Iris ID

iCAM7000 Series User Guide

For iCAM7000 & 7100 Camera Units

Ver 1.01.00

January 2012

iCAM7000 Series User Guide – For iCAM 7000 & 7100 Camera Units

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

Document Number: IRISIDICAM7000-01-0100-1012

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 iCAM7000 Series is the latest generation of iris biometric cameras in the IrisAccess™ series. The iCAM7000 is designed not only to be a direct replacement to the successful iCAM4000/4100 series camera, but also to provide enhanced features, flexibility, and compatibility with current and future Iris ID software offerings. Each iCAM contains multiple operational modes standard, which are easily selectable within the iCAM7000's internal configuration web-based interface. The configuration web interface for the iCAM does not require installed software since it is accessible directly through an internet browser connected to the iCAM network.

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 iCAM7000 Series device. (If you do not have an iCAM7000 series camera unit, please refer to the "IrisAccess WebConfig Guide – For iCAM Series" as it refers to iCAM4000 Series devices.)

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 a "Software Manual, Hardware guides, 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 iCAM Configuration Equipment Requirements

Required Equipment (not included) for use with iCAM7000 Series

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

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

- Software
  - Required Software for desired system type (IrisAccess EAC, iData SDK, etc.)

Minimum Computer requirements (for Initial Configuration) of iCAM 7000 Series

- 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

- iCAM7000 Series Camera unit
- Hardware Guide
- L wrench

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

Power Source

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

Network

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

Software

- Required Software for desired system type (IrisAccess EAC, iData SDK, etc)

4. Model Descriptions

The below chart describes the various models and unit types (and options available) by model/part number for the iCAM7000 series.

4.1 iCAM7000 Series Model Detail Description

iCAM7000 (non-LCD models)						
Model Number	**LCD Display**	**On-Screen PIN PAD**	**125Khz Prox Card**	**13.56Mhz iClass, MiFARE, & DESFire Cards**	**Read/Write Iris Data to Card***	**Description**
iCAM7000	No	No	No	No	No	Dual iris recognition camera, TCP/IP enabled, with embedded 5M pixel face camera (Base Model)
iCAM7010-U1	No	No	No	Yes	Yes	iCAM7000 with built-in smart card reader/writer (iClass, MiFARE, DESFire, 13.56Mhz cards)
iCAM7010-M1	No	No	Yes	Yes	Yes	iCAM7000 with built-in smart card reader/writer (iClass, MiFARE, DESFire, 13.56Mhz cards) and built-in 125Khz Prox reader.
iCAM7100 (LCD models)						
Model Number	**LCD Display**	**On-Screen PIN PAD**	**125Khz Prox Card**	**13.56Mhz iClass, MiFARE, & DESFire Cards**	**Read/Write Iris Data to Card***	**Description**
iCAM7101	Yes	Yes	No	No	No	Dual iris recognition camera, TCP/IP enabled, with embedded 5M pixel face camera, 4.3" Touch Screen LCD, On-Screen PIN Pad, 6 Function Buttons, and Front Panel USB Port (Base Model with LCD)
iCAM7111-U1	Yes	Yes	No	Yes	Yes	iCAM7101 with built-in smart card reader/writer (iClass, MiFARE, DESFire, 13.56Mhz cards)
iCAM7111-M1	Yes	Yes	Yes	Yes	Yes	iCAM7000 with built-in smart card reader/writer (iClass, MiFARE, DESFire, 13.56Mhz cards) and built-in 125Khz Prox reader.

***** Iris data cannot be stored on 125Khz cards, or on Smart Cards with insufficient capacity.

5. iCAM7000 & 7100 Model Series Hardware Information

The iCAM7000 series cameras are available in two model series:

- The iCAM7000 model series cameras are the base model with only the option for a built-in card reader.

- The iCAM7100 model series cameras have a LCD touch-screen, six function keys, and other enhancements in addition to the option for a built-in card reader.

All iCAM7000 series cameras contain an intuitive and easy to operate user interface designed around an optical system containing an integrated high-speed multi-sensor iris imager array. The iCAM7000 series is capable of processing and outputting high quality ISO standards compliant iris images of a subject in less than one second.

The iCAM7000 series also contain a 5MP CMOS face camera with flash, a front panel multi-color LED status indicator, voice/sound prompt indication, and motorized tilt adjustment.

5.1 iCAM7000/7100 Series - General Specifications:

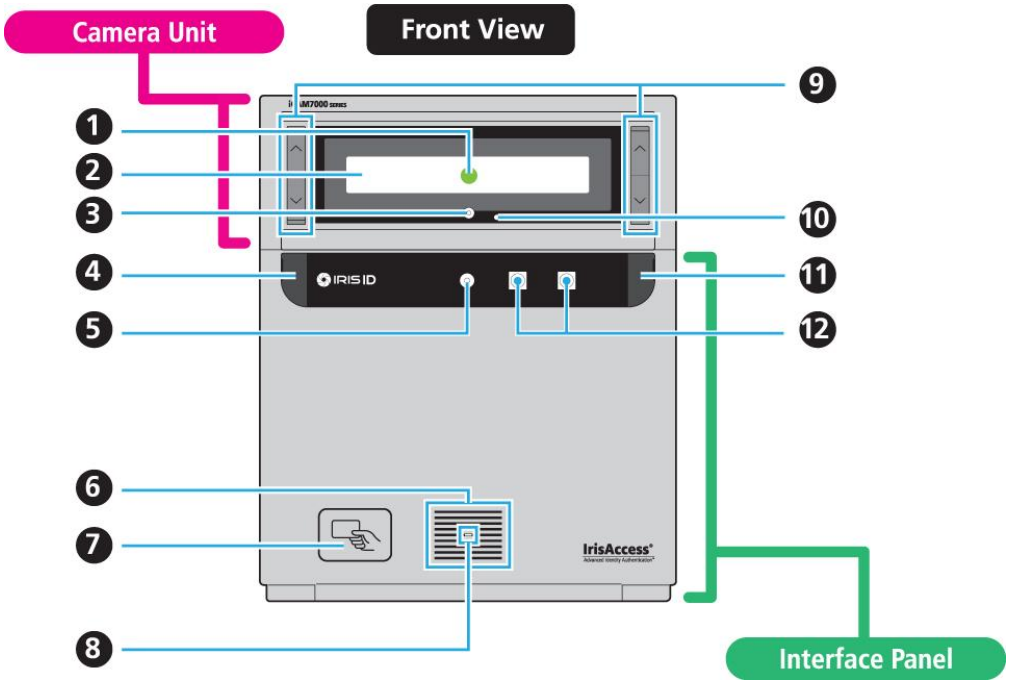
The iCAM7000 and iCAM7100 Model specifications:

Dimension (W x H x D)	7.01” x 8.31” x 2.52” (178mm x 211mm x 64mm)
Weight	3.5lbs (1.6kg)
Power Input / Consumption	12-24VDC, 2.0Amps @ 12VDC/24W
Status LED	Multi-Color: Red, Green, Blue for status and alarm indication
Iris Operating Range Indicator	Dual Color: Orange (out of range), Green (in range)
Voice Indication	English standard, other available by download
Iris Capture Range	12” ~ 14” (31cm ~ 35cm)
Flash	High output flash for face capture
Face Image Camera	Face camera CMOS – 5MP
Relays x 2	Control for user defined operations
Operating Temperature	32 °F ~ 113°F (0°C ~ 45°C)
Storage Temperature	-4°F ~ 203°F (-20°C ~ 95°C)
Humidity	Up to 90% non-condensing
Iris & Face Camera Rotation Angle	+35°/-25°
Communications	Ethernet (LAN, WAN), RS422, RS232
Inputs/Outputs	Wiegand In, Wiegand Out, Dry Contact Relay x 2, Programmable GPIO x 4, Optional Embedded Proximity Card Reader, Optional Embedded Smart Card Reader
Equipment Supplied with iCAM	Instruction Manual – Hardware Guide

Additional iCAM7100 Model specifications:

User Input	Function keys six (user definable)
Touch Screen LCD	4.3” diagonal (480 x 272 pixels)
PIN Pad	Pop-up on screen PIN pad
External Media Device Connectivity	Secure user accessible USB port

5.2 iCAM7000 Series - Front View

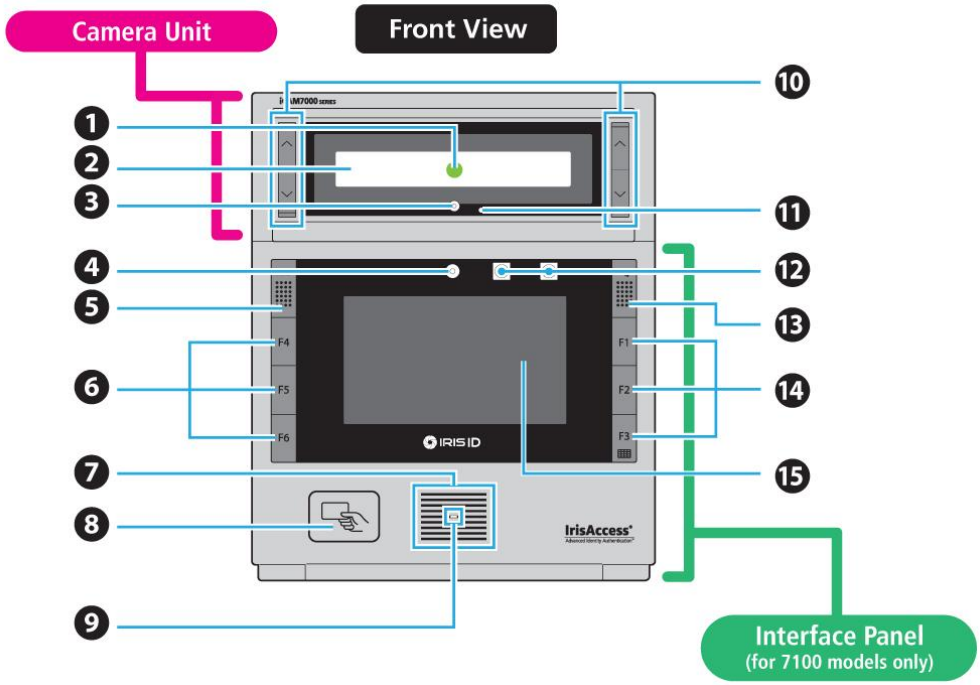


iCAM7010-U1 shown

1. **Alignment Guide –** An LED indicator light that will change color to help the user determine the proper position when using the iris camera.
2. **Mirror** – A cold mirror designed to assist with the acquisition of an iris image. Both eyes are to be viewable in the mirror when in use.
3. **Face Camera** – A camera that is capable of taking up to a 5 Megapixel face image capture.
4. **Screw Cap** – These caps hide the screws that secure the Interface Panel door. One screw cap is on each side of the door panel. The right screw cap hides the right screw. The left screw cap hides the left screw.
5. **CCTV Camera (optional)** – Closed Circuit Television camera (CCTV) is available for use with a DVR or other CCTV device(s). This camera is available as an option to the iCAM7000 series units.
6. **Speaker –** Internal mono speaker used for audible announcements.
7. **Card Reader (optional)** – Built-in Card reader available with select models. (Refer to model description list for card reader details specific to your model.)
8. **Status LED** – Tri-Color LED indicating unit ready status. Red = Not ready or not connected, or the unit has rejected the identification/verification of a user. Blue – Powered and attempting to establish a connection or function sequence. Green = Unit is in the ready/active state or has successfully identified/verified a user.
9. **Up / Down Tilt Buttons –** Located on both sides of the camera assembly, the tilt buttons are used to adjust the tilt position of the camera unit. Tilting of the camera assembly allows the user to properly align the camera position for iris or face image capture. The Up tilt button(s) will tilt the camera unit to a higher user height setting. The Down tilt button(s) will tilt the camera unit to a lower user height setting. The tilt range of the camera unit assembly is Up = +35 degrees and Down = -25 degrees from the default position.
10. **Face Camera Flash** – A white LED that works in conjunction with the Face Camera only.

11. **Screw Cap** – These screw caps hide the screws that allow for the unit door to open. One screw cap is placed on each side of the door panel. The left screw cap hides the left screw and the right screw cap hides the right screw.
12. **Proximity Sensor** – Detects the presence of a user within a fixed distance from the camera unit. The proximity sensor is primarily used to activate the camera and/or engage the unit from power-save mode.

5.3 iCAM7100 Model line - Front View



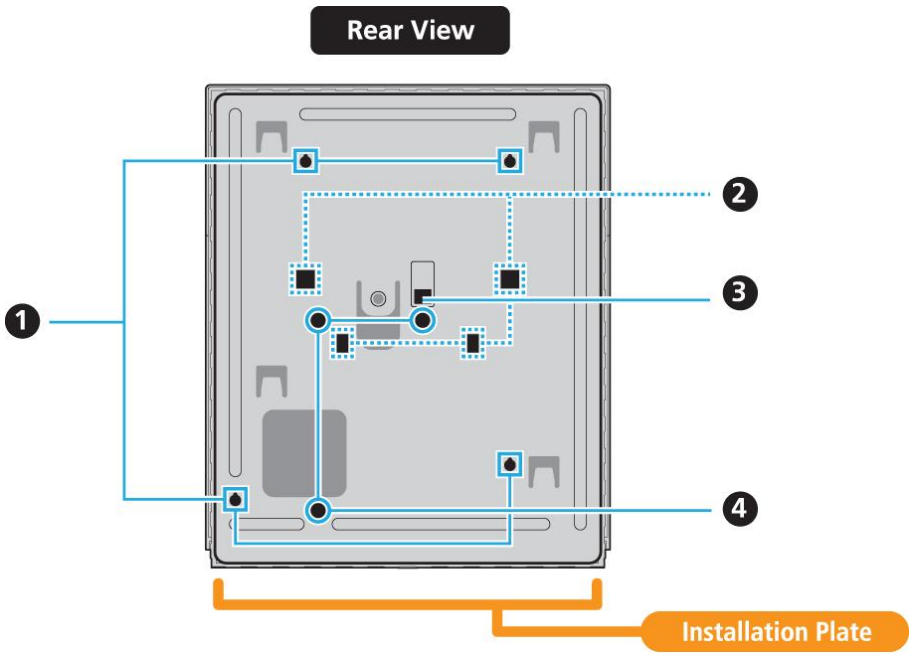
iCAM7111-U1 shown

1. **Alignment Guide –** An LED indicator light that will change color to help the user determine the proper position when using the iris camera.
2. **Mirror** – A cold mirror designed to assist with the acquisition of an iris image. Both eyes are to be viewable in the mirror when in use.
3. **Face Camera** – A camera that is capable of taking up to a 5 Megapixel face image capture.
4. **CCTV Camera (optional)** – Closed Circuit Television camera (CCTV) is available for use with a DVR or other CCTV device(s). This camera is available as an option to the iCAM7000 series units.
5. **MIC / Screw Cap** – These caps hide the screws that secure the Interface Panel door. One screw cap is on each side of the door panel. The right screw cap hides the right screw. The left screw cap hides the left screw and internal microphone (selectable by software).
6. **Function Buttons** (Left Side of Unit) –F4, F5, and F6 are 3 of the Function buttons available on the iCAM7100 model unit. The Function of these buttons are software/firmware dependent.
7. **Speaker –** Internal mono speaker used for audible announcements.
8. **Card Reader (optional)** – Built-in Card reader available with select models. (Refer to model description list for card reader details specific to your model.)
9. **Status LED** – Tri-Color LED indicating unit ready status. Red = Not ready or not connected to controlling software or device, or the unit has rejected the identification/verification of a user. Blue – Powered and attempting to establish a connection or function sequence. Green = Unit is in the ready/active state or has successfully identified/verified a user.

10. **Up / Down Tilt Buttons –** Located on both sides of the camera assembly, the tilt buttons are used to adjust the tilt position of the camera unit. Tilting of the camera assembly allows the user to properly align the camera position for iris or face image capture. The Up tilt button(s) will tilt the camera unit to a higher user height setting. The Down tilt button(s) will tilt the camera unit to a lower user height setting. The tilt range of the camera unit assembly is Up = +35 degrees and Down = -25 degrees from the default position.
11. **Face Camera Flash** – A white LED that works in conjunction with the Face Camera only.
12. **Proximity Sensor** – Detects the presence of a user within a fixed distance from the camera unit. The proximity sensor is primarily used to activate the camera and/or engage the unit from power-save mode.
13. **USB Connector / Screw CAP** - These screw caps hide the screws that allow for the unit door to open. One screw cap is placed on each side of the door panel. The right screw cap hides the right screw and external USB Port. The USB Port is software enabled and the operation and function is determined by camera software and firmware.
14. **Function Buttons** - (Right Side of Unit) –F1, F2, and F3 are 3 of the Function buttons available on the iCAM7100 model unit. The Function of these buttons are software/firmware dependent.
15. **4.3" Touch Screen LCD** – A color Liquid Crystal Display (LCD) that allows for PIN pad, and additional options to be used directly from the screen. The LCD is also used for providing user instructions, operating status, Additional visual information and cues are provided to enhance the user experience for an intuitive usage process.

Note: The F3 Key by default is designated to display the on-screen PIN PAD.*
The On-screen PIN PAD can be disabled in the web interface.

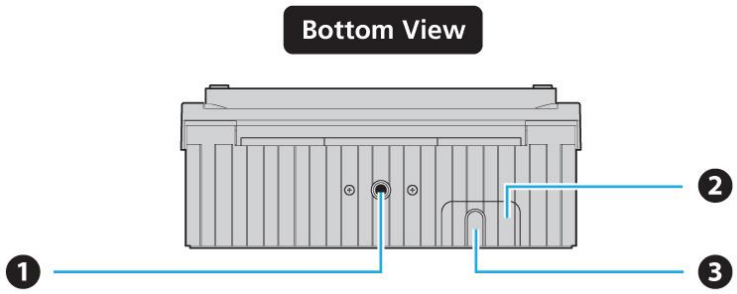
5.4 iCAM7000 & iCAM7100 – Rear View



Installation Plate – A plate located on the back of the unit that can be used to perform surface mount installations. This plate connects the unit to the desired installation surface. The plate is connected to the iCAM by an Installation plate screw and supplemental screws on the back of the unit.

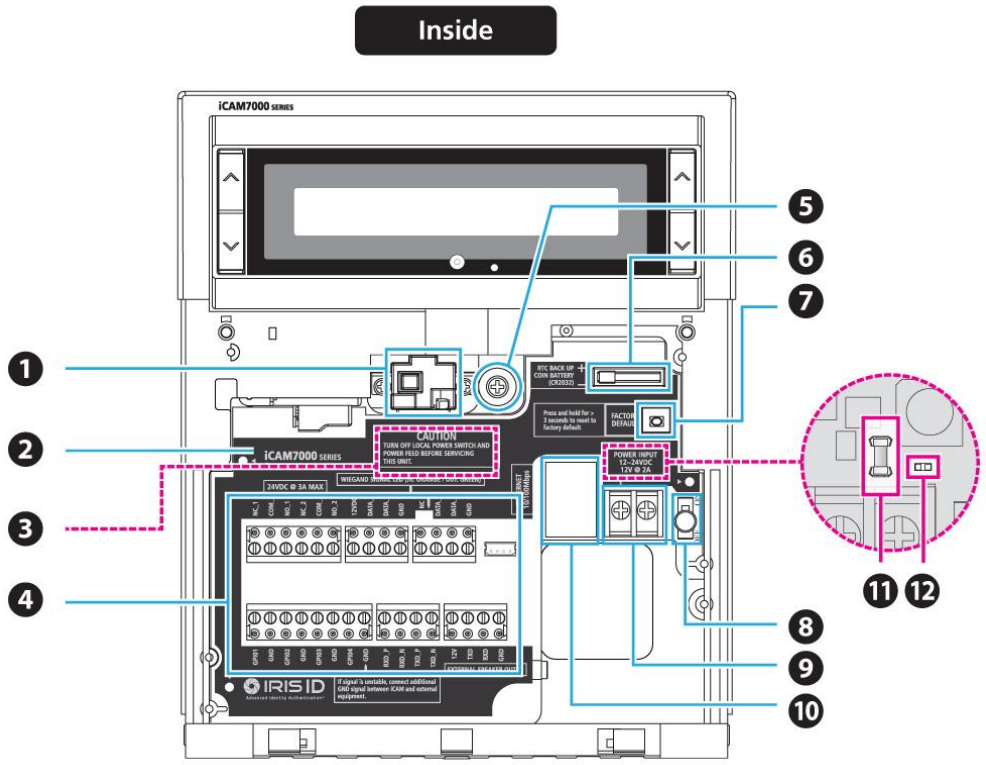
1. **Surface Mounting Screw Hole** – A hole that allows a screw to connect the back plate to the interior of the main unit. When removed, the exterior back plate can be removed.
2. **Gang Box Screw Hole** – Screw hole positions allowing for a unit to be directly connected/mounted onto a Gang Box for installation.
3. **Tamper Switch** – Two switches found in the front and back of the unit. Operation of the tamper switch is software selectable.
4. **Desktop Stand Hole** – screw hole designed for use with the optional Desktop Stand kit. A screw will be provided with the Desktop stand kit that will affix to the stand hole.

5.5 iCAM7000 & 7100 Series - Bottom View



1. **Tripod Socket** (1/4-20 (1/4 diameter, 20 threads per inch))
2. **Cable Channel** – An area within the unit to run wire through for purposes of connection and install.
3. **Knock-out** – A plastic covering that can be removed for the purposes of installation and ease of wire management, etc.

5.6 iCAM7000 and iCAM7100 - Inside View



1. **Tamper Switch** - Two switches found in the front and back of the unit. Operation of the tamper switch is software selectable.
2. **Wiring Legend Guide** – A guide located inside of the iCAM unit. This guide provides detail of the internal input/output connections and wiring needs for various options available for use with the iCAM unit.
3. **Extra Fuse** – Located behind the wiring legend guide, an extra fuse is provided in the event that replacement of a fuse is needed.
4. **Input / Output Connections** – Internal connections providing Relays, Wiegand Input, Wiegand output, GPI/O, RS422 Output, Serial Card Reader, and external speaker output.
5. **Installation Plate Screw** – A screw located in the interior of the unit that affixes the installation plate to the unit. Unscrew this plate to remove the installation plate from the unit.
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 iCAM 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. **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.
9. **Power Connection** – Consists of 2 screw down connections. These connections are positive and ground. (12VDC~ 24VDC input – 12VDC @ 2A.)
10. **Ethernet Connection** – An RJ-45 connection allowing for CAT-5e, CAT-6, CAT-6e wire connections at a speed of up to 100 MBPS.

11. **Fuse** – Protects the iCAM circuitry from excessive current draw or incorrect polarity.
12. **Power LED** – Indicated that the unit is powered on and functioning correctly.

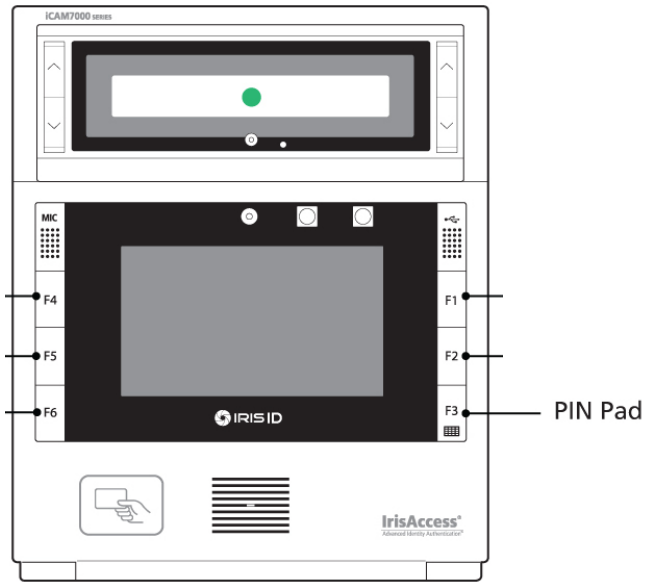
6. iCAM7100 Model Interface Panel Function Buttons

6.1 6 Function Buttons (7100 models only)

Function buttons have been designed to further enhance the experience of the iCAM7100 model units. Typically, such function buttons can be made available for purposes of time and attendance based applications, on-screen selections without direct use of the touch screen, and customizable options that can be set by the user.

–F1, F2, and F3 are on the right side of unit, and F4, F5, and F6 are on the left side of unit. The functions of these buttons are software/firmware dependent.

**Note: The F3 Key by default is designated to display the on-screen PIN PAD.*



6.2 Function key operation description

In Option 3 Mode, the function keys on the iCAM7100 models are currently used to provide a means of recording the purpose of a transaction.

Typical usage is performed in conjunction with a Time and Attendance application where the purpose of the transaction needs to be entered by the user and recorded.

When enabled the function keys act as follows:

- All six keys have installer definable labels (shown on LCD) to indicate the purpose of the keys.

- After a successful identification the function key selection screen appears, this allows the user to select the purpose of the transaction.

    - Once entered, the transaction record (time/date/location) along with the function key press is sent to the IrisServer and recorded in the transaction log.

- The recorded function key is simply a 1,2,3,4,5, or 6 corresponding to the function key pressed.

- This key record can then be resolved in the time attendance application along with the normal transaction data.

  ***Note:** This is only available on the iCAM7100 when used in Option 3 operational mode (iCAM provides matching on the camera).*

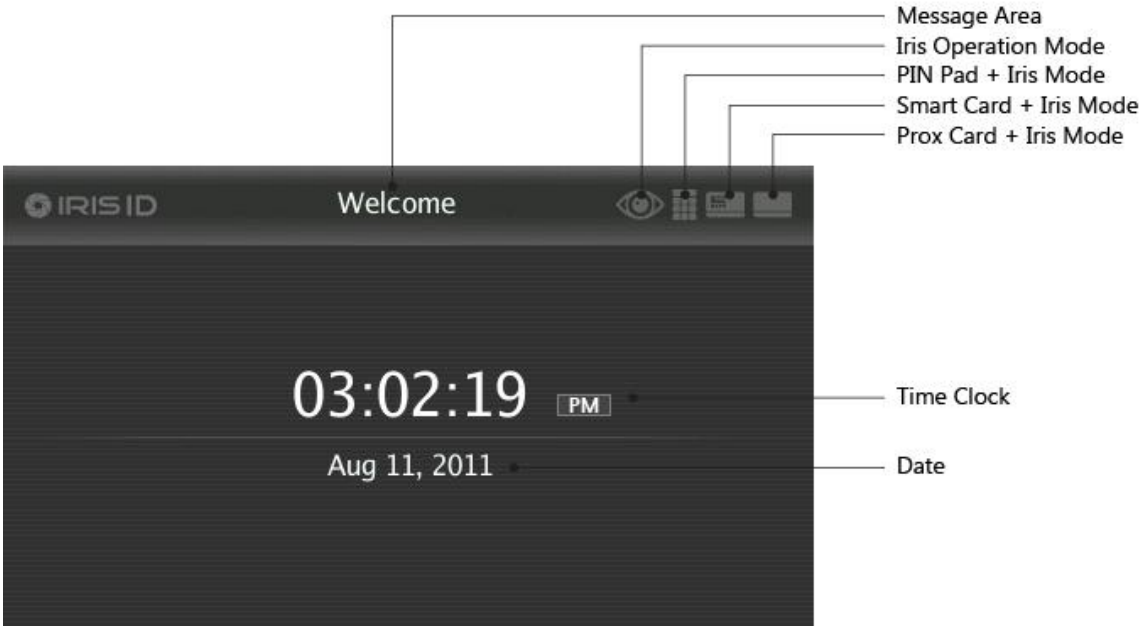
7. iCAM7100 Model LCD Screen

7.1 Overview

The following screen is a view of the Main LCD Screen. View the following Main Screen layout image to understand the items viewable on the screen.

7.2 Main LCD Screen Layout

Main Screen



7.3 Additional LCD Screens

Depending on the configuration and usage function of the device, different screens may be displayed on the iCAM7100 models. View the following images for a description of some of these screens.

Initial Start-up LCD Main Screen

This screen appears at the initial boot up of the iCAM. The dashes in the time and date fields display when the iCAM time and date has not been set.

The time/date setting is provided to the unit based on the iCAM operational mode.

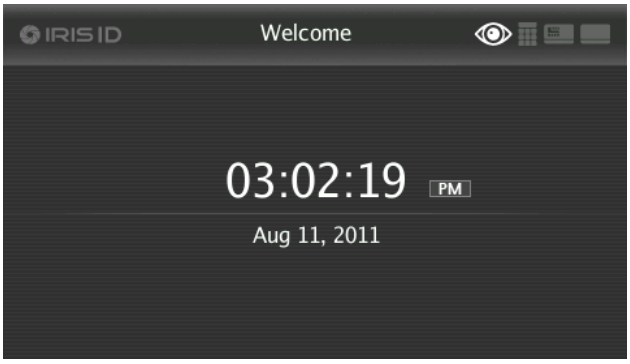
Operational Mode 1 (Option 1): When controlled by either an ICU, IrisEnroll4000, or iDATA SDK based application.

Operational Mode 2 (Option 2): Time and Date set in the iCAM (web) configuration interface.

Operational Mode 3 (Option 3): When connected to the IrisServer (EAC software).

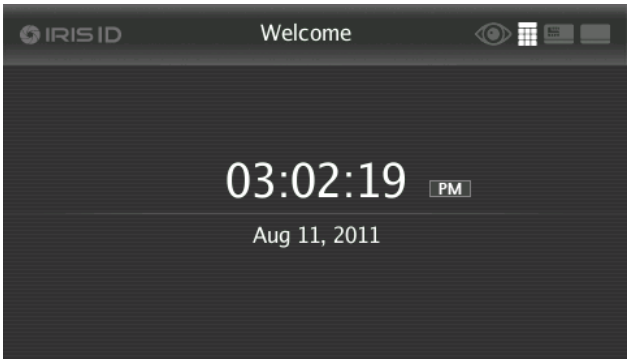
**Note: The display of the clock is unable to be turned off in Option 1 and 2 modes. 24 hour –time is only available in Option 3 mode.*

Main LCD Screen in Iris Identification Mode (with time set)



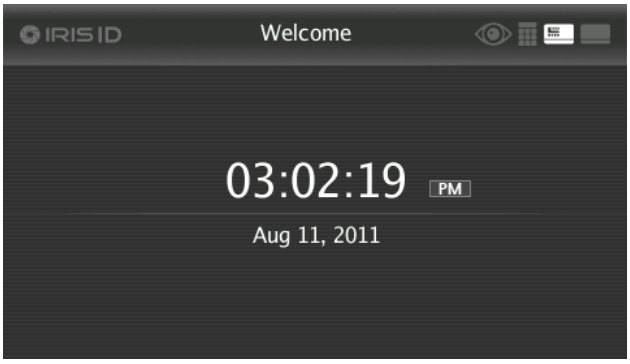
The mode selection will display on the top right corner (Iris only mode shown) for the appropriate usage.

Main LCD Screen in Pin Verification Mode – PIN + Iris (with time set)



The mode selection will display on the top right corner (Iris + PIN mode shown) for the appropriate usage.

Main LCD Screen in Smart Card Mode – Smart Card + Iris (with time set)

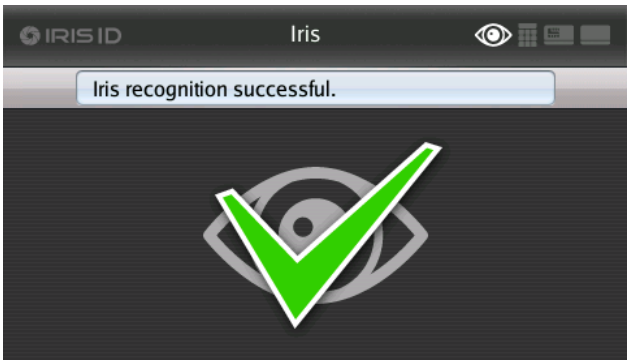


The mode selection will display on the top right corner (Iris + Smart Card mode shown) for the appropriate usage.

Main LCD Screen in Prox Verification Mode – Prox Card + Iris (with time set)

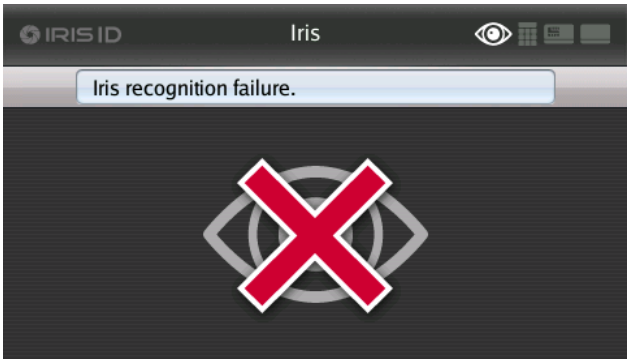
The mode selection will display on the top right corner (Iris + Prox Card mode shown) for the appropriate usage.

Successful Recognition



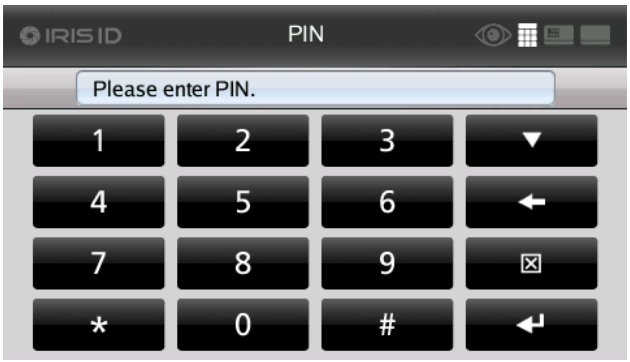
When a successful recognition is performed (in this case, Iris Only mode) a green check-mark will appear on the LCD display - indicating a successful event (iCAM71xx units only).

