Iris ID

ICU7000 User Guide

-Identity Controller Unit for use with iCAM7000 series

Ver 1.00.00

December 2012

ICU7000 User Guide – Identity Controller Unit for use with iCAM7000 series

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

Document Number: IRISIDICU7000-01-0100-1231

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 fourth 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 Overview

The ICU7000 is the latest generation of Identity Controller Unit designed for use with the iCAM7000 camera series only. This product is to be a direct replacement to the successful ICU4000, and also to provide enhanced features such as an internal configuration web-based interface, flexibility, and compatibility with current and future Iris ID software offerings. Each ICU7000 provides a single channel which can control a single iCAM7000 series unit. The configuration web interface for the ICU7000 does not require installed software since it is accessible directly through an internet browser connected to the iCAM network. The ICU7000 has been specifically designed for use with the iData IrisAccess™ software suite 3.07.08 (and above).

This document will not only provide hardware features and functions, but also assist in demonstrating the purpose and usage of many of the products features and available configurable options.

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.

This Guide is intended to be used as a reference for your product and its accessories. This document includes detailed background on the product technology, as well as general configuration options to assist in setup of the ICU7000 device.

This guide provides detailed and specific information that is catered to the trained installer with an existing base of knowledge in; computer usage, network configuration, low voltage electrical wiring, physical installation techniques, and access control systems or electronic control devices (as required).

Installation and integration of this product does require some level of knowledge of computers using the Microsoft Windows operating system and Ethernet network wiring and configuration.

If integration with access control systems or other electronic control devices is required, intimate knowledge of the wiring and configuration of such systems is the responsibility of the installer/integrator. Iris ID can only provide examples and information as to the usage, configuration, and general operation of the interfaces available in our products. Any wiring or integration examples described in this document, the Iris ID web site, other Iris ID documentation, or from Iris ID representatives are only for use as a basic reference and in no way implies that the examples/suggestions given comply with the codes and requirements of the country/county/state/city/or local authorizes in which this equipment is installed.

1.3 Reference Materials

In addition to this guide, your software CD should contain an "ICU7000 Hardware guide, IrisAccess EAC User Guide, iCAM7000 User Manual and additional documentation designed to provide detailed information and options of your product.

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

2. Minimum ICU7000 Configuration Equipment Requirements

Required Equipment (not included) for use with ICU7000

- Power Source
  - 12-24 VDC +/- 10% / Minimum 24W (12VDC @ 2AMPS) (Measured at ICU unit)
  - Uninterruptable Power Supply (strongly recommended)

- Network
  - Ethernet Wiring CAT5e Ethernet Cabling (or better)
  - Ethernet Switch

- Software
  - Required compatible IrisAccess iData EAC software v.3.07.08 (or above).

Minimum Computer requirements (for Initial Configuration) of ICU 7000

- Windows 2000, XP Pro, Server 2003, Vista or Window 7 Operating System
- Internet Browser (such as Internet Explorer)
- Pentium 4 compatible 1.6GHz Processor
- 512MB Memory (RAM)
- Ethernet Port (100 Mbps recommended)
- Mouse, SVGA Monitor, Keyboard

3. What's In the Box

3.1 Items included

- ICU7000 Series Camera unit
- Hardware Guide
- Grommet
- Keys (x2)

3.2 Required Equipment (<u>not</u> included)

Power Source

- Power supply - 12-24 VDC +/- 10% / Minimum 24W (12VDC @ 2AMPS) (Measured at ICU7000)
- Uninterruptable Power Supply (strongly recommended)

Network

- Ethernet Wiring -> CAT5e Ethernet Cabling (or better)
- Ethernet Switch

Software

- iData EAC Software (version 3.07.08 or above)

4. ICU7000 Hardware Information

The ICU7000 is available currently as one model option only:

- The ICU7000 contains one channel for controlling a single iCAM7000 series device.
- The ICU7000 contains a single Wiegand output, 2 relays, and 4 GPIOs.

All ICU7000 units contain an intuitive and easy to operate user interface. The ICU7000 is compatible with iCAM7000 series units in option 1 mode for use with iData EAC software only.

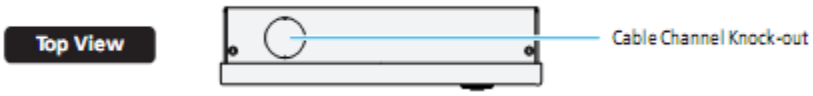
The ICU7000 also contain selectable use tamper switch, audible IP announcement voice prompt, factory default resets, and a dedicated RTC battery for time management.

4.1 ICU7000 - General Specifications:

ICU7000 Model specifications:

Dimension (W x H x D)	8.66” x 9.65” x 2.0” (220mm x 245mm x 51mm)
Weight	3.0lbs (1.4kg)
Power Input / Consumption	12-24VDC, 2.0Amps @ 12VDC/24W
Indication	External Green LED for Power Indication
Operating Temperature	32 °F ~ 122°F (0°C ~ 50°C)
Storage Temperature	-4°F ~ 203°F (-20°C ~ 95°C)
Humidity	Up to 90% non-condensing
Communications	Ethernet (LAN, WAN)
Inputs/Outputs	Wiegand Out, Dry Contact Relay x 2, Programmable GPIO x 4, RS422
Certifications	CE, FCC, KCC, UL294
Equipment Supplied with ICU7000	• Grommet • Keys (x2) • Hardware Guide

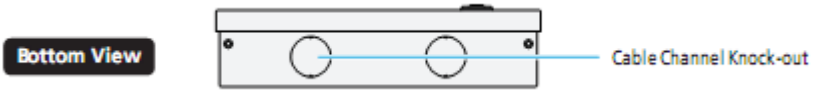
4.2 ICU7000 – Top View



4.3 ICU7000 - Front View

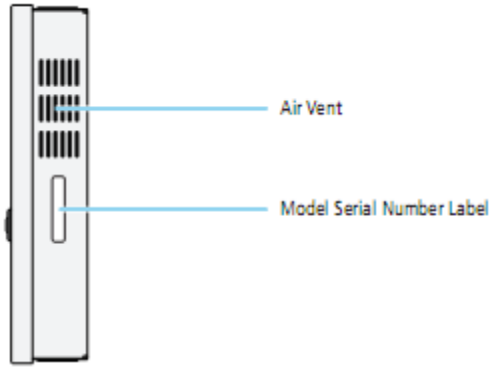
1. **Power Light Indicator –** An LED indicator light that will turn green when the unit is powered on.
2. **Case Lock** – A locking mechanism that allows the provided keys to lock and unlock the panel door.

4.4 ICU7000 – Bottom View



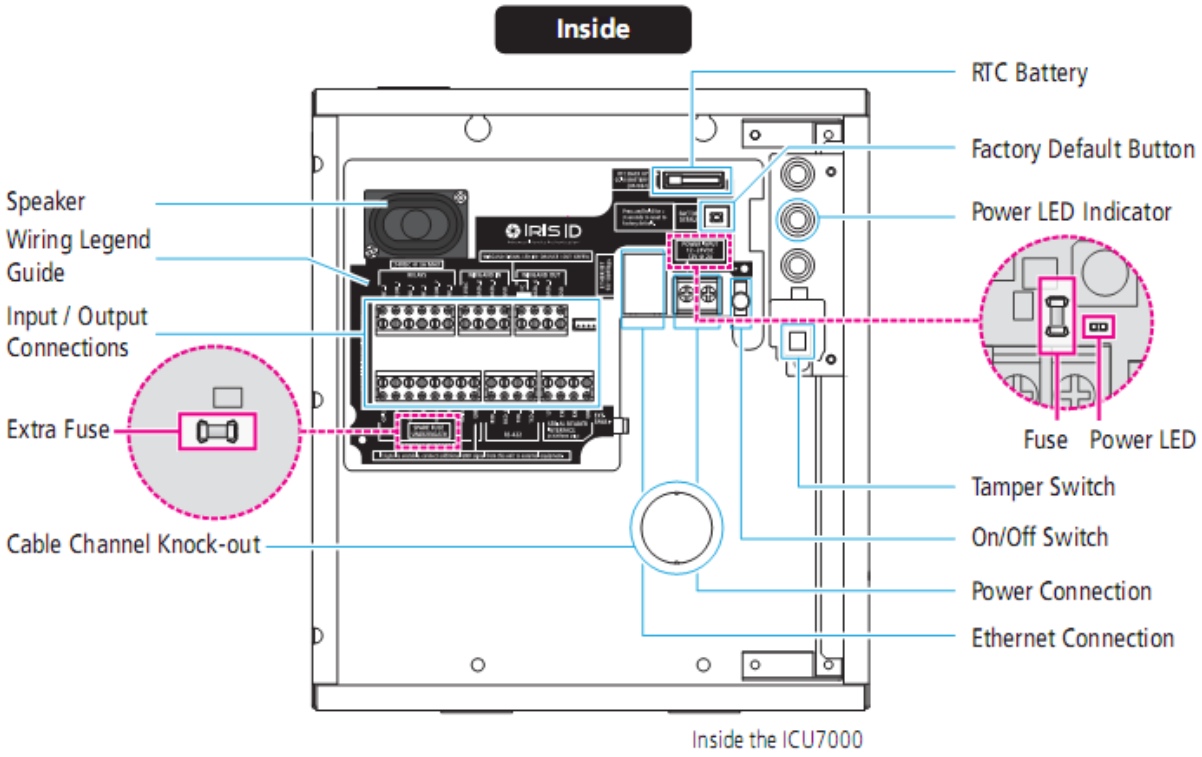
1. **Cable Channel Knock-out** – 2 holes located at the bottom of the unit that can be removed for the purposes of installation and ease of wire management, etc.

4.5 ICU7000 - Side View



1. **Air Vent** – Slits within the case that allow the unit to breath and recycle air. Do not block these vents.
2. **Model Serial Number Label** – A sticker label placed on the side of each unit that indicates the exact model type and serial number.

4.6 ICU7000 - Inside View



Inside the ICU7000

1. **Speaker** – Provides for audible tones and announcements such as tamper alarm and IP address settings.
2. **Wiring Legend Guide** – A guide located inside of the ICU7000 unit. This guide provides detail of the internal input/output connections and wiring needs for various options available for use with the ICU7000 controller unit.
3. **Input / Output Connections** – Internal connections providing Relays, Wiegand Input, Wiegand output, GPI/O, RS422 Output, and external speaker output.
4. **Extra Fuse** – Located behind the wiring legend guide, an extra fuse is provided in the event that replacement of a fuse is needed.
5. **Cable Channel knock-out** – An opening located in the unit that can be removed for the purposes of installation and ease of wire management, etc.
6. **RTC Battery** – Real-Time Clock Battery used for maintaining and accurate date and date time-clock on the unit. (Initial time and date may be set by the controlling software device.)
7. **Factory Default Button** – Allows the unit to be restored back to the default factory setting of IP address and ICU7000 login credential (when unit is powered on), or can restore back to complete factory defaults for all settings and iCAM firmware when button is pressed for at least 5 seconds while unit is powering on.
8. **Power LED Indicator** – Indicated that the unit is powered on and functioning correctly.
9. **Fuse** – Protects the ICU7000 circuitry from excessive current draw or incorrect polarity.
10. **Tamper Switch** - Two switches found in the front and back of the unit. Operation of the tamper switch is software selectable.
11. **On/Off Switch** – A switch to toggle the unit from the ON position (Up) to the OFF position (OFF). When this switch is in the down position (OFF), flip the switch upward to turn ON the unit.
12. **Power Connection** – Consists of 2 screw down connections. These connections are positive and ground. (12VDC~ 24VDC input – 12VDC @ 2A.)

13. **Ethernet Connection** – An RJ-45 connection allowing for CAT-5e, CAT-6, CAT-6e wire connections at a speed of up to 100 MBPS.

5. Compatibility and Usage

Follow the below requirements for installation and usage compatibility:

- The ICU7000 Series control unit is compatible with iCAM7000 series camera units only. An iCAM7000 or iCAM7100 series model is required for use with ICU7000.
- The iCAM7000 must be set to operational mode: Option 1 for communication compatibility with the ICU7000. iCAM firmware version 7.07.03 (or above) is required for use with an ICU7000.
- The use of iData EAC software is required with the ICU7000 product. . However, the configuration web interface for the ICU does not require installed software since it is accessible directly through an Internet browser connected to the iCAM network. Therefore the ICU7000 can be configured independent of the required EAC software for usage.

6. Installation Guidelines

Before installing your ICU7000 controller unit, review the recommended installation guidelines. These guidelines provide information on the recommended mounting information, general wiring information, and electrical/current requirements.

- The ICU7000 should be installed in a location that will discourage tampering with the unit, but is easily accessible for maintenance (such as a locked room, utility closet, or other secure locations), preferably within the restricted area.
- This installation location requires power and a network communication to the IrisServer and iCAM7000 series unit(s). If used with an access control panel, the ICU can reside close to the access panel.
- This installation location requires that the ICU be placed in the same physical building as the iCAM unit that it will be controlling. All system components including the Ethernet network should be powered through an Uninterruptible Power Supply (UPS) whenever possible. The UPS should provide power line filtering as well as power back-up operation.
- The ICU7000 is designed for surface mounting only.
- Each IrisAccess® system component on the Ethernet network system must have a unique assigned IP Address.

6.1 General Wiring and Electrical/Current Requirements

The iCAM7000 Series of camera units require at least the following wires:

- Ethernet network wiring to connect with the network switch for communication.
  - Cable Type: CAT5e Cable - 8 conductors with RJ-45 connectors.
  - Maximum Length: 100 meters (328 feet) between network devices.

  ****Note**: For systems consisting of only an ICU and an iCAM7000, an Ethernet cross-over cable may be used.*

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. MAXIMUM CAT-5e CABLE LENGTH MUST NOT EXCEED IEEE STANDARDS OF 328 FEET (~100 METERS)

- Power Supply and Wiring:

  Use of a stable power supply and proper gauge wire is required. Wire length voltage drop must be accounted for in order to maintain the correct power at the ICU7000 unit (with ICU7000 connected).

  For example; with a 12VDC source and 16AWG (1.0mm2) copper wire, the maximum distance is 71.5 Feet (21 Meters). If a longer power wire distance is required, it is recommended that a 24VDC power source be used. Voltages within the range of 12VDC and 24VDC are acceptable as long as 24W of power is supplied to each ICU7000 unit. (e.g. 12VDC @ 2AMPS = 24Watts OR 24VDC @ 1AMP = 24Watts).

