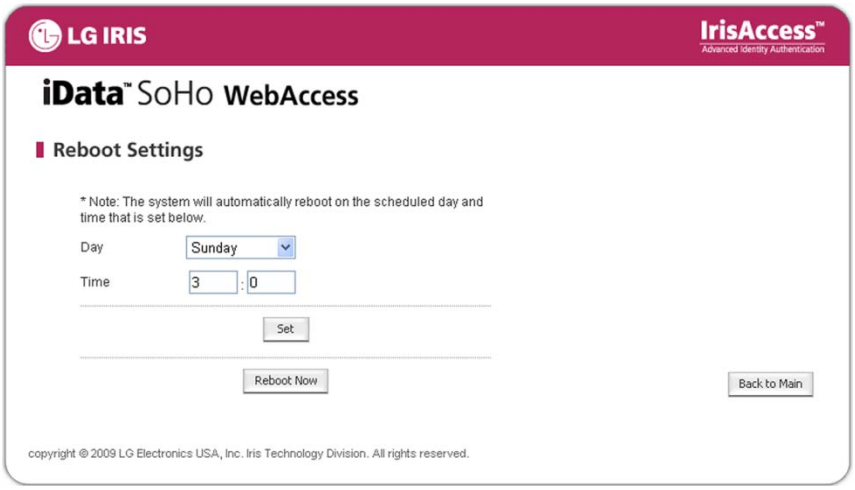
Browse Imposter Images: Provides the administrator or rights authorized user the ability to view a log listing of non-enrolled or authorized attempted users of one or more iCAM4000 camera units. From this location, it is possible when applicable to view an image of the unauthorized user, provided with a time and date stamp, and with which iCAM camera units were attempted to gain access.



Browse Access Records: Provides the administrator or rights authorized user the ability to run log reports of access information registered by the system. From this location it is possible to query the system by date, specific user, camera, and event type.



Reboot Settings: The Reboot Settings screen Provides an Automatic reboot of the panel PC that can be scheduled for a specific day and time by the administrator. This reboot is a required feature in the system, used for maintenance purposes that allows for optimal system performance and efficiency. It is recommended to have the reboot scheduled for a day and time that the system is most likely to be idle. A reboot now option is also available from this screen to allow for immediate rebooting of the panel PC.



5. Troubleshooting

In the event that an error occurs with your system, installation or its functionality, please review the Frequently Asked Questions section below for assistance with finding answers to common issues.

If your issue persists, locate the Technical support section in this document for assistance in resolving questions and concerns.

5.1 FAQs

Please read below for commonly asked questions and answers for your Iris ID SoHo Product

Q: Why does my Panel PC sometimes "beep"?:

A: When the Panel PC is unable to connect to a programmed iCAM, the Panel will may beep every 30 seconds until network communication is restored.

Q: Why does my Panel show Camera unit icons at the bottom right of the Initial Panel Screen?:

A: When the Panel PC is unable to connect to a programmed iCAM, the Panel will display in red at the bottom portion of the Panel PC and icon indicating that no connection to that camera unit can be made. Grey icons may also appear indicating that iCAM units have not been configured for the Panel through its configuration settings. Check your physical network cabling and network configuration settings of the iCAM and Panel PC to attempt to resolve this issue. Additionally, when these icons appear as red this shows the iCAM tamper has been initialized.

Q: Is my Iris ID SoHo Product an Alarm system?

A: No. The Iris ID SoHo Product suite is a biometric enabled, Iris recognition access control device. This product is not designed to be an alarm system, however can integrate and work well with most standard active and passive monitored alarm systems.

Q: Why can I not connect to the iCAM4000 Web interface screen to change its IP?

A: The iCAM4000 has a default IP address of 192.168.5.100 that can be accessed through your computers Internet Browser. In order to connect to the IP address of the ICAM your computer's network IP address information must have a similar scheme to the iCAM4000. Make sure you IP address has been modified appropriately.

Q: If I do not have a switch, how can I setup my system?

A: It is recommended that a switch be installed when configuring and when using your system. However, you can use a crossover CAT-5 cable as an alternative if necessary (and only if using one iCAM with your Panel PC). For you to use this method, initially connect the iCAM to your stand –alone IBM compatible PC directly with the crossover cable and continue to follow setup steps for your iCAM4000. Once setup of the iCAM has been completed successfully, connect your crossover cable directly from your iCAM4000 to your Panel PC.

Q: Does the Iris ID SoHo come with a system to lock and un-lock a door or entryway?

A: No. This and other similar products are not provided or sold by Iris ID, however will function with many 3rd party products.