Recognition Failure



When a recognition failure is performed (in this case, Iris Only mode) a red “x” will appear on the LCD display - indicating a failure/rejection event (iCAM71xx units only).

PIN Pad Pop-up Screen (F3 function Key to show/hide when not in iCAM + PIN recognition mode)

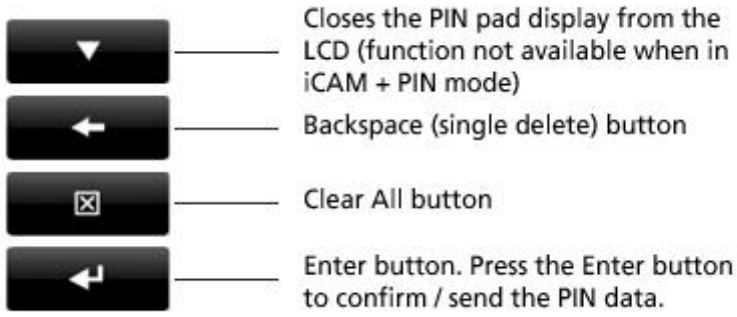


PACS (Physical Access Control System) PIN Mode is enabled by default and can be used to directly output a Wiegand signal from the iCAM to an Access Control System. The PACS PIN Wiegand output format is selectable in the iCAM configuration interface. The PACS PIN screen can be displayed on the LCD screen using the F3 function key. The F3 Key can be pressed again to hide the PIN Pad.

The PIN Pad is also available by placing the iCAM (or controlling device) in Iris + PIN (local) verification mode. When in this mode the PIN screen will appear continuously and PIN entry must be used to enable iCAM operation. (PACS PIN Mode will not be available while in Iris+PIN Mode)

In Iris + PIN mode, press the number keys and press the Enter (bottom right) key to input your selection. A maximum of 8 characters can be selected. The PIN entered will be matched against the user database in the EAC system.

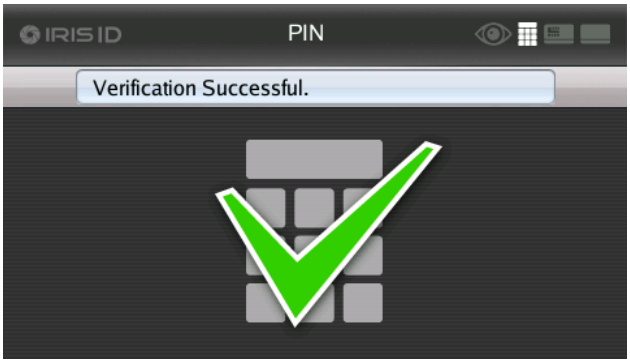
PIN Pad Pop-up Screen Action Key Details



The Pin Pad screen displays 4 action key virtual buttons on the LCD Display when the PIN Pad is engaged. These action keys are located on the right hand side of the LCD display when the Pin Pad is displayed.

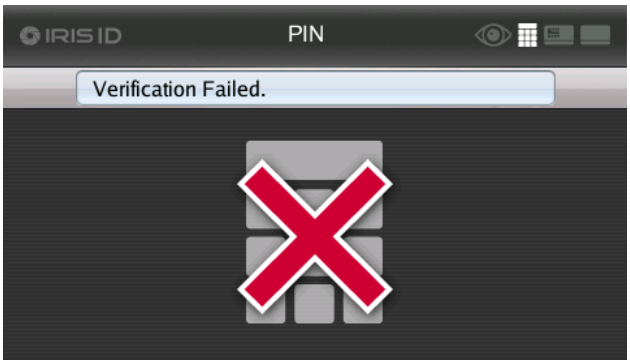
- Close Pin Pad – Allows you to close/hide the virtual Keyboard from the LCD display of an iCAM7100 model camera unit. This key will perform the same function as the physical F3 button. When in Iris + Pin recognition mode, the close pin virtual action button and F3 key will not function.
- Backspace – This virtual action button located on the Pin pad LCD display allows for a single character deletion from left to right (per press).
- Clear All - This virtual action button located on the Pin Pad LCD display allows for a full line deletion of any characters currently typed. This places the cursor back in the beginning position, ready for typing in a full Pin.
- Enter Button – This virtual action button located on the bottom right most part of the Pin Pad executes the information typed in the Pin Pad. Press the Enter button when the pin has been entered correctly.

Successful Verification of PIN + Iris



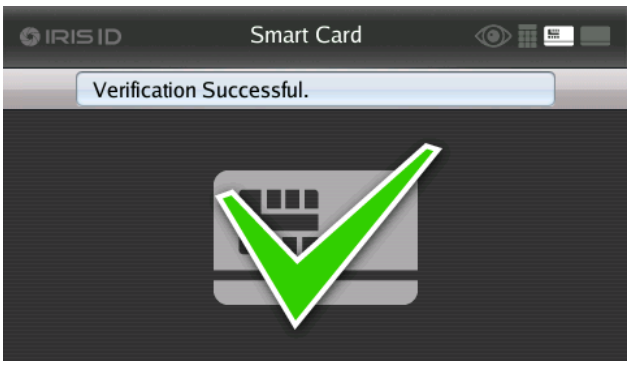
When a successful verification is performed (in this case, entering the correct PIN + Iris) a green check-mark will appear on the LCD display - indicating a successful event (iCAM71xx units only).

Verification Failure of PIN + Iris



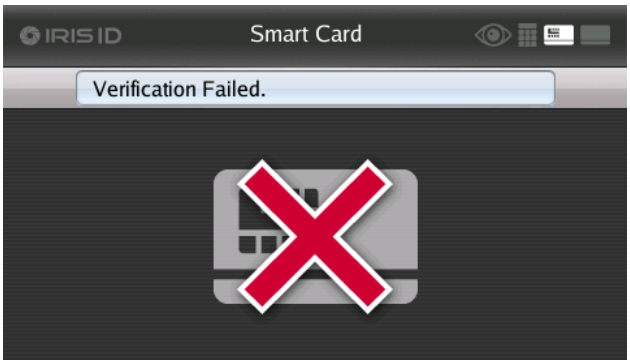
When a failure/verification is performed (in this case, presenting either the wrong pin and/or Iris) a red "X" will appear on the LCD display - indicating a verification failure / rejection event (iCAM71xx units only).

Successful Verification of Smart Card + Iris



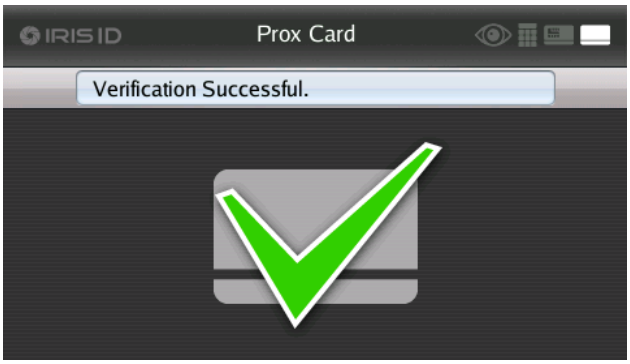
When a successful verification is performed (in this case, presenting the correct SmartCard + Iris) a green check-mark will appear on the LCD display - indicating a successful event (iCAM71xx units only).

Verification Failure of Smart Card + Iris



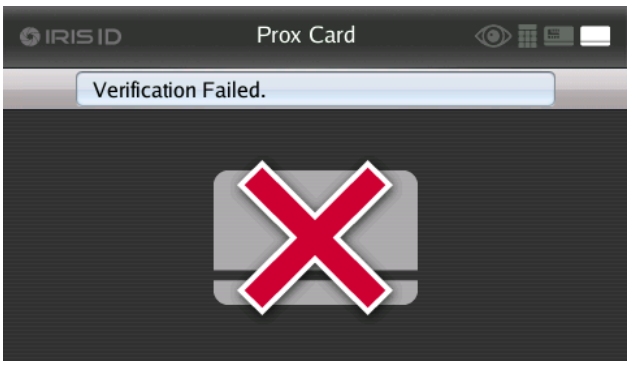
When a verification failure is performed (in this case, presenting the incorrect SmartCard + Iris) a red "X" will appear on the LCD display - indicating a verification failure / rejection event (iCAM71xx units only).

Successful Verification of Prox Card + Iris



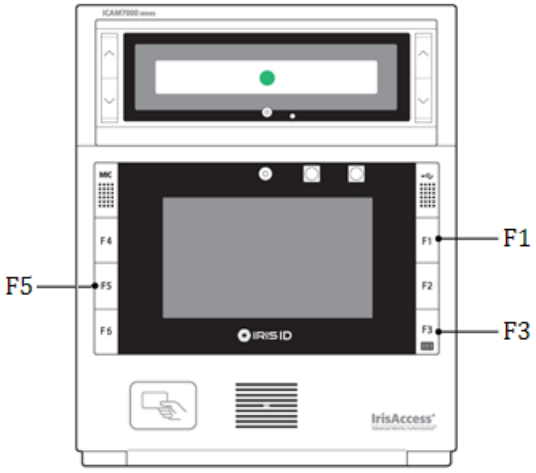
When a successful verification is performed (in this case, presenting the correct Prox Card + Iris) a green check-mark will appear on the LCD display - indicating a successful event (iCAM71xx units only).

Verification Failure of Prox Card + Iris



When a verification failure is performed (in this case, presenting the incorrect Prox Card + Iris) a red "X" will appear on the LCD display - indicating a verification failure event (iCAM71xx units only).

Touch-Screen Calibration Utility



The iCAM7100 model camera units contain a touch-screen display that can be calibrated if needed by the installer. To initiate the iCAM7100 touch-screen calibration utility the unit must be powered on properly and follow the below step procedure:

- Hold the following Function keys located on the front door panel:
  - **F1**, **F3**, & **F5** down *simultaneously* for (at least) 10 seconds.
- The Calibration screen will be displayed on the LCD.
- Touch the top of your finger to touch the cross-hair images as the display. A total of 5 will be displayed.

**Note*: After the 5th cross-hair is touched the iCAM will reboot.

8. Operational Mode Descriptions

The iCAM7000 Series camera includes multiple operational modes which allows it to not only to be a direct replacement to the iCAM4000 series camera, but also provides enhanced features, flexibility, and compatibility with current and future Iris ID software offerings. Each iCAM contains multiple operational modes standard, which are easily selectable within the iCAM7000's internal configuration web-based interface. The configuration web interface for the iCAM does not require installed software since it is accessible directly through an Internet browser connected to the iCAM network.

Before using your iCAM7000 series unit, determine how the unit is going to be used. View the diagram images in this section to determine which operational mode is best for the installation requirements in which the iCAM will be used.

8.1 Available Operational Modes and device feature compatibility

Depending on the type of iCAM7000 Series camera unit and desired functions, the iCAM can be used to perform in different ways with your system.

The below chart describes the iCAM7000 Series Model versions by available option and operational mode option:

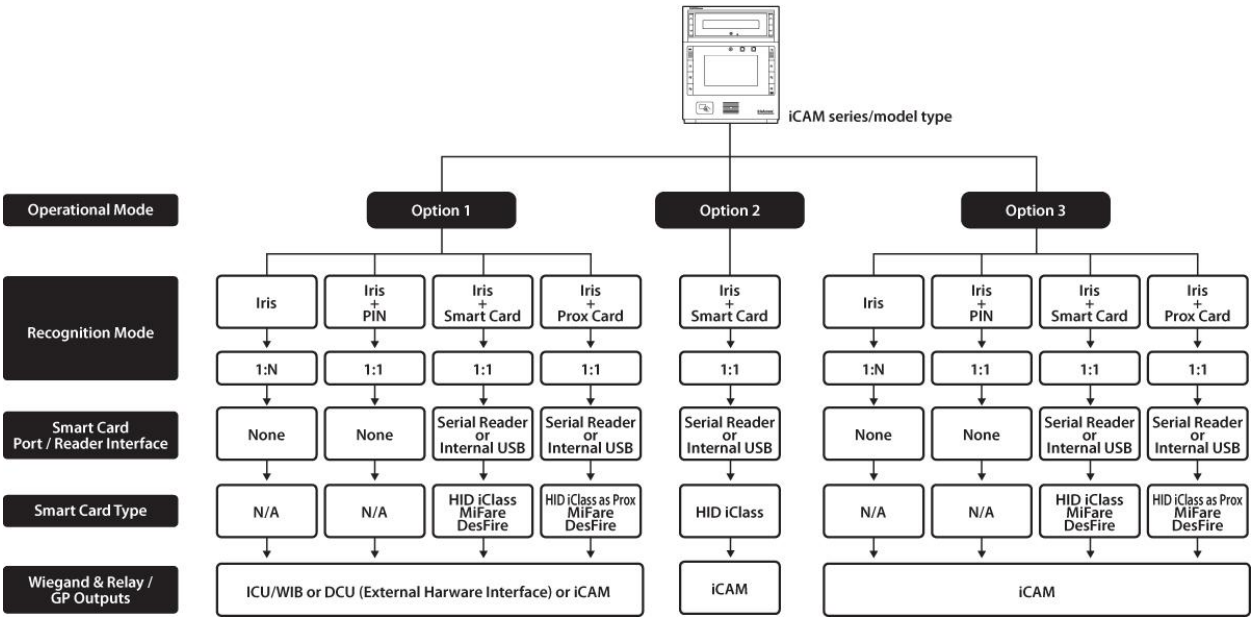
	Iris Only	125Khz Prox Card	13.56Mhz iClass, MiFARE, & DESFire Cards	Read/Write Iris Data to Card*	LCD Display included	Popup PIN-pad	Option1 iCAM+ICU	Option2 iCAM+card	Option3 iCAM, no ICU
iCAM7000	Yes	No	No	No	No	No	Yes	No	Yes
iCAM7010-U1	Yes	No	Yes	Yes (Option 2 - write only via CMA / Option 3 - Read only)	No	No	Yes	Yes (No MiFARE or DESFire)	Yes
iCAM7010-M1	Yes	Yes (option 1 & 3)	Yes	Yes (Option 2 - write only via CMA / Option 3 - Read only)	No	No	Yes	Yes (No MiFARE or DESFire)	Yes
iCAM7101	Yes	No	No	No	Yes	Yes	Yes	No	Yes
iCAM7111-U1	Yes	No	Yes	Yes (Option 2 - write only via CMA / Option 3 - Read only)	Yes	Yes	Yes	Yes (No MiFARE or DESFire)	Yes
iCAM7111-M1	Yes	Yes (option 1 & 3)	Yes	Yes (Option 2 - write only via CMA / Option 3 - Read only)	Yes	Yes	Yes	Yes (No MiFARE or DESFire)	Yes

***** Iris data cannot be stored on 125Khz cards, or on Smart Cards with insufficient capacity.

8.2 Operational Flow

Flow chart by model, option and usage:

The Flow chart describes the usage of an iCAM7000 Series camera unit per operational mode option, recognition/verification mode, modality options, and outputs.



*** Note:** Option 1 recognition modes require an ICU4000.

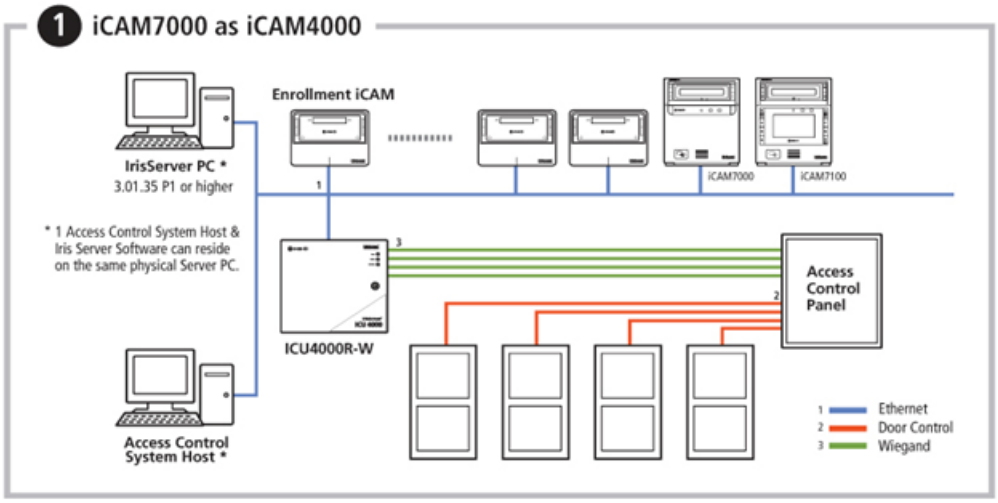
8.3 Operational Mode Breakdown

Available Operational Modes:

- **Option 1**: Networked iCAM Control
- **Option 2**: Smart-Card On-Device Verification Mode
- **Option 3**: On-Device iCAM Control and Iris Matching Mode

View the following diagrams to determine the best type of operation to use with your installation:

Operational Mode - Option 1: Networked iCAM Control / Iris Matching Mode"

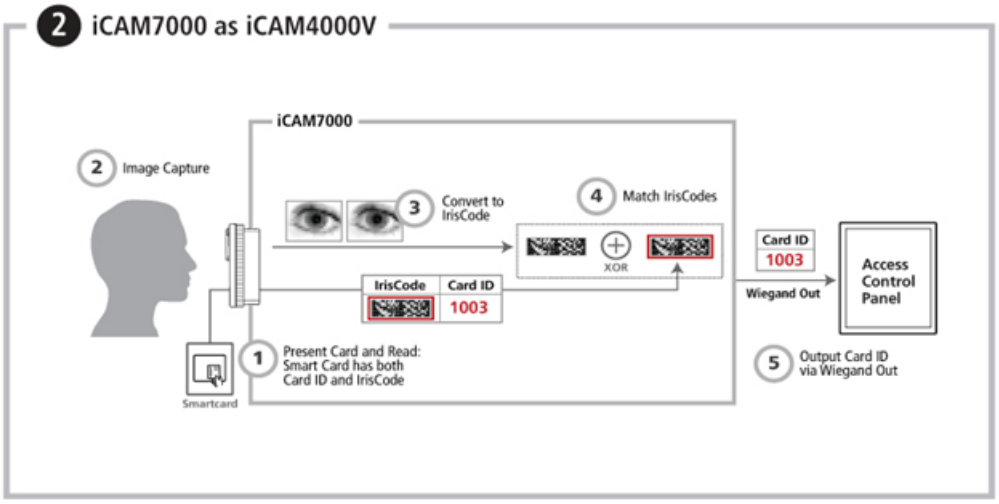


When Option 1 is selected, the iCAM will operate as part of an IrisAccess™ Entry Access Control System in conjunction with an ICU4000R, IrisEnroll4000, or an application based on the EAC iDATA Toolkit. In addition Option 1 should be selected for use with applications written using the iData™ SDK (iCAM4000 Series compatibility).

In Option 1 Mode, the iCAM will only provide images to other devices or software. iCAM control and iris matching would then be performed by the device or software controlling the iCAM via the network.

IMPORTANT: *Option 1 is the mode which needs to be selected for using the iCAM with an enrollment application. If the same iCAM is also used in Option 3 mode as a "remote unit", then the iCAM must be switched to Option 1to be accessible by an enrollment application.*

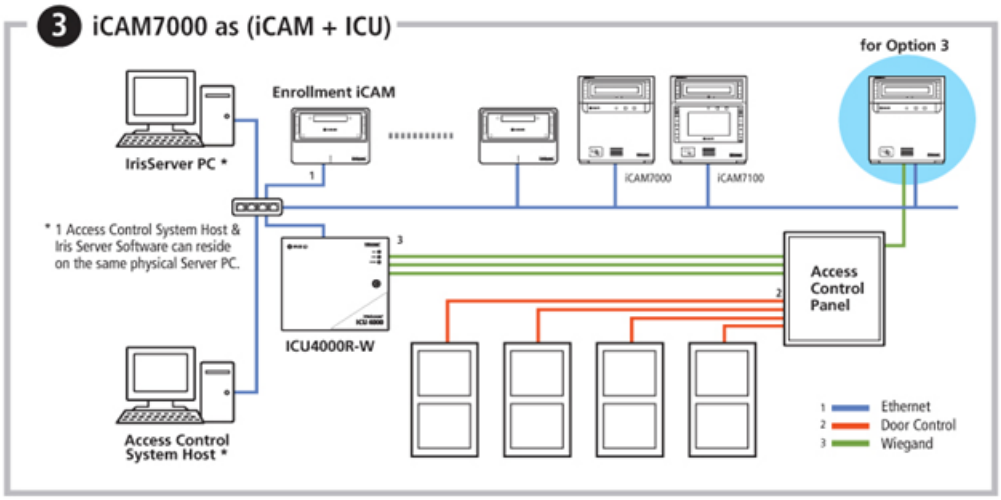
Operational Mode - "Option 2: Smart Card On-Device Verification Mode"



When Option 2 is selected, the iCAM7000 operates as a stand-alone device for verification (1:1) of the iris templates on a smart card. This mode is generally for use with iData CMA software and/or pre-existing smart cards with iris templates created by IrisAccess EAC or compatible 3rd party applications.

**Note: "iCAM7000 Stand-Alone SmartCard Verification Mode" can only be used when a card reader (internal or external) is used with the iCAM7000 series unit.*

Operational Mode - "Option 3: On Device iCAM Control and Iris Matching Mode"



When option 3 is selected, the iCAM is controlled and iris matched inside the iCAM. This mode provides the most of the functions of the iCAM4000, ICU4000, DCU4000 all within the iCAM7000. This option is designed for use with compatible IrisAccess EAC software.

**Note: If attempting to use an iCAM7000 series unit in operational mode "Option 3", compatible IrisAccess EAC software MUST be used for full functionality of this option.*

***IMPORTANT**: If you are using an iCAM7000 in "Option 3" operational mode – when performing enrollments, and when trying to connect to the IrisEnrol4000 application within IrisAccess EAC software, the user must switch the operational mode to "option 1". Once enrollments have completed, the iCAM can be set back to operational mode "option 3" (if a dedicated iCAM is not being used for enrollment).*

9. The iCAM Configuration Interface

From a computer with an Internet browser (and connected to the network in which the iCAM7000 series unit is connected), type the IP address of the iCAM. For example, if the IP address of an iCAM is 192.168.5.100 (default IP), access the configuration web interface by typing http://192.168.5.100 in the Internet browser line.

Note: *An Internet connection is not required to access or use the iCAM web configuration. Only a network connection between the computer and iCAM is required.*

To login, the User ID required when prompted is **iCAM7000**. The Password is **iris7000**.

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

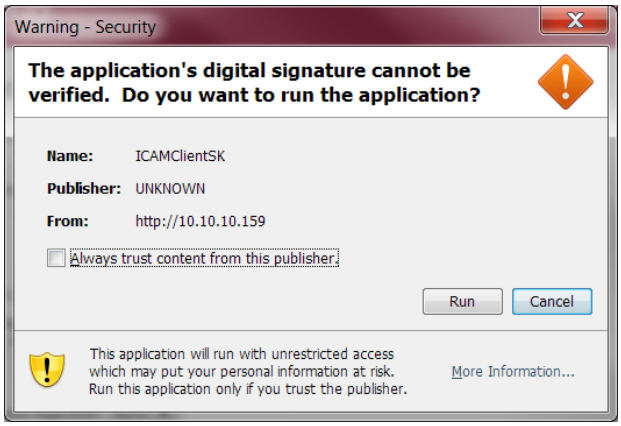
Once you have connected to the Web Configuration Interface of the iCAM7000, a wide variety of in depth setting configurations, information, and options become available to further resource your system.

** Note: The IP Address of each iCAM must be configured individually. Do not connect more than one un-configured iCAM to the network at any time to avoid IP Address conflicts. Standard web browsers (ex. Internet Explorer) can be used to configure the iCAM4000/4100.*

9.1 Initial Configuration Setup of iCAM7000 Series

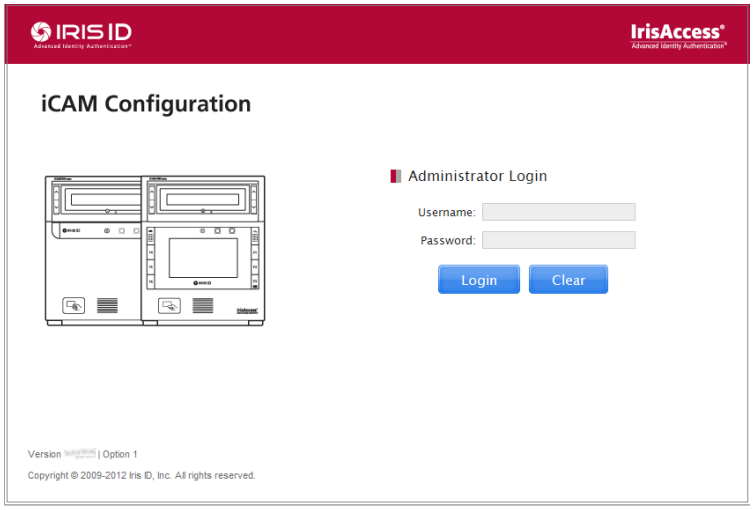
The IP Address of each iCAM must be changed individually. Do not connect more than one un-configured iCAM to the network at any one time to avoid IP Address conflicts. Any computer with a web browser (ex. Internet Explorer) can be used to configure the iCAM7000/7100. (Default IP settings used as reference.)

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



9.2 Configure IP address & Operational Mode using "iCAM Configuration Start Up Screen"

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://192.168.5.100 in the address bar then press ENTER. The iCAM login screen will appear
3. Enter the default Username: **iCAM7000** and Password: **iris7000** (both are case sensitive)



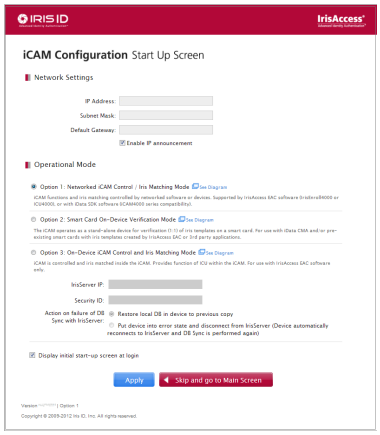
**Note: The "Start Up Screen" is displayed by default. This screen can be disabled by un-selecting the check box for "Display initial start-up screen at login". If the "Start Up Screen" does not appear, or to simply bypass the Start Up Screen" and enter the Main Menu, press the "Skip and go to Main Screen Button".*

****IMPORTANT***

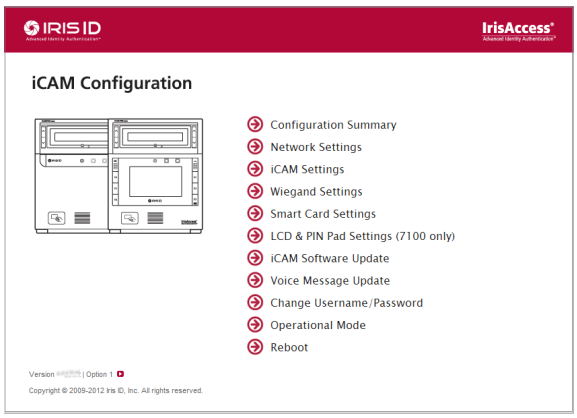
4. One of two Screens will appear (as shown in the following images). Follow the directions based on the screen that appears for your iCAM.

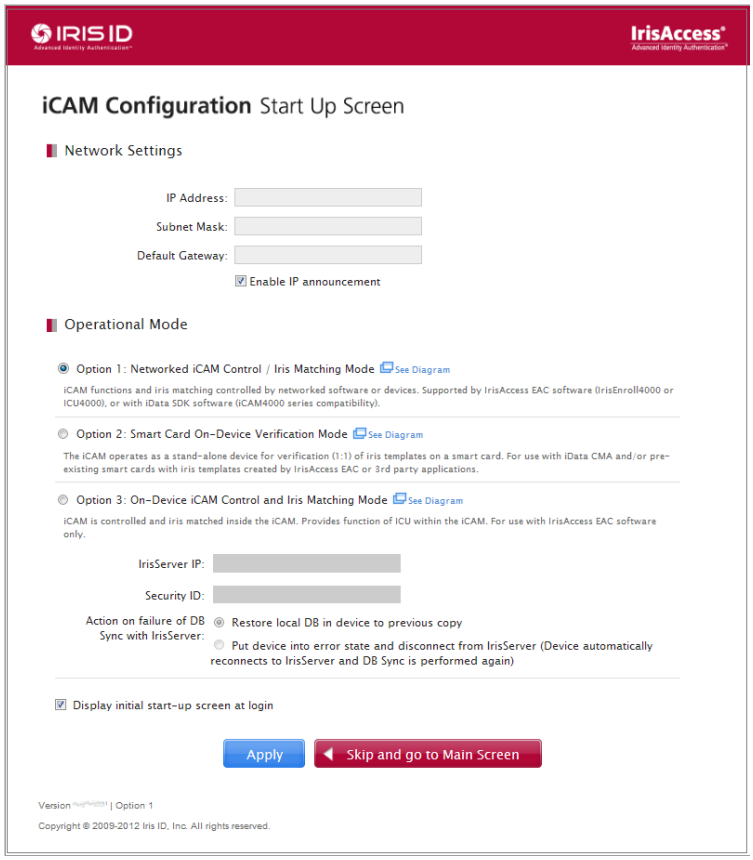
*iCAM Configuration *"Start Up Screen"* **OR** *iCAM Configuration "Main Menu" Screen

-Proceed to step 5 -Proceed to section 9.3



OR





iCAM IP Address Settings:

5. Enter the desired IP address data of the iCAM7000 series camera unit.
   - IP Address – Enter IP address (For example: 192.168.5.100)
   - Subnet Mask – Enter Subnet address (For example: 255.255.255.0)
   - Default Gateway – Enter Gateway address (For example: 192.168.5.254)

6. A selection to enable or disable IP announcement will also be available (set by default as active - Recommended).

Selecting or Modifying the Operational mode for iCAM:

7. Select the desired Operational Mode settings for the iCAM found in this screen as needed. (See following data for details.)

   - "**Option 1: Networked iCAM Control / Iris Matching Mode**" – When option 1 is selected, the iCAM will operate as part of an IrisAccess™ Entry Access Control System, or for use with iData™ SDK (iCAM4000 Series compatibility). The iCAM functions and iris matching are controlled by networked software or devices.
     IMPORTANT: If you are generally using option 3, this "option 1" mode may be needed to be used when performing enrollment.

   - "**Option 2: Smart Card On-Device Verification Mode**" - When option 2 is selected, the iCAM7000 operates as a stand-alone device for verification (1:1) of the iris templates on a

smart card. This mode is generally for use with iData CMA and/or pre-existing smart cards with iris templates created by IrisAccess EAC or compatible 3rd party applications.
***Note**: "iCAM7000 Stand-Alone Smart Card Verification Mode" can only be used when a card reader (internal or external) is used with the iCAM7000 series unit.*

- "**Option 3: On Device iCAM Control and Iris Matching Mode**" – When option 3 is selected, the iCAM is controlled and iris matched inside the iCAM. This mode provides the function of an ICU within the iCAM. This option is designed for use with compatible IrisAccess EAC software.

  ***Note**: If attempting to use an iCAM7000 series unit in operational mode "Option 3", compatible IrisAccess EAC software MUST be used for functionality of this option.*

  ***IMPORTANT**: If you are using an iCAM7000 in "Option 3" operational mode – when performing enrollments, and when trying to connect to the IrisEnrol4000 application within IrisAccess EAC software, the user must switch the operational mode to "option 1". Once enrollments have completed, the iCAM can be set back to operational mode "option 3" (if a dedicated iCAM is not being used for enrollment).*

In option 3 mode –the iCAM is controlled and iris matched inside the iCAM while providing function of an ICU within the iCAM. In order for these processes to work correctly the below information is required to be provided when "Option 3" is selected:

a. **IrisServer IP** - Enter the Iris Server IP address
b. **Security ID** - Enter a unique security ID for this unit (16 character requirement).
c. Action on Failure of 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).**

8. Display Initial Start-up screen at login – This checkbox can be selected to enable or unchecked to disable the initial start-up screen from appearing when the iCAM Configuration is logged into.

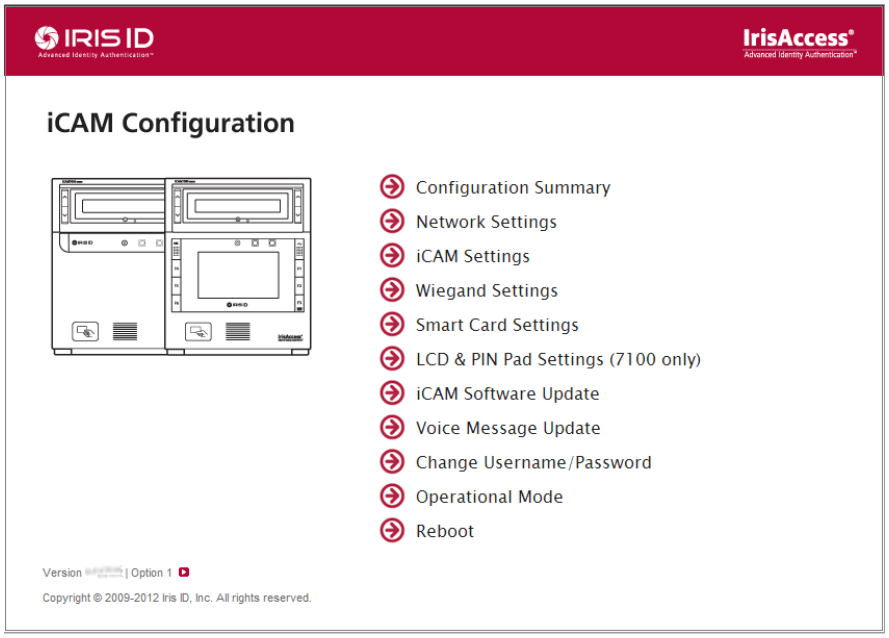
9. Once changes have been made to this screen, the iCAM will reboot for the changes to take effect. Allow the iCAM to complete the reboot process.