  - Power Requirements at the iCAM:
    - 12-24VDC +/- 10% / Minimum 24W (12VDC @ 2AMPS)
  - Power Wiring:
    - 16 AWG (1.31mm^2) Stranded Copper Wire or better.

    ***DISCLAIMER:** Change in wire gauge or material will affect the voltage drop calculation. Please refer to industry standard methods for voltage drop calculations. These calculations must be based on the wire length and materials that are required (to be used) by the installation location. Refer to local safety and electrical codes for any and all installation requirements.

    ***IMPORTANT:** To account for the voltage drop over a wire length, the power supply and wire distance limitations must be adhered to for proper operation of the ICU7000 unit. Listed below is the maximum wire distance. It is always recommended to keep the wire distance 10% shorter than this maximum length to assure proper voltage at the ICU.

    12 VDC Supply (2 AMPS):
    - Power Supply (at source) = 12.0 VDC
    - Wire Gauge = 16AWG (1.31mm^2)
    - Maximum Wire Length = 21 meters (71.5 feet)
    - Power Supplied to iCAM = 10.8 VDC (Minimum Allowed)

    24 VDC Supply (1 AMP):
    - Power Supply (at source) = 24.0 VDC
    - Wire Gauge = 16AWG (1.31mm^2)
    - Maximum Wire Length = 478 meters (1570 feet)
    - Power Supplied to iCAM = 10.8 VDC (Minimum Allowed)

IMPORTANT: THE CORRECT AMOUNT OF POWER MUST BE SUPPLIED TO THIS UNIT. ANY OVER OR UNDER VOLTAGE APPLIED TO THIS PRODUCT MAY CAUSE PERMANENT DAMAGE AND VOID THE WARRANTY.

- Other Wiring Used with ICU:

  - *Relay wiring:*
    - Typically 16 AWG (1.31mm^2) Stranded Copper Wire or better.
    - Relay wiring requirements are determined by the device/system that the relay is switching power to.

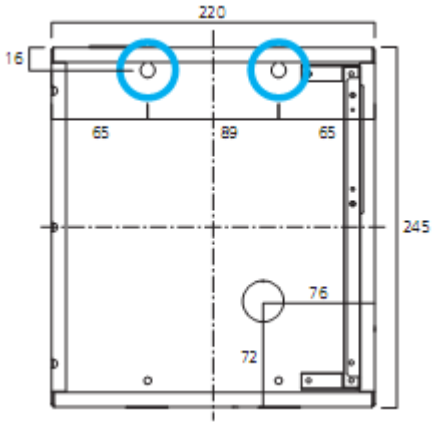
  - *Wiegand wiring:*
    - 16 AWG (1.31mm^2) Stranded Copper Wire or better.
    - 3 Conductors (Data 1, Data 0, Ground).
    - Maximum Length: 152 Meters (500 Feet).

- *RS422 wiring:*
  - 22 AWG (0 .33mm²) Solid Copper – Twisted Pair Wire or better.
  - 4 Conductors (RxD -, RxD +, TxD -, TxD +).
  - Maximum Length: 304 Meters (1000 Feet).

- *GPI wiring:*
  - 16 AWG (1.31mm²) Stranded Copper Wire or better.
  - 2 Conductors (Input, Ground).
  - Maximum Length: 60 Meters (190 Feet).

- *External Speaker*
  - 22 AWG (0 .33mm²) Stranded Copper – Shielded Wire or better.
  - 3 Conductors (Audio, Audio Ground, Shield), 3.5mm Mono Audio Jack Connector (at iCAM end) – **Note:** 3.5mm Stereo Audio Jack Connector can also be used.
  - Maximum Length: 15.2 Meters (50 Feet).

6.2 Mounting the ICU7000



Mounting

1. Using the key(s) provided, unlock the enclosure.
2. Determine the point of entry into the enclosure for each cable. Remove the appropriate 2.8cm (1.1") knockouts or if a knockout is not available at the desired location, drill holes using a hole-punch commonly used for penetrating steel enclosures. Protect internal electronics from metal filings.
3. Install the supplied wire grommet or another connector to protect the wires.
4. Hold the enclosure in the desired location on the mounting surface using it as a template; mark the location of installation holes. There are two types of screw holes, the diameter of one type is 10m (0.39 inch) and the other type is 5mm (0.20 inch).
5. Drill or punch holes in the mounting surface on the marks.
6. Insert the cables into the enclosure.
7. Mount the enclosure on the wall using appropriate hardware.

***Note**: The ICU7000 is designed for surface mounting only.*

7. The ICU7000 Configuration Interface

From a computer with an Internet browser (and connected to the network in which the iICU7000 unit is connected), type the IP address of the ICU. For example, if the IP address of an ICU7000 is 192.168.5.200 (default IP), access the configuration web interface by typing http://192.168.5.200 in the Internet browser line. *(An Internet connection is not required to access or use the ICU700 web configuration. Only a network connection between the computer and ICU is required.)*

Note: The IP address of the ICU7000 can be audibly announced by pressing the Factory Default button twice consecutively (located on the ICU main board).

To login, the User ID required when prompted is **ICU7000**. The Password is **iris7000**.

IMPORTANT: THE SYSTEM IS CASE SENSITIVE WHEN ENTERING IN YOUR LOGIN CREDENTIALS.

Once you have connected to the Web Configuration Interface of the ICU7000, a wide variety of in depth setting configurations, information, and options become available to further resource your system.

** Note: The IP Address of each ICU7000 must be configured individually. Do not connect more than one un-configured ICU to the network at any time to avoid IP Address conflicts. Standard web browsers (ex. Internet Explorer) can be used to configure the ICU7000.*

7.1 Initial Configuration Setup of ICU7000 Series

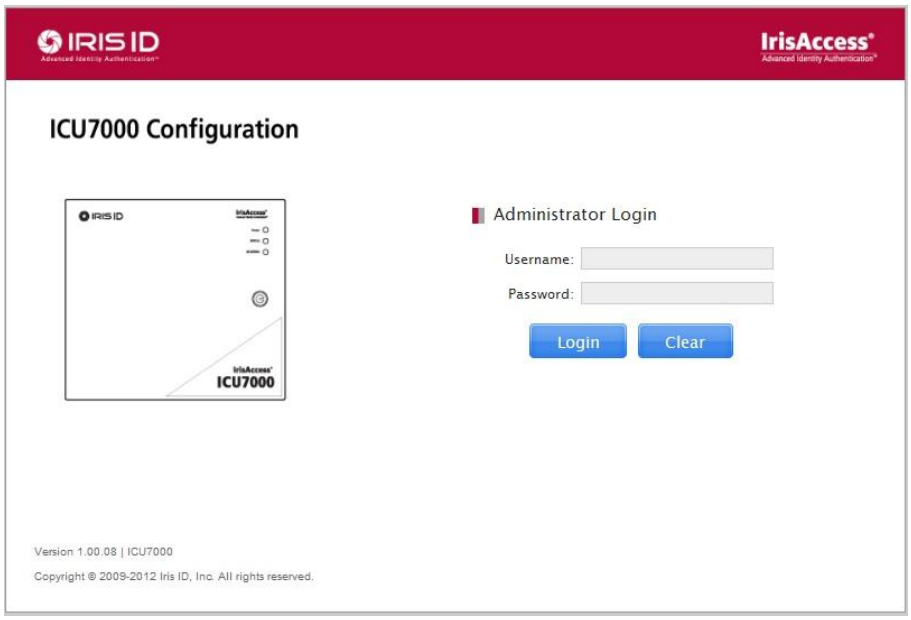
The IP Address of each ICU must be changed individually. Do not connect more than one un-configured ICU7000 to the network at any one time to avoid IP Address conflicts. Any computer with a web browser (ex. Internet Explorer) can be used to configure the ICU7000. (Default IP settings used as reference.)

IMPORTANT*: If a Windows Warning screen appears as displayed in the following image, select the check box and press "Run" to view the webpage correctly.*

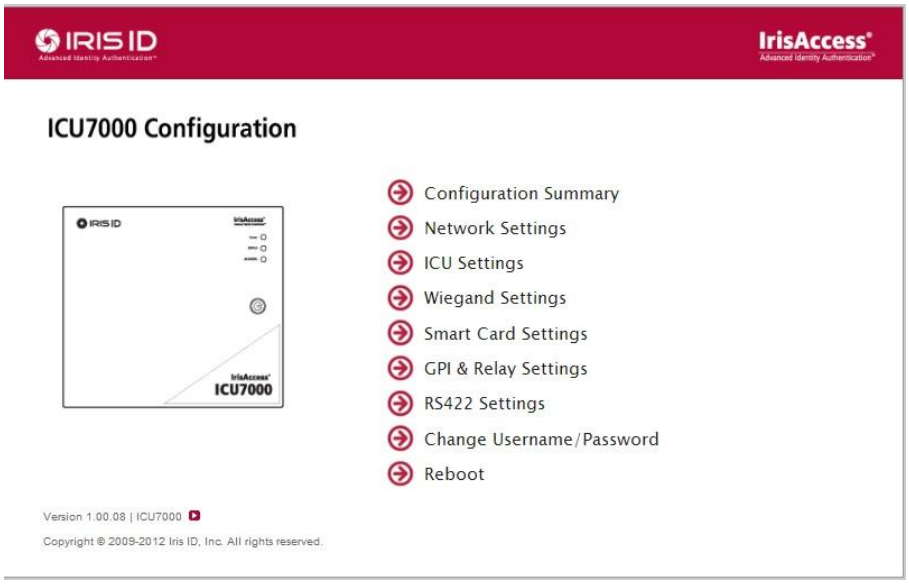
7.2 ICU7000 Configuration Setup

Setting the IP address and Security ID / Server IP

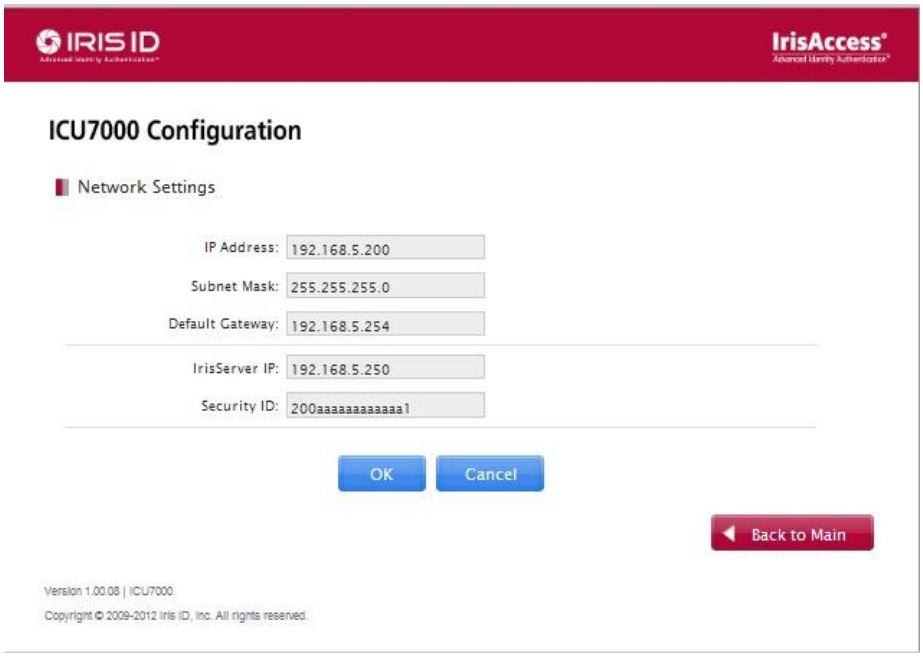
1. Set the computer to the static IP of 192.168.5.250 - subnet 255.255.255.0
2. Open the web browser and enter http://192.168.5.200 in the address bar then press ENTER. The ICU700 Configuration login screen will appear.
3. Enter the default Username: **ICU7000** and Password: **iris7000** (both are case sensitive)



4. The ICU7000 Configuration Main Menu will appear.



5. Select Network Settings.



6. Enter the new IP address for the ICU (default = 192.168.5.200)
7. Enter the new Subnet Mask for the iCAM (default = 255.255.255.0)
8. Enter the new Default Gateway for the iCAM. (default = 192.168.5.254)
9. Enter the IrisServer IP address. (This is the IP address that the iData EAC software is running on.)
10. Enter a unique Security ID for the ICU channel. (Security ID's must contain 16 characters.)
11. Click OK to save changes and to open network settings verify screen.

***Note**: The ICU may require a reboot. When prompted, press OK and enter the required username and password authentication (*default Username: **ICU7000** and Password: **iris7000**) *to reboot the ICU and apply the setting changes.*

The ICU7000 FACTORY DEFAULT is located on the ICU7000 interface board below the RTC battery. While the unit is in the powered on state, pressing and holding the FACTORY DEFAULT button for at least 5 seconds will reset the ICU IP Address to the factory default (192.168.5.200) and the login ID credentials for the ICU7000 (User ID = ICU7000 / Password = iris7000).

If the FACTORY DEFAULT button is pressed for at least 5 seconds while the unit is *being powered on*, the unit will be reset to the original factory default settings – ALL settings will be defaulted and any uploaded data including ICU firmware/software updates may be reverted back to the original software version that the unit was originally received with.