Q: Where is the best place to locate or mount by SoHo Panel PC?

A: It is recommended that the Panel PC be placed in a location that is located by the interior of the perimeter or door location(s) you wish to limit or restrict access. Keeping the Panel PC in a location that is safe to get to, but out of public visibility is recommended. Also, be sure to keep your panel PC in a temperature controlled environment away from large variations in temperature or areas where the Panel PC can get wet.

Q: Why won't my iCAM4000 power on?

A: The iCAM does not have a power switch. All that is needed for the iCAM to power is the power supply. Verify that you are using the Power Supply that came with your iCAM4000 unit and that it is properly screwed into the iCAM and plugged into a working wall outlet. Once powered, the iCAM will indicate a power/activity light at the bottom center of the unit.

Q: The iCAM4000 is powered on but nothing is happening, why?

A: The iCAM4000 us a Camera based unit that requires the Panel PC to be setup to communicate with your iCAM. First verify that your iCAM is connected to your network via a CAT5 cable. Verify that your Panel PC is ON, and connected to the network, and that the iCAM door unit is configured correctly. Make sure to verify that the iCAM is enabled, and has user's assigned to it.

Q: Trying to initially configure my iCAM4000 for the first time with a stand-alone PC connected directly to the iCAM but it is not working, why?

A: When connecting an iCAM4000 directly to a computer to access the iCAM configuration web utility, you must use a CAT5 Crossover cable. You must also make sure that your computers IP address is set to the same segment as the iCAM (default) of 192.168.5.XXX.

Q: How does the tamper on the iCAM operate?

A: The tamper switch works on a "change of state" once, where as once the iCAM is powered on, the tamper will detect a press or release of the tamper switch as long as the tamper has been depressed in the correct position of the camera unit initially. The tamper alarm at the iCAM is indicated by a single shutter sound, not a continuous beep.

Recognition processes will cease at the iCAM and a message will be sent back to the Iris Server to log the event.

Q: Why can I not get identified if I am enrolled in the system with proper rights access permissions to an iCAM?

A: An iCAM can be selected to work with a relay output or a Wiegand Output. If a Wiegand output is selected for a camera unit and a user has not been enrolled with a proper facility code and Card ID, the system will not allow for rights identification. To correct, modify the users settings and provide the Facility code and Card ID for the user as needed. If this Camera unit does not require Wiegand output, you can modify the iCAM configuration to use a relay instead of Wiegand, and therefore will not require any user setting changes.

Q: What is the Password to login to the Panel PC?

A: The Panel PC is given an IP address by the installer when initially configuring the Panel during installation. This password is not known by Iris ID. Because no standard default password was provided by the factory, you would need to consult the individual(s) who initially configured your Panel, or has since reset the password to gather this information. If you are unable to find the IP address of the Panel PC, contact your authorized vendor or Iris ID electronics so that we may assist in providing further available options to resolve this issue.

Q: How do I re-calibrate the Panel PC touch Panel Screen?

A: The Panel PC is calibrated during initial configuration of the system. Once the Panel has been calibrated using the touch screen it cannot be re-calibrated at a later time. In the event that the calibration was performed improperly, or an issue with the touch screen occurs, contact your authorized vendor or Iris ID electronics so that we may assist in providing further available options to resolve this issue.

Q: My remote camera unit stopped working because the tamper from the camera unit was triggered and now it is not working. How do I correct this?

A: The iCAM4000 uses a change of state tamper trigger. Two tamper buttons are on the unit and if triggered will place the camera unit into a halted state indefinitely. You can verify the tamper alarm has been triggered by looking at the front screen of the Panel PC (a yellow icon on the screen at the bottom right corner). Tamper switches are located in the front, and the other in the back of the iCAM. If the tamper was triggered on one or multiple iCAM units, first make sure to place the camera unit back in the physical state it was in prior to the tamper having been triggered. Once the tamper button is back in its original position your iCAM unit(s) will not work again until a rights authorized operator or administrator logs into the Panel PC and goes to the Config>iCAM area of the software interface. From this location, select the desired iCAM(s) that is not working because of the tamper switch and press the “Reset tamper” button found on the bottom of the screen. If no button appears, make sure that you have selected the correct remote unit. If these steps have been performed and the camera unit is still not working, make sure to check for any network connection issues. Properly reboot the camera unit if the issue persists to attempt to resolve the issue.

6. Technical Support

Additional Information and Technical assistance is available on the Iris ID’s support web site at www.irisid.com, click on Support & Service then Technical Support.