9.3 iCAM Configuration Setup - without use of "iCAM Configuration Start Up Screen"

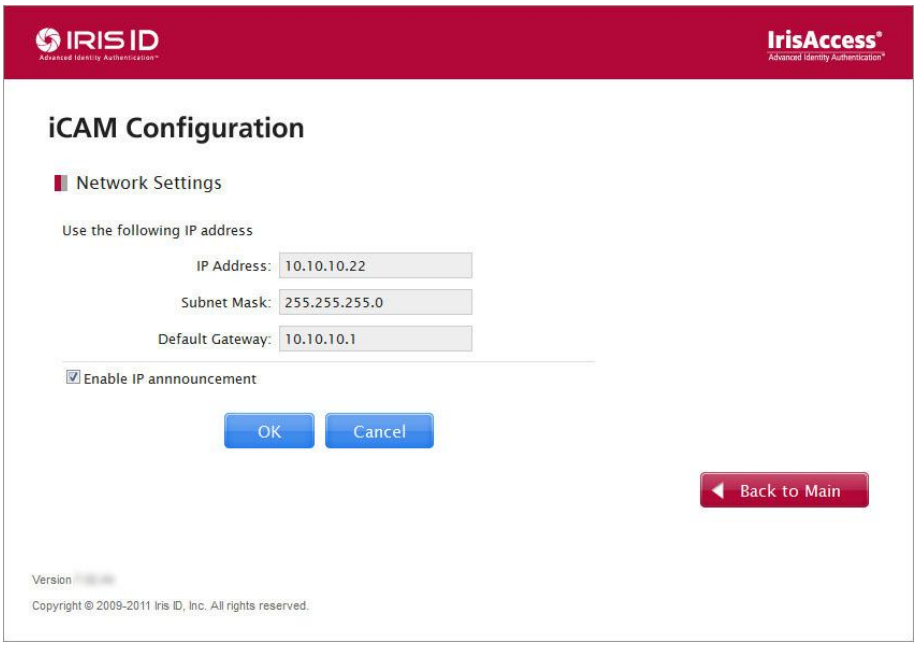
Follow this section to configure the iCAM for initial setup if you are not using the "iCAM Configuration Start Up Screen".

***Note**: Skip this section if you have already setup your iCAM settings using the "iCAM Configuration Start Up Screen".*

1. The iCAM Configuration Main Menu will appear.



2. Select Network Settings.



3. Enter the new IP address for the iCAM (default = 192.168.5.100)
4. Enter the new Subnet Mask for the iCAM (default = 255.255.255.0)
5. Enter the new Default Gateway for the iCAM. (default = 192.168.5.254)
6. Click OK to save changes and to open network settings verify screen.

The iCAM FACTORY DEFAULT is located on the iCAM7000 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 (192.168.5.100) and the login ID credentials for the iCAM (User ID = iCAM7000 / 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 iCAM firmware/software updates may be reverted back to the original software version that the unit was originally received with.

**** Note:*** *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.*

**** Note:*** *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.*

9.4 How to Test the IP Address Network settings of an iCAM

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 192.168.5.120)
6. Close the command prompt window.

9.5 How to change the IP Address of Multiple iCAMs

If changing the IP Address of multiple iCAMs:

*** Note:** *After each iCAM 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 iCAM to be configured on the network and perform the configuration to the next iCAM

- Once all iCAMs 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.

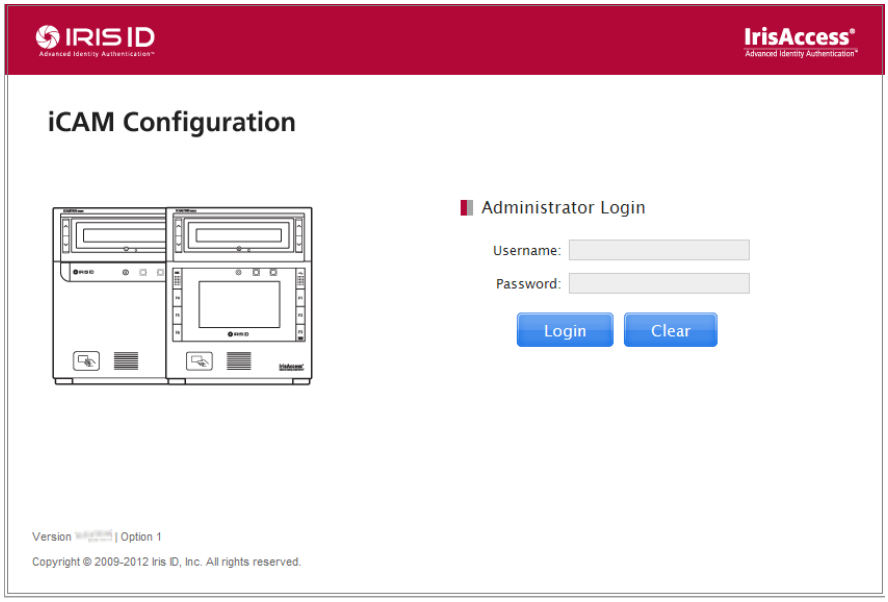
10. Using the iCAM Configuration Interface Option 1: Networked iCAM Control / Iris Matching Mode

The iCAM Configuration interface can be used to gather information about your iCAM as well as perform modifications and setting changes to your camera unit. If using more than one iCAM, each iCAM needs to be configured to the desired specifications required – configuring one iCAM from the configuration interface will only change the settings of that particular iCAM unit. Please see below for a screen by screen break-down of the iCAM configuration interface for reference to the iCAM Configuration Interface when used in iCAM7000 EAC Mode.

10.1 Login and Main Menu Screen

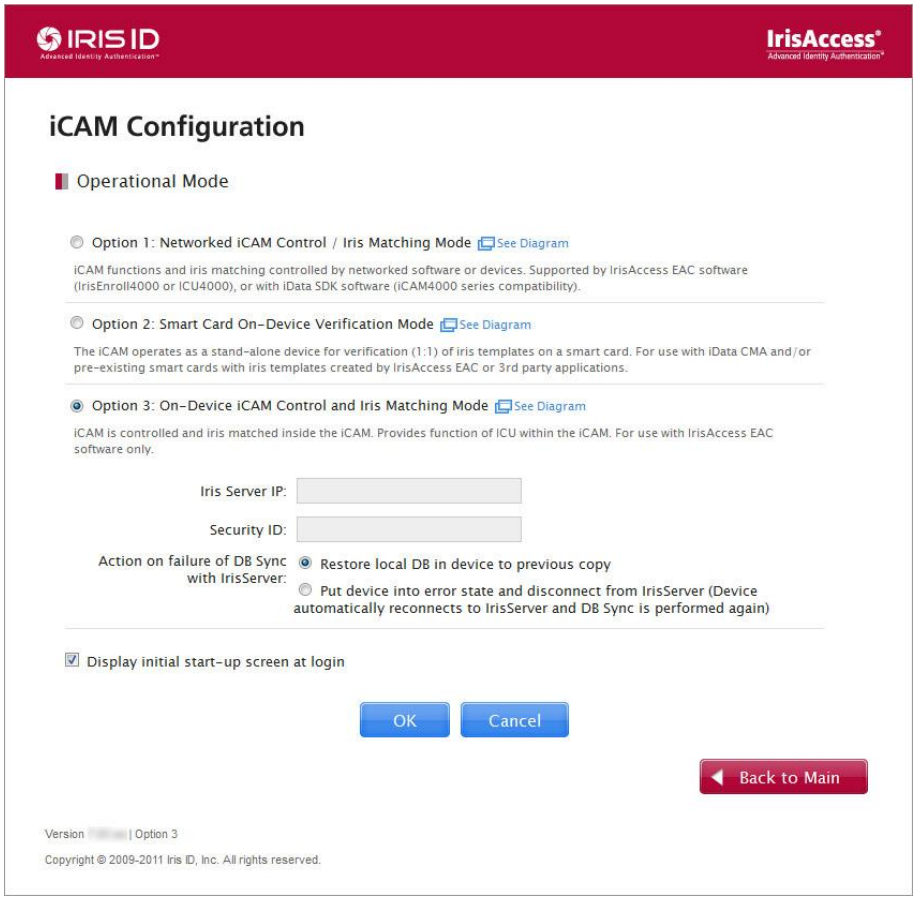
10.1.1 Login Screen

Enter the default Username: iCAM7000 and Password: iris7000 (both are case sensitive) if still set to default settings.



12.1.1 iCAM Configuration Start Up Screen

Once you have logged into the iCAM Configuration, an initial start-up screen may appear. This screen allows for settings to be entered that will determine how the iCAM will be used. This screen is viewable ONLY in the Operational Mode of "Option 3".



1. Enter the desired IP address data of the iCAM7000 series camera unit.
    - **IP Address** – Enter IP address
    - **Subnet Mask** – Enter Subnet address
    - **Default Gateway** – Enter Gateway address
2. A selection to enable or disable IP announcement will also be available (set by default as active).
3. Select the desired Operational mode that will be used for the camera unit.

In option 3 mode –the iCAM is controlled and iris matched inside the iCAM while providing the function of an ICU within the iCAM.

1. **IP Address** - Enter the Iris Server IP address
2. **Security ID** - Enter a unique security ID for this unit (16 character requirement).
3. **Action on failure of DB Sync with IrisServer** - Select the radio button desired for this setting. These options are:
    - **Restore local DB in device to previous copy** – This selection setting will use the internal iCAM database for matching when there is NO connection to the IrisServer.
      Or
    - **Put device into error state and disconnect from IrisServer (Device automatically reconnects to IrisServer and DB Sync is performed again)** – If he iCAM cannot establish a connection to the IrisServer, the iCAM will enter into a non-operational error-state. Once the iCAM connection is restored with the IrisServer, the iCAM will resume its proper operation.

Note: In other above option, if the iCAM is unable to establish communication with the IrisServer, enrollment data and database/system changes will not take effect until communication is re-established between the device and the IriServer.

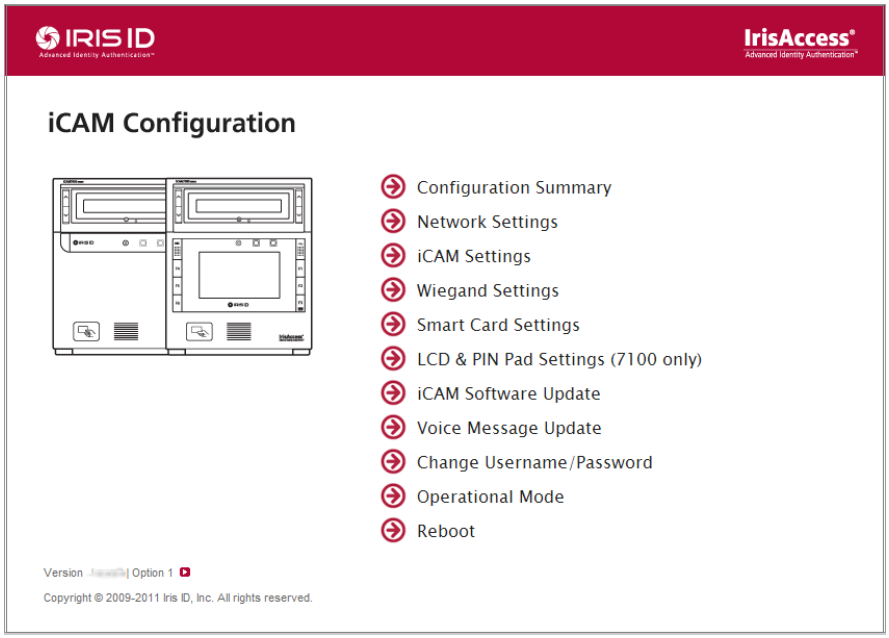
- **Display Initial Start-up Screen at Login** - If you do not wish to see this screen start automatically at the time of iCAM configuration login, check the box "Do not display this screen" to stop this screen from appearing.

  NOTE: *This Start up screen can be re-enabled in the iCAM Settings of the iCAM located in the 'Operational Mode section'.*

- Click **Apply** to save changes or press Skip and return to main screen as needed.

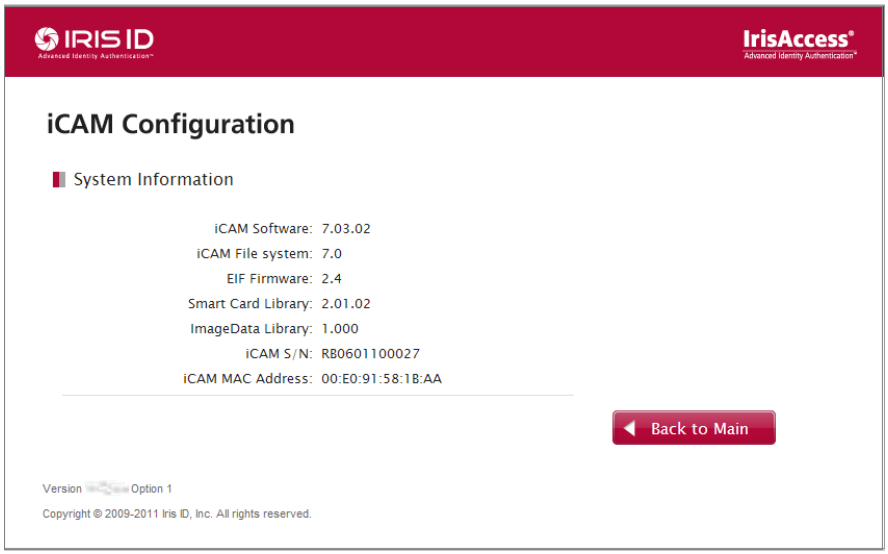
10.1.2 Main Screen

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.



10.1.3 System Information Screen

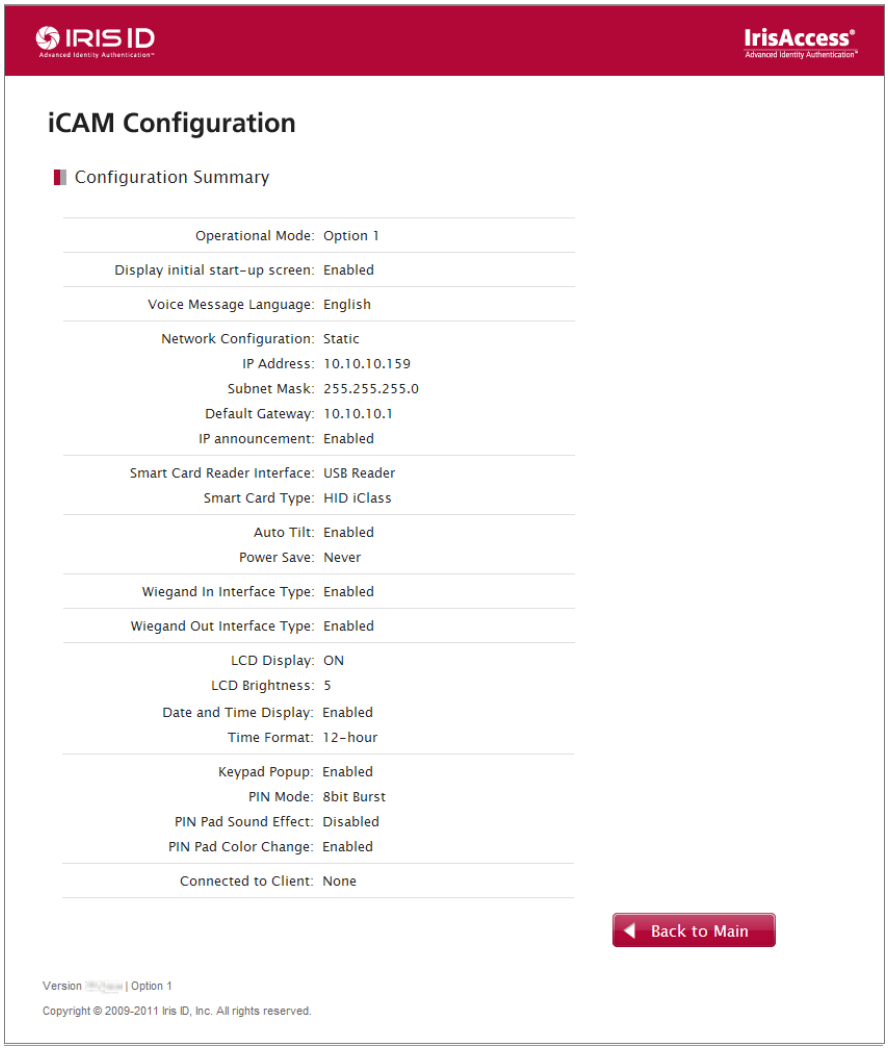
The iCAM Configuration System Information screen provides detailed (viewable only) information about the specific iCAM connected. Such information is shown to help identify the iCAM software version, iCAM File system version, Firmware version/type, HID iClass library, image data library, and command process along with the full iCAM serial number. 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.



10.2 Breakdown of the Configuration Interface

10.2.1 Configuration Summary

These settings are viewable only, and indicate the specific (currently configured) settings which include Language type, Network configuration type, IP address settings, smart card setting, and connected client. Please see below for detailed information for each item.

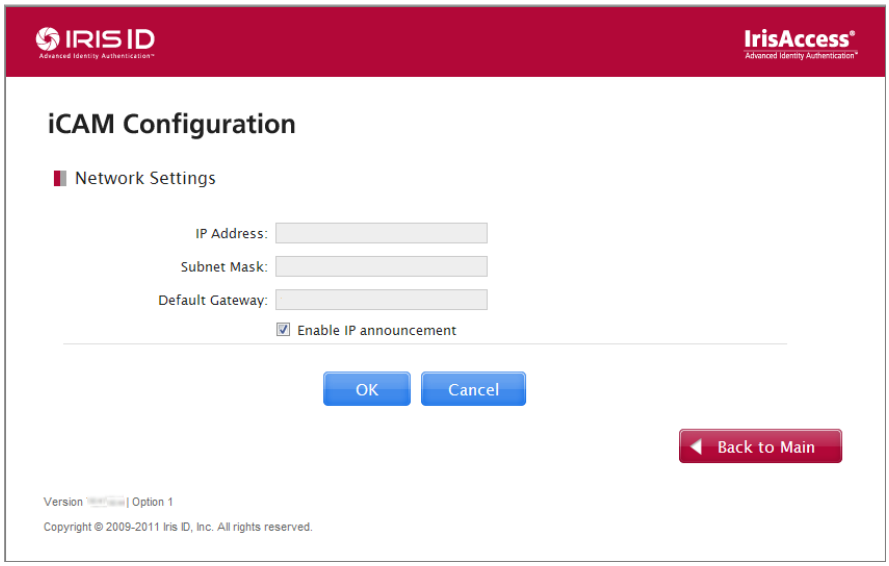


- *Operational Mode* – Displays the Operational Mode state of the iCAM.
- *Display initial start-up screen* - Displays the enabled or disabled state determined by the current setting of the iCAM.
- *Voice Message Language* - Displays the Language that is set in the Camera. (English, Korean, Other language).
- *Network Configuration* – Displays the type of network configuration enabled for the iCAM (i.e.: Static).
- *IP Address* - Displays the IP address of the Camera unit in the iCAM Configuration.
- *Subnet Mask* - Displays the Subnet address of the Camera unit in the iCAM Configuration.
- *Default Gateway* - Displays the Default Gateway address of the Camera unit in the iCAM Configuration.
- *IP Announcement* – Set to "Enabled" or "Disabled" selection for audible announcement of IP address when the iCAM tilt button is pressed continuously for over ~8 seconds. By default, the setting is enabled.
- *Smart Card Reader Interface* – Displays the Card Port Status as set in the iCAM Configuration of the camera unit. None, Serial Reader, or Internal USB Reader. (If a smart card port is selected, and no card is present in the port, the port will not appear as active.)
- *Smart Card Type* – Displays the type of card that is set to be used.

- *Auto-Tilt*- Displays the auto-tilt selection Status in the iCAM Configuration of the Camera as either Enable or Disable.
- *Power Save* – Shows the Power-Save Status in the iCAM Configuration of the Camera unit. Never, 1, 3, 5, or 30. (Default setting is Never.)
- *Wiegand In* - Displays whether the Wiegand In is set to Enabled or Disabled in the iCAM Configuration.
- *Wiegand Out* - Displays whether the Wiegand Out is set to Enabled or Disabled in the iCAM configuration.
- *LCD Display* – Displays the LCD Display Status in the iCAM Configuration of the Camera unit (7100 models only). ON or OFF. If shown as off, the LCD on an iCAM7100 model unit will not be enabled.
- *LCD Brightness* – Displays the Brightness Status of LCD in the iCAM Configuration of the Camera unit (7100 models only). Setting range is 1 through 5. Determines the Brightness of the LCD Display (for iCAM7100 model units only). 1 indicates the least bright and 5 indicates the brightest setting.
- *Date and Time Display* – Set to Enable or Disable. This option allows for the date and time to appear on the iCAM unit when enabled. By default, this setting is enabled.
- *Time Format* – This setting allows for either 12 hour or 24 hour time (military time) to be viewed as the time display layout on the iCAM.
- *Keypad Popup* – Shows the Keypad Popup Status in the iCAM Configuration of the Camera unit (7100 models only). Enabled, or Disabled (for iCAM7100 model units only).
- *Pin Mode* – Displays the Pin Mode setting in the iCAM Configuration of the Camera unit (7100 models only). When using the Keypad, the Pin mode of IrisAccess + Pin, 8bit burst, 4bit burst, and Galaxy format are available for selection.
- *Pin Pad Sound Effect* – Displays the Pin Sound Status (7100 models only). Enabled or Disabled. This option can be set to either enable or Disable.
- *Connected to Client* - Displays whether the camera unit is connected to a controlling device for usage (None, Yes).

10.2.2 Network Settings

This screen provides the ability to get detailed information on the IP settings of the iCAM connected on the network. From this location you can set IP address information for Dynamic (automatic) or static IP addressing for specific network protocol based information. You can also designate whether to enable IP announcement which allows the ability to audibly hear the IP address of an iCAM by holding down the UP tilt button for 12 seconds.



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. Click OK to save changes and to open network settings verify screen.

* Note: *There is a FACTORY DEFAULT located on the iCAM7000 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 (192.168.5.100) and the login ID credentials for the iCAM (User ID = iCAM7000 / Password = iris7000).*

- 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.

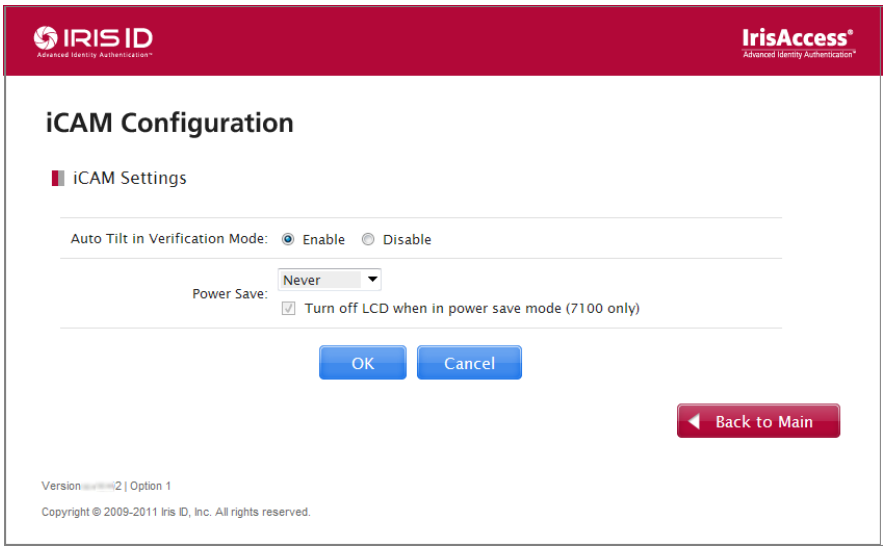
** Note: Pressing and holding the up tilt button for 10 seconds will cause the iCAM to announce the iCAM configured IP Address (Unless de-selected in this menu screen, or if volume is muted on the unit).*

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.

10.2.3 iCAM Settings

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



- **Auto-Tilt**- Enables or Disables the auto-tilt feature of the Camera. This option allows the Camera unit to auto-tilt to the last position manually selected by the specific user when the iCAM is in *verification* mode (with use of Iris + Pin, or Iris + card only).

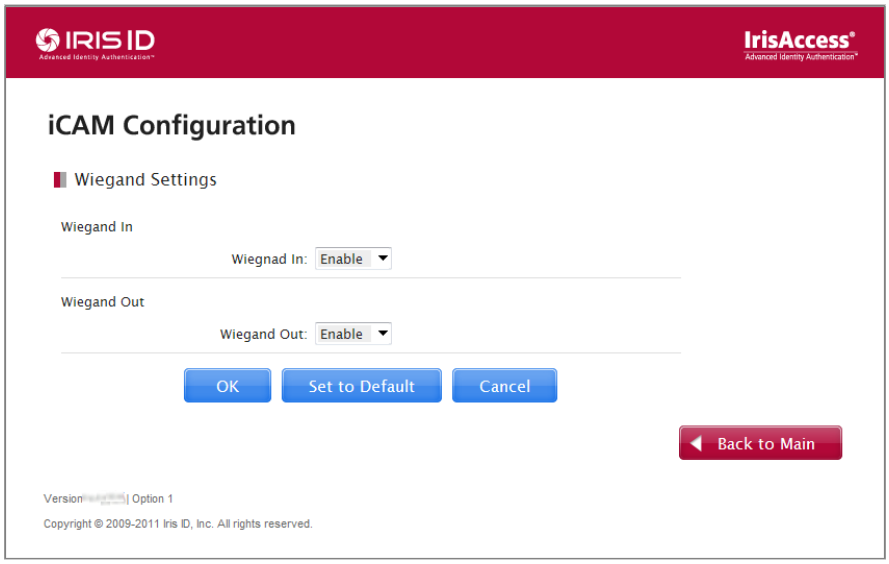
- **Power Save** – Selectable by dropdown box, this feature allows the iCAM to be placed in a more energy efficient state after a length of iCAM inactivity. Power Save can be enabled to engage after the length of time selected (Never, 1, 5, 15, 30, 1 hour).
    - **Turn off LCD when in power save mode (7100 only)** – This option, selectable by checkbox allows the user to define whether the LCD screen of an iCAM7100 model unit will be temporarily turned off. This setting can only be used in conjunction with the Power Save selection, and is controlled by the length of time set for the power save option.

  The unit can be taken out of power-save mode (which includes turning on the LCD (when selected) in several different ways. The iCAM will be removed from power-save mode by any of the following processes or operations:

    - *Proximity sensor* –The user is within proximity range of the iCAM sensor.
    - *Tilt buttons* – If any of the iCAM UP/DOWN tilt buttons is pressed.
    - *Function Keys* – If any of the Function keys are pressed (7100 models only).
    - *LCD Touch-Screen* - If the touch-screen is pressed (7100 models only).

10.2.4 Wiegand Settings

From this screen selectable Wiegand settings can be enabled. Specifically, Wiegand In (Interface type-Disable or Enable, and Wiegand Out Interface type-Disable or Enable) are configurable for direct iCAM Wiegand output.



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

1. Login to the iCAM configuration screen (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 Enable to enable the Wiegand Output.

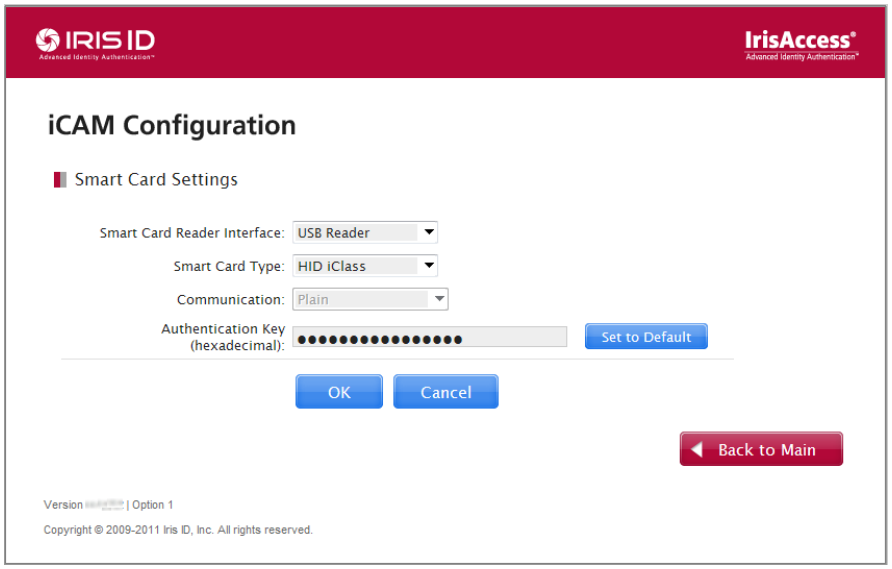
- Select the Set to Default button to restore settings to the original factory default state for Wiegand Settings. By default, the Wiegand In and Wiegand Out are both set to *Enabled*.

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

Additional Note: *The software controlling the iCAM is used to configure the Wiegand input and output settings. The supported Wiegand formats are determined and limited by the software application.*

10.2.5 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 iCAM.



1. Login to the iCAM 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 iCAM found in this screen. (See following data for details.)

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

A. Smart Card reader interface:
   a. **Serial Reader** – This selection is used to enable an iClass reader through the Serial Smart Card Interface of the iCAM7000/7100 model unit.
   b. **USB reader** – This selection enables the use of iClass Smart Cards through the optional internal USB Smart Card reader. (This reader type is selected by default.)

B. Smart Card Type:
Select the type of Smart Card that will be used.
   a. None
   b. HID iClass
   c. MiFARE
   d. DESFire

C. Communication: (Selectable for DESFire cards only)
   a. Plain
   b. Encrypted (Air Link) - DESFire only
   c. Lenel - Select only if using DESFire cards encoded by On-Guard.

D. Authentication Key:

Also known as an Application Key, this can be set by entering a valid key in the application key text box. This key is masked on display. Once the user clicks on the application key text box, the key is cleared and user can enter key in normal text mode and appropriate authentication key. (Pressing the 'set to default' button will place the offset value to factory settings.)

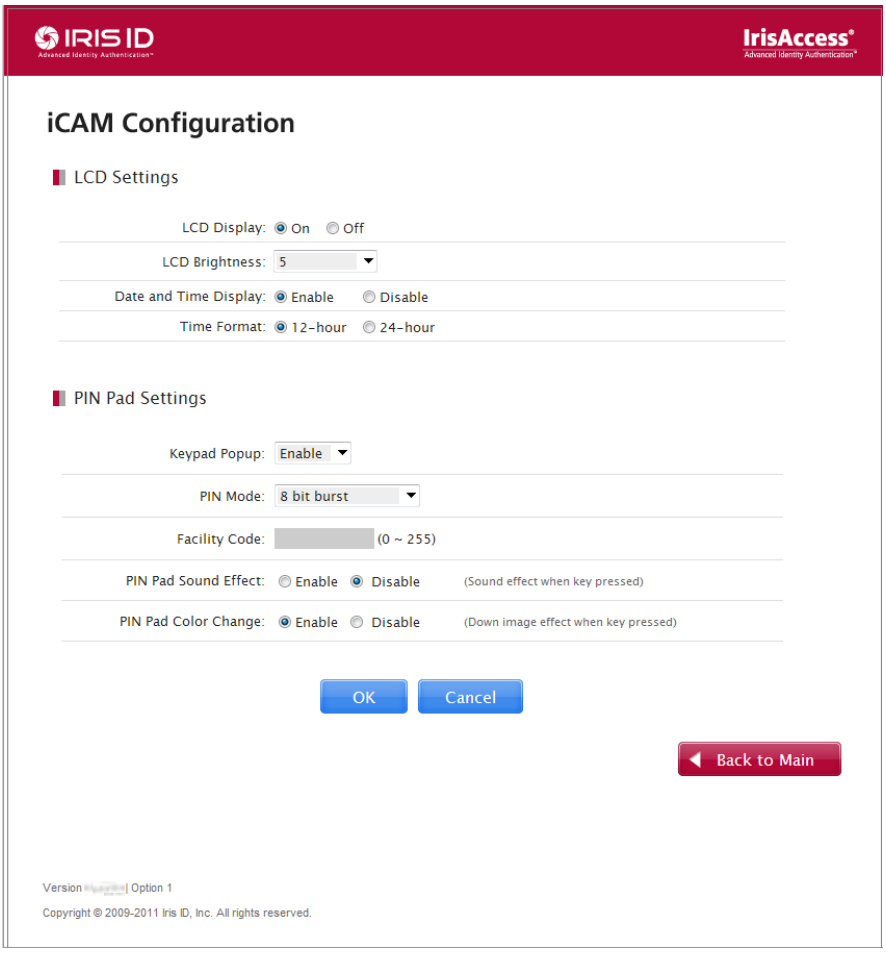
***Note:** Authentication Key, also known as application key is the primary security of the card. Without the correct application key, card reads and writes will not be possible. Any cards created with a specific application key will only be able to be used with devices containing an identical matching application key program.*

*-Modify the **Authentication Key** as needed. Make sure to use a Hexadecimal value in this field.*

E. Click on "Set to Default" button to set the default authentication key.

12.1.2 LCD & PIN Pad Settings (7100 models only)

This section is for use with iCAM7100 Series camera units only. The settings and information available in this area contain feature sets that are only compatible with the7100 series. Specific LCD settings can be modified and customized. Additionally, the iCAM7100 series units can be used with a built in Pin Pad that can pop-up on the LCD display. The usage of the Pin Pad can be modified by an installer for custom use. Read the following information for details.