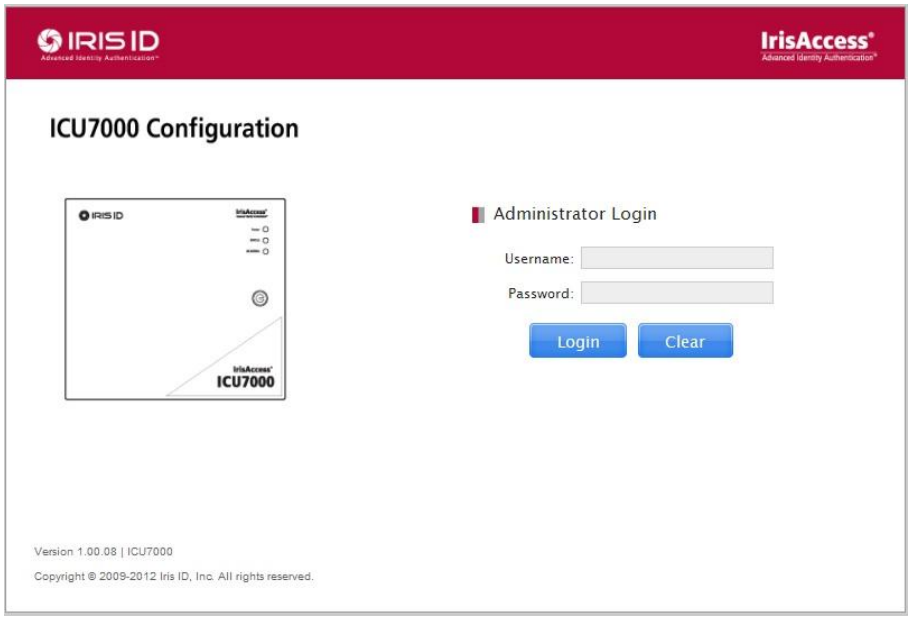
*** Note:** *If the new ICU IP address is still on the same subnet as the computer - After 10 seconds the web browser will resolve to the new IP address and the login screen will appear again.*

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

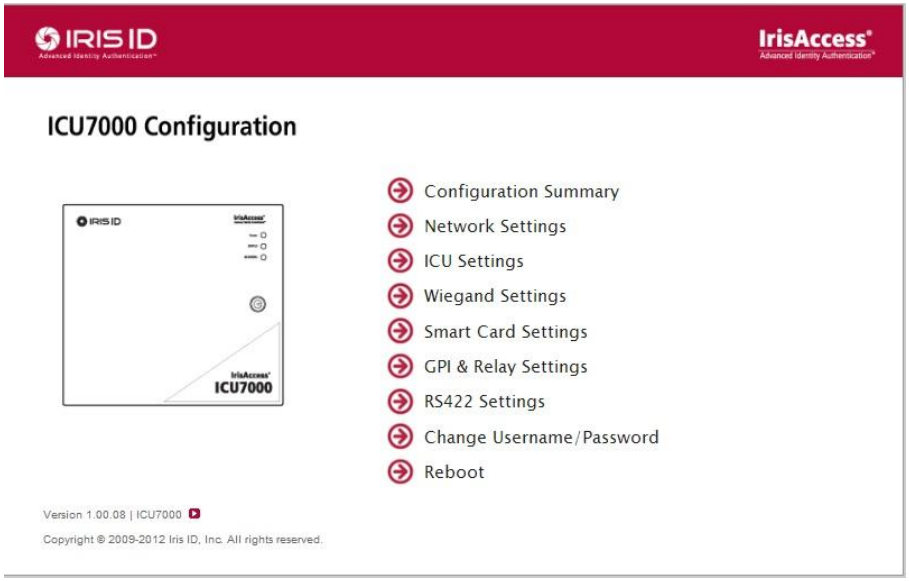
*** Note:** *Pressing the Factory default button two times consecutively will cause the ICU to announce the current configured IP Address of the unit.*

Configuring the Initial ICU settings for use with an ICAM

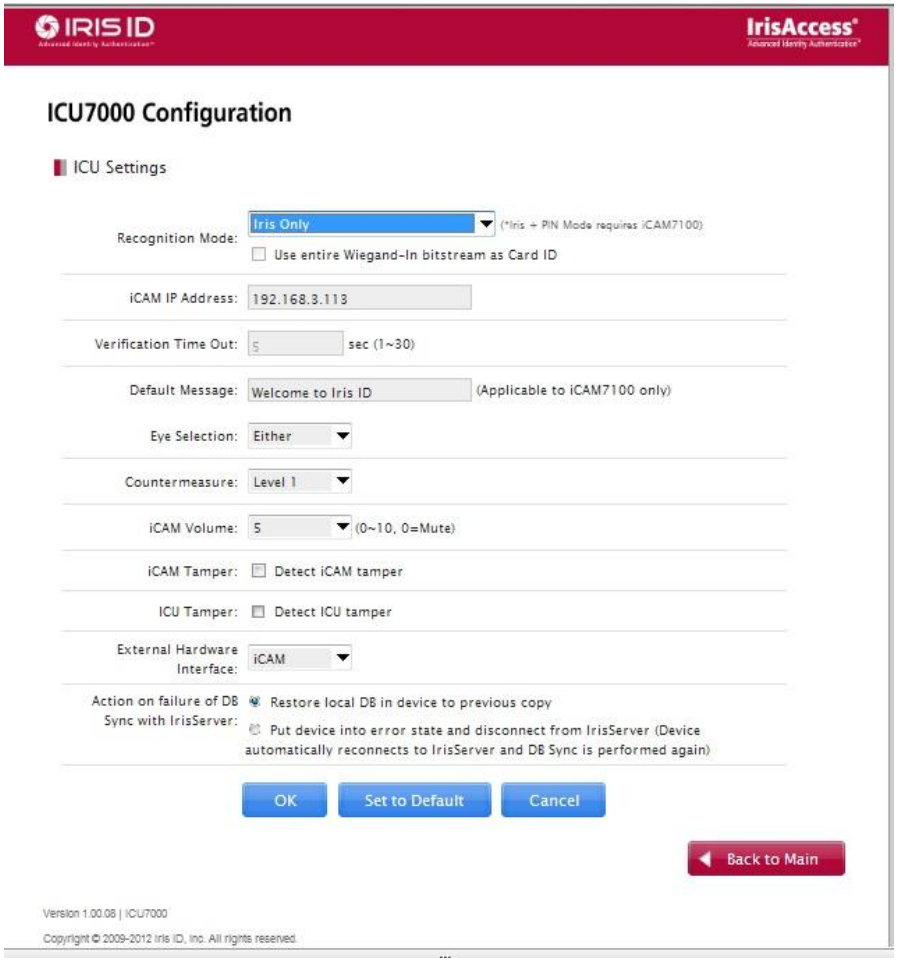
12. Open the web browser and enter ICU IP address in the address bar then press ENTER (http://192.168.5.200). The ICU700 Configuration login screen will appear.
13. Enter the default Username: **ICU7000** and Password: **iris7000** (both are case sensitive)



14. The ICU7000 Configuration Main Menu will appear.



15. Select ICU Settings.



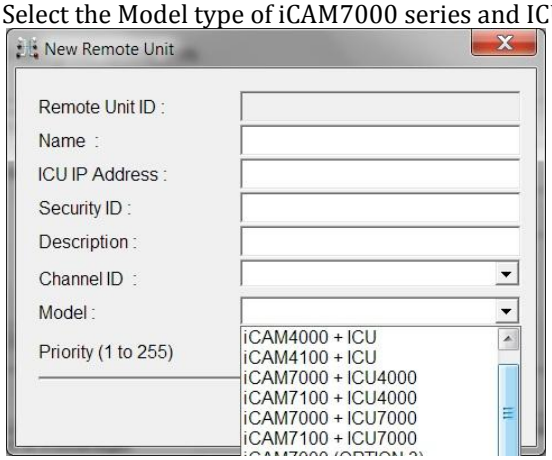
16. Select the Recognition mode to be used from the dropdown box. (Iris Only, Iris + PIN *, Iris + Prox Card, or Iris + Smart Card).
17. Enter the iCAM7000 series IP address that is to be used with this ICU (for this ICU channel 1).
18. Modify the Eye selection, volume, tamper, as needed
19. Modify the External Hardware interface setting to either EIB, or iCAM as needed.
    Note: This setting refers to the wiegand output, and defines whether the wiegand output will be provided from the iCAM or the EIB (ICU7000).
20. Click OK to save changes reboot the ICU if prompted.

7.3 Configuring iData EAC software for use with ICU7000

The ICU7000 settings should be configured prior to performing the configuration setup procedures performed in this section. Follow this section to properly assign the ICU7000 settings into the IrisManager section of the iData EAC software (version 3.07.08 and above).

1. Open the IrisServer.exe application (if not open already).
2. Open the IrisManager application (default User ID = administrator / Password = iris3000).

3. Select > Creation >Remote Unit
4. Press > New
    a. Fill in the Name field (any description desired can be entered).
    b. Enter the ICU7000 IP address.
    c. Enter the ICU7000 security ID.
    d. Fill in the ICU channel description field (this can be left blank of entered with any description).
    e. Select Channel ID 1 from the dropdown box.
    f. Select the Model type of iCAM7000 series and ICU7000 from the dropdown box.



    g. Enter a priority level from 1–255 (default of 1 is standard).
    h. Press > OK to apply settings.
5. Repeat above steps for any additional ICU7000 units that are to be used on the system.

7.4 How to Test the IP Address Network settings of an ICU7000

To test the IP Address change, perform a ping to the new IP Address (as described below):

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 192.168.5.200)
6. Close the command prompt window.

7.5 How to change the IP Address of Multiple ICUs

If changing the IP Address of multiple ICUs:

*** Note:** *After each ICU configuration the arp cache on the computer must be deleted.*

1. Click on Start (in the Windows task bar)
2. Select Run
3. Type cmd
4. Press Enter

5. At the command prompt type: arp –d
6. Close the command prompt window
7. Connect the next ICU to be configured on the network and perform the configuration to the next iCAM

- Once all ICU units have been configured, the computer IP Address can then be changed back to its original IP Address or to the new IP Address as required to communicate to the rest of the IrisAccess™ system.

8. Updating the IrisICUAdmin7000

The ICU7000 makes use of an application called ICUAdmin7000 that is provided with the iData EAC software 7.07.08 and above versions. This application can also be downloaded directly from the irisid.com website. This application should be used before attempting to install and integrate the ICU7000 into a deployed running environment.

ICU7000Update is an application utility that allows for management of an ICU7000. ICU7000Admin is used for new installation and upgradation of the ICU7000 controller unit.

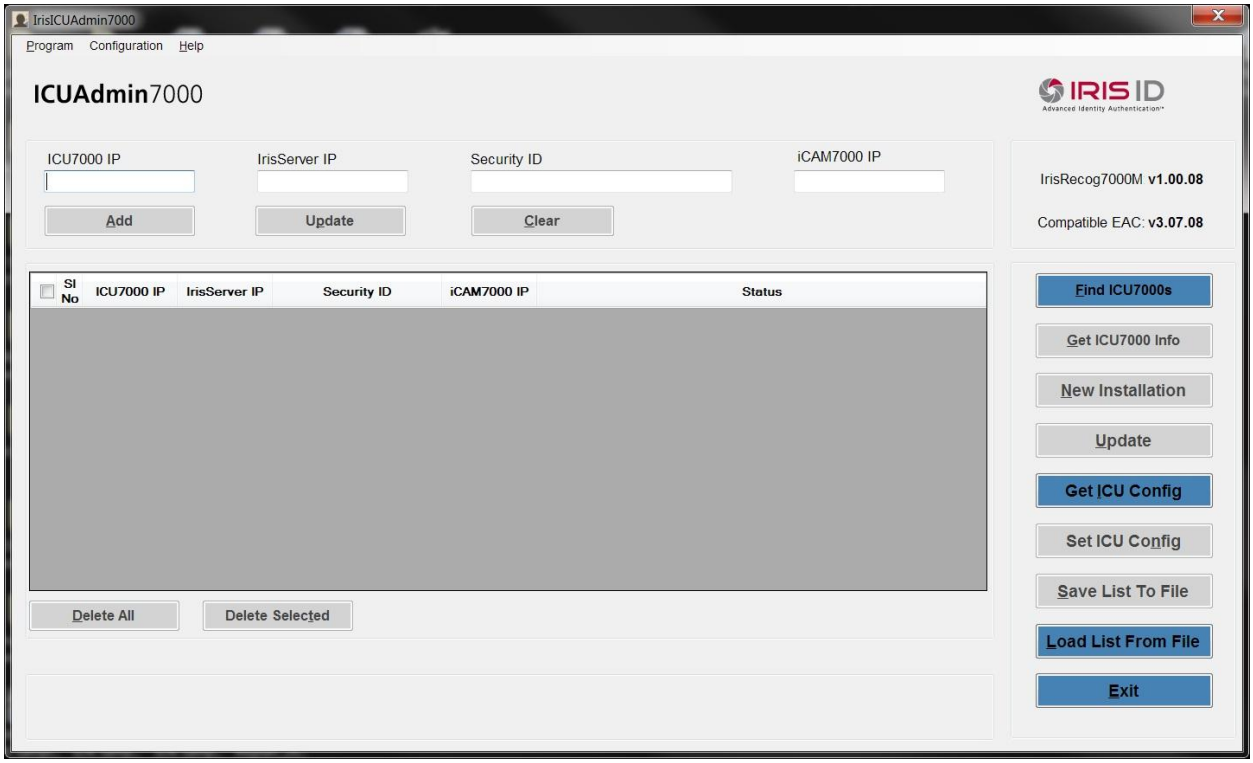
8.1 Using the IrisICUAdmin7000 during Installation

The ICU7000 must be updated prior to use as part of the installation process. The following information is provided as general step reference. Refer to the IrisICUAdmin7000 user guide for full details and instruction for this application.

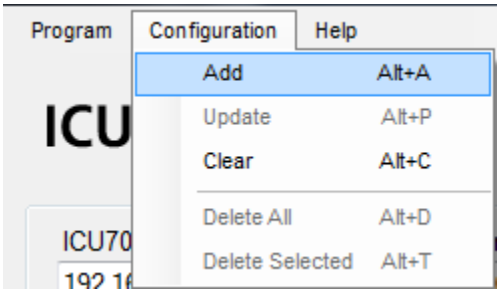
How to Use IrisAccess™ ICUAdmin7000

Follow these steps to perform either a New Installation or Update to the ICU7000.

1. To start the ICUAdmin7000, click **IrisICUAdmin7000.exe** (or Click on IrisICUAdmin7000 shortcut in start menu or desktop).
2. The application window will be displayed as shown in the following image.

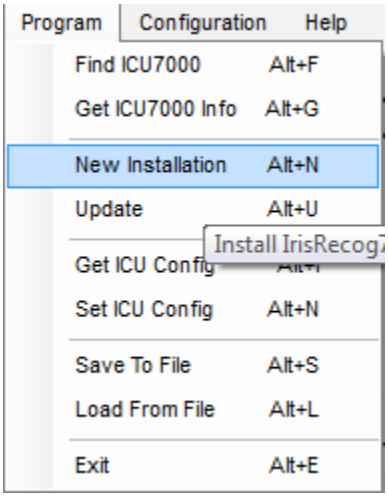


3. Enter a valid **ICU7000 IP**, **IrisServer IP** and **Security ID (iCAM7000 IP optional)**, click on **Add** button or select **Add** option from **Configuration** menu.



***Note**: The **FindICU7000** button function can be used instead of the manual Add function if desired. It will search the network for available ICU7000 controller units and display them in the list. To perform this process Click on > Find ICU7000 button or select Find ICU7000s option from Program menu. (Network settings, windows firewall, available ports, routers, and anti-virus applications can block the applications ability to find/detect ICU7000s on the network.)*

4. Click on **New Installation** button or select **New Installation** option from **Program** menu to perform required installation. (New installation of iCUAdmin7000 will install IrisRecog7000M software in ICU7000.)