1. Login to the iCAM configuration screen as shown above (if not already logged in).

2. Select the Function Key & LCD Settings (7100 only) Settings option from the main screen.
3. Configure desired settings for the iCAM found in this screen. (See following data for details.)

7100 LCD Settings:

- **LCD Display** – Select On or Off. Select the On radio button to enable the LCD display. Select the Off radio button to disable the use/view of the LCD display on an iCAM7100 model camera unit.
- **LCD Brightness** – Select the desired brightness level of the LCD when enabled. The setting options for brightness range from 1 – 5. 1 is the least bright image available for this LCD, and 5 is the Brightest. By default, the LCD setting is enabled and set to 5.
- **Date & Time Display** – Select Enable or Disable. When enabled the Time and Date will display on the main screen of the iCAM7100 LCD display. Other time and date displays (during transactions) will always be displayed.
- **Time Format** – Selection of 12-Hour time or 24-Hour time display.

PIN Pad Settings:

- **Keypad Popup** - Shows the selectable Keypad Popup State of the Camera unit (7100 models only). Enabled or Disabled options are available. When enabled, the *F3* function button on an iCAM71xx model unit will allow the Pin-pad to appear. When this option is disabled, the *F3* function button will not perform any function, and the Pin-pad is not in an active state.
- **Pin Mode** – Shows the selectable PACS Pin Mode setting of the Camera unit (7100 models only). The Wiegand Output mode of Iris Access PIN, 8 bit burst, 4 bit burst, and Galaxy format are available for selection. Pin Mode selections include 8bit Burst, 4bit Burst and Galaxy Mode, and Disabled. Details of these available modes are as follows:
    - **Iris Access PIN** - Utilizes the Pin field in IrisAccess EAC software for Pin verification of a user. Refer to EAC documentation for further details.
    - **8bit Burst** – Each key pressed on the Pin Pad outputs an 8-Bit binary code from the Wiegand output of the camera unit (for use with a Physical Access Control System).

8 Bit Burst

Key	Wiegand Output	Key	Wiegand Output	Key	Wiegand Output
1	11100001	5	10100101	9	01101001
2	11010010	6	10010110	*	01011010
3	11000011	7	10000111	0	11110000
4	10110100	8	01111000	#	01001011

    - **4bit Burst** – Each key pressed on the Pin Pad outputs a 4-Bit binary code from the Wiegand output of the camera unit (for use with a Physical Access Control System).

4 Bit Burst

Key	Wiegand Output	Key	Wiegand Output	Key	Wiegand Output
1	0001	5	0101	9	1001
2	0010	6	0110	*	1010
3	0011	7	0111	0	0000

4	0100	8	1000	#	1011

- **Galaxy Format** – Each key press is stored in a buffer and is sent only when the # Key or enter key is pressed. The number entered (key presses) will be sent as the Card ID along with the Facility Code entered in the Facility code field. The Wiegand output is sent from the camera in a 26-Bit format to the PACS panel.

Galaxy Format

Parity	Facility Code	Card ID	Parity
P	FFFFFFFF	CCCCCCCCCCCCCCCC	P

Start Parity Bit = 1 Bit (Even*)
Facility Code = 8 Bit
Card ID = 16 Bit**
Stop Parity Bit = 1 Bit (Odd*)

** **Note**: Start bit is determined by the first 13 bits and the Stop Parity Bit is determined by the last 13 bits.*

- **Disabled** - Set to disable when not using this feature. When disabled, pressing the F3 key will not display the PIN pad.

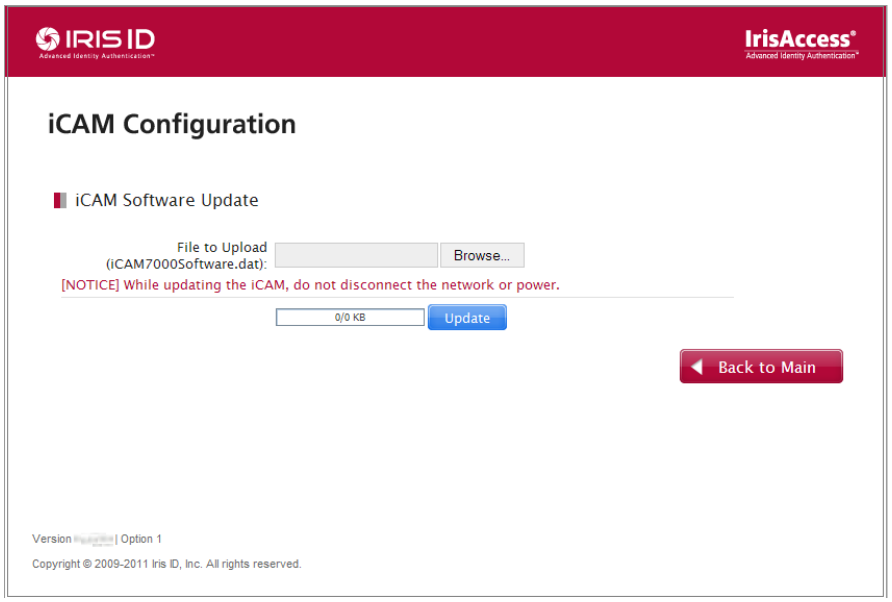
** **Note**: When Iris + Pin mode is currently in use, this option is not available (as the PIN mode is already active by default based on the Recognition mode usage).*

- **Facility Code** – When Galaxy Format is selected, the Facility Code value in this field will be output as part of the Galaxy formatted Wiegand Output. Enter the desired facility code between 0 ~254 as needed.
- **Pin Pad Sound Effect** – Enables or Disables a Pin Sound of an iCAM7100 model unit. This option can be set to either Enable or Disable. The pin sound option allows for a button press on the touch screen LCD to produce an audible sound. (This option is set to disable by default).
- **Pin Pad Color Change** - Selectable by radio button, enable this option to see a visual change to the key pressed on the PIN Pad.

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.

10.2.6 iCAM Software Update

iCAM software updates are generally performed automatically when used with the EAC application. However, from time to time, an iCAM software update may become available from Iris ID Systems, Inc. that may require a manual upgrade. Such updates may often be downloadable from the http://www.IrisID.com website. Consult with your system integrator or IRIS ID directly before attempting to perform any updates of this type. This section allows for you to update the camera unit with a compatible software update directly from the iCAM.



***NOTE**: Java VM must be installed on your computer in order to perform these procedures correctly.* Verify that Java VM is installed and working on your windows pc. (If Java VM is not installed, go to http://www.java.com/en/download/index.jsp for download and installation instruction.

Verify that Internet Options settings are set to *allow local directory path when uploading to a server*.

1. Open Internet Explorer
2. Go to the *tools* Menu> *Internet Options* > *Security* > *Custom Level* > *Miscellaneous* section > *Include local directory path when uploading files to a server* > Select *Enable* radio button > press *OK*.

Manually upgrading iCAM Software:

WARNING! Do not disconnect the power or disturb the network connection during the upgrade process unless instructed to do so. If power or network is disconnected during file transfer, this could cause corruption in the iCAM OS and render the iCAM non-operational.

Verify that Internet Options settings are set to *allow local directory path when uploading to a server*.

a. Open Internet Explorer

b. Go to the *tools* Menu> *Internet Options* > *Security* > *Custom Level* > *Miscellaneous* section > *Include local directory path when uploading files to a server* > Select *Enable* radio button > press *OK*.

Download the file "iCAM7000software.dat"; make a new folder on the c: drive and place the file in that new folder.

Updating the iCAM Software:

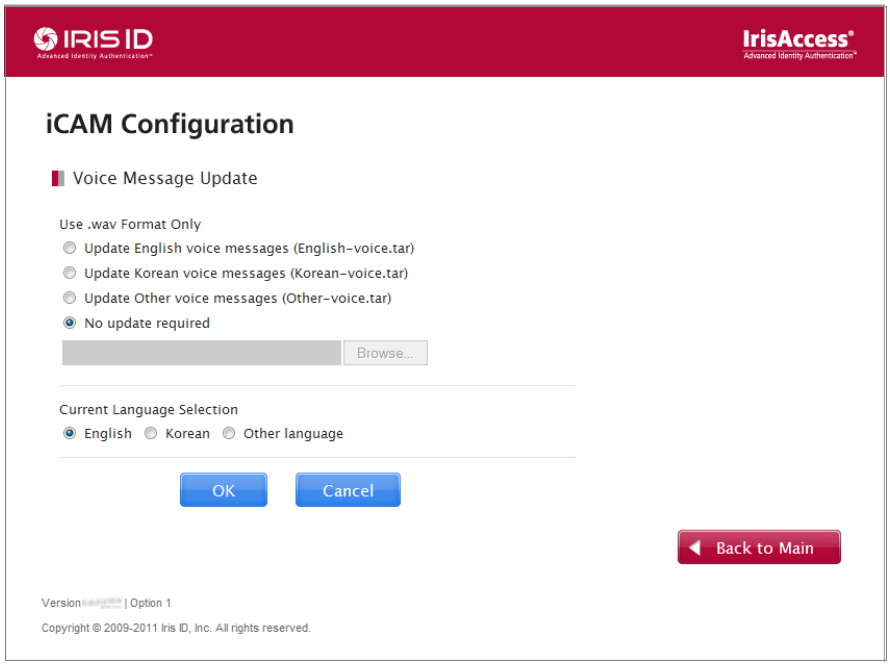
- Log into the iCAM (web browser interface)
- From the main menu select iCAM Software Update
- Select Browse
- Select the path to the *"iCAM7000Software.dat"* file
- Double click on the "Update" button. (Files will transfer and iCAM software will update, this may take several minutes)
- When complete a summary screen will display
- Click Yes to reboot the iCAM
- Enter the username (iCAM7000) and password (iris7000)
- Click OK to reboot iCAM
- Wait 2 minutes for the reboot to completely.

Confirming the iCAM Software version:

- Log into the iCAM (web browser interface)
- From the main menu click on the arrow symbol next to the version number.
- This window will display the iCAM software and firmware versions.
- iCAM software version indicates a successful upgrade of the iCAM.

10.2.7 Voice Message Update

If the camera unit requires different voice messages then what was provided (default standard messages language announced in English), Korean language can be selected or other .WAV formatted messages can be uploaded using a .TAR format to the camera unit in this section.



Procedures to upload the voice files to your iCAM:

1. Place the 'Other-voice.tar' file on a computer that can be connected to the iCAM.
2. Log into the iCAM Configuration screen using 'iCAM7000' as the username and 'iris7000' as the password.
3. Select 'Voice Message Update'.
4. Select 'Update Other language messages (Other-voice.tar)'
5. Press the 'Browse' button to browse for the 'Other-voice.tar' file and select it for use.
6. Set the 'Current language selection' to 'Other language'.
7. Press 'Ok'.
8. A message will display confirming the action success (or failure).
9. When the upload is complete, reboot the iCAM.

If you want to convert the voices back to English, log in to the iCAM's web interface and select Voice Message Update.
Select 'No Update required' and set Current language selection to English.
Press Ok.
Enter the server IP address, username 'anonymous' and password 'r'.
Press Ok.
When the authentication page comes up, enter 'iCAM7000' for username and 'iris7000' for password. This will reboot the iCAM with English voice files.

Here is the list of .wav files.
You must use these exact file names (These are case-sensitive) and place them in a folder named "Other-voice", then create a tar file of the entire folder. Name the tar file "Other-voice.tar". The wav files inside the tar file must have the path "Other-voice\"

The format of the sound files and translation are listed below.

Audio format: PCM 16 kHz, 16 bit, Stereo

16k_beepbeep.wav - (beeping sound)
16k_Capture.wav - (camera shutter sound)
16k_EnrollmentCommencement_B.wav - "Please present your card to the card reader."
16k_IDMessages_A.wav - "Thank you! You have been identified."
16k_IDMessages_C.wav - "Sorry, we cannot confirm your identity."
16k_ImageAquisitionMessages_A.wav - "Please come a little closer to the camera."
16k_ImageAquisitionMessages_B.wav - "Please move back a little from the camera."
16k_ImageAquisitionMessages_G.wav - "Please center your eyes in the mirror."
16k_OpenEyes.wav - "Please open your eyes wide"
16k_Post_ImageAcquisitionMessagesA.wav - "We finish taking pictures of your eyes."
16k_smartcard.wav - (Smart Card accepted sound)
16k_TryAgain.wav - "Please try again."
16k_VerificationResultMessages_A.wav - "Thank you! Your identity has been verified."

Recording your Own Sound files to use as voice prompts:

You may create your own sound files using Windows Sound Recorder (Included with Microsoft Windows). By following the below procedure we had success in creating different sound files which we could then upload to the Optical Units. The biggest problem is keeping the file size small enough to use.

In Windows
Click Start -> Accessories -> Sound Recorder

Record your message

Click File -> Save As -> (Name the file)
Click File -> Properties
Select "Format Conversion"
Select "All Formats"
Click "Convert Now"

Choose
Format: PCM
Attributes: 16 kHz, 16 bit, Stereo

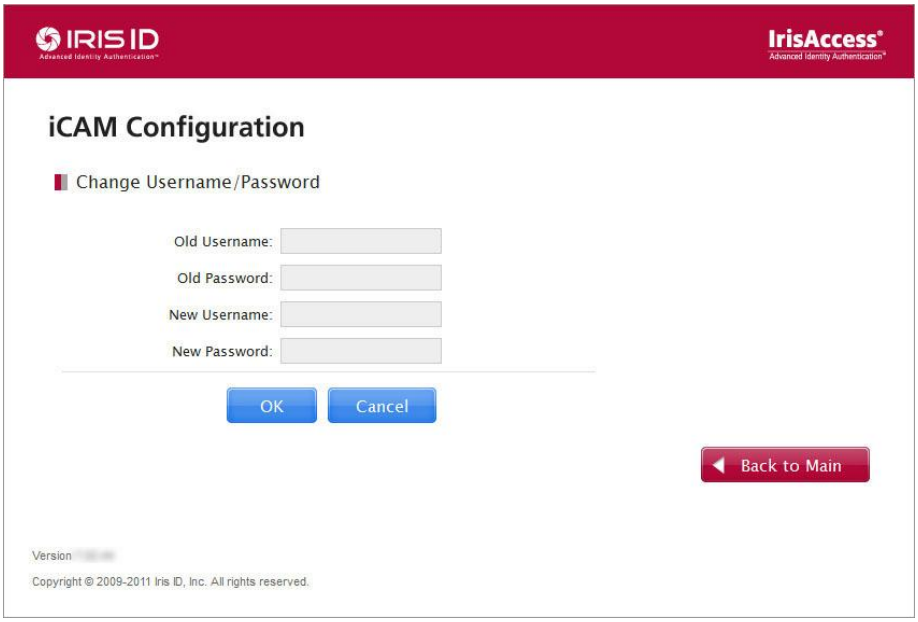
Click OK
Click OK
Click File -> Save

If the volume is too low, you may need a better quality microphone (this was a problem we had experienced), you may also increase the volume of the capture sound in Sound Recorder.

**Note: Sound files created must be packaged as a .tar file using a .tar compatible software of 1.15 or higher (standard). This file folder must be named "Other-voice.tar". In the event that an existing "Other-voice.tar" file has been created for an iCAM4000, it may be necessary to re-package the voice files into a new "Other-voice.tar" file folder using a utility/software (not provided by Iris ID) that conforms to 1.15 or higher standard .tar file creation.*

10.2.8 Change Username/Password

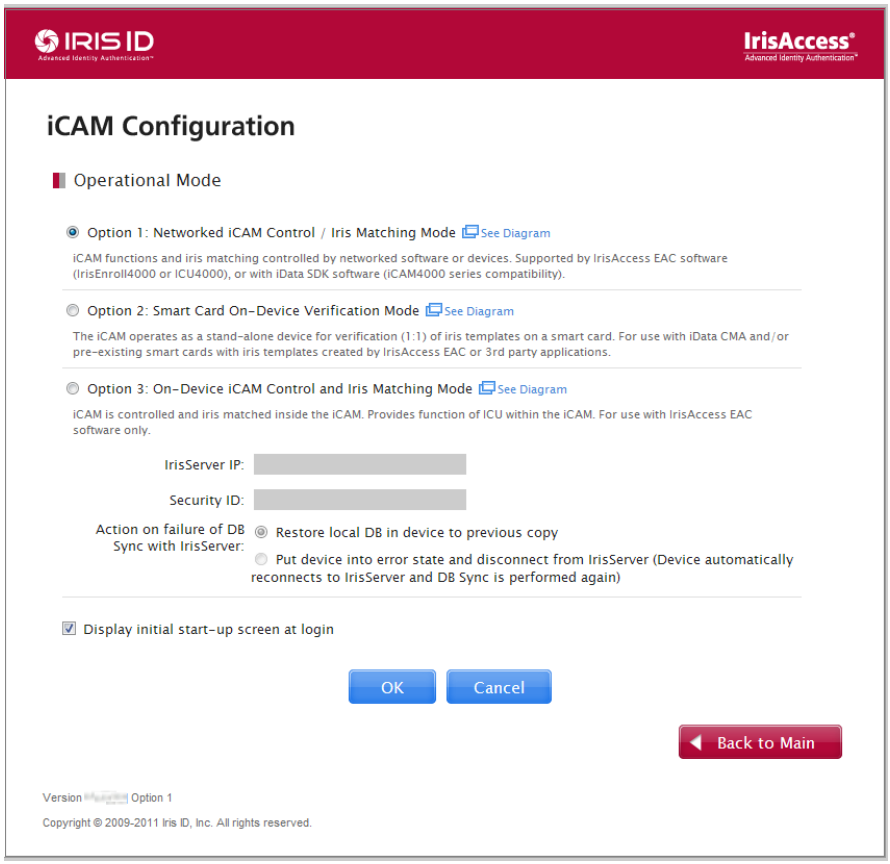
This menu provides the ability to change the Username and Password settings currently existing in the iCAM. In order to change the settings first the old user id and password must be entered in addition to the new user id and password credentials desired. Please note that all fields are case sensitive.



** **Note**: The iCAM FACTORY DEFAULT is located on the iCAM7000 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 (192.168.5.100) and the login ID credentials for the iCAM (User ID = iCAM7000 / Password = iris7000).*

10.2.9 Operational Mode

This screen allows for the iCAM to be set in Networked iCAM control / Iris image capture mode (Option 1), Smart-Card On-Device Verification Mode (Option 2), or On-Device iCAM control and iris matching mode (Option 3).



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

- "**Option 1: Networked iCAM Control / Iris Matching Mode**" – When option 1 is selected, the iCAM will operate as part of an IrisAccess™ Entry Access Control System, or for use with iData™ SDK (iCAM4000 Series compatibility). The iCAM functions and iris matching are controlled by networked software or devices.
  IMPORTANT: If you are generally using option 3, this "option 1" mode may be needed to be used when performing enrollment.

- "**Option 2: Smart Card On-Device Verification Mode**" - When option 2 is selected, the iCAM7000 operates as a stand-alone device for verification (1:1) of the iris templates on a smart card. This mode is generally for use with iData CMA and/or pre-existing smart cards with iris templates created by IrisAccess EAC or compatible 3rd party applications.
  ***Note**: "iCAM7000 Stand-Alone Smart Card Verification Mode" can only be used when a card reader (internal or external) is used with the iCAM7000 series unit.*

- "**Option 3: On Device iCAM Control and Iris Matching Mode**" – When option 3 is selected, the iCAM is controlled and iris matched inside the iCAM. This mode provides the function of an ICU within the iCAM. This option is designed for use with compatible IrisAccess EAC software.

**Note: If attempting to use an iCAM7000 series unit in operational mode "Option 3", compatible IrisAccess EAC software MUST be used for functionality of this option.*

***IMPORTANT**: If you are using an iCAM7000 in "Option 3" operational mode – when performing enrollments, and when trying to connect to the IrisEnrol4000 application within IrisAccess EAC software, the user must switch the operational mode to "option 1". Once enrollments have completed, the iCAM can be set back to operational mode "option 3" (if a dedicated iCAM is not being used for enrollment).*

In option 3 mode –the iCAM is controlled and iris matched inside the iCAM while providing function of an ICU within the iCAM. In order for these processes to work correctly the below information is required to be provided when "Option 3" is selected:

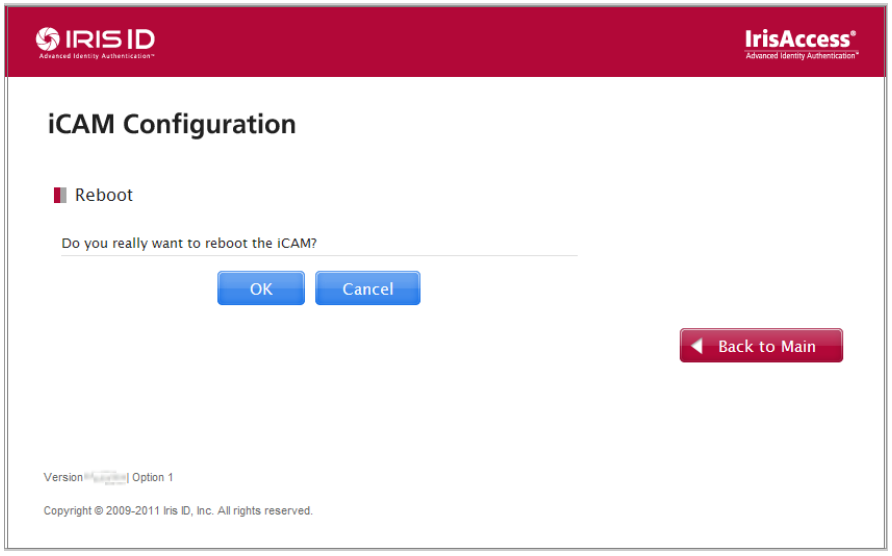
a. **IrisServer IP** - Enter the Iris Server IP address
b. **Security ID** - Enter a unique security ID for this unit (16 character requirement).
c. Action on Failure of DB Sync with IrisServer - Select the radio button desired for Action on failure of DB Sync with IrisServer. These options are:

- **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).**

4. Display Initial Start-up screen at login – This checkbox can be selected to enable or unchecked to disable the initial start-up screen from appearing when the iCAM Configuration is logged into.

10.2.10 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.)



11. Using the iCAM Configuration Interface Option 2: Smart Card On-Device Verification Mode

The iCAM Configuration interface can be used to gather information about your iCAM as well as perform modifications and setting changes to your camera unit. If using more than one iCAM, each iCAM needs to be configured to the desired specifications required – configuring one iCAM from the configuration interface will only change the settings of that particular iCAM unit. Please see below for a screen by screen break-down of the iCAM configuration interface for reference to the iCAM Configuration Interface when used in iCAM7000 Stand-Alone Smart Card Verification Mode.

The use of Operational mode: Option 2 requires a Smart Card reader (either built-in to the iCAM, or as an external reader with use of the "Smart Card Reader Interface" port and "Wiegand IN" port in the iCAM.

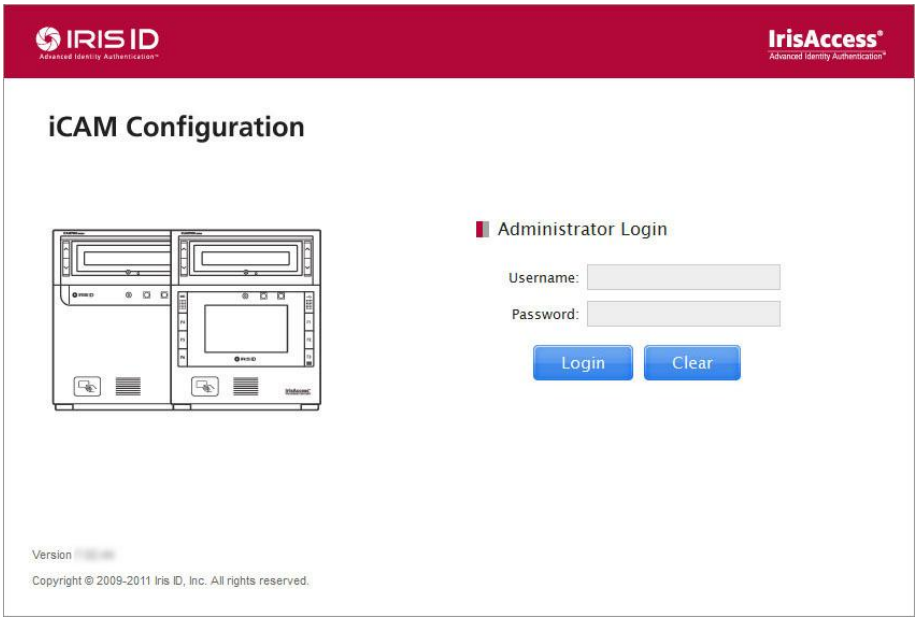
Additionally, the Operational mode: Option 2 only allows support for HID iClass cards (16K/2, 16K/16, and 32K).

The following external card readers are supported (not provided by Iris ID):

- HID RW400 *or* HID RWK400
- HID OEM150

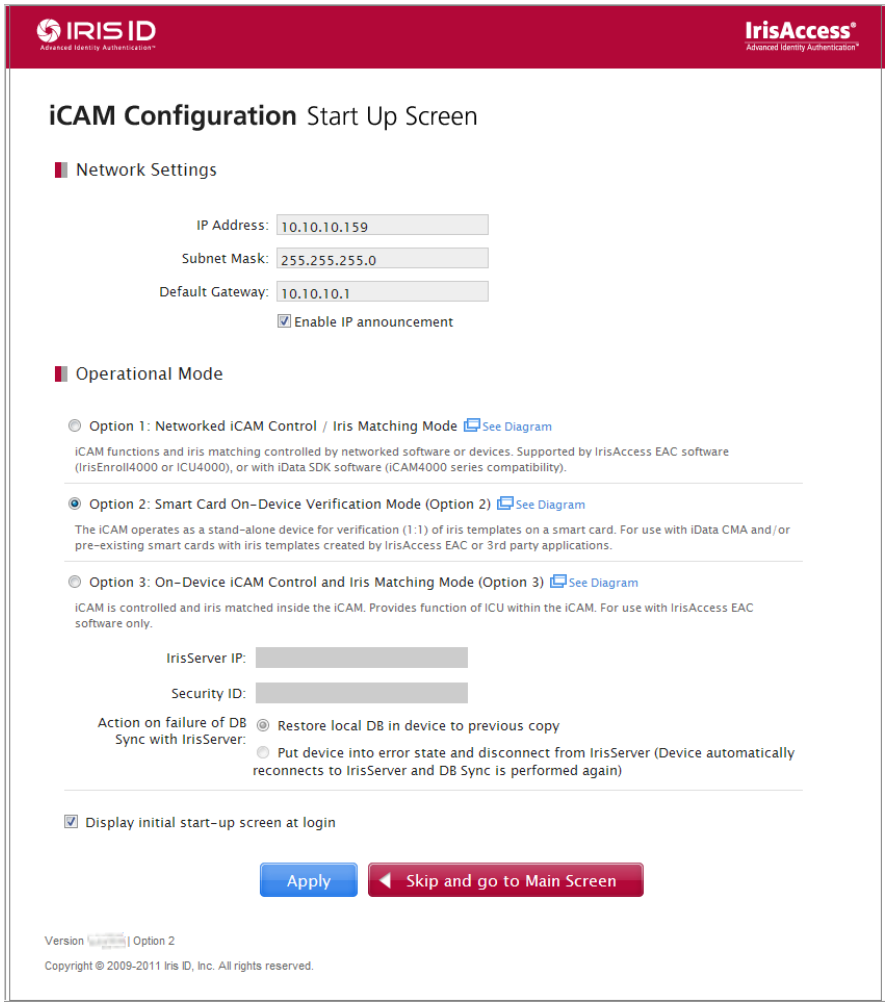
10.1.4 Login Screen

Enter the default Username: iCAM7000 and Password: iris7000 (both are case sensitive) if still set to default settings.



12.1.3 iCAM Configuration Start Up Screen

Once you have logged into the iCAM Configuration, an initial start-up screen may appear. This screen allows for settings to be entered that will determine how the iCAM will be used. This screen is viewable ONLY in the Operational Mode of "Option 3".



1. Enter the desired IP address data of the iCAM7000 series camera unit.
    - **IP Address** – Enter IP address
    - **Subnet Mask** – Enter Subnet address
    - **Default Gateway** – Enter Gateway address
2. A selection to enable or disable IP announcement will also be available (set by default as active).
3. Select the desired Operational mode that will be used for the camera unit.

In option 3 mode –the iCAM is controlled and iris matched inside the iCAM while providing the function of an ICU within the iCAM.

4. **IP Address** - Enter the Iris Server IP address
5. **Security ID** - Enter a unique security ID for this unit (16 character requirement).
6. **Action on failure of DB Sync with IrisServer** - Select the radio button desired for this setting. These options are:
    - **Restore local DB in device to previous copy** – This selection setting will use the internal iCAM database for matching when there is NO connection to the IrisServer.
    Or
    - **Put device into error state and disconnect from IrisServer (Device automatically reconnects to IrisServer and DB Sync is performed again)** – If he iCAM cannot establish a connection to the IrisServer, the iCAM will enter into a non-operational

error-state. Once the iCAM connection is restored with the IrisServer, the iCAM will resume its proper operation.

Note: In other above option, if the iCAM is unable to establish communication with the IrisServer, enrollment data and database/system changes will not take effect until communication is re-established between the device and the IriServer.

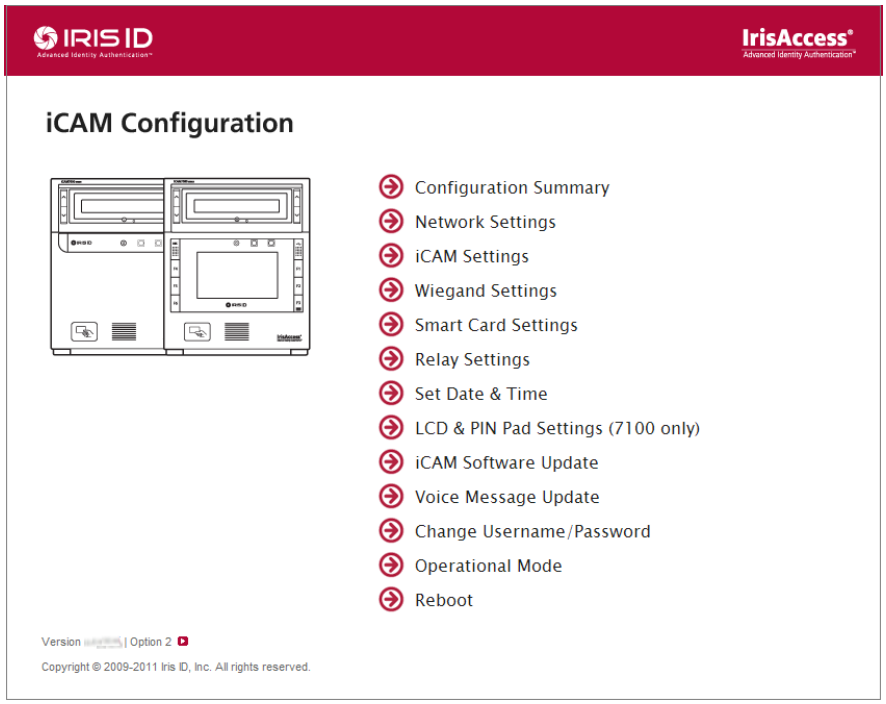
- **Display Initial Start-up Screen at Login** - If you do not wish to see this screen start automatically at the time of iCAM configuration login, check the box "Do not display this screen" to stop this screen from appearing.

  NOTE: *This Start up screen can be re-enabled in the iCAM Settings of the iCAM located in the 'Operational Mode section'.*

- Click **Apply** to save changes or press Skip and return to main screen as needed.

11.1.1 Main Screen

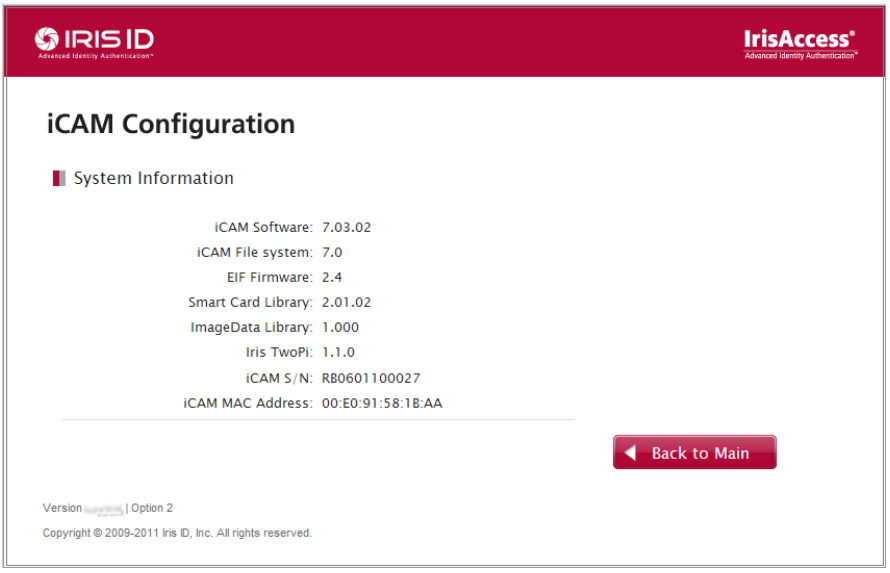
Once you have accessed the iCAM Configuration Main Screen (Menu screen), configurations such as changing of administrator password, date and time settings, Smart Card Configuration, Network Settings, Wiegand Settings, iCAM software update, Voice Message Update, and Reboot options are available for you 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.



11.1.2 System Information Screen

System Information

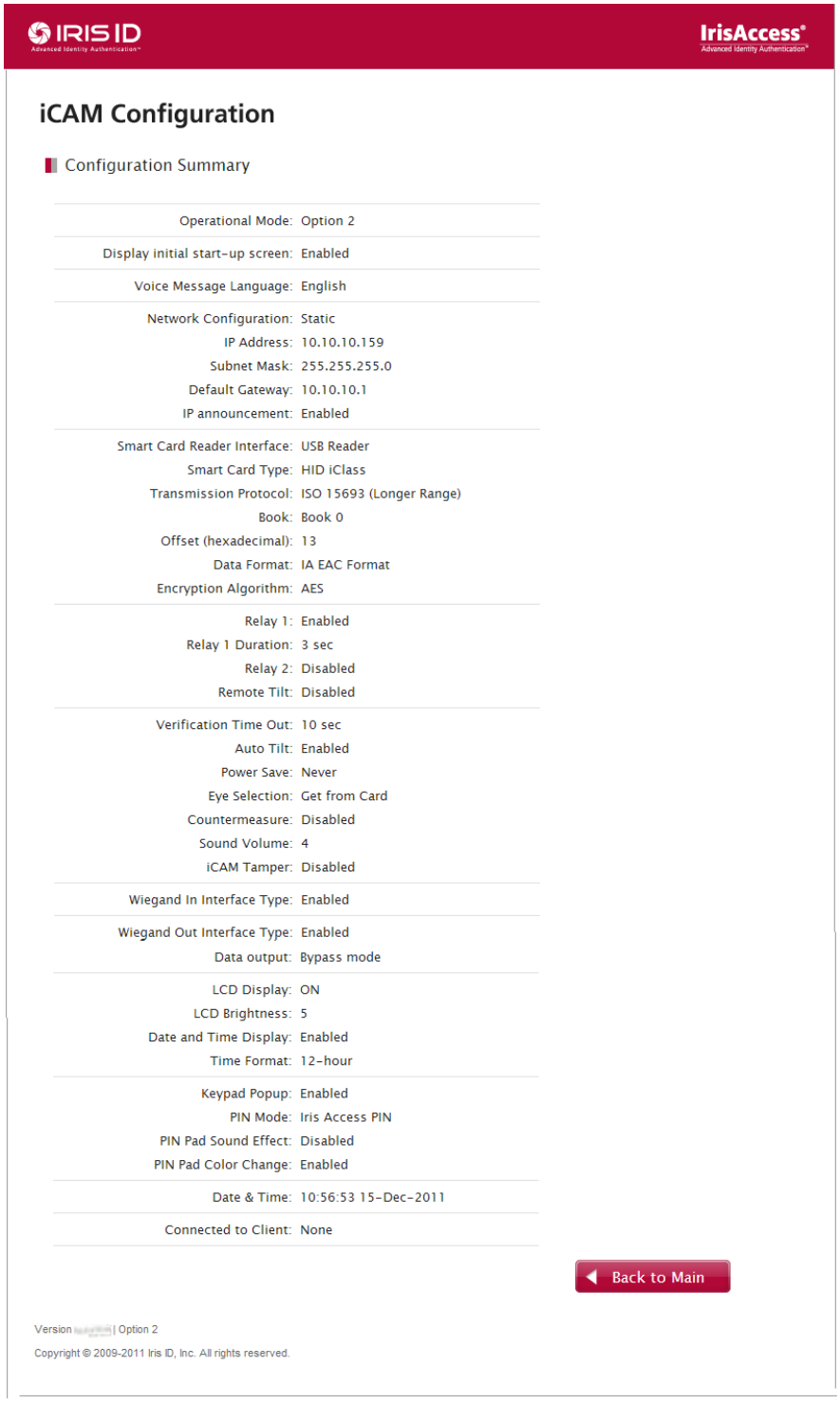
The iCAM Configuration System Information screen provides detailed (viewable only) information about the specific iCAM connected. Such information is shown to help identify the iCAM software version, iCAM File system version, Firmware version/type, HID iClass library, image data library, and command process along with the full iCAM serial number. 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.



11.1 Login Breakdown of the iCAM Configuration

11.2.1 Configuration Summary

These settings are viewable only, and indicate the specific (currently configured) settings which include Language type, Network configuration type, IP address settings, smart card setting, and connected client. Please see below for detailed information for each item.



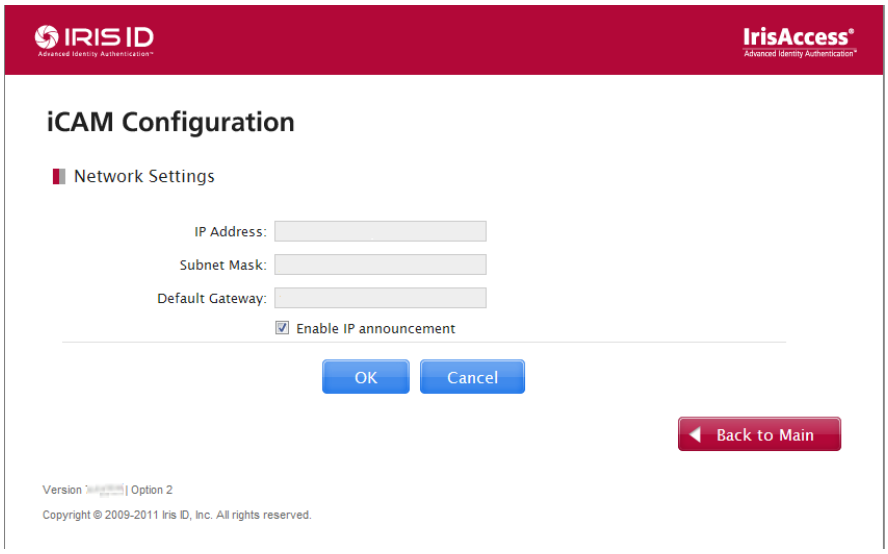
- *Operational Mode* – Displays the Operational Mode state of the iCAM.
- *Display initial start-up screen* - Displays the enabled or disabled state determined by the current setting of the iCAM.
- *Voice Message Language* - Displays the Language that is set in the Camera. (English, Korean, Other language).

- *Network Configuration* – Displays the type of network configuration enabled for the iCAM (i.e.: Static).
- *IP Address* - Displays the IP address of the Camera unit in the iCAM Configuration.
- *Subnet Mask* - Displays the Subnet address of the Camera unit in the iCAM Configuration.
- *Default Gateway* - Displays the Default Gateway address of the Camera unit in the iCAM Configuration.
- *IP Announcement* – Set to "Enabled" or "Disabled" selection for audible announcement of IP address when the iCAM tilt button is pressed continuously for over ~8 seconds. By default, the setting is enabled.
- *Smart Card Reader Interface* – Displays the Card Port Status as set in the iCAM Configuration of the camera unit. None, Serial Reader, or Internal USB Reader. (If a smart card port is selected, and no card is present in the port, the port will not appear as active.)
- *Smart Card Type* – Displays the type of card that is set to be used.
- *Transmission Protocol* – Displays the current transmission protocol setting for the iCAM (Faster Range, or Longer Range).
- *Book* – Displays the current setting for Book value. (0 or 1.)
- *Offset (Hexadecimal)* – Displays the current offset value in a hexadecimal format.
- *Data Format* – Displays the current selected Data Format.
- *Encryption Algorithm* – Displays the current encryption algorithm.
- *Relay 1 – User Accepted* – Displays the length of time that the relay has been set.
- *Relay 1 Duration* - Displays the setting selection configured for the iCAM.
- *Relay 2 – Tamper Notification* – Displays if the Tamper Notification has been enabled.
- *Remote Tilt* - Displays the setting selection configured for the iCAM.
- *Verification Time Out* – Displays the verification time-out interval currently selected. The verification time out will be in the range of 1 to 30 sec.
- *Auto-Tilt*- Displays the auto-tilt selection Status in the iCAM Configuration of the Camera as either Enable or Disable.
- *Power Save* – Shows the Power-Save Status in the iCAM Configuration of the Camera unit. Never, 1, 3, 5, or 30. (Default setting is Never.)
- *Eye Selection* – Displays the current eye selection setting (by default the iCAM is set to 'Either').
- *Countermeasure* – Displays the current setting Level for the iCAM.
- *Sound Volume* – Displays the current volume setting (Mute, 1, 2, 3, 4, 5, 6, 7, High).
- *iCAM Tamper* – Two physical tamper switches located in the iCAM. Displays the Tamper detection state for the iCAM of Enable, or Disable. This feature is software selectable.
- *Wiegand In Interface Type* - Displays whether the Wiegand In is set to Enabled or Disabled in the iCAM Configuration of the unit.
- *Wiegand Out Interface Type* - Displays whether the Wiegand Out is set to Enabled or Disabled in the iCAM configuration of the unit.
    - *Data Output* – Displays the mode that the data is to be output.
- *LCD Display* – Shows the LCD Display Status in the iCAM Configuration of the Camera unit (7100 models only). ON or OFF.
- *LCD Brightness* – Shows the Brightness Status of LCD in the iCAM Configuration of the Camera unit (7100 models only). Setting range is 1 through 5*Which Eye* – This setting displays the eye selection type that the unit will verify. (These options include Left, Right, Both, Either, and Get from Card).
- *Date & Time Display* – Displays the set date and time of the iCAM unit.
    - *Time Format* – This setting allows for either 12 hour or 24 hour time (military time) to be viewed as the time display layout on the iCAM.
- *Keypad Popup* – Shows the Keypad Popup Status in the iCAM Configuration of the Camera unit (7100 models only). Enabled, or Disabled (for iCAM7100 model units only).
- *Pin Mode* – Shows the Pin Mode setting in the iCAM Configuration of the Camera unit (7100 models only).
- *Pin Pad Sound Effect* – Displays the Pin Sound Status (7100 models only). Enabled or Disabled. This option can be set to either enable or Disable.

- *Pin Pad Color Change* - Displays the Enabled or Disabled setting selection used for the iCAM.
- *Date & Time* – Displays the connected time and date.
- *Connected to Client* - Displays whether the camera unit is connected to a controlling device for usage (None, Yes).

11.2.2 Network Settings

This screen provides the ability to get detailed information on the IP settings of the iCAM connected on the network. From this location you can set IP address information for Dynamic (automatic) or static IP addressing for specific network protocol based information. You can also designate whether to enable IP announcement which allows the ability to audibly hear the IP address of an iCAM by holding down the UP tilt button for 12 seconds.



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. Click OK to save changes and to open network settings verify screen.

** Note: The iCAM FACTORY DEFAULT is located on the iCAM7000 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 (192.168.5.100) and the login ID credentials for the iCAM (User ID = iCAM7000 / Password = iris7000).*

- 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.

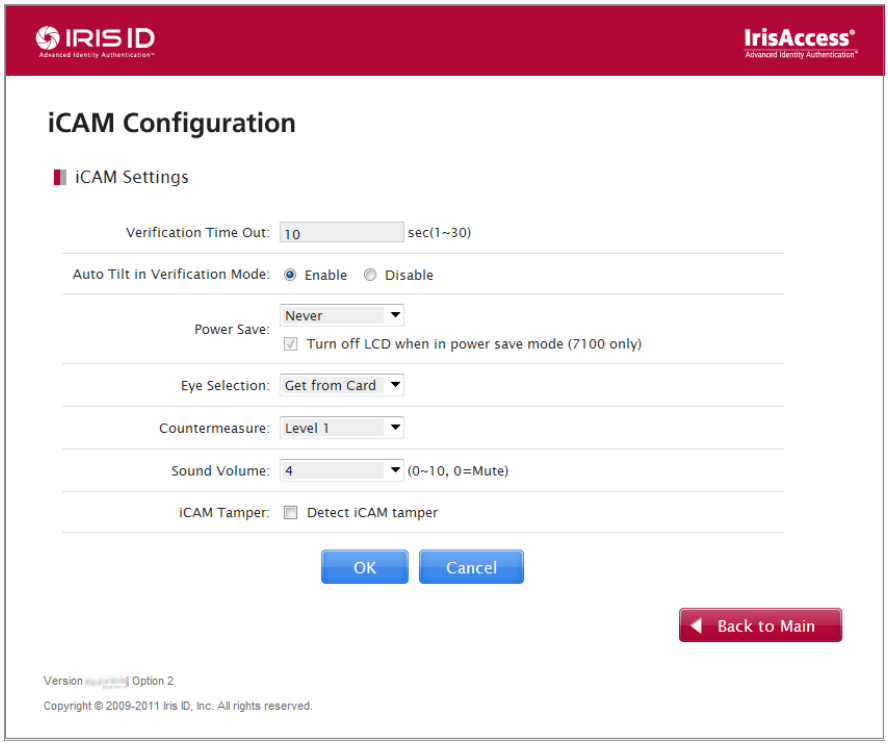
** Note: Pressing and holding the up tilt button for 10 seconds will cause the iCAM to announce the iCAM configured IP Address (Unless de-selected in this menu screen, or if volume is muted on the unit).*

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.

11.2.3 iCAM Settings

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



- **Verification Time Out** – Verification time out can be set by entering a value in verification time out text box. The verification time out should be in the range of 1 to 30 sec.

- **Auto-Tilt**- Enables or Disables the auto-tilt feature of the Camera. This option allows the Camera unit to auto-tilt to the last position manually selected by the specific user when the iCAM is in *verification* mode (with use of Iris + Pin, or Iris + card only).

- **Power Save** – Selectable by dropdown box, this feature allows the iCAM to be placed in a more energy efficient state after a length of iCAM inactivity. Power Save can be enabled to engage after the length of time selected (Never, 1, 5, 15, 30, 1 hour).

- **Turn off LCD when in power save mode (7100 only)** – This option, selectable by checkbox allows the user to define whether the LCD screen of an iCAM7100 model unit will be temporarily turned off. This setting can only be used in conjunction with the Power Save selection, and is controlled by the length of time set for the power save option.

The unit can be taken out of power-save mode (which includes turning on the LCD (when selected) in several different ways. The iCAM will be removed from power-save mode by any of the following processes or operations:

- *Proximity sensor* –The user is within proximity range of the iCAM sensor.
- *Tilt buttons* – If any of the iCAM UP/DOWN tilt buttons is pressed.
- *Function Keys* – If any of the Function keys are pressed (7100 models only).
- *LCD Touch-Screen* - If the touch-screen is pressed (7100 models only).

- **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.

- **Sound 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.

Note:

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

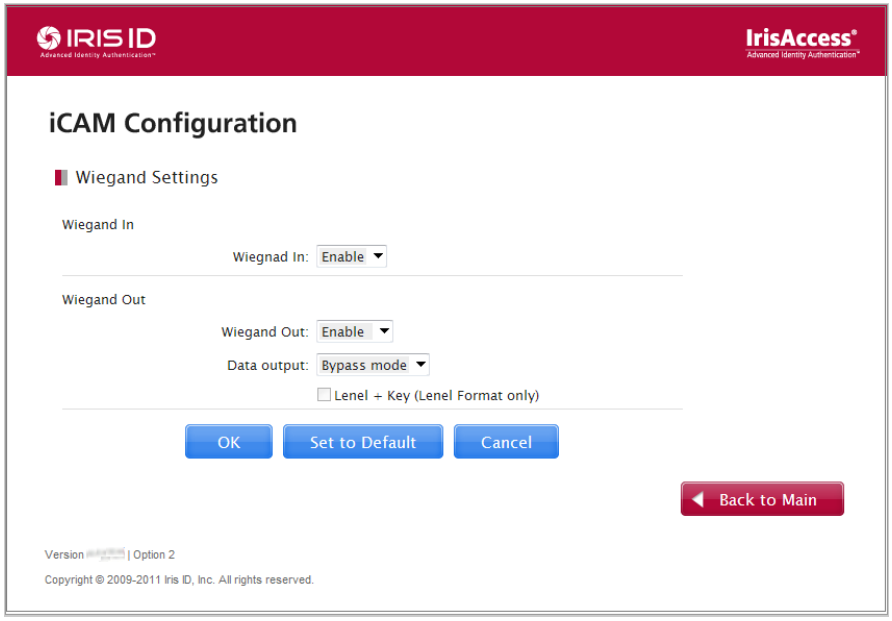
Select "Set to Default" to change setting values back to the default settings.

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.

11.2.4 Wiegand Settings

From this screen selectable Wiegand settings can be enabled. Specifically, Wiegand In -Disable or Enable, and Wiegand Out -Disable or Enable) are configurable for direct iCAM Wiegand output.



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

1. Login to the iCAM configuration screen (if not already logged in).
2. Select the Wiegand Settings option from the main screen.
3. Select the dropdown box from *Wiegand In* (Wiegand IN interface,). This setting MUST be enabled to work in this verification mode as a card reader utilizing the Wiegand input is required.
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 Enable to enable the Wiegand Output.
5. Select dropdown box from Wiegand Out area called "Data Output". The Bypass mode must be selected for correct usage of this mode.

    a. Select the "Lenel + Key" box only to enable key/pin-pad for 8 bit burst (Lenel format only with use of key/pin-pad).

        - 8bit Burst – Each key pressed on the Pin Pad outputs an 8-Bit binary code from the Wiegand output of the camera unit (for use with a Physical Access Control System).

8 Bit Burst

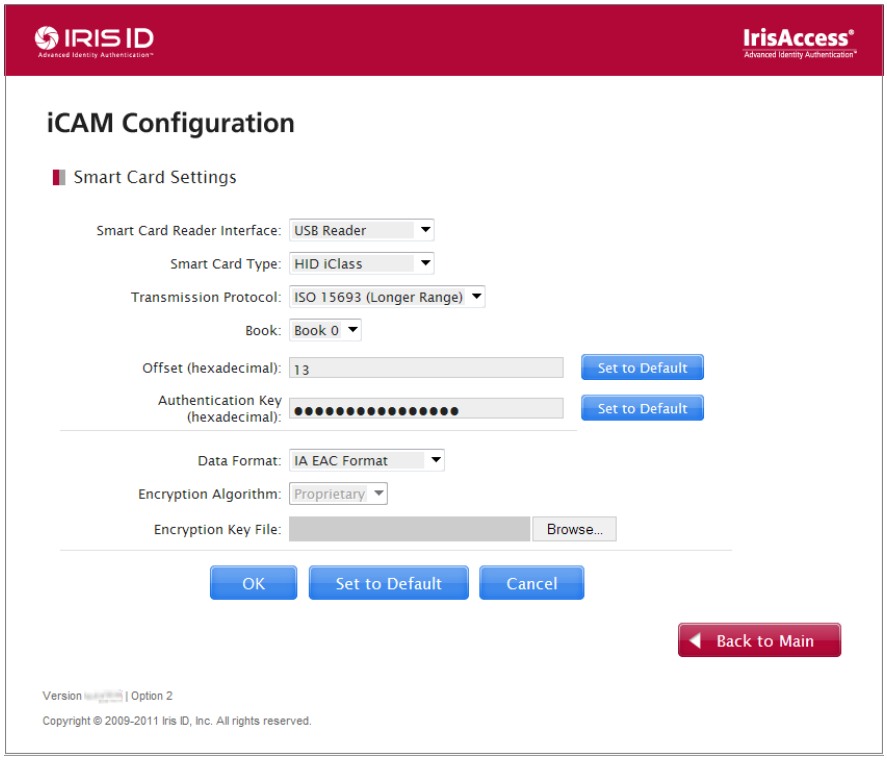
Key	Wiegand Output	Key	Wiegand Output	Key	Wiegand Output
1	11100001	5	10100101	9	01101001
2	11010010	6	10010110	*	01011010
3	11000011	7	10000111	0	11110000
4	10110100	8	01111000	#	01001011

- Select the Set to Default button to restore settings to the original factory default state for Wiegand Settings when needed. By default, the Wiegand In and Wiegand Out are both set to *Enable*.

> ***Note:*** *The Total Wiegand Bits, Facility Code, and Valid Bits are determined by the card or Access system configuration.*
>
> ***Additional Note:*** *The software controlling the iCAM is used to configure the Wiegand input and output settings. The supported Wiegand formats are determined and limited by the software application.*

11.2.5 Smart Card Configuration

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 iCAM.



1. Login to the iCAM 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 iCAM found in this screen. (See following data for details.)

A. Smart Card reader interface:

c. **Serial Reader** – This selection is used to enable an iClass reader through the Serial Smart Card Interface of the iCAM7000/7100 model unit.

d. **USB reader** – This selection enables the use of iClass Smart Cards through the optional internal USB Smart Card reader. (This reader type is selected by default.)

B. Smart Card Type:

Select the type of Smart Card that will be used.

a. HID iClass – This selection enables the use of iClass Smart Cards through the optional internal USB Smart Card reader. (This reader type is selected by default.)
b. BC - This selection is a proprietary format. (Do not select this option unless specifically instructed.)

C. Transmission Protocol:

(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. ISO 14443B (Faster Read)
b. ISO 15693 (longer Range)

D. 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

E. 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).

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

G. Authentication Key:

Also known as an Application Key, this can be set by entering a valid key in the application key text box. This key is masked on display. Once the user clicks on the application key text box, the key is cleared and user can enter key in normal text mode and appropriate authentication key. (Pressing the 'set to default' button will place the offset value to factory settings.)

***Note:** Authentication Key, also known as application key is the primary security of the card. Without the correct application key, card reads and writes will not be possible. Any cards created with a specific application key will only be able to be used with devices containing an identical matching application key program.*

H. Click on "Set to Default" button to set the default authentication key.

I. 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.

J. Encryption Algorithm:

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

Encryption Algorithm types are depends on type of data format.

- If data format is **"IA EAC Format"**, only applicable encryption algorithm is **"Proprietary"**.
- If data format is either **"GSC-IS Format"** or **"Lenel Format"**, applicable encryption algorithms are **"None"**,**"AES"**,**"DES"** and **"DES3"**.

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

K. 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),

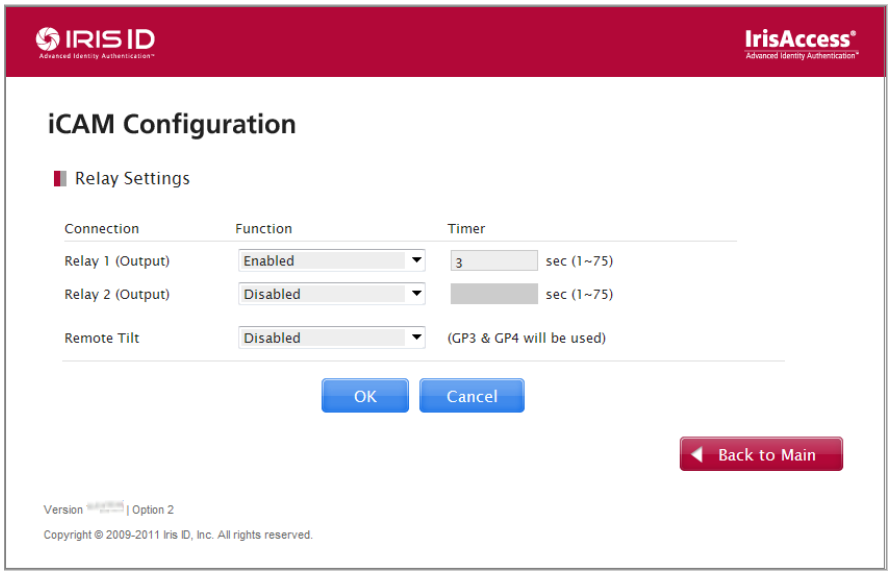
***Note:** If "Encryption Key file" is already configured and there is no change in "Data Format" and "Encryption Algorithm", then the installer need not upload a security key file.

****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.

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.

11.2.6 Relay Settings

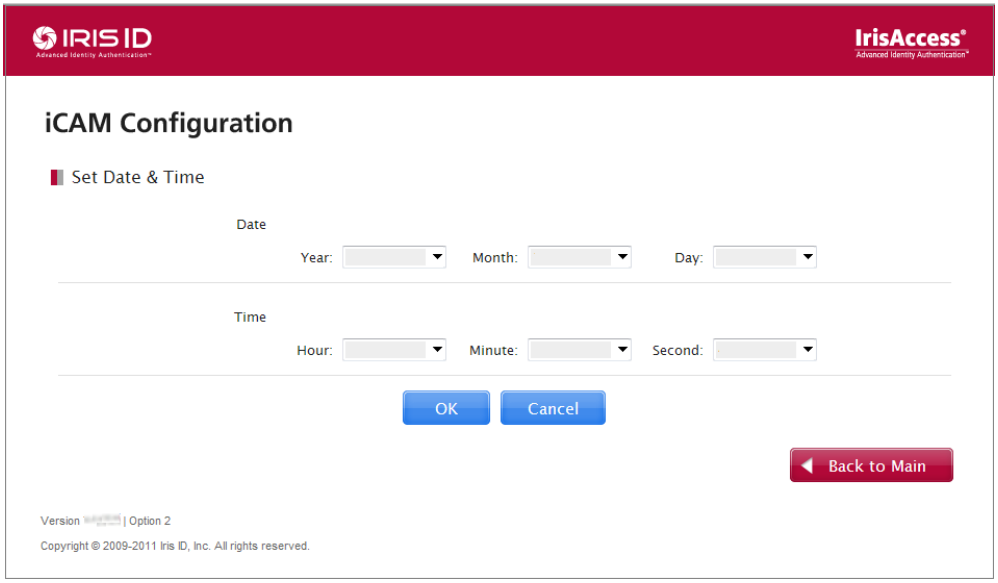
From this screen, selectable Relay configuration settings are available for Relay 1 and Relay 2.



- Relay 1 (Output) - can be enabled when a user is accepted along with a relay duration period to define this field value. By default, relay 1 is set to enable.
- Relay 2 (Output) - can be enabled for the purpose of tamper notification. By default, Relay 2 is set to disable.
- Remote Tilt - can be enabled when used in conjunction with either GP3 or GP4. When enabled, this feature will allow for the tilt buttons to be operated remotely.

11.2.7 Set Date & Time

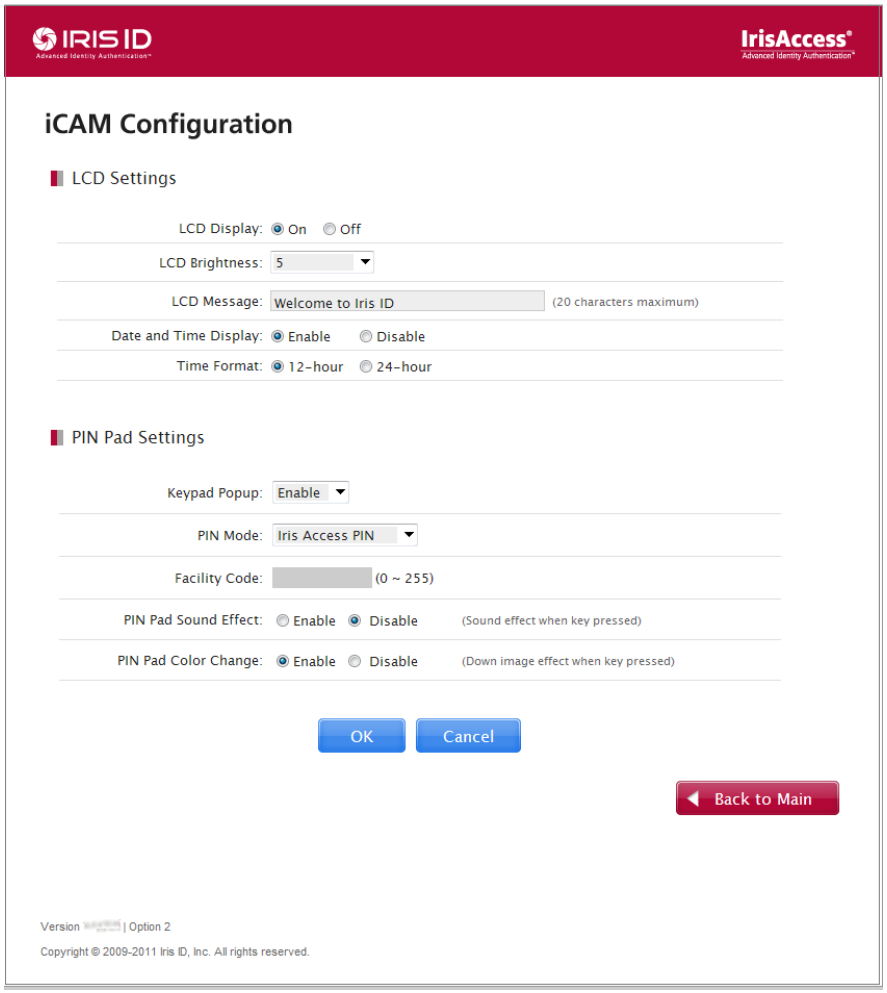
This screen provides the ability to enter the specific time and date for the unit. Enter each field for accurate time display.



- **Note*: **Time Format** is available for Selection of 12-Hour time or 24-Hour time display in the LCD & PIN Pad Settings screen. Additionally, adjust the LCD & PIN Pad Settings as needed to enable or disable the display of the Date and Time on an iCAM71xx device. (Review "LCD & PIN Pad Settings" section for details.)

12.1.4 LCD & PIN Pad Settings (7100 models only)

This section is for use with iCAM7100 model camera units only. The settings and information available in this area contain feature sets that are only compatible with the7100 models. Specific LCD settings can be modified and customized. Additionally, the iCAM7100 model units can be used with a built in Pin Pad that can pop-up on the LCD display. The usage of the Pin Pad can be modified by an installer for custom use. Read the following information for details.



4. Login to the iCAM configuration screen as shown above (if not already logged in).
5. Select the Function Key & LCD Settings (7100 only) Settings option from the main screen.
6. Configure desired settings for the iCAM found in this screen. (See following data for details.)

7100 LCD Settings:

- **LCD Display** – Select On or Off. Select the On radio button to enable the LCD display. Select the Off radio button to disable the use/view of the LCD display on an iCAM7100 model camera unit.
- **LCD Brightness** – Select the desired brightness level of the LCD when enabled. The setting options for brightness range from 1 – 5. 1 is the least bright image available for this LCD, and 5 is the Brightest. By default, the LCD setting is enabled and set to 5.
- **Date & Time Display** – Select Enable or Disable. When enabled the Time and Date will display on the main screen of the iCAM7100 LCD display. Other time and date displays (during transactions) will always be displayed. (Review additional time settings by going to the "Date & Time Settings section".)
- **Time Format** – Selection of 12-Hour time or 24-Hour time display.

PIN Pad Settings:

- **Keypad Popup** - Shows the selectable Keypad Popup State of the Camera unit (7100 models only). Enabled, or Disabled options are available. When enabled, the *F3* function button on an iCAM71xx model unit will allow the Pin-pad to appear. When this option is disabled, the *F3* function button will not perform any function, and the Pin-pad is not in an active state.
- **Pin Mode** – Shows the selectable PACS Pin Mode setting of the Camera unit (7100 models only). The Wiegand Output mode of Iris Access PIN, 8 bit burst, 4 bit burst, and Galaxy format are available for selection. Pin Mode selections include 8bit Burst, 4bit Burst and Galaxy Mode, and Disabled. Details of these available modes are as follows:
    - **Iris Access PIN** - Utilizes the Pin field in IrisAccess EAC software for Pin verification of a user. Refer to EAC documentation for further details.
    - **8bit Burst** – Each key pressed on the Pin Pad outputs an 8-Bit binary code from the Wiegand output of the camera unit (for use with a Physical Access Control System).

8 Bit Burst

Key	Wiegand Output	Key	Wiegand Output	Key	Wiegand Output
1	11100001	5	10100101	9	01101001
2	11010010	6	10010110	*	01011010
3	11000011	7	10000111	0	11110000
4	10110100	8	01111000	#	01001011

    - **4bit Burst** – Each key pressed on the Pin Pad outputs a 4-Bit binary code from the Wiegand output of the camera unit (for use with a Physical Access Control System).

4 Bit Burst

Key	Wiegand Output	Key	Wiegand Output	Key	Wiegand Output
1	0001	5	0101	9	1001
2	0010	6	0110	*	1010
3	0011	7	0111	0	0000
4	0100	8	1000	#	1011

- **Galaxy Format** – Each key press is stored in a buffer and is sent only when the # Key or enter key is pressed. The number entered (key presses) will be sent as the Card ID along with the Facility Code entered in the Facility code field. The Wiegand output is sent from the camera in a 26-Bit format to the PACS panel.

Galaxy Format

Parity	Facility Code	Card ID	Parity
P	FFFFFFFF	CCCCCCCCCCCCCCCC	P

Start Parity Bit = 1 Bit (Even*)
Facility Code = 8 Bit
Card ID = 16 Bit**
Stop Parity Bit = 1 Bit (Odd*)

** **Note**: Start bit is determined by the first 13 bits and the Stop Parity Bit is determined by the last 13 bits.*

- **Disabled** - Set to disable when not using this feature. When disabled, pressing the F3 key will not display the PIN pad.