5. A new installation progress bar will be seen indicating the progress of the installation.
6. After successful update, iCAM7000 will reboot.
7. Repeat steps with additional ICU7000 controller units as needed.

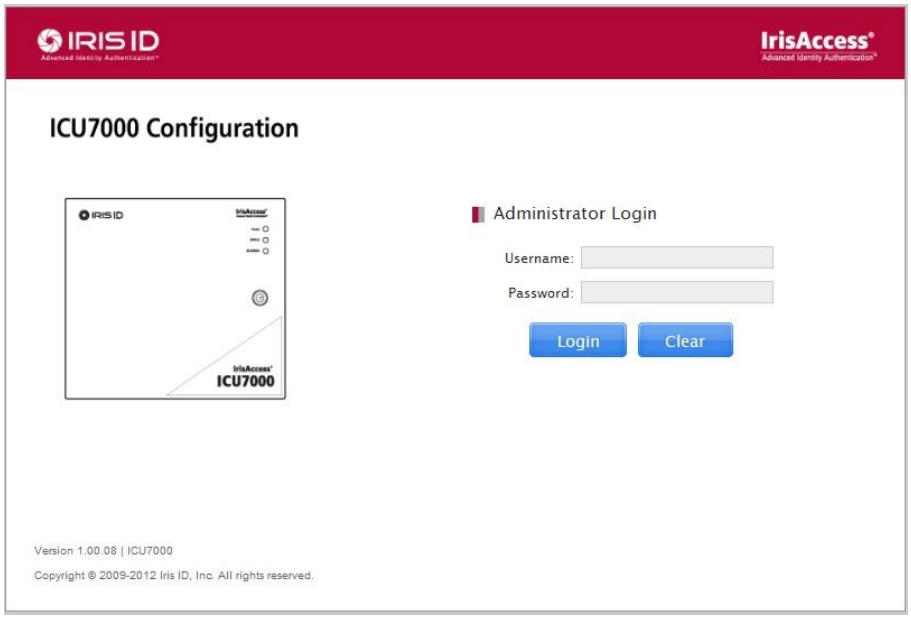
9. Using the ICU7000 Configuration Interface

The ICU7000 Configuration interface can be used to gather information about your ICU as well as perform modifications and setting change/configurations to your identity controller unit. If using more than one ICU, each ICU needs to be configured to the desired specifications required – configuring one ICU from the configuration interface will only change the settings of that particular ICU7000 unit for use with one iCAM7000 series camera. Please see below for a screen by screen break-down of the ICU7000 configuration interface.

9.1 Login and Main Menu Screen

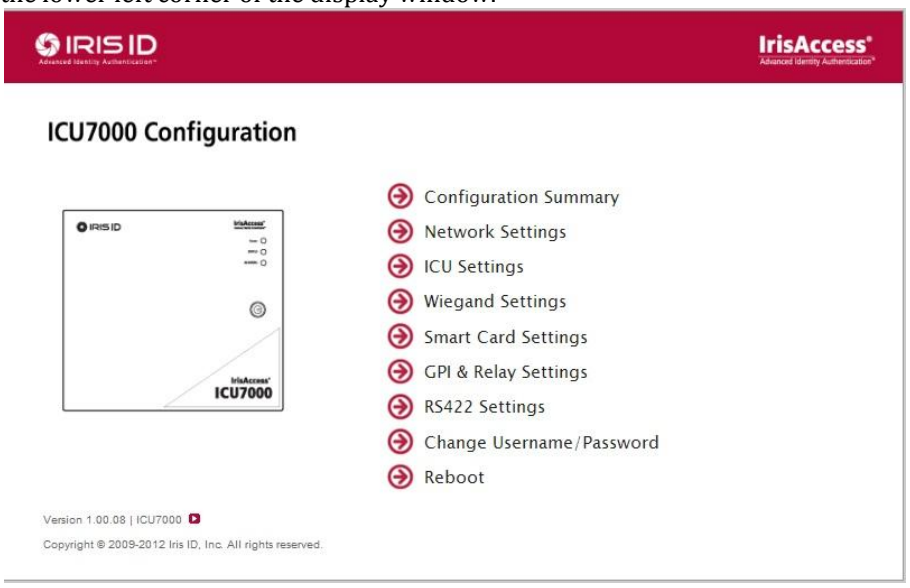
Login Screen

Enter the default Username: ICU7000 and Password: iris7000 (both are case sensitive) if still set to default settings.



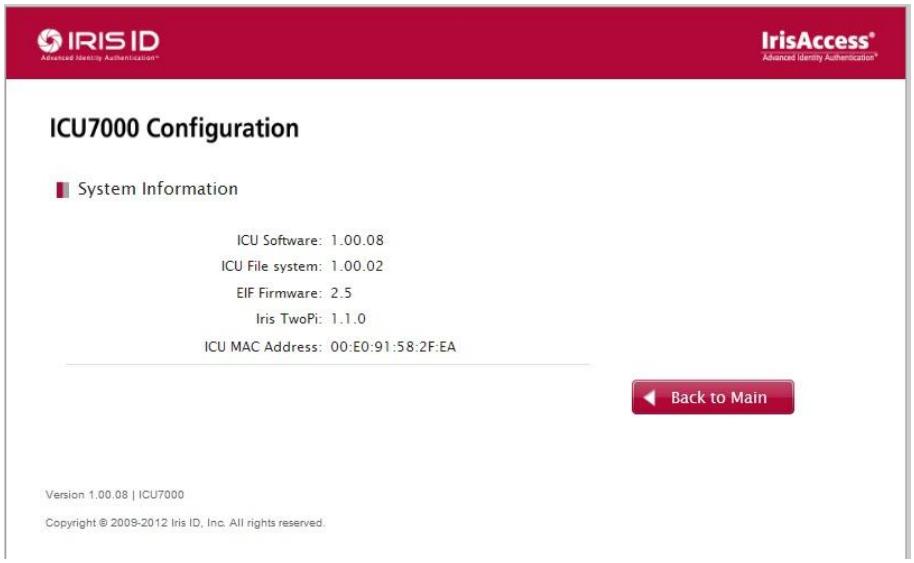
Main Screen

Once you have accessed the iCAM Configuration Main Screen (Menu screen), configurations such as changing of administrator password, date and time settings, Smart Card Configuration, Network Settings, Wiegand Settings, iCAM software update, Voice Message Update, and Reboot options are available for you to help further utilize and configure your IrisAccess™ system. Additionally, the iCAM software version is displayed in the lower left corner of the display window.



System Information Screen

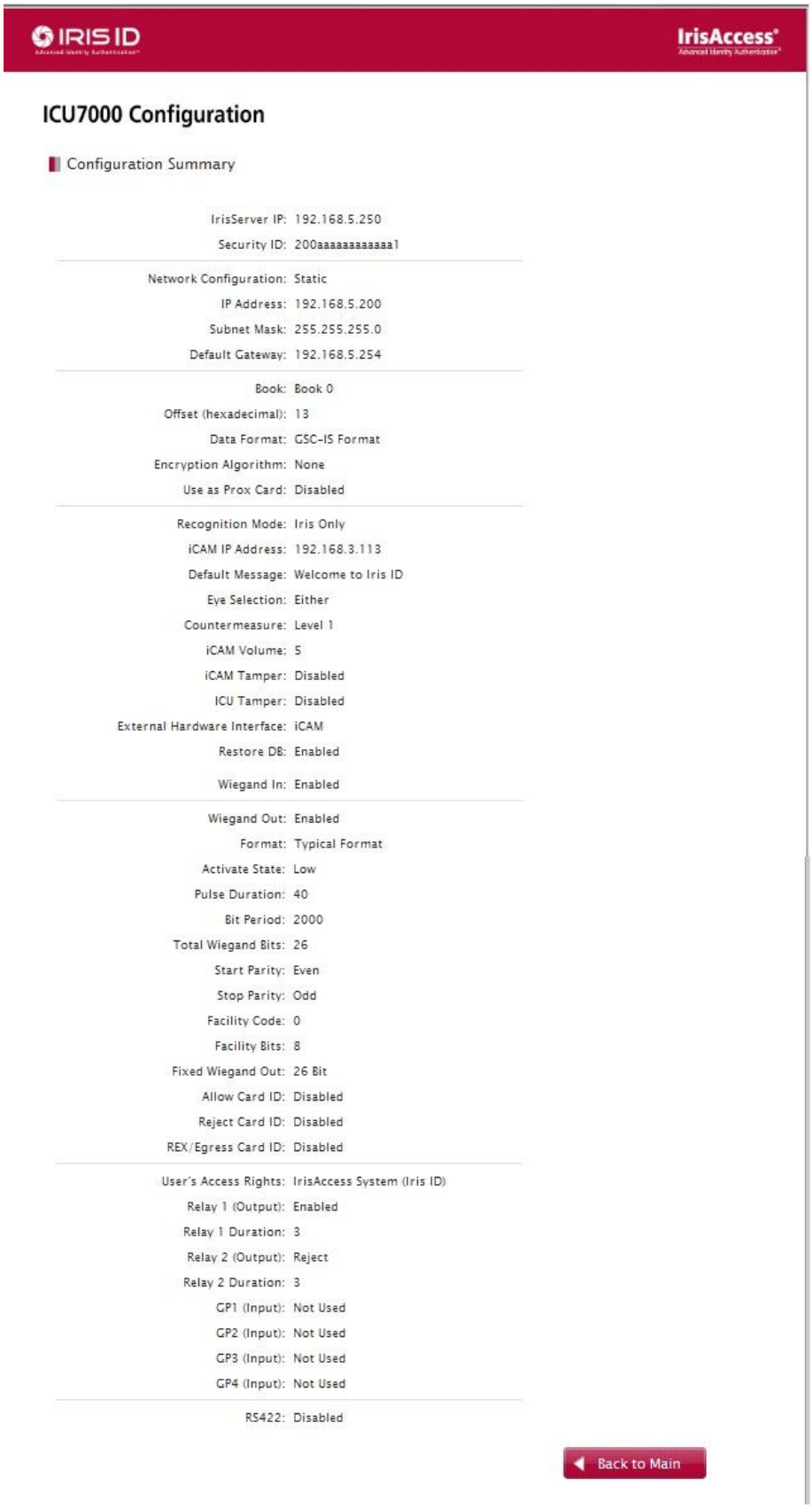
The ICU Configuration System Information screen provides detailed (viewable only) information about the specific ICU connected. Such information is shown to help identify the ICU software version, ICU File system version, EIF Firmware version/type, Algorithm, along with the ICU MAC Address. This screen is accessible from the Main Screen by clicking on the small red icon located to the right of the version number listing on the bottom left side of the display window.



9.2 Breakdown of the Configuration Interface

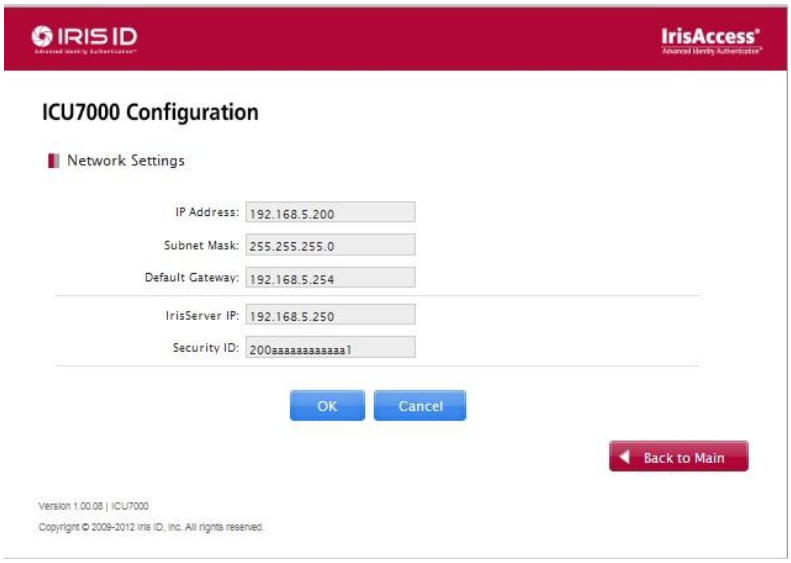
Configuration Summary

These settings are viewable only, and indicate the specific (currently configured) settings which include Server IP, Security ID, Network configuration type, IP address settings, and details additional settings as displayed in the following image.


IRIS ID
IrisAccess
ICU7000 Configuration
Configuration Summary
IrisServer IP: 192.168.5.250
Security ID: 200aaaaaaaaaaa1
Network Configuration: Static
IP Address: 192.168.5.200
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.5.254
Book: Book 0
Offset (hexadecimal): 13
Data Format: GSC-IS Format
Encryption Algorithm: None
Use as Prox Card: Disabled
Recognition Mode: Iris Only
iCAM IP Address: 192.168.3.113
Default Message: Welcome to Iris ID
Eye Selection: Either
Countermeasure: Level 1
iCAM Volume: 5
iCAM Tamper: Disabled
ICU Tamper: Disabled
External Hardware Interface: iCAM
Restore DB: Enabled
Wiegand In: Enabled
Wiegand Out: Enabled
Format: Typical Format
Activate State: Low
Pulse Duration: 40
Bit Period: 2000
Total Wiegand Bits: 26
Start Parity: Even
Stop Parity: Odd
Facility Code: 0
Facility Bits: 8
Fixed Wiegand Out: 26 Bit
Allow Card ID: Disabled
Reject Card ID: Disabled
REX/Egress Card ID: Disabled
User's Access Rights: IrisAccess System (Iris ID)
Relay 1 (Output): Enabled
Relay 1 Duration: 3
Relay 2 (Output): Reject
Relay 2 Duration: 3
GP1 (Input): Not Used
GP2 (Input): Not Used
GP3 (Input): Not Used
GP4 (Input): Not Used
RS422: Disabled
Back to Main

Network Settings

This screen provides the ability to get detailed information on the IP settings of the ICU7000 connected on the network. From this location you can set IP address information. You can also designate the IrisServer IP settings and security ID information.



Configuration settings:

1. Enter the new IP address for the iCAM (default = 192.168.5.100).
2. Enter the new Subnet Mask for the iCAM (default = 255.255.255.0).
3. Enter the new Default Gateway for the iCAM (default = 192.168.5.254).
4. Enter the Iris Server IP.
5. Enter the security ID (unique 16 characters).
6. Click OK to save changes.