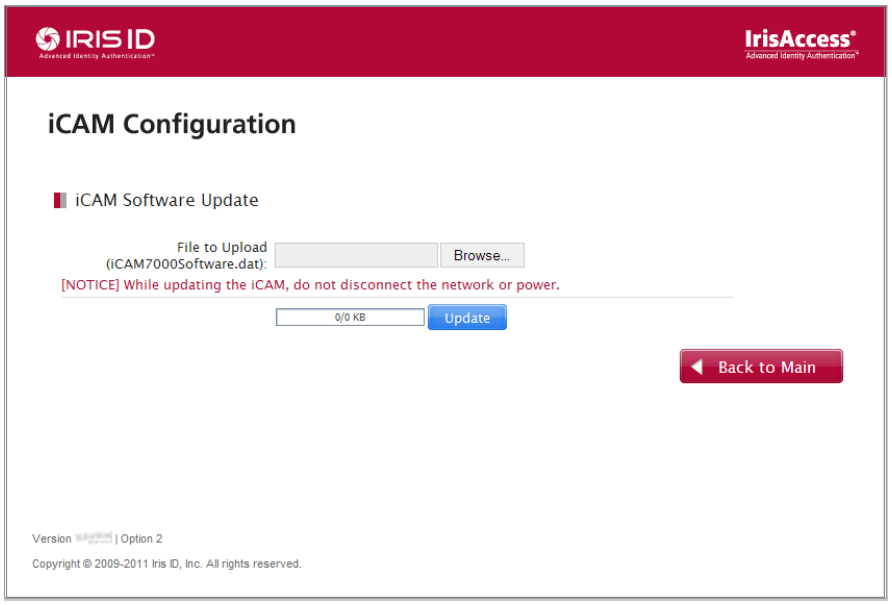
** **Note**: When Iris + Pin mode is currently in use, this option is not available (as the PIN mode is already active by default based on the Recognition mode usage).*

- **Facility Code** – When Galaxy Format is selected, the Facility Code value in this field will be output as part of the Galaxy formatted Wiegand Output. Enter the desired facility code between 0 ~254 as needed.
- **Pin Pad Sound Effect** – Enables or Disables a Pin Sound of an iCAM7100 model unit. This option can be set to either Enable or Disable. The pin sound option allows for a button press on the touch screen LCD to produce an audible sound. (This option is set to disable by default).
- **Pin Pad Color Change** - Selectable by radio button, enable this option to see a visual change to the key pressed on the PIN Pad.

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.

11.2.8 iCAM Software Update

iCAM software updates are generally performed automatically when used with the EAC application. However, from time to time, an iCAM software update may become available from Iris ID Systems, Inc. that may require a manual upgrade. Such updates may often be downloadable from the http://www.IrisID.com website. Consult with your system integrator or IRIS ID directly before attempting to perform any updates of this type. This section allows for you to update the camera unit with a compatible software update directly from the iCAM.



***NOTE**: Java VM must be installed on your computer in order to perform these procedures correctly.* Verify that Java VM is installed and working on your windows pc. (If Java VM is not installed, go to http://www.java.com/en/download/index.jsp for download and installation instruction.

Verify that Internet Options settings are set to *allow 'local directory path when uploading to a server'*.

1. Open Internet Explorer
2. Go to the *tools* Menu> *Internet Options* > *Security* > *Custom Level* > *Miscellaneous* section > *Include local directory path when uploading files to a server* > Select *Enable* radio button > press *OK*.

Manually upgrading iCAM Software:

WARNING! Do not disconnect the power or disturb the network connection during the upgrade process unless instructed to do so. If power or network is disconnected during file transfer, this could cause corruption in the iCAM OS and render the iCAM non-operational.

Download the file "iCAM7000software.dat"; make a new folder on the c: drive and place the file in that new folder.

Updating the iCAM Software:

- Log into the iCAM (web browser interface)
- From the main menu select iCAM Software Update
- Select Browse

- Select the path to the *"iCAM7000Software.dat"* file
- Double click on the "Update" button. (Files will transfer and iCAM software will update, this may take several minutes)
- When complete a summary screen will display
- Click Yes to reboot the iCAM
- Enter the username (iCAM7000) and password (iris7000)
- Click OK to reboot iCAM
- Wait 2 minutes for the reboot to completely.

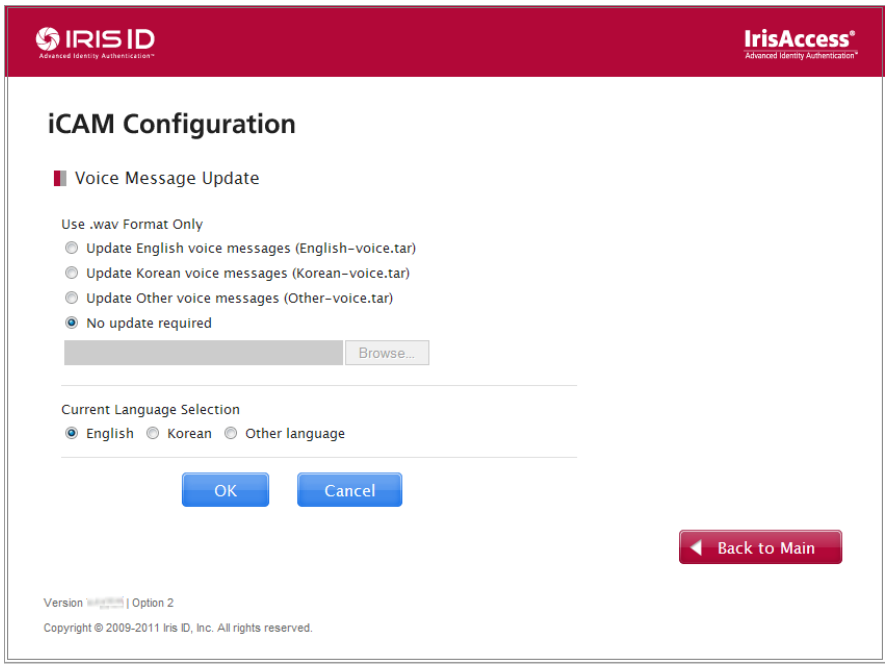
Confirming the iCAM Software version:

- Log into the iCAM (web browser interface)
- From the main menu click on the arrow symbol next to the version number.
- This window will display the iCAM software and firmware versions.

iCAM software version indicates a successful upgrade of the iCAM.

11.2.9 Voice Message Update

If the camera unit requires different voice messages then what was provided (default standard messages language announced in English), Korean language can be selected or other .WAV formatted messages can be uploaded using a .TAR format to the camera unit in this section.



Procedures to upload the voice files to your iCAM:

1. Place the 'Other-voice.tar' file on a computer that can be connected to the iCAM.
2. Log into the iCAM Configuration screen using 'iCAM7000' as the username and 'iris7000' as the password.

3. Select ‘Voice Message Update’
4. Select ‘Update Other language messages (Other-voice.tar)’
5. Press the ‘Browse’ button to browse for the ‘Other-voice.tar’ file and select it for use.
6. Set the ‘Current language selection’ to ‘Other language’
7. Press ‘OK’
8. A message will display confirming the action success (or failure).
9. When the upload is complete, reboot the iCAM.

If you want to convert the voices back to English, log in to the iCAM's web interface and select Voice Message Update.

Select ‘No Update required’ and set Current language selection to English.

Press Ok.

Enter the server IP address, username 'anonymous' and password 'r'.

Press Ok.

When the authentication page comes up, enter 'iCAM7000' for username and 'iris7000' for password. This will reboot the iCAM with English voice files.

Here is the list of .wav files.
You must use these exact file names (These are case-sensitive) and place them in a folder named “Other-voice”, then create a tar file of the entire folder. Name the tar file "Other-voice.tar". The wav files inside the tar file must have the path "Other-voice\"
The format of the sound files and translation are listed below.

Audio format: PCM 16 kHz, 16 bit, Stereo

16k_beepbeep.wav - (beeping sound)
16k_Capture.wav - (camera shutter sound)
16k_EnrollmentCommencement_B.wav - "Please present your card to the card reader."
16k_IDMessages_A.wav - "Thank you! You have been identified."
16k_IDMessages_C.wav - "Sorry. We cannot confirm your identity."
16k_ImageAquisitionMessages_A.wav - "Please come a little closer to the camera."
16k_ImageAquisitionMessages_B.wav - "Please move back a little from the camera."
16k_ImageAquisitionMessages_G.wav - "Please center your eyes in the mirror."
16k_OpenEyes.wav - "Please open your eyes wide"
16k_Post_ImageAcquisitionMessagesA.wav - "We finish taking pictures of your eyes."
16k_smartcard.wav - (Smart Card accepted sound)
16k_TryAgain.wav - "Please try again."
16k_VerificationResultMessages_A.wav - "Thank you! Your identity has been verified."

Recording your Own Sound files to use as voice prompts:

You may create your own sound files using Windows Sound Recorder (Included with Microsoft Windows). By following the below procedure we had success in creating different sound files which we could then upload to the Optical Units. The biggest problem is keeping the file size small enough to use.

In Windows
Click Start -> Accessories -> Sound Recorder

Record your message

Click File -> Save As -> (Name the file)
Click File -> Properties
Select "Format Conversion"
Select "All Formats"
Click "Convert Now"

Choose
Format: PCM
Attributes: 16 kHz, 16 bit, Stereo

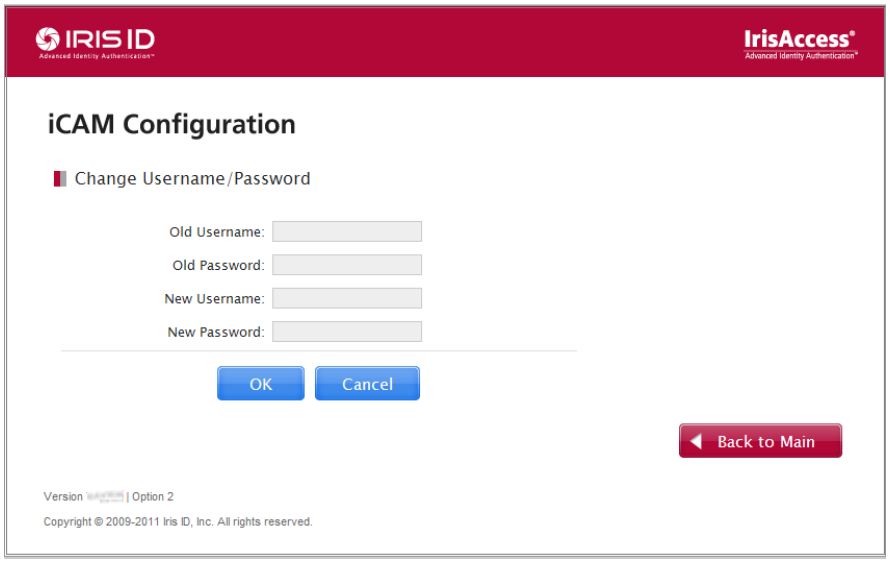
Click OK
Click OK
Click File -> Save

If the volume is too low, you may need a better quality microphone (this was a problem we had experienced), you may also increase the volume of the capture sound in Sound Recorder.

**Note: Sound files created must be packaged as a .tar file using a .tar compatible software of 1.15 or higher (standard). This file folder must be named "Other-voice.tar". In the event that an existing "Other-voice.tar" file has been created for an iCAM4000, it may be necessary to re-package the voice files into a new "Other-voice.tar" file folder using a utility/software (not provided by Iris ID) that conforms to 1.15 or higher standard .tar file creation.*

11.2.10 Change Username/Password

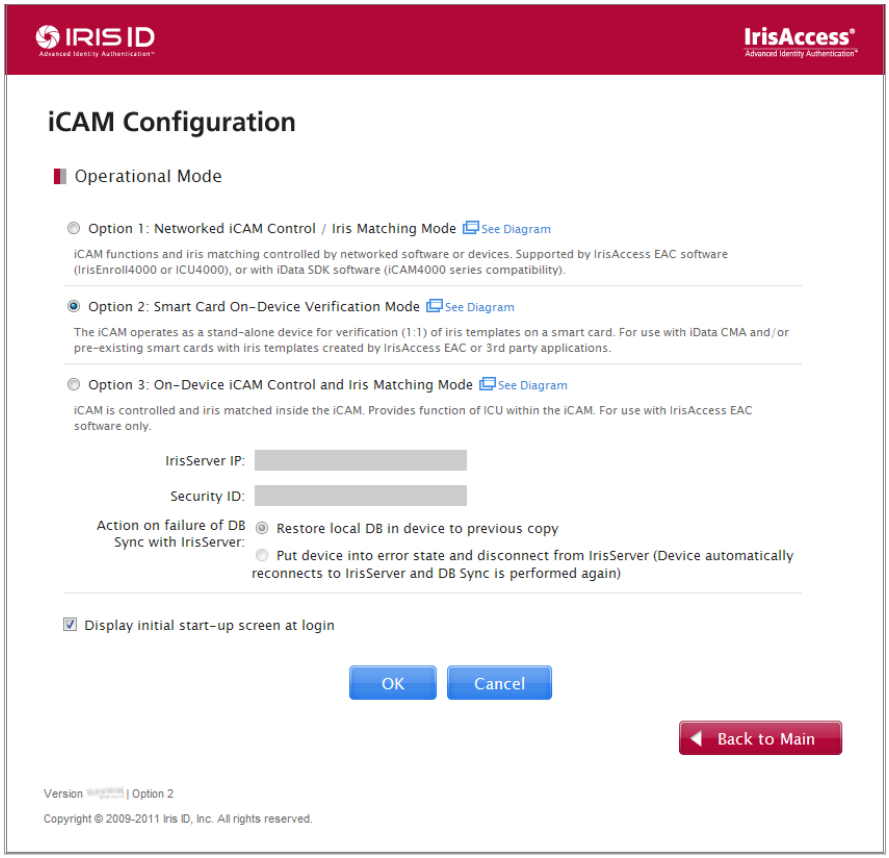
This menu provides the ability to change the Username and Password settings currently existing in the iCAM. In order to change the settings first the old user id and password must be entered in addition to the new user id and password credentials desired. Please note that all fields are case sensitive.



** **Note**: The iCAM FACTORY DEFAULT is located on the iCAM7000 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 (192.168.5.100) and the login ID credentials for the iCAM (User ID = iCAM7000 / Password = iris7000).*

11.2.11 Operational Mode

This screen allows for the iCAM to be set in Networked iCAM control / Iris image capture mode (Option 1), Smart-CardOn-Device Verification Mode (Option 2), or On-Device iCAM control and iris matching mode (option 3).



5. Login to the iCAM configuration screen as shown above (if not already logged in).
6. Select the Operational Mode option from the main screen.
7. Configure desired settings for the iCAM found in this screen. (See following data for details.)

- "**Option 1: Networked iCAM Control / Iris Matching Mode**" – When option 1 is selected, the iCAM will operate as part of an IrisAccess™ Entry Access Control System, or for use with iData™ SDK (iCAM4000 Series compatibility). The iCAM functions and iris matching are controlled by networked software or devices.
  IMPORTANT: If you are generally using option 3, this "option 1" mode may be needed to be used when performing enrollment.

- "**Option 2: Smart Card On-Device Verification Mode**" - When option 2 is selected, the iCAM7000 operates as a stand-alone device for verification (1:1) of the iris templates on a

smart card. This mode is generally for use with iData CMA and/or pre-existing smart cards with iris templates created by IrisAccess EAC or compatible 3rd party applications.
***Note**: "iCAM7000 Stand-Alone Smart Card Verification Mode" can only be used when a card reader (internal or external) is used with the iCAM7000 series unit.*

- "**Option 3: On Device iCAM Control and Iris Matching Mode**" – When option 3 is selected, the iCAM is controlled and iris matched inside the iCAM. This mode provides the function of an ICU within the iCAM. This mode provides the function of an ICU within the iCAM. This option is designed for use with compatible IrisAccess EAC software.

  ***Note**: If attempting to use an iCAM7000 series unit in operational mode "Option 3", compatible IrisAccess EAC software MUST be used for functionality of this option.*

  ***IMPORTANT**: If you are using an iCAM7000 in "Option 3" operational mode – when performing enrollments, and when trying to connect to the IrisEnrol4000 application within IrisAccess EAC software, the user must switch the operational mode to "option 1". Once enrollments have completed, the iCAM can be set back to operational mode "option 3" (if a dedicated iCAM is not being used for enrollment).*

In option 3 mode –the iCAM is controlled and iris matched inside the iCAM while providing function of an ICU within the iCAM. In order for these processes to work correctly the below information is required to be provided when "Option 3" is selected:

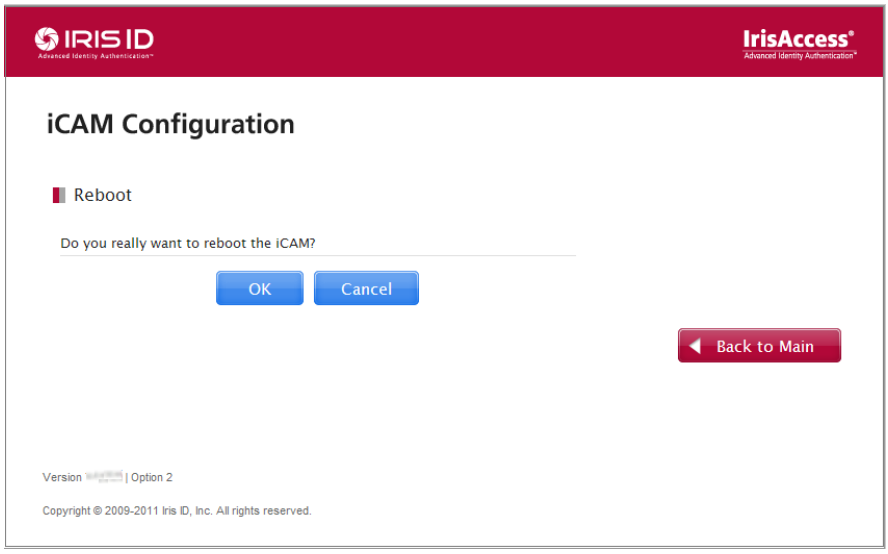
d. **IrisServer IP** - Enter the Iris Server IP address
e. **Security ID** - Enter a unique security ID for this unit (16 character requirement).
f. Action on Failure of DB Sync with IrisServer - Select the radio button desired for Action on failure of DB Sync with IrisServer. These options are:

   - **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).**

8. Display Initial Start-up screen at login – This checkbox can be selected to enable or unchecked to disable the initial start-up screen from appearing when the iCAM Configuration is logged into.

11.2.12 Reboot

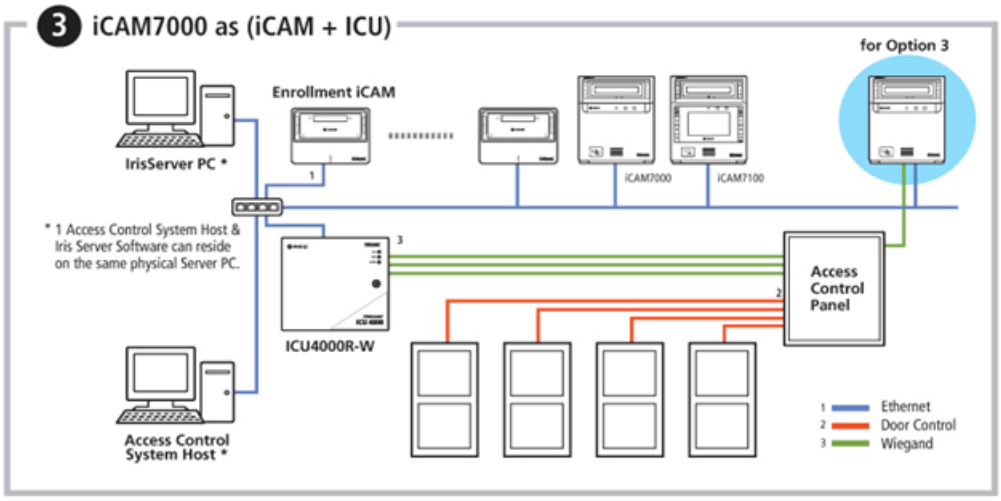
This screen allows for a reboot of the iCAM unit. Once OK is pressed, the iCAM may prompt for an authentication of the specific User ID and Password of the camera unit. The unit with reboot once the okay button is selected. (Please wait for this process to complete as this may take several minutes.)


IRIS ID
IrisAccess
iCAM Configuration
Reboot
Do you really want to reboot the iCAM?
OK
Cancel
Back to Main
Version | Option 2
Copyright © 2009-2011 Iris ID, Inc. All rights reserved.

12. Using the iCAM Configuration Interface - Option 3: On-Device iCAM Control and Iris Matching Mode

On-Device iCAM Control and Iris Marching Mode (Option 3) – The iCAM is controlled and iris matched inside the iCAM. This option provides a function of an ICU within the iCAM. This option is for use with IrisAccess EAC software.

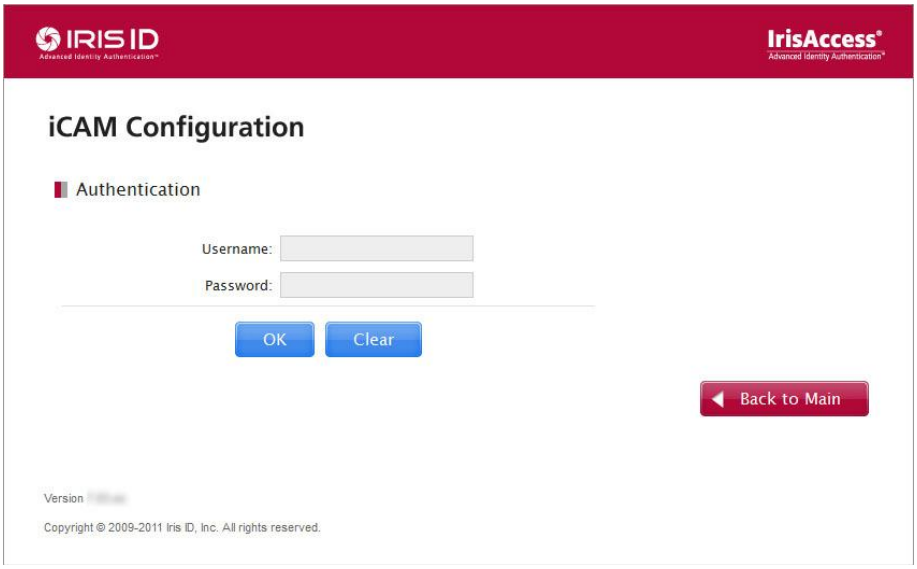
It is important to have an understanding of the screens and options available in the iCAM configuration interface. This area can be used to gather information about your iCAM as well as perform modifications and setting changes to your camera unit. If using more than one iCAM, each iCAM needs to be configured to the desired specifications required – configuring one iCAM from the configuration interface will only change the settings of that particular iCAM unit. Please see below for a screen by screen break-down of the iCAM configuration interface for reference and review.



12.1 Login and Main Menu Screen

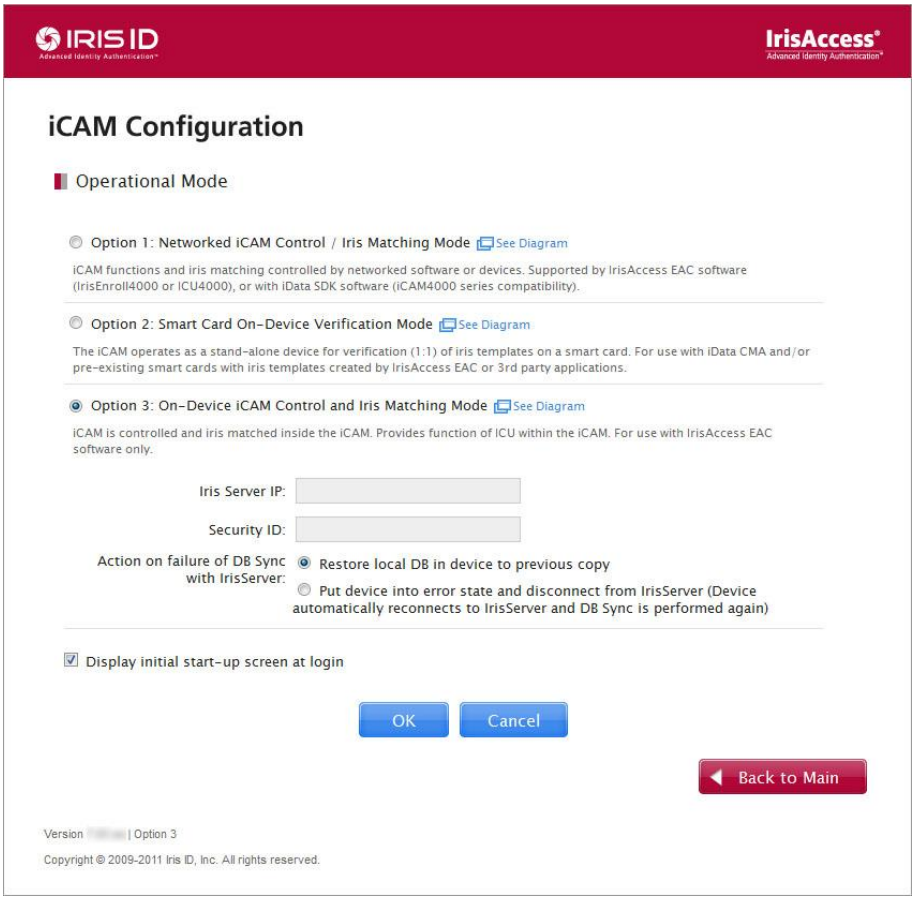
12.1.5 Login Screen

Enter the default Username: iCAM7000 and Password: iris7000 (both are case sensitive) if still set to default settings.



12.1.6 iCAM Configuration Start Up Screen

Once you have logged into the iCAM Configuration, an initial start-up screen may appear. This screen allows for settings to be entered that will determine how the iCAM will be used. This screen is viewable ONLY in the Operational Mode of “Option 3”.



4. Enter the desired IP address data of the iCAM7000 series camera unit.
    - **IP Address** – Enter IP address
    - **Subnet Mask** – Enter Subnet address
    - **Default Gateway** – Enter Gateway address
5. A selection to enable or disable IP announcement will also be available (set by default as active).
6. Select the desired Operational mode that will be used for the camera unit.

In option 3 mode –the iCAM is controlled and iris matched inside the iCAM while providing the function of an ICU within the iCAM.

7. **IP Address** - Enter the Iris Server IP address
8. **Security ID** - Enter a unique security ID for this unit (16 character requirement).
9. **Action on failure of DB Sync with IrisServer** - Select the radio button desired for this setting. These options are:
    - **Restore local DB in device to previous copy** – This selection setting will use the internal iCAM database for matching when there is NO connection to the IrisServer. *Or*
    - **Put device into error state and disconnect from IrisServer (Device automatically reconnects to IrisServer and DB Sync is performed again)** – If the iCAM cannot establish a connection to the IrisServer, the iCAM will enter into a non-operational error-state. Once the iCAM connection is restored with the IrisServer, the iCAM will resume its proper operation.

Note: In other above option, if the iCAM is unable to establish communication with the IrisServer, enrollment data and database/system changes will not take effect until communication is re-established between the device and the IriServer.

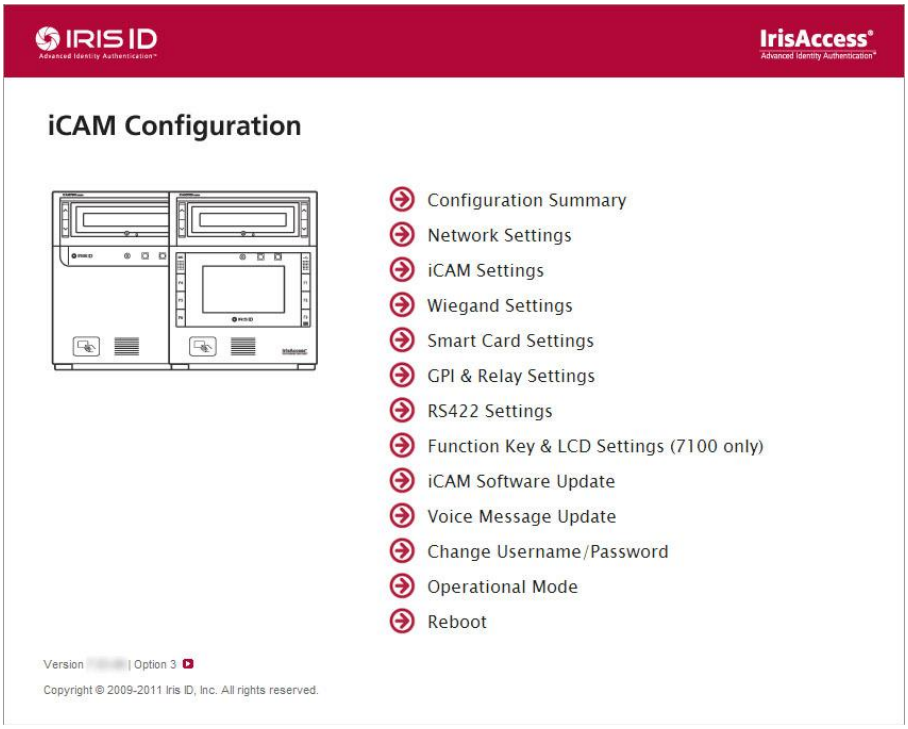
- **Display Initial Start-up Screen at Login** - If you do not wish to see this screen start automatically at the time of iCAM configuration login, check the box "Do not display this screen" to stop this screen from appearing.

  NOTE: *This Start up screen can be re-enabled in the iCAM Settings of the iCAM located in the 'Operational Mode section'.*

- Click **Apply** to save changes or press Skip and return to main screen as needed.

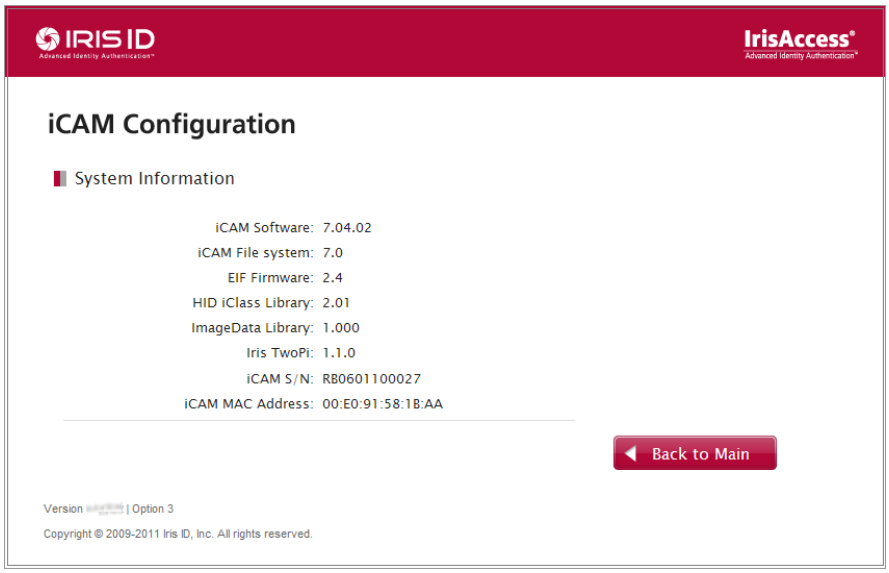
12.1.7 Main Screen

Once you have accessed the iCAM Configuration Main Screen (Menu screen), configurations such as configuration Summary, Network Settings, iCAM Setting, Wiegand Settings, Smart Card Settings, GPI & Relay Settings, RS422 Settings, Function Key & LCD Settings (7100 only), iCAM Software Update, Voice Message Update, Change Username/Password, Operational Mode, and Reboot functionality. Additionally, the iCAM software version is displayed in the lower left corner of the display window (and can be selected for additional version detail).



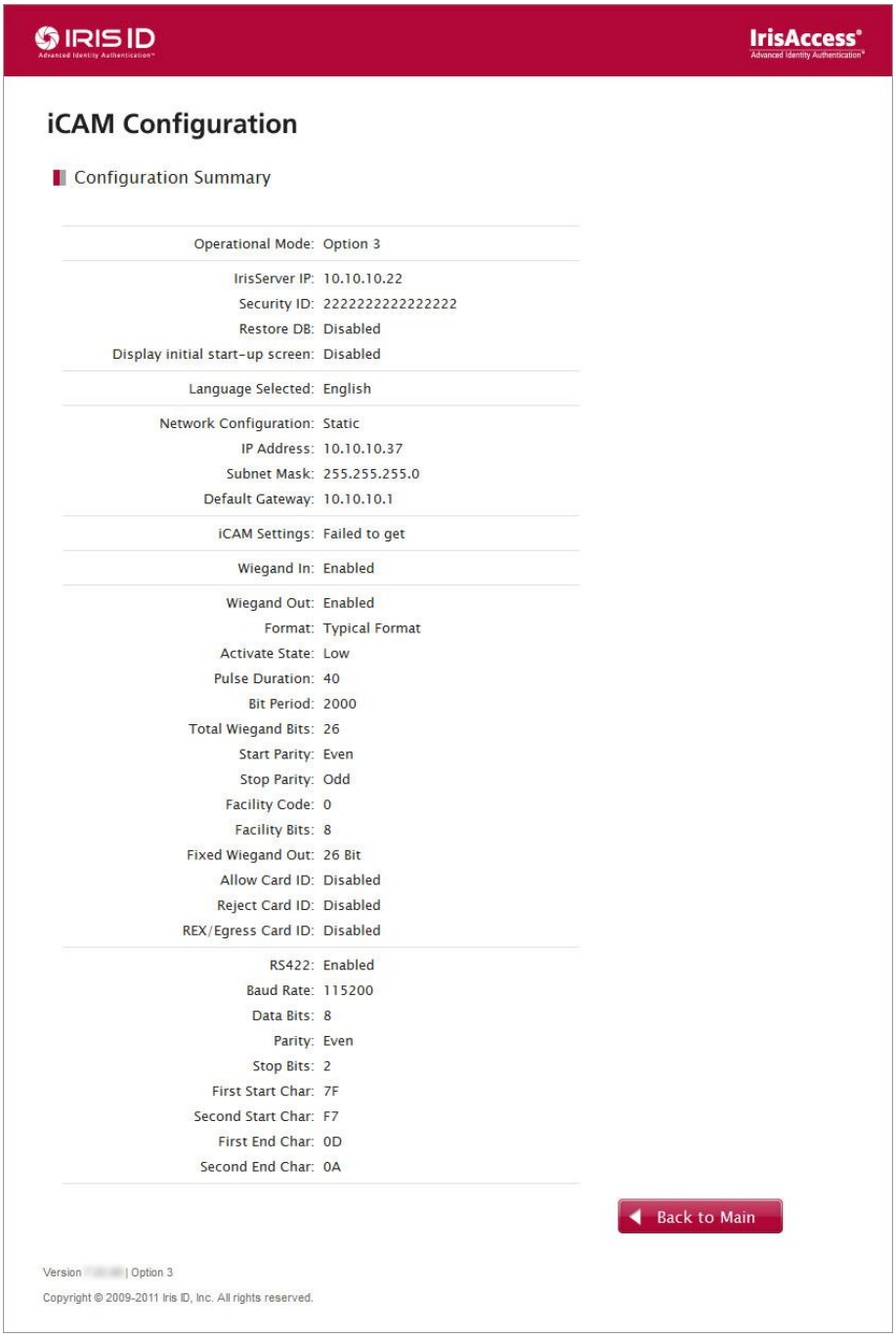
12.1.8 System Information Screen

System Information
The Configuration Summary screen provides detailed (viewable only) information about the specific iCAM connected. Such information is shown to help identify the iCAM software version, iCAM File system version, Firmware version/type, HID iClass library, image data library, and command process along with the full iCAM serial number. 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.