* Note: *There is a FACTORY DEFAULT located on the ICU7000 interface board below the RTC battery. While the unit is in the powered on state, pressing and holding the FACTORY DEFAULT button for at least 5 seconds will reset the ICU IP Address to the factory default (192.168.5.200) and the login ID credentials for the iCAM (User ID = ICU7000 / Password = iris7000).*

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

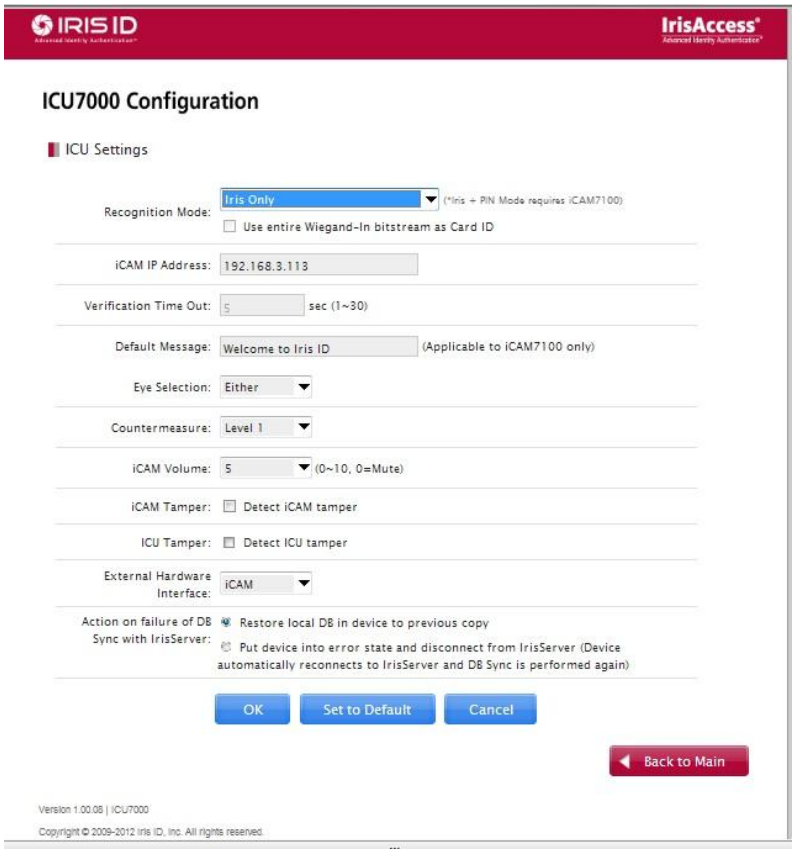
***Note:** Pressing the Factory default button two times consecutively will cause the ICU to announce the current configured IP Address of the unit.*

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.

ICU Settings

This screen provides the ability to configure numerous aspects of the controller unit and its functionality. See below for details on what settings and options are available.



- **Recognition Mode** – Selectable by a dropdown box, this area can be configured to allow for the type of mode that will be used for this iCAM. The modes available for selection are:
    - **Iris Only*** – iCAM will function for use with Iris only. (* PACS PIN Mode is available in this mode.)
    - **Iris + Pin (Local)** – iCAM will function with 2 factors of modality (Pin and Iris). The PIN data must be entered (either during enrollment or using IrisManager) for the user. This mode will use the IrisAccess system to determine the authorization of the user's PIN and iris data. The PIN Pad will appear on the screen allowing the user to enter the appropriate PIN, and then present the eyes to the iCAM. In this mode, the PIN data must be entered first in order to allow for the iris to be presented. Once the Pin is entered, press the enter arrow.

- **Iris + Prox Card*** - iCAM will function with 2 factors of modality (Prox Card and Iris). When using this setting, the iCAM will wait for a prox card to be presented before the users eyes are requested to be presented to the iCAM unit. (* PACS PIN Mode is available in this mode.)
- **Iris + Smart Card*** - iCAM will function with 2 factors of modality (Smart Card and Iris). When using this setting, the iCAM will wait for a Smart Card to be presented before the users eyes are requested to be presented to the iCAM unit. When using a Smart Card, the user can be verified directly off of the Smart Card data of the card presented. (* PACS PIN Mode is available in this mode.)
  - **Use Entire Wiegand-in-bitstream as card ID** – Selectable by check-box, this setting allows the entire Wiegand-in data (bitstream) to be used as the card ID that is to be output. This requires that the entire card data (bitstream) be enrolled at the same time as the iris of the user.

- **iCAM IP Address** – The IP address of the iCAM7000 series camera unit that is to be controlled the ICU.
- **Verification Time Out** – This setting allows the installer to enter the desired time-out length for verification. By default this setting value is 5 seconds. This setting can be changed by the installer from a range of 1 ~ 30 seconds for this time out.
- **Default Message** – Displays a message that can be seen on the LCD screen (7100 series units only). Up to 20 Characters can be typed in this box field. The characters entered will appear on the LCD display when available. The text can be seen in the "message area" of the screen (upper area of the LCD display).
- **Eye Selection** – Selectable as a dropdown box, this option allows the installer to set the iCAM for use with Either Eye (default), Left eye, Right Eye, or Both Eyes.
- **Countermeasure** – Selectable by dropdown box, this option allows the installer to select the sensitivity of countermeasure present in the iCAM. Level 1 is the standard countermeasure protection (set as default). If the highest level of countermeasure protection is required, Level 2 can be selected. The level 2 counter measure will provide enhanced countermeasures, but may perform slower the Level 1.
- **iCAM Volume** – Selectable by Dropdown box, this option controls the volume setting of the iCAM. The level available is 0~10. 0 acts as mute, and volume levels ascend by increased number to 10 being the loudest volume setting.
- **iCAM Tamper** – Selectable by checkbox, this setting allows the installer to enable the iCAM tamper detection. By default, this option is turned off (un-checked). The iCAM has 2 physical tamper locations (In the front of the unit, and in the back). The tamper switch is triggered on when the tamper switch position is no longer in the (depressed) pressed-in - the unit will deactivate and begin to alarm. To reactivate, power reset the unit (ether a physical reset of power or through the iCAM configuration), and verify the tamper switches are depressed. Operation of the tamper switch is software selectable.
- **ICU Tamper** – Selectable by checkbox, this setting allows the installer to enable the ICU tamper detection. By default, this option is turned off (un-checked). The tamper switch is triggered on when the tamper switch position is no longer in the (depressed) pressed-in - the unit will deactivate and begin to alarm. To disengage proper function and reactivate the ICU7000 channel, verify the tamper switch is in the correct state and power reset the unit. (Note: Tamper Operation can be enabled or disabled through the ICU7000 Web Configuration as this setting is selectable.)
- **External Hardware Interface –** A selectable option that can allow the selection of Wiegand output to be enabled through the available selections available. Options include iCAM or EIB. iCAM refers to the iCAM7000 for output and EIB (External Interface board) refers to the ICU7000 as the Wiegand output method. Select the appropriate option needed for Wiegand output from the desired device for output.
- **Action of Failure on DB Sync with IrisServer -** Select the radio button desired for Action on failure of DB Sync with IrisServer. These options are "Restore local DB in device to previous copy" *Or "*Put

device into error state and disconnect from IrisServer" (Device automatically reconnects to IrisServer and DB Sync is performed again).

Note:

Select "OK" to apply settings (a reboot may be required).

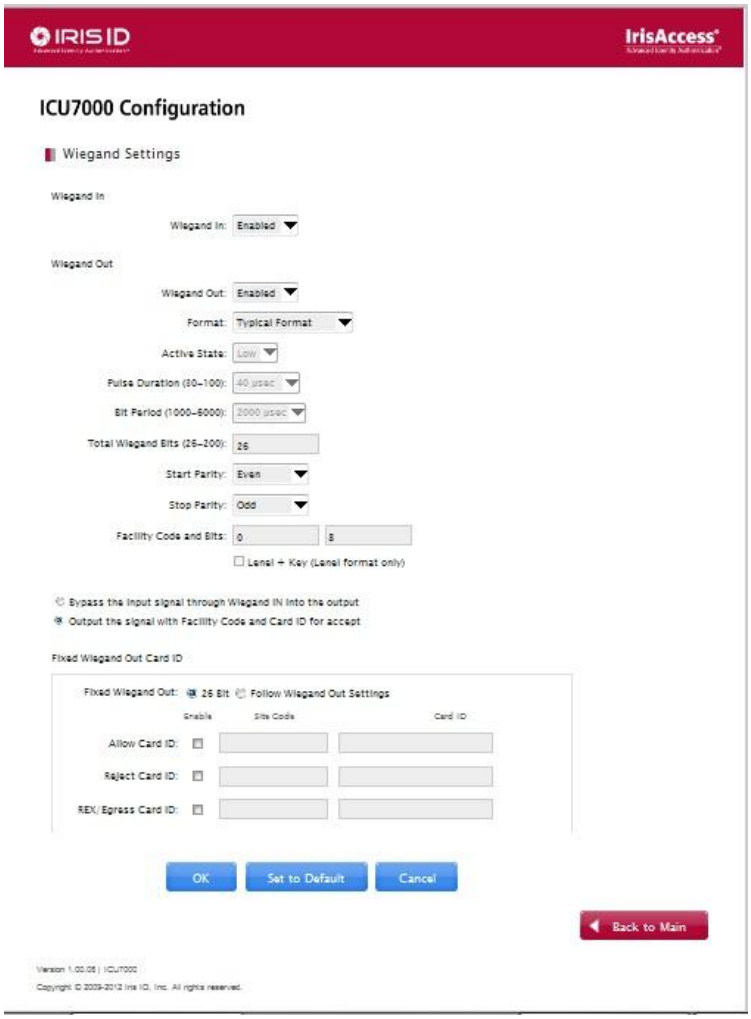
Select "Set to Default" to change setting values back to the default settings.

Press "Cancel" to disregard any changes that may have been selected.

Press "Back to Main" to view the main screen of the iCAM configuration without saving changes.

Wiegand Settings

From this screen selectable Wiegand settings can be enabled. Specifically, Wiegand In (Interface type-Disable or General Wiegand, and Wiegand Out (Interface type-Disable or general Wiegand, Pulse Duration, Bit Period) are configurable for direct iCAM Wiegand output. See the following information for details:



***Note**: Verify that the correct External Hardware Interface type has been selected in ICU Settings for proper configuration and usage.*

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

1. Login to the ICU 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* to select the "Disable" option for the Wiegand IN interface,), or select "Enable" to Enable the Wiegand Input (used for such devices as a card reader).
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 format type of Wiegand that will need to be output from the dropdown menu.
6. ***Note*:** The displayed active state, pulse duration, and bit period values are shown for reference only and cannot be modified or changed. The fixed settings provided for these are listed below:
    - Active state – Low
    - Pulse Duration – 40u sec (microseconds)
7. If typical format is selected, the values for the Wiegand total bits are selectable with the following available option: Set the total number of Wiegand bits (26~200) that are required for output.
8. Set the Start Parity to either Even or Odd.
9. Enter the Facility Code and Bits (as needed)
    a. Select the Lenel + Key check-box only if using with Lenel software with Lenel + Key format. (LENEL SOFTWARE ONLY)
10. Select the radio box to either "Bypass the input signal through Weigand IN into the Output", *OR* select "Output the signal with Facility Code and Card ID for accept". This is to be selected only if the entire Wiegand-In bitstream of the card is being used or if when in Smart Card+Iris recognition mode; the HID iClass HIDAPP value (Card ID) is to be passed through to the Wiegand Output upon verification.
11. The "Output the signal with Facility Code and Card ID for accept" should be selected if a Card ID is manually entered for the user. If selected, the Wiegand Output card format and facility code must be configured.

Fixed Wiegand Out Card ID:

The Fixed Wiegand Out Card ID provides a specific value of Facility Code and Card ID to be output upon certain events.

- Fixed Wiegand Out:
    - 26 Bit: Fixed Wiegand Out will be in a 26-Bit format. (Facility Code range is 0~255, Card ID range is 0~65535.)
    - Follow Wiegand Out Settings: Fixed Wiegand Output will be in the card format as defined in the Wiegand Out Settings fields.

    - Check mark the desired *events* that will be required as listed by the following options:

        a. Allow Card ID – The Facility Code and Card ID values in this field will be output upon the activation of the GPI set for Allow Access.
        b. Reject Card ID - The Facility Code and Card ID values in this field will be output upon the user rejection (all recognition modes).
        c. REX / Egress Card ID - The Facility Code and Card ID values in this field will be output upon the activation of the GPI set for REX/Egress.

Note:

Select "OK" to apply settings (a reboot may be required).

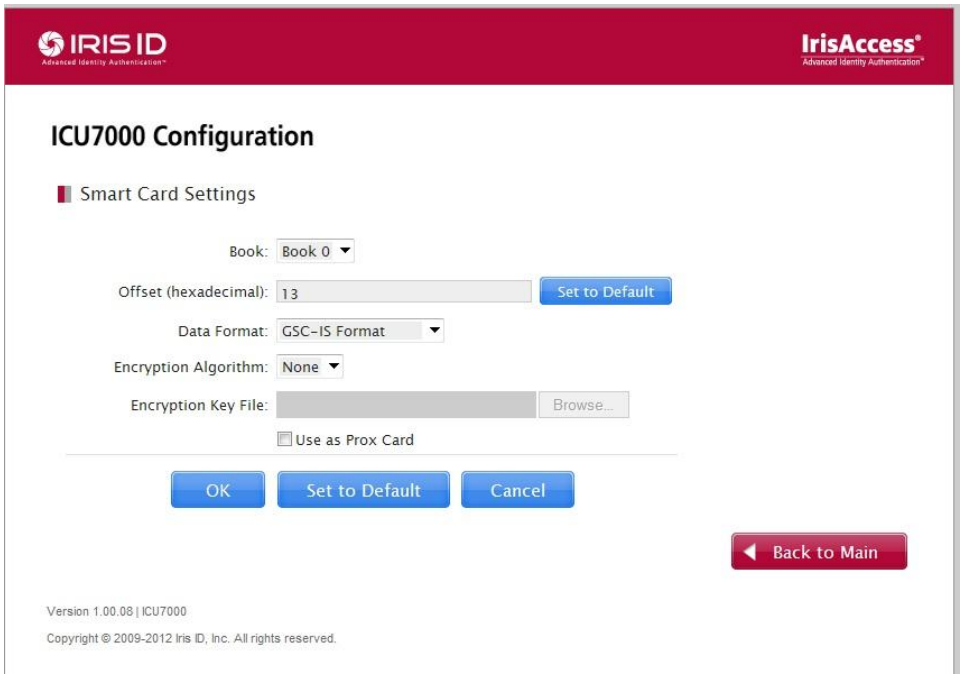
Select "Set to Default" to change setting values back to the default settings.

Press "Cancel" to disregard any changes that may have been selected.

Press "Back to Main" to view the main screen of the ICU configuration without saving changes.

Smart Card Settings

This screen allows for the modification and selection of a Smart Card type, and further allows for the input of an authentication key (hexadecimal), as well as the ability to restore back to the default settings of the ICU.



1. Login to the ICU7000 configuration screen as shown above (if not already logged in).
2. Select the Smart Card Settings option from the main screen.
3. Configure desired settings for the ICU Channel found in this screen. (See following data for details.)

The options available for "Smart Card settings" selection are:

A. Book:

(HID iCLASS 32K Cards only)**:** On an HID iCLASS 32K card there are two books available in which data can be stored. This selection allows for data placement to be selected for either book 0 or book 1. If a card other than an HID iCLASS 32K card is being used, make sure to configure the book field at book 0. When using 32K cards, you can select to use the book 0 or book 1 area(s) of the card by selecting the appropriate selection from the dropdown box list.

a. Book0
b. Book1

B. Offset (hexadecimal):

Described as the location on the card in which the iris data will be written or read from. This is a hexadecimal value, and can be set to any valid offset value in the smartcard. This offset will be used by iData CMA application to issue / reissue smartcards. (By default, this value is set to 13).

C. Click on "Set to Default" button to set to default offset value.

D. Data Format:

Data Format can be set by selecting item in data format combo box list.

a. IA EAC Format
b. GSC-IS Format
c. Lenel Format
d. Custom-ML Format

***Note: Custom-ML format**: Is a proprietary format and should only be selected for use by the integrators in which it was specifically designed for.

E. Encryption Algorithm:

Encryption Algorithm can be set by selecting item in encryption algorithm box.

Encryption Algorithm types are dependent on the type of data format used/selected.

• If data format is **"IA EAC Format"**, the only applicable encryption algorithm is: **"Proprietary"**.

• If data format is either **"GSC-IS Format"** or **"Lenel Format"**, the applicable encryption algorithms are: **"None"**,**"AES"**,**"DES"** and **"DES3"**.

a. None
b. AES
c. DES
d. DES3

F. Encryption Key File:
An Encryption Key file can be selected by browsing to an existing key file. Browse the correct file based on the selected "**Data Format**" and "**Encryption Algorithm**". Error message is displayed if selected file is invalid.

a. Choose file (to upload key file as needed),

***Note:** If "Encryption Key file" is already configured and there is no change in "Data Format" and "Encryption Algorithm", then the installer need not upload a security key file.

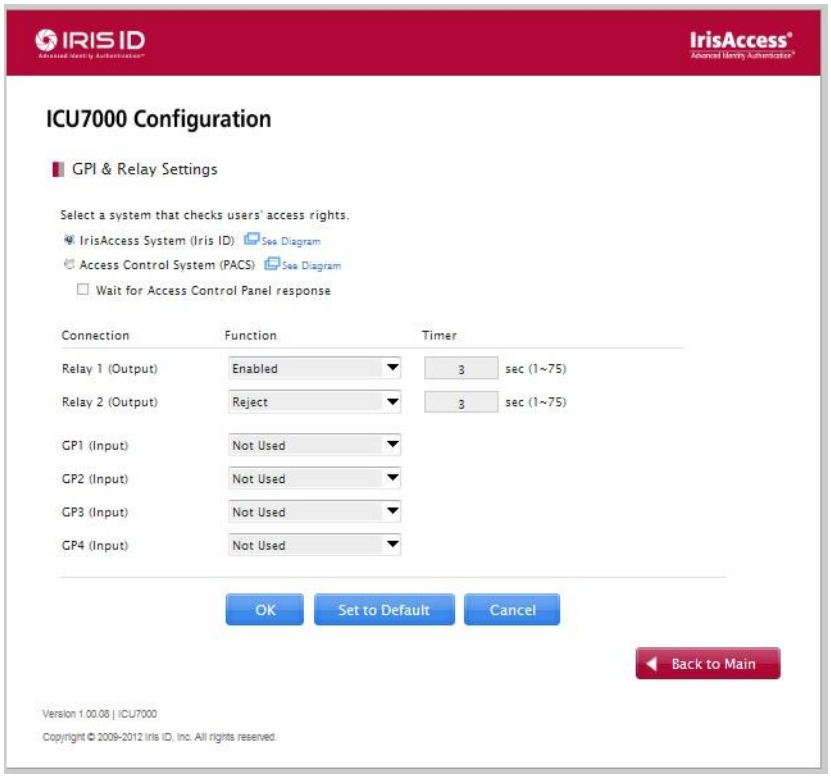
****Note:** Encryption Key files must be saved as a name without any spaces. Make sure to name the .DAT file with a file name that does not contain any character symbols or any spaces in the saved name as this may prevent the file from working correctly in the iCAM.

G. Use as Prox Card:
Select the check-box "use as prox card" when requiring use of a MiFare/DESFire Card as a proximity card. The Card ID entered during enrollment time and card creation using IrisEnroll4000 will be the Card ID output during user verification. When selected, if any iris data is on the card, it will be ignored. Iris verification will be performed against the stored iris data in the ICU database.

Note:
Select "OK" to apply settings (a reboot may be required).
Select "Set to Default" to change setting values back to the default settings.
Press "Cancel" to disregard any changes that may have been selected.
Press "Back to Main" to view the main screen of the iCAM configuration without saving changes.

GPI & Relay Settings

The GPI & Relay Settings screen allows for selection of the ICU7000 series camera built-in General Purpose Input and Relay operation.



1. Login to the ICU7000 configuration screen as shown above (if not already logged in).
2. Select the GPI & Relay Settings option from the main screen.
3. Configure desired settings for the ICU7000 channel found in this screen. (See following data for details.)

- Select a system that checks users' access rights
    - **IrisAccess System (Iris ID)** – When selected, the credential (Iris, PIN, Prox Card, Smart Card) information is verified against the enrolled credential information stored in the IrisServer/iCAM database. See diagram.

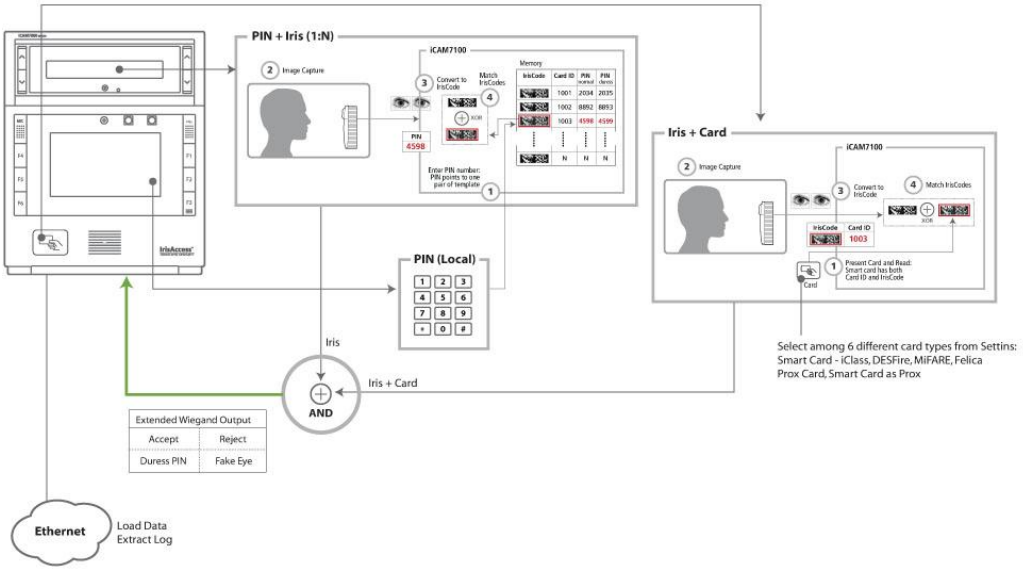


Diagram of IrisAccess System checks users' rights

- **Access Control System (PACS)** – When selected, the permissions of the users are determined by the Access Control Systems permission set. The iCAM provides a Wiegand Output of the user (stored Facility Code and Card ID, or bypassed Wiegand bit stream) to the Access Control System. See diagram.

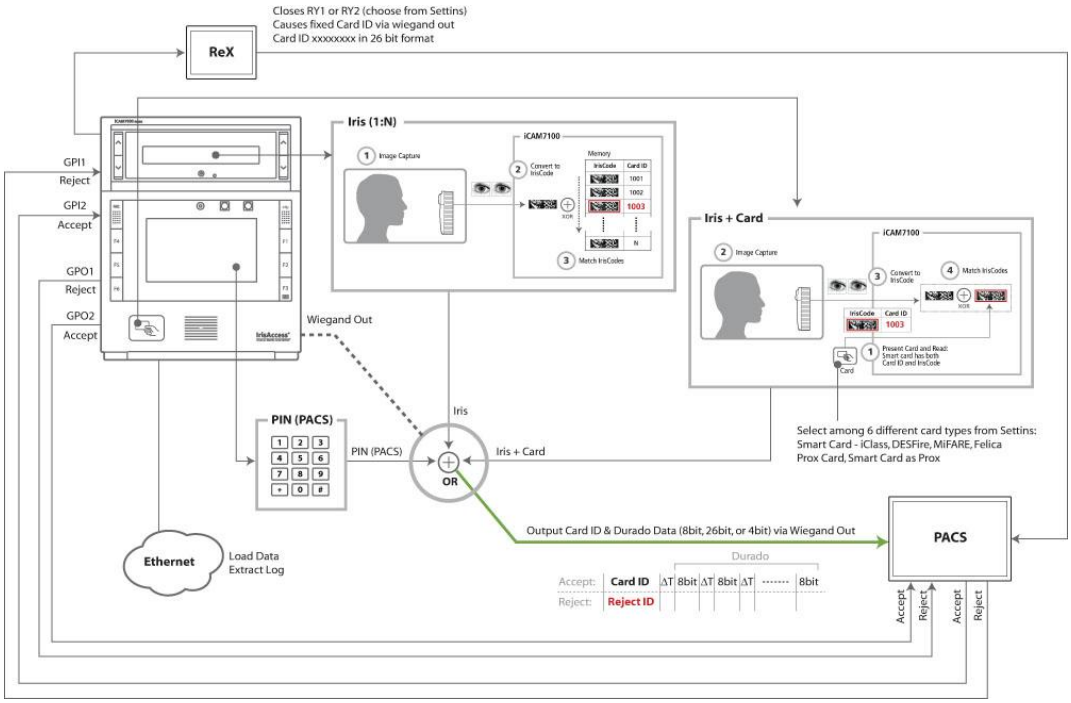


Diagram of Access Control System Checks users' rights

  - **Wait for Access Control Panel Response** – When used, the results of the identification/verification will *NOT* be announced until a GPI is triggered signifying either accept or reject of the user (from the PACS system).

- **Relay 1 (output)** – Set to either *Enabled* to *Disabled* and provide a timer value from 1 ~ 75 seconds.
  - *Disable* – Relay 1 is disabled
  - *Enabled* – Relay 1 will activate upon identification/verification of the user, or as per implementation of the selected GPI.

- **Relay 2 (output)** - Set to either disabled, reject, or tamper, and provides a timer value from 1 ~ 75 seconds.
  - *Disable* – Relay 2 is disabled
  - *Reject* – Relay 2 will activate upon a rejection of the users credentials (Iris, etc.), also upon "Reject" GPI (in PACS Mode)
  - *Tamper* – Relay 2 will activate upon an iCAM tamper event. (Relay active during the duration of the tamper condition.)

- **GP1 (Input)** – Set to either *Not used*, *Accept*, *Activate iCAM*, or *REX/Egress*.
  - *Not used* – Input is disabled
  - *Accept* – Used only when "Wait for Access Control Panel Response" (PACS Mode) is selected. If the user is successfully identified / verified by the iCAM, and the user permissions are authorized by the PACS - the PACS will activate the GPI. Once activated, the iCAM will provide a voice announcement of the user's acceptance, and send the transaction to the IrisServer.
  - *Activate iCAM* – When selected, the iCAM will remain in a stand-by (a non-active state) until an event triggered by this GPI. This input must remain active for the duration of the desired iCAM activation. Activate iCAM is only applicable when the iCAM is set to IRIS Only recognition mode. (This input must be held for the duration of the transaction in order for it to complete.)
  - *REX/Egress* – When GPI is activated, the Relay 1 is activated for the specified duration determined by the Relay 1 timer value, and (if selected) the Fixed Wiegand Output for REX/Egress Card ID is sent from the Wiegand Output of the iCAM. The iCAM sends a message to the IrisServer of "Egress on / Egress Off".

- **GP2 (Input)** – Set to either *Not used, Reject, Reject-A mode, Activate iCAM*, or *REX/Egress*.
  - *Not used* – Input is disabled
  - *Reject* – Used only when "Wait for Access Control Panel Response" (PACS Mode) is selected. If the user is successfully identified / verified by the iCAM, but the user permissions are denied by the PACS - the PACS will activate the GPI. Once activated, the iCAM will provide a voice announcement of the user's denial and send the transaction to the IrisServer.
  - *Reject-A mode* - Used only when "IrisAccess System – Checks Users Rights" is selected. Upon input to the GPI, the iCAM will provide a voice announcement "Sorry, you are not authorized" from the iCAM. No output (Relay or Wiegand) is sent.
  - *Activate iCAM* – When selected, the iCAM will remain in a stand-by (non-active state) until an event is triggered by this GPI. This input must remain active for the duration of the desired iCAM activation. Activate iCAM is only applicable when the iCAM is set to IRIS Only recognition mode. (This input must be held for the duration of the transaction for it to complete.)
  - *REX/Egress* – When GPI is activated, the Relay 1 is activated for the specified duration determined by the Relay 1 timer value, and (if selected) the Fixed Wiegand Output for REX/Egress Card ID is sent from the Wiegand Output of the iCAM. The iCAM sends a message to the IrisServer of "Egress on / Egress Off".