12.1.9 Configuration Summary

These settings are viewable only, and indicate the specific (currently configured) settings which include Language type, Network configuration type, IP address settings, smart card setting, and connected client. Please see below for detailed information for each item.



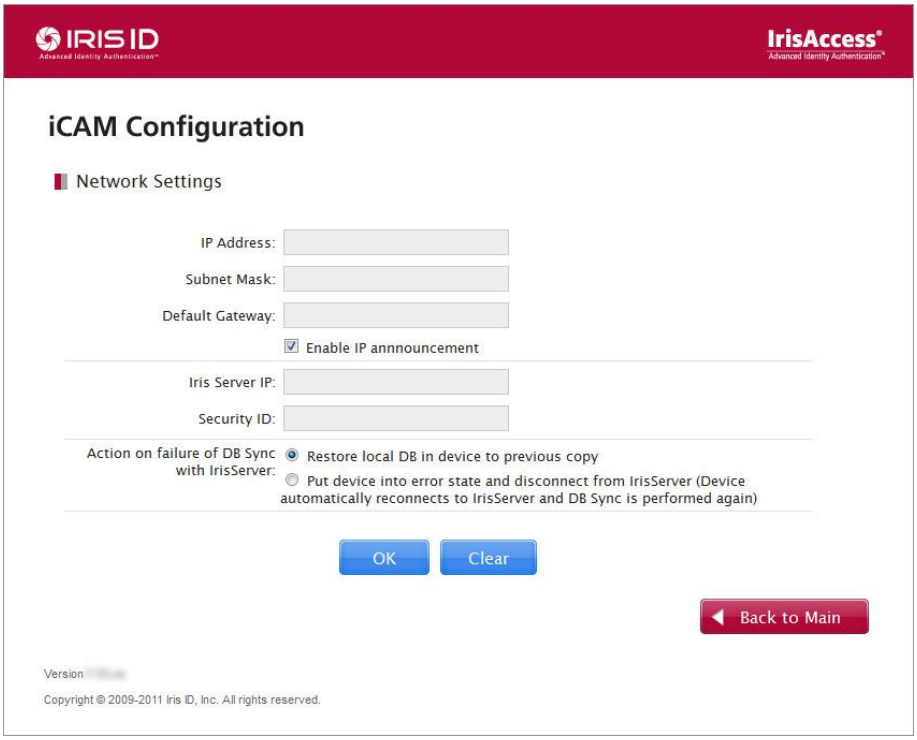
- *Operational Mode* – Displays the Operational Mode state of the iCAM.
- *Iris Server IP* – Displays the current IrisServer IP address setting for the iCAM.
- *Security ID* – Displays the 16 character unique security ID programmed for use with this iCAM.
- *Restore DB* – Displays the enabled or disabled state determined by the current setting of the iCAM.
- *Display initial start-up screen* - Displays the enabled or disabled state determined by the current setting of the iCAM.
- *Language Selected* – Displays the current language selected for the ICAM.
- *Network Configuration* – Displays the type of network configuration enabled for the iCAM (i.e.: Static).

- *IP Address* - Displays the IP address of the Camera unit in the iCAM Configuration.
- *Subnet Mask* - Displays the Subnet address of the Camera unit in the iCAM Configuration.
- *Default Gateway* - Displays the Default Gateway address of the Camera unit in the iCAM Configuration.
- *Smart Card Reader Interface* - Displays the Card Port Status as set in the iCAM Configuration of the camera unit. None, Serial Reader, or Internal USB Reader. (If a smart card port is selected, and no card is present in the port, the port will not appear as active.)
- *Smart Card Type* – Displays the type of card that is set to be used.
- *Offset (hexadecimal)* – Displays the current offset setting for the iCAM.
- *Data Format* - Displays the current data format setting for the ICAM.
- *Encryption Algorithm* – Displays the current encryption setting for the iCAM.
- *Transmission Protocol* – Displays the current transmission protocol setting for the iCAM (Faster Range, or Longer Range).
- *Book* – Displays the current Book value setting for the iCAM (Book 0, or Book 1).
- *Use as Prox Card* – Displays the setting of Enabled or Disabled for the current iCAM setting.
- *Recognition Mode* – Displays the mode of recognition that the iCAM is currently set to.
- *Verification Time Out* – Displays the current time out setting value for the iCAM.
- *Auto-Tilt*- Displays the auto-tilt selection Status in the iCAM Configuration of the Camera as either Enable or Disable.
- *Power Save* – Shows the Power-Save Status in the iCAM Configuration of the Camera unit. Never, 1, 3, 5, or 30. (Default setting is Never.)
- *Turn off LCD in power save mode* – Displays the current setting (Enabled, or Disabled) for use with power save.
- *Eye Selection* – Displays the current eye selection setting (by default the iCAM is set to 'Either').
- *Countermeasure* – Displays the current setting Level for the iCAM.
- *Sound Volume* –Displays the current sound volume setting of the iCAM (range from highest volume of 10 to 0 for mute).
- *iCAM Tamper* - Displays the current setting of the tamper state (Enabled, or Disabled).
- *Wiegand In* - Displays whether the Wiegand In is set to Enabled or Disabled in the iCAM Configuration.
- *Wiegand Out* - Displays whether the Wiegand Out is set to Enabled or Disabled in the iCAM configuration.
- *Format* – Displays the format selected for the iCAM.
- *Activate State* – Displays the iCAM selection (low or high) for the iCAM. (By default set to Low.)
- *Pulse Duration* – Displays the pulse duration setting of the iCAM (by default set to 40).
- *Bit Period* – Displays the current setting of the iCAM setting (by default set to 2000).
- *Total Wiegand Bits* – Displays the number of Wiegand bits set for output in the iCAM. (26-bits are the default value.)
- *Start Parity* – Displays the value for the setting of start parity of the iCAM. (The Even state is the default value.)
- *Stop Parity* - Displays the value for the setting of stop parity of the iCAM. (The Odd state is the default value.)
- *Facility Code* – Displays the current facility code configured for the iCAM.
- *Facility Bits* – Displays the current facility bits configured for the iCAM.
- *Fixed Wiegand Out* – Displays the current value configured for the iCAM (between 0-254).
- *Allow Card ID* – Displays the Enabled or Disabled setting selection used for the iCAM.
- *Reject Card ID* - Displays the Enabled or Disabled setting selection used for the iCAM.
- *Rex/Egress Card ID* - Displays the Enabled or Disabled setting selection used for the iCAM.
- *User's Access Rights* - Displays the setting selection used for the iCAM.
- *Relay 1 (Output)* - Displays the setting selection configured for the iCAM.
- *Relay 1 Duration* - Displays the setting selection configured for the iCAM.
- *Relay 2 (Output)* - Displays the setting selection configured for the iCAM.

- *Relay 2 Duration* - Displays the setting selection configured for the iCAM.
- *GP1Input* - Displays the setting selection configured for the iCAM (if used).
- *GP2Input* - Displays the setting selection configured for the iCAM (if used).
- *GP3Input* - Displays the setting selection configured for the iCAM (if used).
- *GP4Input* - Displays the setting selection configured for the iCAM (if used).
- RS422 - Displays the setting selection configured for the iCAM (enabled or disabled).
- Baud Rate – Displays the current setting configuration for the iCAM setting (configurable when RS422 is enabled).
- *Data Bits* - Displays the setting selection configured for the iCAM specific for RS422 output.
- *Parity* - Displays the setting selection configured for the iCAM specific for RS422 output.
- *Stop Bits* - Displays the setting selection configured for the iCAM specific for RS422 output.
- *First Start Char* - Displays the setting selection configured for the iCAM specific for RS422 output.
- *Second Start Char* - Displays the setting selection configured for the iCAM specific for RS422 output.
- *First End Char* - Displays the setting selection configured for the iCAM specific for RS422 output.
- *Second End Char* - Displays the setting selection configured for the iCAM specific for RS422 output.
- *LCD Display* – Displays the LCD Display Status in the iCAM Configuration of the Camera unit (7100 models only). ON or OFF. If shown as off, the LCD on an iCAM7100 model unit will not be enabled.
- *LCD Brightness* – Displays the Brightness Status of LCD in the iCAM Configuration of the Camera unit (7100 models only). Setting range is 1 through 5. Determines the Brightness of the LCD Display (for iCAM7100 model units only). 1 indicates the least bright and 5 indicates the brightest setting.
- *LCD Message* – For use with iCAM 7100 models only, the LCD message shows the currently configured message that will be displayed on the iCAM.
- *Display User ID* – Displays the setting of enabled or disabled for the iCAM.
- *Function Key Settings* - Displays the setting of enabled or disabled for the iCAM.
- *Function Key Timeout* – Displays the timeout value for the iCAM.
- *Display Function Key Result* - Displays the setting of enabled or disabled for the iCAM.
- *F1 Key* – Available when the Function Key settings are enabled, the currently configured setting for the function key is displayed for this iCAM. (By default, this function is set for "Punch In".) – For use with iCAM 7100 models only.
- *F2 Key* – Available when the Function Key settings are enabled, the currently configured setting for the function key is displayed for this iCAM. (By default, this function is set for "Punch Out".) ".) – For use with iCAM 7100 models only.
- *F3 Key* – Available when the Function Key settings are enabled, the currently configured setting for the function key is displayed for this iCAM (Dedicated for the Pin-pad pop-up). ".) – For use with iCAM 7100 models only.
- *F4 Key* – Available when the Function Key settings are enabled, the currently configured setting for the function key is displayed for this iCAM. (By default, this function is set for "Lunch In".) ".) – For use with iCAM 7100 models only.
- *F5 Key* – Available when the Function Key settings are enabled, the currently configured setting for the function key is displayed for this iCAM. (By default, this function is set for "Lunch Out".) ".) – For use with iCAM 7100 models only.
- *F6 Key* - Available when the Function Key settings are enabled, the currently configured setting for the function key is displayed for this iCAM. (By default, this function is set to "Disabled".) ".) – For use with iCAM 7100 models only.
- *Pin Mode* – Displays the Pin Mode setting in the iCAM Configuration of the Camera unit (7100 models only). When using the Keypad, the Pin mode of IrisAccess + Pin, 8bit burst, 4bit burst, and Galaxy format are available for selection.
- *PIN Pad Sound Effect* - Displays the Pin Sound Status (7100 models only). Enabled or Disabled. This option can be set to either enable or Disable.
- *PIN Pad Color Change* - Displays the Enabled or Disabled setting selection used for the iCAM.

12.1.10 Network Settings

This screen provides the ability to get detailed information on the IP settings of the iCAM connected on the network. From this location you can set IP address information (static IP) for specific network protocol based information. You can also designate whether to enable IP announcement which allows the ability to audibly hear the IP address of an iCAM by holding down the UP tilt button for ~10 seconds.



Settings:

7. Enter the desired IP address data of the iCAM7000 series camera unit.
   - IP Address – Enter IP address
   - Subnet Mask – Enter Subnet address
   - Default Gateway – Enter Gateway address
8. A selection to enable or disable IP announcement will also be available (set by default as active).
9. **Iris Server IP Address** - Enter the Iris Server IP address
10. **Security ID** - Enter a unique security ID for this unit (16 character requirement).
11. **Action on failure of DB Sync with IrisServer** - Select the radio button desired for this setting. These options are:
    - **Restore local DB in device to previous copy** – This selection setting will use the internal iCAM database for matching when there is NO connection to the IrisServer.
      Or
    - **Put device into error state and disconnect from IrisServer (Device automatically reconnects to IrisServer and DB Sync is performed again)** – If he iCAM cannot establish a connection to the IrisServer, the iCAM will enter into a non-operational error-state. Once the iCAM connection is restored with the IrisServer, the iCAM will resume its proper operation.

Note: In other above option, if the iCAM is unable to establish communication with the IrisServer, enrollment data and database/system changes will not take effect until communication is re-established between the device and the IriServer.

12. Click OK to save changes, or press clear to clear the screen from current settings.
    - Press the Back to Main button to return to the main page without saving any changes.

Additional information for setting /configuring of IP address information:

** **Note**: The iCAM FACTORY DEFAULT is located on the iCAM7000 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 (192.168.5.100) and the login ID credentials for the iCAM (User ID = iCAM7000 / Password = iris7000).*

- If the new iCAM IP address is still on the same IP address scheme/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 IP address scheme/subnet: the web browser will display the standard "The page cannot be displayed" message.

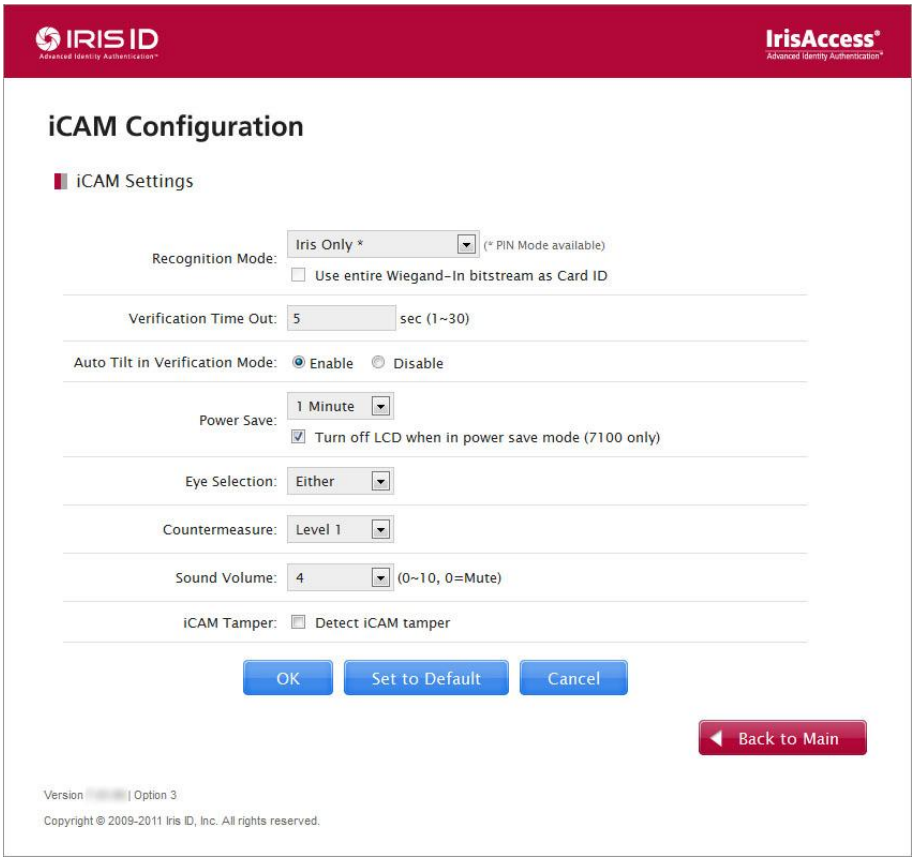
** **Note**: Pressing and holding the up tilt button for 10 seconds will cause the iCAM to announce the iCAM configured IP Address (Unless de-selected in this menu screen, or if volume is muted on the unit).*

To test the IP address change of the iCAM, 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.

12.1.11 iCAM Settings

This screen allows for specific settings to be configured/modified for the iCAM. Such settings include type of recognition mode, verification timeout, auto-tilt in verification mode, power save settings, eye selection type, countermeasures, sound volume, and iCAM tamper detection. See the following figure and information for details.



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

- **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.

- **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.
- **Auto-Tilt in Verification Mode** – Selectable by radio button this option can be set to enable or disable. When enabled, the iCAM will automatically tilt the last set position of the user – this setting will only work when the unit is performing verification (in a verification mode). Such modes are Iris + Pin, Iris + Smart Card, and Iris + Prox Card.
- **Power Save** – Selectable by dropdown box, this feature allows the iCAM to be placed in a more energy efficient state after a length of iCAM inactivity. Power Save can be enabled to engage after the length of time selected (Never, 1, 5, 15, 30, 1 hour).
    - **Turn off LCD when in power save mode (7100 only)** – This option, selectable by checkbox allows the user to define whether the LCD screen of an iCAM7100 model unit will be temporarily turned off. This setting can only be used in conjunction with the Power Save selection, and is controlled by the length of time set for the power save option.

  The unit can be taken out of power-save mode (which includes turning on the LCD (when selected) in several different ways. The iCAM will be removed from power-save mode by any of the following processes or operations:

    - *Proximity sensor* –The user is within proximity range of the iCAM sensor.
    - *Tilt buttons* – If any of the iCAM UP/DOWN tilt buttons is pressed.
    - *Function Keys* – If any of the Function keys are pressed (7100 models only).
    - *LCD Touch-Screen* - If the touch-screen is pressed (7100 models only).

- **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.
- **Sound 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.

Note:

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

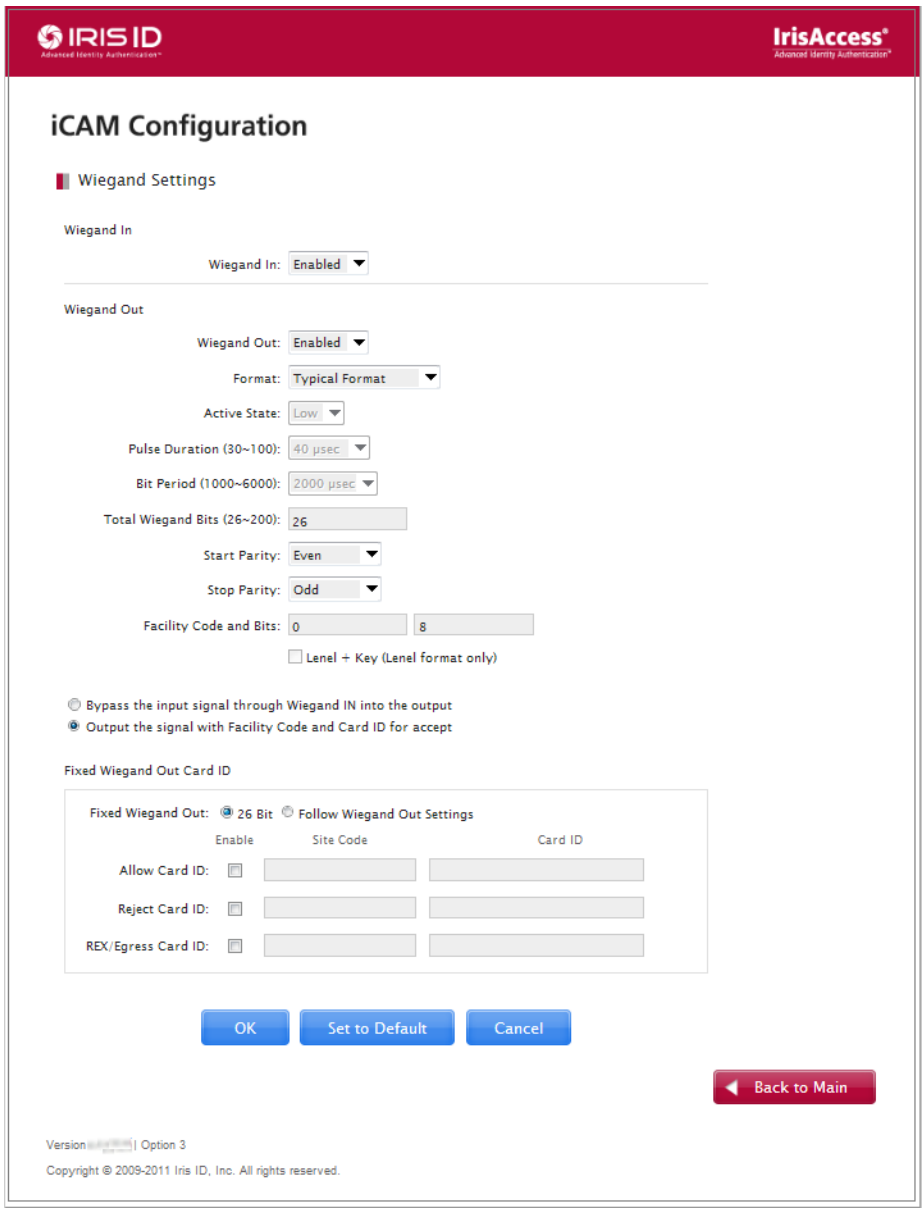
Select "Set to Default" to change setting values back to the default settings.

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.

12.1.12 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:



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

1. Login to the iCAM 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. Select the active state from the dropdown box (Low, or High)
7. Select the desired Pulse Duration (between 30~100).
8. 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 Valid Bits are determined by the card or Access system configuration.*

Additional Note: *The software controlling the iCAM is used to configure the Wiegand input and output settings. The supported Wiegand formats are determined and limited by the software application.*

9. Set the total number of Wiegand bits (26~200) that are required for output.
10. Set the Start Parity to either Even or Odd.
11. 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)
12. 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.
13. 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).

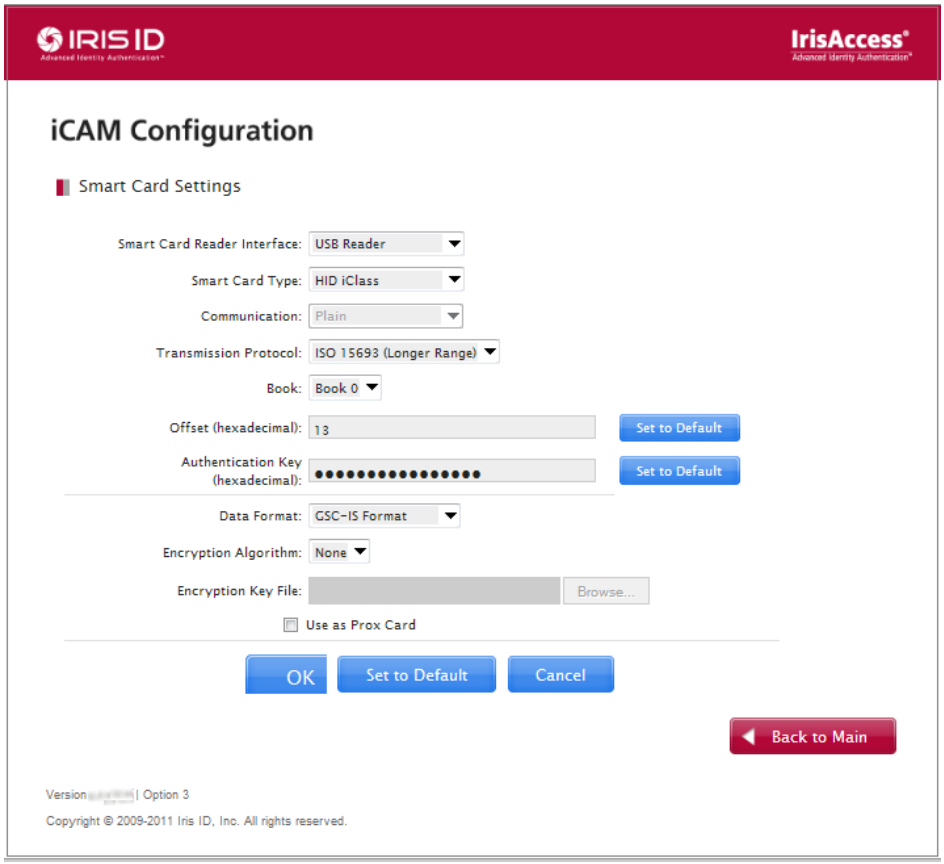
Select "Set to Default" to change setting values back to the default settings.

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

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

12.1.13 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 iCAM. The options available for "Smart Card Type" selection are:



1. Login to the iCAM 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 iCAM found in this screen. (See following data for details.)

A. Smart Card reader interface:

a. **Serial Reader** – This selection is used to enable an iClass reader through the Serial Smart Card Interface of the iCAM7000/7100 model unit.

b. **USB reader** – This selection enables the use of iClass Smart Cards through the optional internal USB Smart Card reader. (This reader type is selected by default.)

B. Smart Card Type:

Select the type of Smart Card that will be used.

a. None
b. HID iClass
c. MiFARE
d. DESFire

C. Communication: (Selectable for DESFire cards only)

a. Plain
b. Encrypted (Air Link) - DESFire only
c. Lenel - Select only if using DESFire cards encoded by On-Guard.

D. Transmission Protocol:

(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. ISO 14443B (Faster Read)
b. ISO 15693 (longer Range)

E. 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

F. 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).

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

H. Authentication Key:

Also known as an Application Key, this can be set by entering a valid key in the application key text box. This key is masked on display. Once the user clicks on the application key text box, the key is cleared and user can enter key in normal text mode and appropriate authentication key. (Pressing the 'set to default' button will place the offset value to factory settings.)

***Note:** Authentication Key, also known as application key is the primary security of the card. Without the correct application key, card reads and writes will not be possible. Any cards created with a specific application key will only be able to be used with devices containing an identical matching application key program.*

I. Click on "Set to Default" button to set the default authentication key.

J. 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.

K. 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

L. 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.

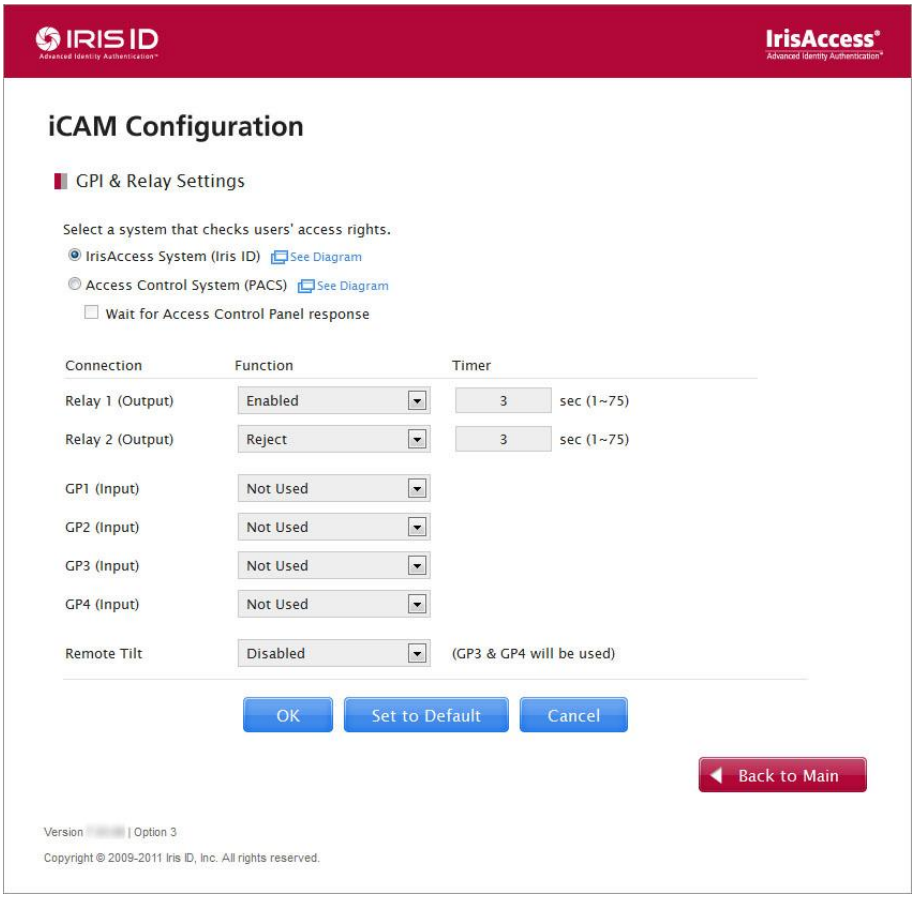
****Note:** Encryption Key files must be saved as a name without any spaces. Make sure to name the .DAT file with a file name that does not contain any character symbols or any spaces in the saved name as this may prevent the file from working correctly in the iCAM.

M. 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 iCAM 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.

12.1.14 GPI & Relay Settings

The GPI & Relay Settings screen allows for selection of the iCAM7000 series camera built-in General Purpose Input and Relay operation.



1. Login to the iCAM 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 iCAM 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.

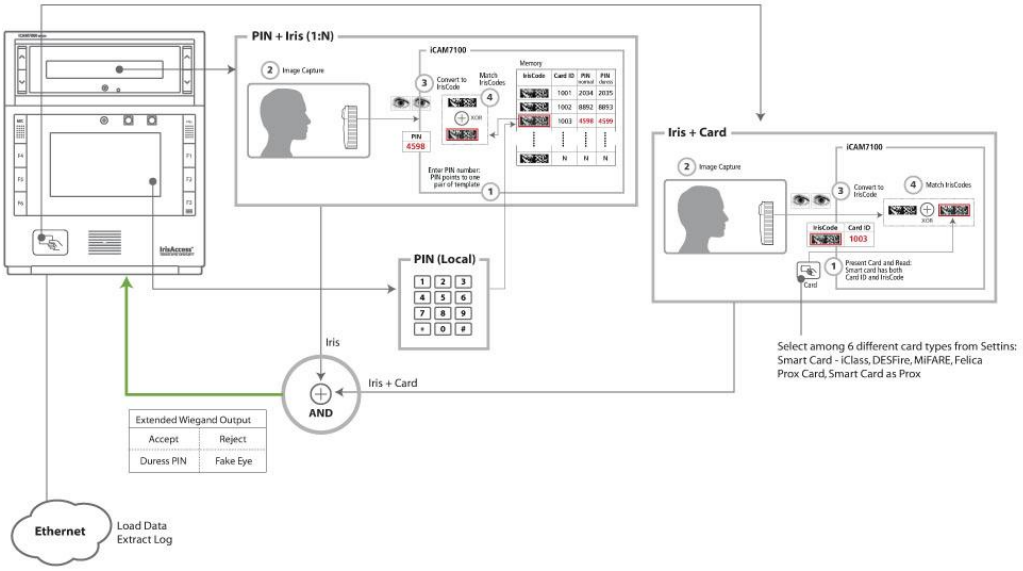


Diagram of IrisAccess System checks users' rights

- **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.

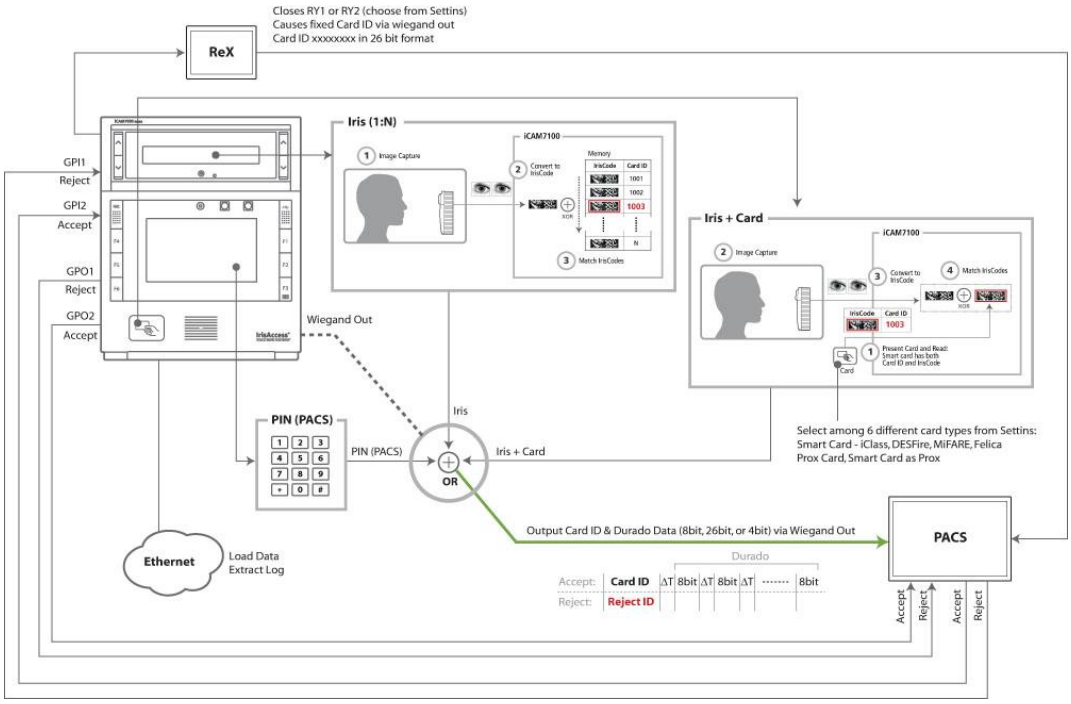


Diagram of Access Control System Checks users' rights

- **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.