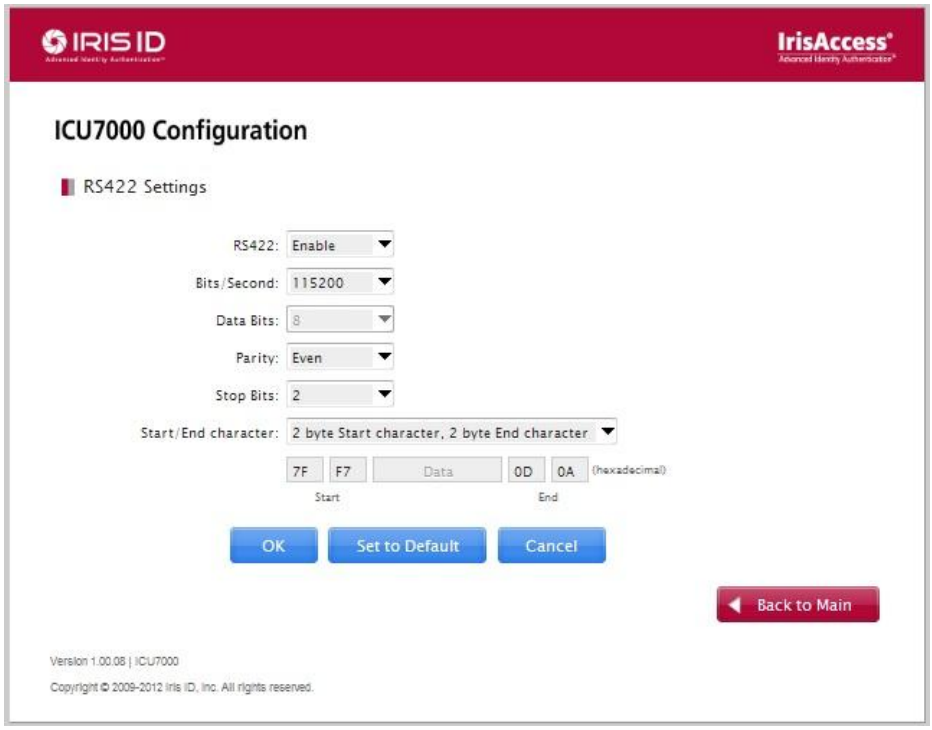
- **GP3 (Input)** – Set to either *Not used, Activate iCAM*, or *Reject-A Mode*.
    - *Not used* – Input is disabled
    - *Activate iCAM* – When selected, the iCAM will remain in a stand-by (non-active state) until an event is triggered by this GPI. This input must remain active for the duration of the desired iCAM activation. Activate iCAM is only applicable when the iCAM is set to IRIS Only recognition mode. (This input must be held for the duration of the transaction in order for it to complete.)
    - *Reject-A mode* - Used only "IrisAccess System – Checks Users Rights" is selected. Upon input to the GPI the iCAM will provide a voice announcement "Sorry, you are not authorized" from the iCAM. No output (Relay or Wiegand) is sent.

- **GP4 (Input)** – Set to either *Not used, Fire Alarm, REX/Egress, Access Allow*, or *Reject-A Mode*.
    - *Not used* – Input is disabled
    - *Fire Alarm* – When the GPI is initiated and held, Relay 1 is activated for the duration of time that the GPI is held. The iCAM sends a message to the IrisServer of "Alarm On" / "Alarm Off".
    - *REX/Egress* – When GPI is activated, the Relay 1 is activated for the specified duration determined by the Relay 1 timer value, and (if selected) the Fixed Wiegand Output for REX/Egress Card ID is sent from the Wiegand Output of the iCAM. The iCAM sends a message to the IrisServer of "Egress on / Egress Off".
    - *Access Allow* - When GPI is activated, the Relay 1 is activated for the specified duration determined by the Relay 1 timer value, and (if selected) the Fixed Wiegand Output for Allow Card ID is sent from the Wiegand Output of the iCAM. The iCAM sends a message to the IrisServer of "Allow On / Allow Off".
    - *Reject-A mode* - Used only when "IrisAccess System – Checks Users Rights" is selected. Upon input to the GPI, the iCAM will provide a voice announcement "Sorry, you are not authorized" from the iCAM. No output (Relay or Wiegand) is sent.

Note:
Select "OK" to apply settings (a reboot may be required).
Select "Set to Default" to change setting values back to the default settings.
Press "Cancel" to disregard any changes that may have been selected.
Press "Back to Main" to view the main screen of the ICU7000 configuration without saving changes.

RS422 Settings

The RS422 Settings screen allows for specific settings to be configured for use with the RS422 Output. See the following information for detail descriptions.



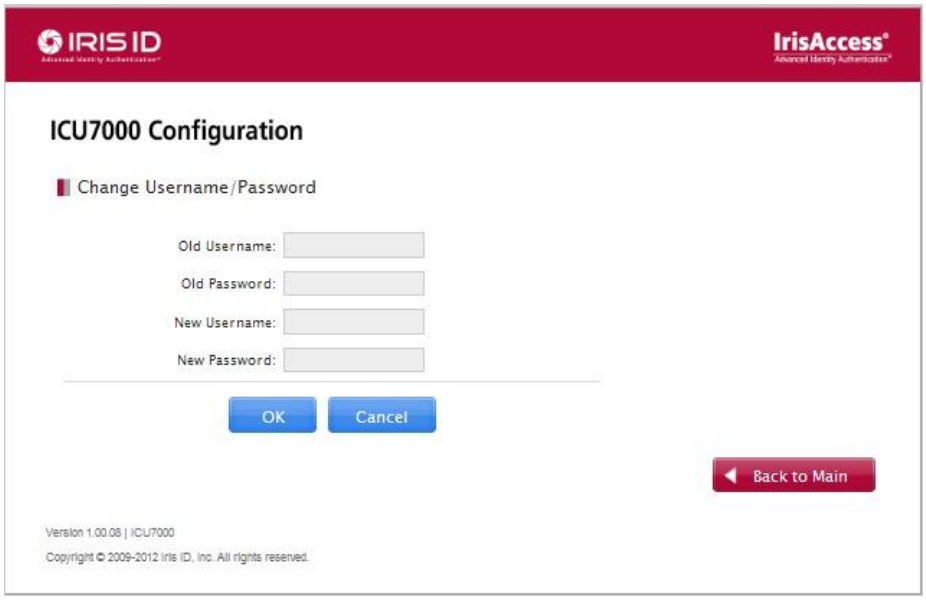
1. Login to the ICU7000 configuration screen as shown above (if not already logged in).
2. Select the RS422 Settings option from the main screen.
3. Configure desired settings for the ICU7000 found in this screen. (See following data for details.)

- **RS422** - Select *Enable* or *Disable.* Enabling this dropdown box allows for other items on the screen to be modified.
- **Bit / Second** – Select the desired bit / second. By default this value is set to 115200.
- **Data Bits** – Select the desired Data Bits. By default, this value is set to 8.
- **Parity** - Select the desired Parity. By default, this value is set to Even.
- **Stop Bits** - Select the desired stop bits. By default, this value is set to 2.
- **Start/End character** - Select the desired start/end character. By default, this value is set to 2 byte Start Character, 2 byte End character. The values entered into these fields are to be the hexadecimal value of the desired ASCII character code.

Note:
Select "OK" to apply settings (a reboot may be required).
Select "Set to Default" to change setting values back to the default settings.
Press "Cancel" to disregard any changes that may have been selected.
Press "Back to Main" to view the main screen of the ICU7000 configuration without saving changes.

Change Username/Password

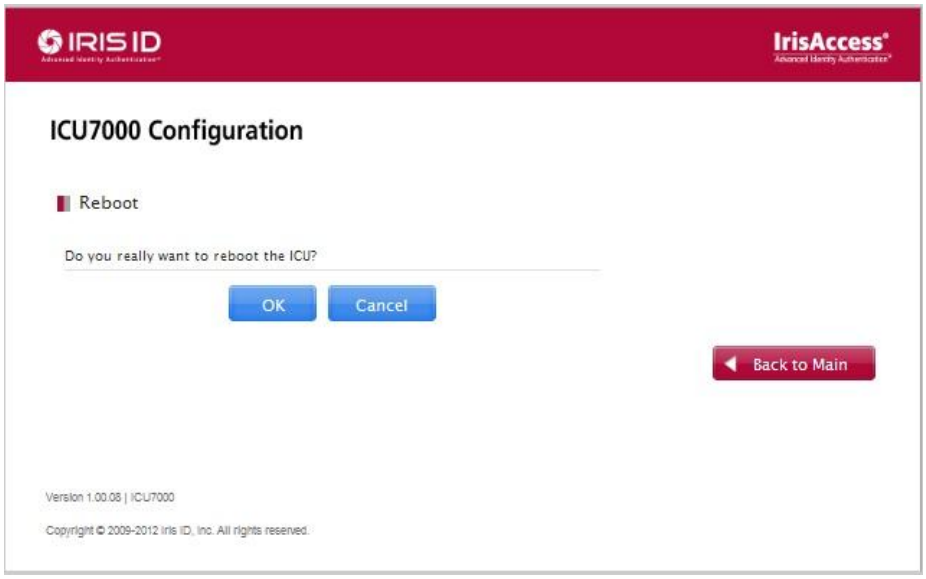
This menu provides the ability to change the Username and Password settings currently existing in the ICU7000. In order to change the settings first the old user id and password must be entered in addition to the new user id and password credentials desired. Please note that all fields are case sensitive.



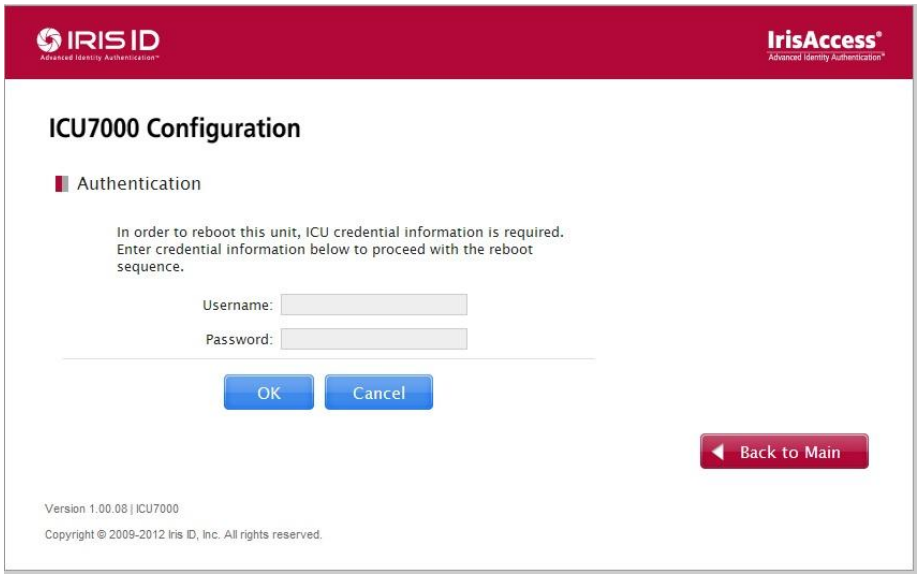
** **Note**: The ICU7000 FACTORY DEFAULT is located on the ICU7000 interface board below the RTC battery. While the unit is in the powered on state, pressing and holding the FACTORY DEFAULT button for at least 5 seconds will reset the iCAM IP Address to the factory default (192.168.5.200) and the login ID credentials for the iCAM (User ID = ICU7000 / Password = iris7000).*

Reboot

This screen allows for a reboot of the iCAM unit. Once OK is pressed, the iCAM may prompt for an authentication of the specific User ID and Password of the camera unit. The unit with reboot once the okay button is selected. (Please wait for this process to complete as this may take several minutes.)

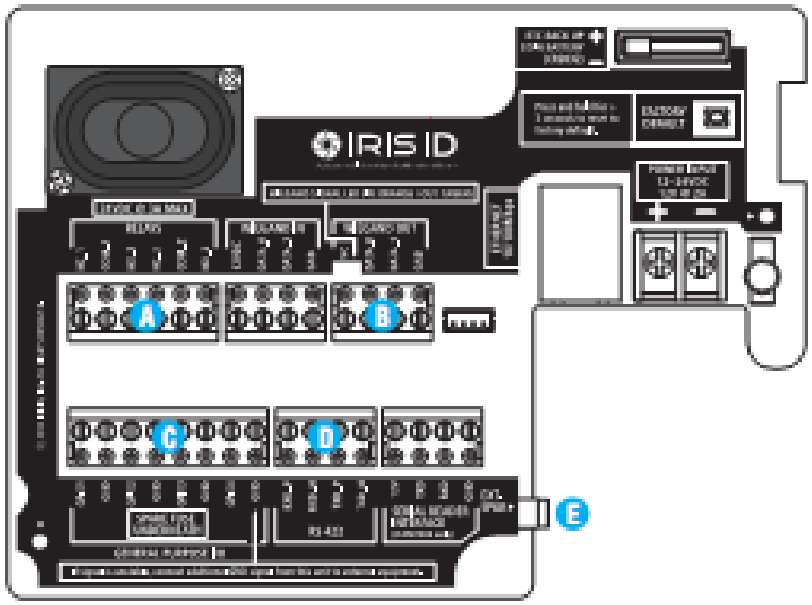


***Note**: The ICU may require a reboot. When prompted, press OK and enter the required username and password authentication (*default Username: **ICU7000** and Password: **iris7000**) *to reboot the ICU and apply the setting changes.*



10. Connection Details for Wiring ICU7000 Series

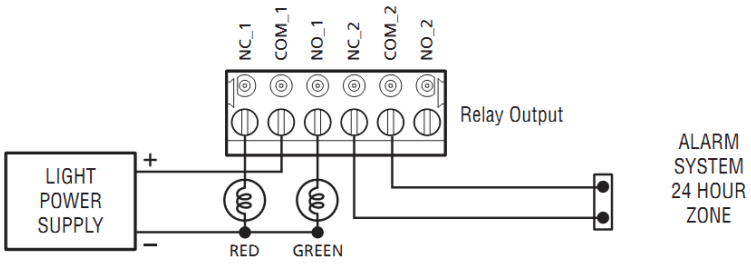
The ICU Camera units contain six connectors located on the interior of the unit. These connectors are surrounded by a wiring legend guide (black with white writing). This legend guide provides specific details for connection details for each connector. Below Each connector (when the connector is removed) displays the function for the connector port. The five connector parts are for relay output, Wiegand output, external GPI/O, RS422 Output, and External Speaker output.



IMPORTANT: ONLY KNOWLEDGEABLE PROFESSIONAL INSTALLERS SHOULD BE USED TO INSTALL ALL ELECTRONIC ENTRY/EXIT LOCKING DEVICES. DIRECT CONNECTION OF ELECTRONIC ENTRY/EXIT LOCKING DEVICES SHOULDN'T BE MADE FROM THE RELAY OUTPUTS ON THE ICAM. IT IS THE RESPONSIBILITY OF THE INSTALLER TO ASSURE THAT THE INSTALLATION IS PERFORMED IN ACCORDANCE WITH ALL COUNTRY/STATE/ LOCAL FIRE AND SAFETY REGULATIONS AND THAT ANY 3RD PARTY PRODUCTS USED WILL NOT CREATE A HAZARD.

10.1 Relay Output (A)

Two independent dry contact relays. The purpose and the duration of the relays are defined by the controlling software. Typically, Relay_1 (NC_1, COM_1, NO_1) is triggered upon user acceptance (access granted). The diagram shows Relay_1 connected to indicators which changes from Red to Green for an accepted user. Relay_2 (NC_2, COM_2, NO_2) is available for use. In this diagram the relay is activated when the iCAM tamper switch is triggered. The maximum electrical rating for the relay is 3A at 24VDC.

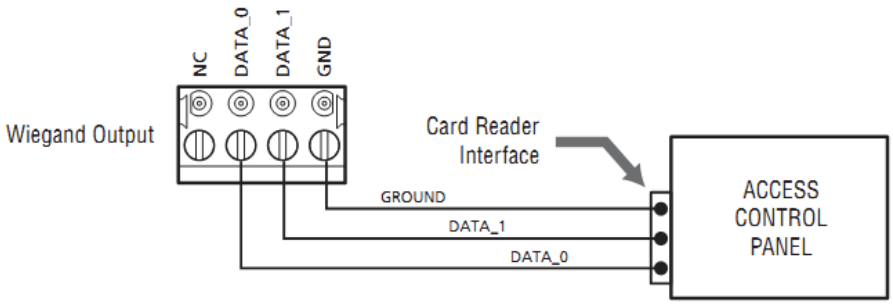


10.2 Wiegand Output

The Wiegand Output from the ICU7000 unit can be used with 3rd party devices capable of receiving Wiegand data. This Wiegand output emulates a typical Access Control Card Reader. Configuration of this output is provided through software. See the associated image for general wiring of Wiegand Output to an Access Control Panel.

Wiegand Specifications:

- Wiegand output uses 3 wire interface (Data0, Data1, and Ground),
- Maximum wire length from iCAM to Access Control Panel is 500feet (152m).



10.3 External GPI/O

GPIO1 through 4 are available to receive input from external switches or devices.

Some examples of GPIO functionality are shown below:

Access Panel response using GPIO:

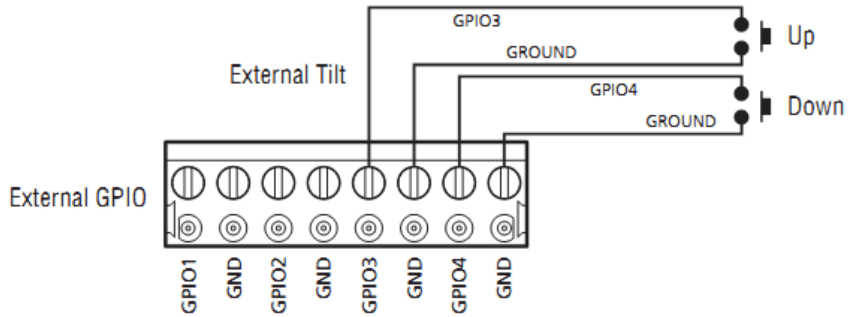
- The Access panel can trigger through the GPIO the appropriate voice response and transaction event to be reported. These responses include user acceptance or rejection by the third party access control panel.

iCAM Activate:

• iCAM activate allows the operation of the iCAM to be enabled ONLY when the GPI is in an enable state. This will activate the iCAM until the input is released.

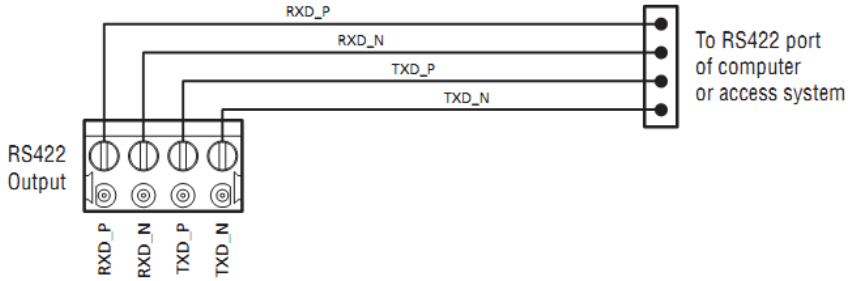
GPIO Specifications:

- For output, the GPIO can provide 5VDC @ 20mA.
- Assignment of GPIO is handled through Software.



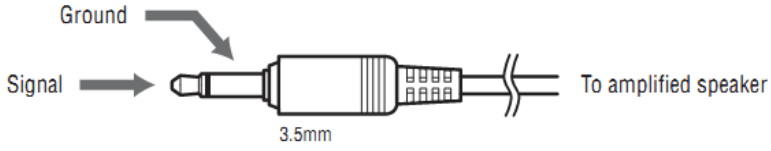
10.4 RS422 Output

RS422 serial communication port can be used for connection with an access panel or to other computer equipment. When configured, the Card ID associated with the user is output from the RS422 output port upon a successful identification.



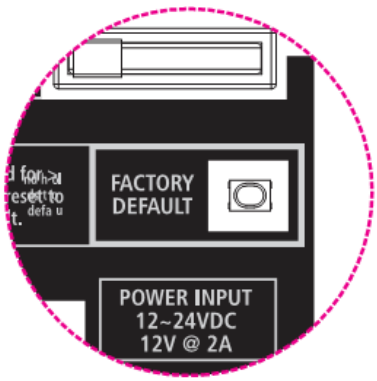
10.5 External Speaker Out

The External Speaker Out allows for a connection of an external amplified speaker. This port provides mono (single channel) audio of voice prompts and other unit sounds. Both the internal and external speakers can operate concurrently.



11. Restoring the Unit to Factory Default

The Factory Default can be used to restore settings of an ICU7000 controller unit to restore settings to factory default. This button is located inside of the unit below the RTC battery (see image), and can be used in two different ways; An IP Address Default, or a Factory Default.



11.1 IP Address Default

This default restores the IP Address and User ID/Password to the Factory Default values.

Note:
Default IP Address = 192.168.5.200, Subnet Mask = 255.255.255.0, Gateway = 192.168.5.254
Default User ID / Password = User ID: ICU7000 / Password = iris7000

Hold the factory default button down for at least 5 seconds while the unit is already powered-on to reset the unit IP address information back to the default settings.

11.2 Factory Default

This factory default resets ALL settings and software to the factory default.

***Note:** Any information, uploaded information (including firmware/software updates) to the unit that may have been performed prior to this reset function may be cleared. All settings will be factory restored to the default level.*

While powering on the ICU7000 controller unit, hold the factory default button down for at least 5 seconds to restore the entire unit back to all factory default settings.

12. Fuse Replacement

The ICU7000 controller unit contains a replaceable fuse which protects the unit from excessive current consumption. In the event that the ICU7000 series unit will not power on, a fuse replacement may be necessary.

If an additional fuse is required, the exact fuse type is required for use with the ICU7000 controller unit. Contact IRIS ID Systems, Inc. for assistance with acquiring additional fuse parts as needed.

12.1 Fuse Specifications

Manufacturer: Littlefuse

Part No.: 0451 004. MRL

Ampere Rating: 4A

12.2 How to Test and Replace the Fuse

CAUTION: FUSE REPLACEMENT SHOULD BE PERFORMED WITHOUT POWER CONNECTED TO THE UNIT.

Before replacing the fuse, it is recommended to test the fuse and determine whether the fuse is actually faulty.

How to Test the Fuse:

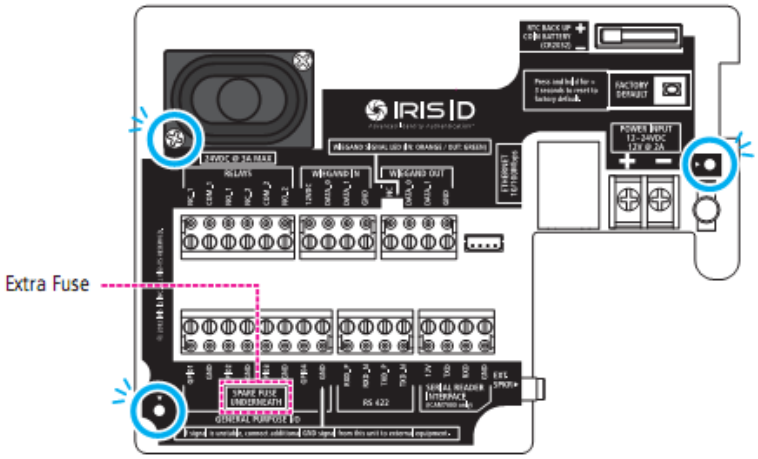
The fuse can be tested by checking the continuity across both sides of fuse with a multi-meter. If no continuity is measured, the fuse must be replaced.

How to Replace the Fuse:

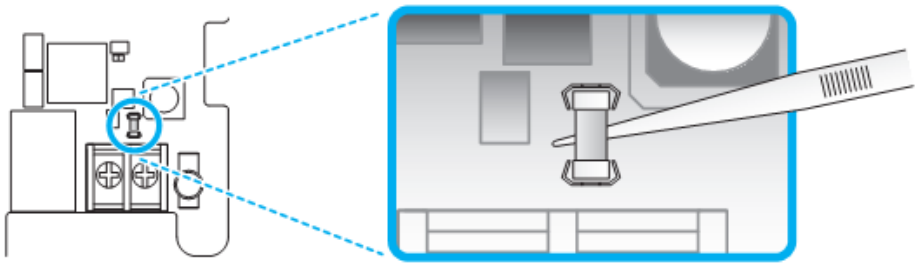
- Turn the unit to the OFF (down) position using the ON/OFF Switch.
- Disconnect power from the unit.

How to Replace the Fuse

1. Remove the screws to release the Wiring Legend Guide.



2. Use tweezers, and replace the Fuse.



Fuse Specification

Manufacturer	Littlefuse
Part No.	0451 004. MRL
Ampere Rating	4A

13. Warranty Information

13.1 Warranty Polices

- **Hardware** is warranted for the period of one year from the date of purchase by the end user.
- **Software** is warranted for the period of 90 days from the date of installation by the end user.
- Customers are entitled to IrisAccess® Software upgrades free of charge for in warranty systems, or systems covered under an extended warranty.
- In Warranty repairs will be free of charge for the duration of the limited warranty period of one year.
    - In Warranty Depot repair service is offered by Iris ID directly. The customer is responsible for shipping to IRIS ID. IRIS ID will pay shipping cost for return of the unit to the customer. The Same level of shipping service will be used to return the unit to the customer or partner.
- Partner/Integrator DOA policy – IRIS ID pays for shipping both ways.
    - DOA must be reported within 60 days of shipment from IRIS ID.
    - Advance Exchange must be secured by credit card or Company Purchase Order (PO).
    - Credit card will be charged at the time of shipment of the specific replacement unit. The credit card that was used will be issued a credit reimbursement for the amount charged for the unit (minus any applicable costs due to unit damage or missing accessories not provided with the returned unit(s)) when the unit(s) is shipped back to IRIS ID within 15 business days.
    - Unit(s) must be received back to Iris ID within 15 business days of the date the replacement unit was shipped. Failure to return the alleged defective unit may result in a default of credit reimbursement.

***NOTE:** Any/All warranty information pertaining to hardware, software, and repair/exchange services are subject to change at any time without notice by Iris ID. Please contact Iris ID for additional information.*

13.2 Out of Warranty Repairs

- Out-of-Warranty repair requests should be initiated with an authorized IRIS ID partner to arrange and accept responsibility for all costs associated. If an authorized IRIS ID partner is not available to handle said repair arrangements, the associated evaluation cost ($80.00 US) must be paid in advance before the unit evaluation will be performed. (Note: An evaluation cost applies to all out-of-warranty units, including units sent in with no problem found.)
- Either to the IRIS ID partner or directly to the customer, an RMA number must be issued by IRIS ID Technical Support prior to shipping the unit in question to IRIS ID. Units delivered to IRIS ID without RMA number may be refused.
- If the unit is confirmed as being out of warranty, the partner/customer will be contacted with an estimate of repair costs after the unit has been evaluated.
- Repairs will not be performed on the unit until the partner/customer accepts and agrees on payment from the estimate.
- Best effort will be made to place the repaired unit in shipment back to the customer within 15 business days from the date the customer accepts the cost estimate. The customer will be notified of any delays.
- A repaired unit will not be shipped until the company purchase order or credit card authorization for payment is received and processed.

- Payment of shipment to and from the Iris ID repair facility for out-of-warranty units is the responsibility of the partner/customer.

***NOTE:** Any/All warranty information pertaining to hardware, software, and repair/exchange services are subject to change at any time without notice by Iris ID. Please contact Iris ID for additional information.*

14. Technical Support

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

14.1 Billable Telephone Support

IRIS ID Authorized Partners in good standing and with up to date training certifications on file will receive at no cost, first and second tier Telephone Support (during standard IRIS ID business hours).

For IRIS ID Partners without training, out-of-date training, or direct customers/end-users (non-partner), live telephone technical support is billed at $120.00 (US) per hour (minimum of 2 hours). Payment for telephone support must be paid in advance by credit card or Company Purchase Order (PO).

Billable support may be subject to pre-arranged time/date scheduling that can be agreed upon by both parties.

Standard business hours for Live Telephone Technical Support are Monday through Friday – 8:30am to 5:30pm Eastern Standard Time (EST), except for IRIS ID scheduled holidays.

14.2 Partner & End-User Installation and Troubleshooting Assistance

- IRIS ID makes its very best effort to provide live training, web based training, comprehensive Quick Start Guides, and ancillary documentation for trouble free set-up, installation, and configuration. Use of these tools ensures trouble free installation and system operation.
- IRIS ID Authorized Reseller Partners agree to set-up and test the system in a staging area on the first system deployed to provide ample time (about 3/4 of a day) for a technician to become familiar with the equipment setup, configuration and operation.
- Authorized IRIS ID Partners are prohibited from attempting to have a Non Certified technician set up a system "at the customer site". We require the IRIS ID Partner to be trained to install the IRIS ID product; however this can be waived under certain pre approved circumstances.
- IRIS ID may choose not support an installing technician on the phone or in an on-site setup and configuration scenario unless the technician has attended either a live training seminar at IRIS ID or successfully completed an IRIS ID web-based training seminar and successfully completed the associated technical certification test.
- Please allow some extra time for a technician for the first system installation. This policy is strictly enforced. Deviation may result in chargeable telephone technical support. Authorized IRIS ID SSP and SI/VAR Certified Technicians are allowed to obtain free telephone technical support assistance from IRIS ID during standard business hours.