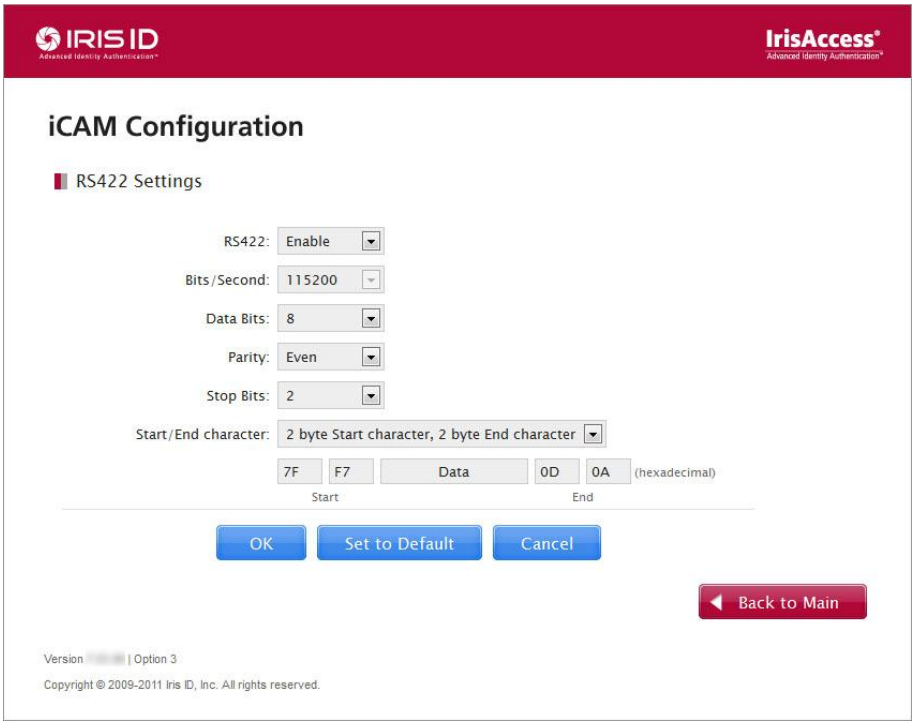
- **GP4 (Input)** – Set to either *Not used, Fire Alarm, REX/Egress, Access Allow*, or *Reject-A Mode*.
  - *Not used* – Input is disabled
  - *Fire Alarm* – When the GPI is initiated and held, Relay 1 is activated for the duration of time that the GPI is held. The iCAM sends a message to the IrisServer 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.

- **Remote Tilt** (GP3 & GP4 will be used) – Set to either *Enabled* to *Disabled*.
  - *Disabled* – External Tilt control is disabled. GP3 and GP4 operate as selected.
  - *Enabled* – External Tilt control of the iCAM optical unit is enabled. When selected the operation of GP3 is for Tilt Up, and GP4 is for Tilt Down. (Refer to chapter "Connection Details for Wiring iCAM7000 Series" – Section "External GPI/O" for wiring details.)

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.

12.1.15 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 iCAM 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 iCAM found in this screen. (See following data for details.)

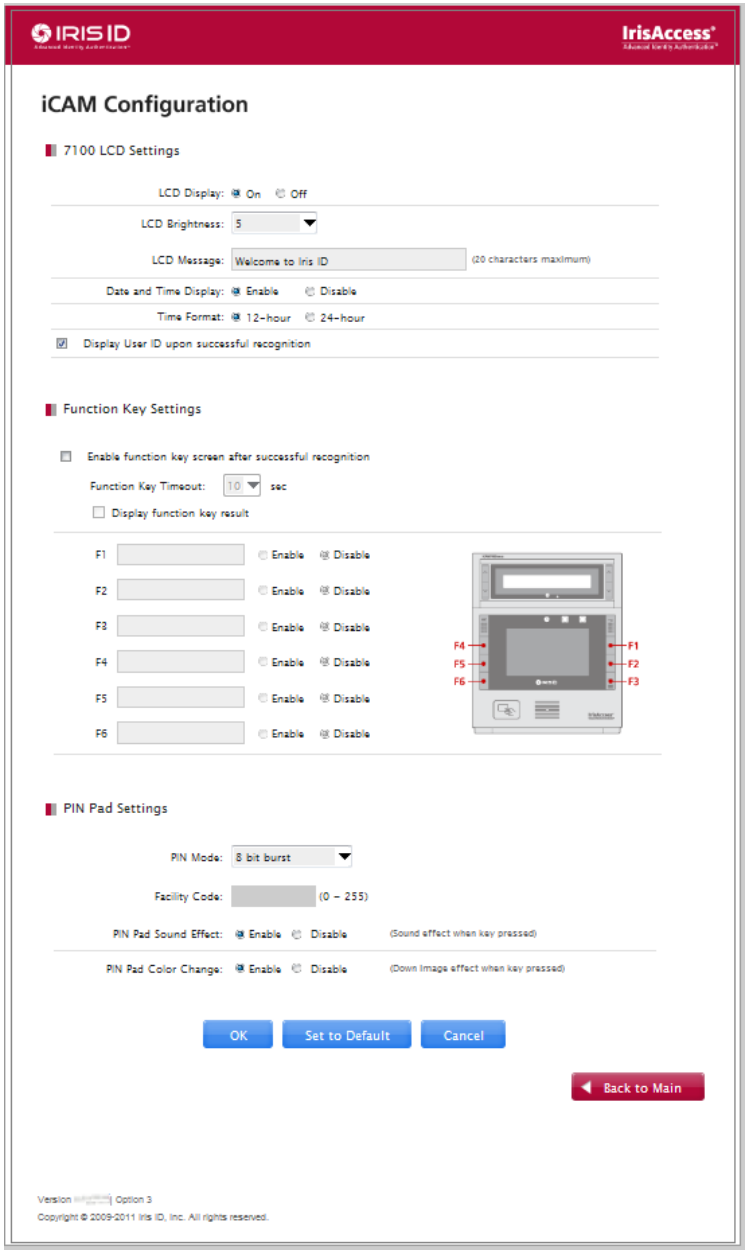
- **RS422** - Select *Enable* or *Disable.* Enabling this dropdown box allows for other items on the screen to be modified.
- **Bit / Second** – Select the desired bit / second. By default this value is set to 115200.
- **Data Bits** – Select the desired Data Bits. By default, this value is set to 8.
- **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 iCAM configuration without saving changes.

12.1.16 Function Key & LCD Settings (7100 models only)

This section is for use with iCAM7100 model camera units only. The settings and information available in this area contain feature sets that are only compatible with the7100 models. Specific LCD settings can be

modified and customized. Additionally, the iCAM7100 model units contain six function keys that can be used. These function keys can be modified by an installer for custom use. Read the following information for details.



1. Login to the iCAM configuration screen as shown above (if not already logged in).
2. Select the Function Key & LCD Settings (7100 only) Settings option from the main screen.
3. Configure desired settings for the iCAM found in this screen. (See following data for details.)

7100 LCD Settings:

- **LCD Display** – Select On or Off. Select the On radio button to enable the LCD display. Select the Off radio button to disable the use/view of the LCD display on an iCAM7100 model camera unit.

- **LCD Brightness** – Select the desired brightness level of the LCD when enabled. The setting options for brightness range from 1 – 5. 1 is the least bright image available for this LCD, and 5 is the Brightest. By default, the LCD setting is enabled and set to 5.
- **LCD Message** – 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).
- **Time & Date Display** – Select Enable or Disable. When enabled the Time and Date will display on the main screen of the iCAM7100 LCD display. Other time and date displays (during transactions) will always be displayed.
- **Time Format** – Selection of 12-Hour time or 24-Hour time display.
- **Display User ID upon successful recognition** – This check box can be selected or unselected. When selected, the User ID of the person identified will appear on the screen. Uncheck this box to remove the User ID from being displayed visibly on the LCD screen upon successful recognition.

Function Key Settings:

- **Enable Function key screen after successful recognition** – This checkbox can be set to enable this option, or disabled if the function keys are not required. When enabled, after a successful identification/verification, the function key selection screen appears on the iCAM7100 LCD. This allows the user to select the purpose of the transaction. This selection is then recorded along with the other transaction data on the IrisServer (when communication back to the IrisServer is available).
    - Function Key Timeout – When the above option is enabled (checked), an installer can set the timeout value in seconds from the available dropdown menu. If the user does not select the Function Key on the iCAM within that range, the function key display will timeout.
        - **Display Function result** – This available checkbox can be selected to display the function key result on the LCD. Uncheck this box to disable this feature.

- **F1 Key** – select enable or disable. If enabled, enter the name of the desired usage for this function button on the iCAM7100 model unit.
- **F2 Key** - select enable or disable. If enabled, enter the name of the desired usage for this function button on the iCAM7100 model unit.
- **F3 Key** - select enable or disable. If enabled, this Function Key is designed for use as the Pin Pad pop-up function for the LCD display. Press the F3 button to activate or hide the Pin Pad.
- **F4 Key** - select enable or disable. If enabled, enter the name of the desired usage for this function button on the iCAM7100 model unit.
- **F5 Key** - select enable or disable. If enabled, enter the name of the desired usage for this function button on the iCAM7100 model unit.
- **F6 Key** - select enable or disable. If enabled, enter the name of the desired usage for this function button on the iCAM7100 model unit.

Example Chart - Output Detail for Function Keys.

The value of the key press is recorded in the transaction log which then can be resolved by a 3rd party Time and Attendance application (T&A).

Key Press	Value
No Key	0
F1	1
F2	2
F3	3

Key Press	Value
F4	4
F5	5
F6	6
Reject	None

Pin Pad Settings:

- **Pin Mode** – Shows the selectable PACS Pin Mode setting of the Camera unit (7100 models only). The Wiegand Output mode of 8 bit burst, 4 bit burst, and Galaxy format are available for selection. Pin Mode selections include 8bit Burst, 4bit Burst and Galaxy Mode, and Disabled. Details of these available modes are as follows:

  - **8bit Burst** – Each key pressed on the Pin Pad outputs an 8-Bit binary code from the Wiegand output of the camera unit (for use with a Physical Access Control System).

8 Bit Burst

Key	Wiegand Output	Key	Wiegand Output	Key	Wiegand Output
1	11100001	5	10100101	9	01101001
2	11010010	6	10010110	*	01011010
3	11000011	7	10000111	0	11110000
4	10110100	8	01111000	#	01001011

  - **4bit Burst** – Each key pressed on the Pin Pad outputs a 4-Bit binary code from the Wiegand output of the camera unit (for use with a Physical Access Control System).

4 Bit Burst

Key	Wiegand Output	Key	Wiegand Output	Key	Wiegand Output
1	0001	5	0101	9	1001
2	0010	6	0110	*	1010
3	0011	7	0111	0	0000
4	0100	8	1000	#	1011

  - **Galaxy Format** – Each key press is stored in a buffer and is sent only when the # Key or enter key is pressed. The number entered (key presses) will be sent as the Card ID along with the Facility Code entered in the Facility code field. The Wiegand output is sent from the camera in a 26-Bit format to the PACS panel.

Galaxy Format

Parity	Facility Code	Card ID	Parity
P	FFFFFFFF	CCCCCCCCCCCCCCCC	P

Start Parity Bit = 1 Bit (Even*)
Facility Code = 8 Bit
Card ID = 16 Bit**
Stop Parity Bit = 1 Bit (Odd*)

** **Note**: Start bit is determined by the first 13 bits and the Stop Parity Bit is determined by the last 13 bits.*

- **Disabled** - Set to disable when not using this feature. When disabled, pressing the F3 key will not display the PIN pad.

** **Note**: When Iris + Pin mode is currently in use, this option is not available (as the PIN mode is already active by default based on the Recognition mode usage).*

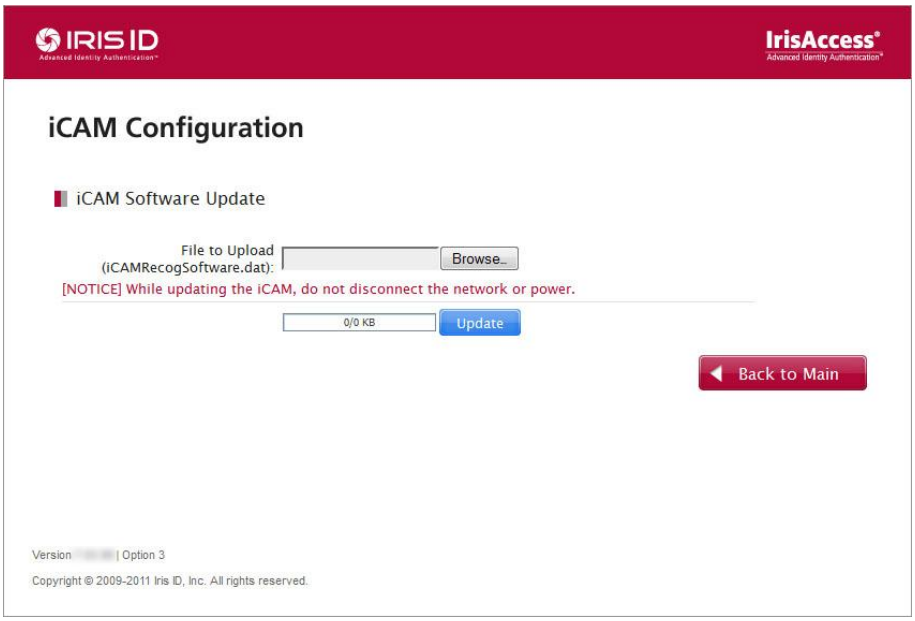
- **Facility Code** – When Galaxy Format is selected, the Facility Code value in this field will be output as part of the Galaxy formatted Wiegand Output. Enter the desired facility code between 0 ~254 as needed.
- **Pin Pad Sound Effect** – Enables or Disables a Pin Sound of an iCAM7100 model unit. This option can be set to either Enable or Disable. The pin sound option allows for a button press on the touch screen LCD to produce an audible sound. (This option is set to disable by default).
- **Pin Pad Color Change** - Selectable by radio button, enable this option to see a visual change to the key pressed on the PIN Pad.

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.

12.1.17 iCAM Software Update

iCAM software updates are generally performed automatically when used with the EAC application. However, from time to time, an iCAM software update may become available from Iris ID Systems, Inc. that may require a manual upgrade. Such updates may often be downloadable from the http://www.irisid.com website. Consult with your system integrator or Iris ID directly before attempting to perform any updates of this type. This section allows for you to update the camera unit with a compatible software update directly from the iCAM.

***Note**: Java VM must be installed on your computer in order to perform these procedures correctly.*



***Note**: Java VM must be installed on your computer in order to perform these procedures correctly.* Verify that Java VM is installed and working on your windows pc. (If Java VM is not installed, go to http://www.java.com/en/download/index.jsp for download and installation instruction.

Verify that Internet Options settings are set to *allow local directory path when uploading to a server*.

1. Open Internet Explorer
2. Go to the *tools* Menu> *Internet Options* > *Security* > *Custom Level* > *Miscellaneous* section > *Include local directory path when uploading files to a server* > Select *Enable* radio button > press *OK*.

Manually Upgrading iCAM Software:

WARNING! Do not disconnect the power or disturb the network connection during the upgrade process unless instructed to do so. If power or network is disconnected during file transfer, this could cause corruption in the iCAM OS and render the iCAM non-operational.

Download the file "iCAMRecogSoftware.dat"; make a new folder on the c: drive and place the file in that new folder.

Updating the iCAM Software:

- Log into the iCAM (web browser interface)
- From the main menu select *iCAM Software Update*
- Select *Browse*
- Select the path to the *"iCAMRecogSoftware.dat"* file
- Double click on the "Update" button. (Files will transfer and iCAM software will update, this may take several minutes)
- When complete a summary screen will display

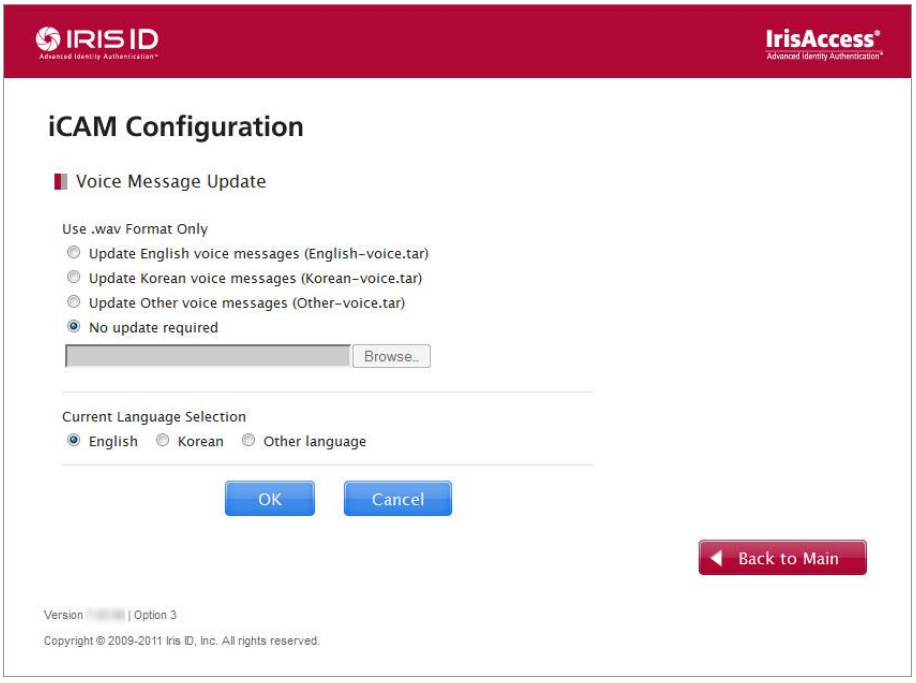
- Click Yes to reboot the iCAM
- Enter the username (iCAM7000) and password (iris7000)
- Click OK to reboot iCAM
- Wait 2 minutes for the reboot to completely.

Confirming the iCAM Software version:

- Log into the iCAM (web browser interface)
- From the main menu click on the arrow symbol next to the version number.
- This window will display the iCAM software and firmware versions.
- iCAM software version indicates a successful upgrade of the iCAM.

12.1.18 Voice Message Update

If the camera unit requires different voice messages then what was provided (default standard messages language announced in English), Korean language can be selected or other .WAV formatted messages can be uploaded using a .TAR format to the camera unit in this section.



Procedures to upload the voice files to your iCAM:

1. Place the 'Other-voice.tar' file on a computer that can be connected to the iCAM.
2. Log into the iCAM Configuration screen using 'iCAM7000' as the username and 'iris7000' as the password.
3. Select 'Voice Message Update'.
4. Select 'Update Other language messages (Other-voice.tar)'
5. Press the 'Browse' button to browse for the 'Other-voice.tar' file and select it for use.
6. Set the 'Current language selection' to 'Other language'.
7. Press 'OK'.

8. A message will display confirming the action success (or failure).
9. When the upload is complete, reboot the iCAM.

If you want to convert the voices back to English, log in to the iCAM's web interface and select Voice Message Update.
Select 'No Update required' and set Current language selection to English.
Press Ok.
Enter the server IP address, username 'anonymous' and password 'r'.
Press Ok.
When the authentication page comes up, enter 'iCAM7000' for username and 'iris7000' for password. This will reboot the iCAM with English voice files.

Here is the list of .wav files.
You must use these exact file names (These are case-sensitive) and place them in a folder named "Other-voice", then create a tar file of the entire folder. Name the tar file "Other-voice.tar". The wav files inside the tar file must have the path "Other-voice\"
The format of the sound files and translation are listed below.

Audio format: PCM 16 kHz, 16 bit, Stereo

16k_beepbeep.wav - (beeping sound)
16k_Capture.wav - (camera shutter sound)
16k_EnrollmentCommencement_B.wav - "Please present your card to the card reader."
16k_IDMessages_A.wav - "Thank You! You have been identified."
16k_IDMessages_C.wav - "Sorry. We can not confirm your identity."
16k_ImageAquisitionMessages_A.wav - "Please come a little closer to the camera."
16k_ImageAquisitionMessages_B.wav - "Please move back a little from the camera."
16k_ImageAquisitionMessages_G.wav - "Please center you eyes in the mirror."
16k_OpenEyes.wav - "Please open your eyes wide"
16k_Post_ImageAcquisitionMessagesA.wav - "We finish taking pictures of your eyes."
16k_smartcard.wav - (SmartCard accepted sound)
16k_TryAgain.wav - "Please try again."
16k_VerificationResultMessages_A.wav - "Thank You! Your identity has been verified."

Recording your Own Sound files to use as voice prompts:

You may create your own sound files using Windows Sound Recorder (Included with Microsoft Windows). By following the below procedure we had success in creating different sound files which we could then upload to the Optical Units. The biggest problem is keeping the file size small enough to use.

In Windows
Click Start -> Accessories -> Sound Recorder

Record your message

Click File -> Save As -> (Name the file)
Click File -> Properties
Select "Format Conversion"
Select "All Formats"
Click "Convert Now"

Choose
Format: PCM
Attributes: 16 kHz, 16 bit, Stereo

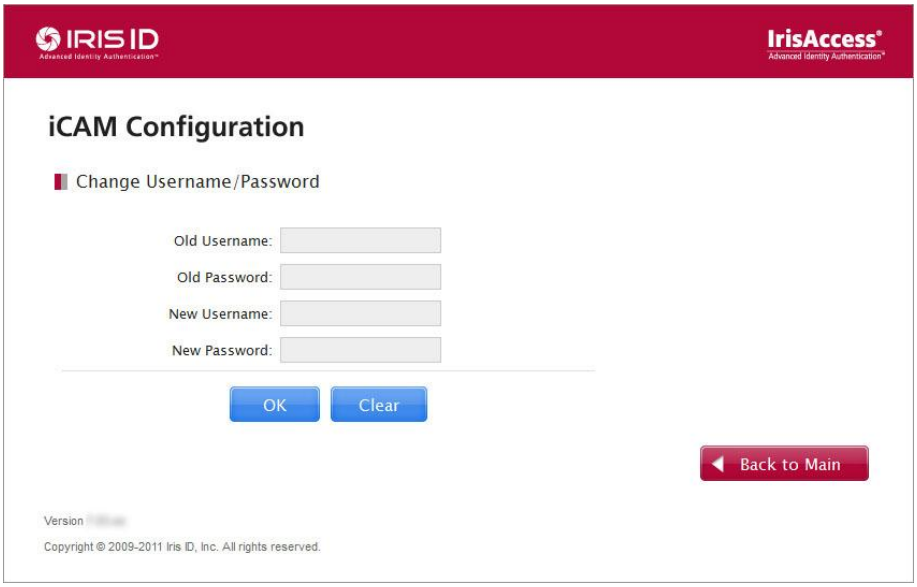
Click OK
Click OK
Click File -> Save

If the volume is too low, you may need a better quality microphone (this was a problem we had experienced), you may also increase the volume of the capture sound in Sound Recorder.

**Note: Sound files created must be packaged as a .tar file using a .tar compatible software of 1.15 or higher (standard). This file folder must be named "Other-voice.tar". In the event that an existing "Other-voice.tar" file has been created for an iCAM4000, it may be necessary to re-package the voice files into a new "Other-voice.tar" file folder using a utility/software (not provided by Iris ID) that conforms to 1.15 or higher standard .tar file creation.*

12.1.19 Change Username/Password

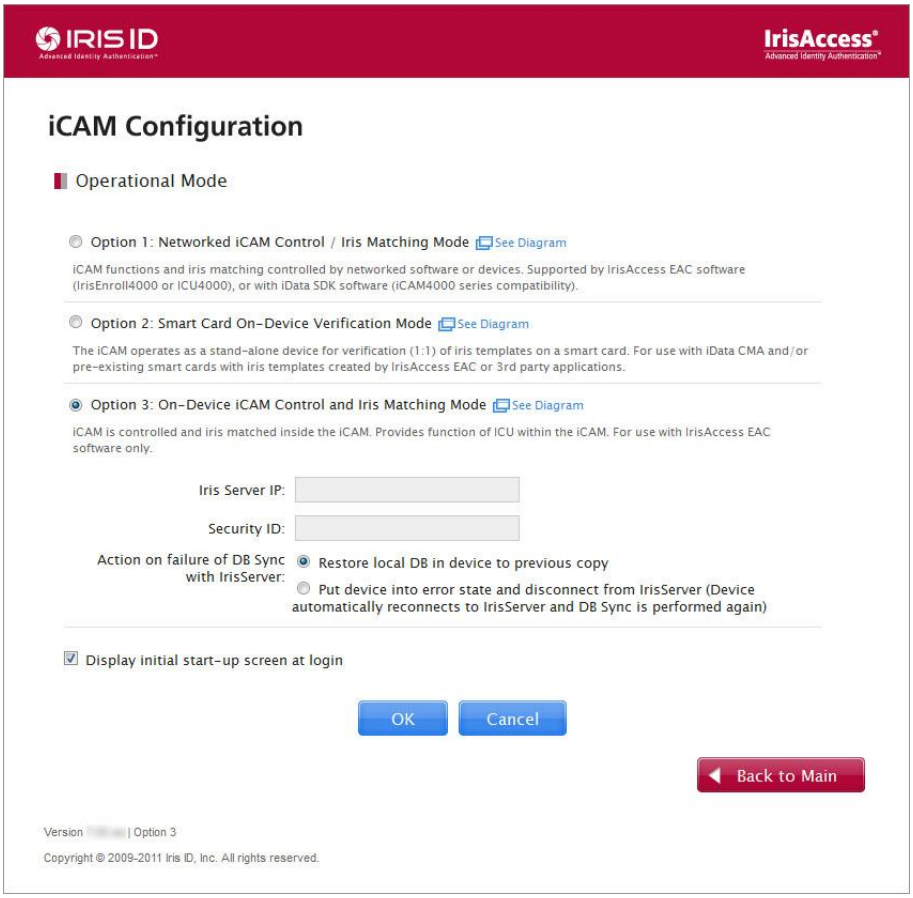
This menu provides the ability to change the Username and Password settings currently existing in the iCAM. In order to change the settings first the old user id and password must be entered in addition to the new user id and password credentials desired. Please note that all fields are case sensitive.



** **Note**: The iCAM FACTORY DEFAULT is located on the iCAM7000 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 (192.168.5.100) and the login ID credentials for the iCAM (User ID = iCAM7000 / Password = iris7000).*

12.1.20 Operational Mode

This screen allows for the iCAM to be set in either *iCAM7000 EAC Mode*, *iCAM7000 Stand-Alone Smart Card Verification mode, or On-Device iCAM Control and Iris Matching Mode.*



13. Login to the iCAM configuration screen as shown above (if not already logged in).
14. Select the Operational Mode option from the main screen.
15. Configure desired settings for the iCAM found in this screen. (See following data for details.)

- "**Option 1: Networked iCAM Control / Iris Matching Mode**" – When option 1 is selected, the iCAM will operate as part of an IrisAccess™ Entry Access Control System, or for use with iData™ SDK (iCAM4000 Series compatibility). The iCAM functions and iris matching are controlled by networked software or devices.
  IMPORTANT: If you are generally using option 3, this "option 1" mode may be needed to be used when performing enrollment.

- "**Option 2: Smart Card On-Device Verification Mode**" - When option 2 is selected, the iCAM7000 operates as a stand-alone device for verification (1:1) of the iris templates on a smart card. This mode is generally for use with iData CMA and/or pre-existing smart cards with iris templates created by IrisAccess EAC or compatible 3rd party applications.
  ****Note**: "iCAM7000 Stand-Alone Smart Card Verification Mode" can only be used when a card reader (internal or external) is used with the iCAM7000 series unit.*

- "**Option 3: On Device iCAM Control and Iris Matching Mode**" – When option 3 is selected, the iCAM is controlled and iris matched inside the iCAM. This mode provides the function of an ICU within the iCAM. This mode provides the function of an ICU within the iCAM. This option is designed for use with compatible IrisAccess EAC software.

  ***Note**: If attempting to use an iCAM7000 series unit in operational mode "Option 3", compatible IrisAccess EAC software MUST be used for functionality of this option.*

  ***IMPORTANT**: If you are using an iCAM7000 in "Option 3" operational mode – when performing enrollments, and when trying to connect to the IrisEnrol4000 application within IrisAccess EAC software, the user must switch the operational mode to "option 1". Once enrollments have completed, the iCAM can be set back to operational mode "option 3" (if a dedicated iCAM is not being used for enrollment).*

In option 3 mode –the iCAM is controlled and iris matched inside the iCAM while providing function of an ICU within the iCAM. In order for these processes to work correctly the below information is required to be provided when "Option 3" is selected:

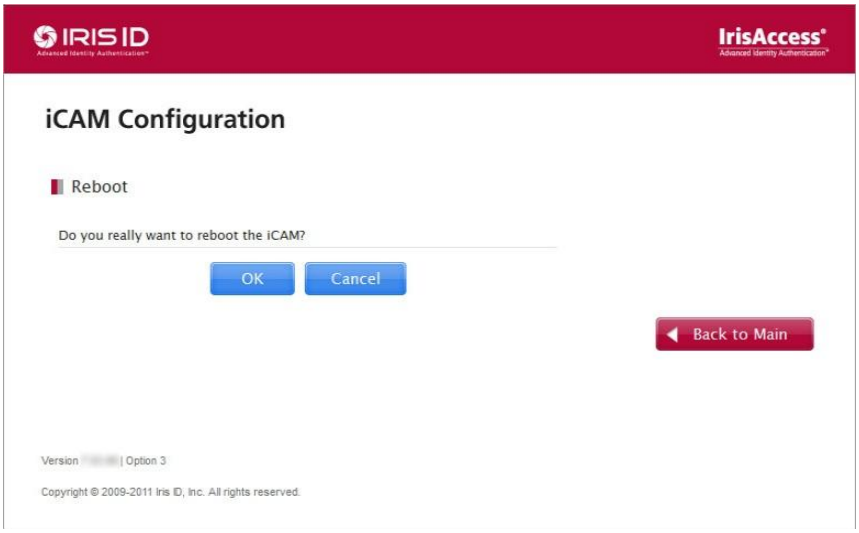
d. **IrisServer IP** - Enter the Iris Server IP address
e. **Security ID** - Enter a unique security ID for this unit (16 character requirement).
f. Action on Failure of DB Sync with IrisServer - Select the radio button desired for Action on failure of DB Sync with IrisServer. These options are:

   - **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).**

16. Display Initial Start-up screen at login – This checkbox can be selected to enable or unchecked to disable the initial start-up screen from appearing when the iCAM Configuration is logged into.

12.1.21 Reboot/Authentication

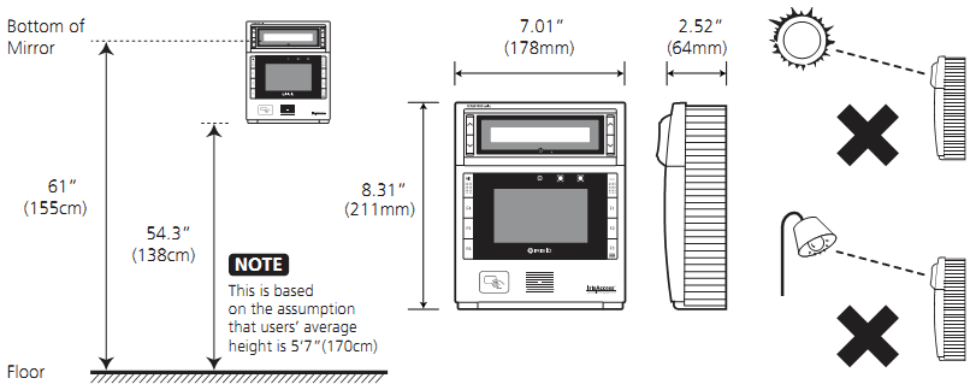
This screen allows for a reboot of the iCAM unit. Once pressed, the iCAM will prompt for an authentication of the specific User ID and Password of the camera unit. When entered correctly the unit with reboot once the okay button is selected. (Please wait for this process to complete as this may take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


IRIS ID
IrisAccess
iCAM Configuration
Reboot
Do you really want to reboot the iCAM?
OK
Cancel
Back to Main
Version | Option 3
Copyright © 2009-2011 Iris ID, Inc. All rights reserved.

13. Installation Guidelines

Before installing your iCAM7000 camera unit, review the recommended installation guidelines. These guidelines provide information on the recommended mounting information, general wiring information, and electrical/current requirements.

13.1 Recommended Mounting Information



- The recommended mounting height for the iCAM7000 Series are 138cm (54.3inches) 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 which may result in an increased "failure to acquire" rate.
- The iCAM was designed for indoor use only. This device is not weatherproof and must not be exposed to precipitation or extreme temperatures. If it is required to use this product in an outdoor or extreme environment, a 3rd Party enclosure may be used to protect the unit from exposure to dust, moisture, and extreme temperatures. See www.irisid.com - Support & Service for more information. Installation in an extreme environment without proper protection may cause permanent damage and void your warranty.

13.2 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 the iCAM and a computer, 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 iCAM unit (with iCAM connected). A 3rd-party power supply is required to power each iCAM on the system.

  ***Note:** The package of the iCAM7000 Series camera does not include a power supply, however for short distance installations (ex. Enrollment Station, Kiosk, ATM, etc.) a 12VDC power supply is available through Iris ID (Part number *iCAM7-PWR*). This external power supply is a "brick" style with an attached 1.52 meter (5 foot) low voltage cable. Any modification to the Iris ID power supply is not recommended.

  - Power Requirements at the iCAM:
    - Voltages between 12 VDC to 24 VDC (+/- 10%) measured at the iCAM (with iCAM connected)
    - Current of 2 AMPS @ 12VDC or 1 AMP @ 24VDC measured at the iCAM (with iCAM connected) – 24 Watts of power supplied to iCAM.
    - It is recommended that each iCAM is supplied power from the power source (Do not "daisy chain" the power from iCAM to iCAM.)

  - Wiring between the Power Supply and the iCAM:
    - 16 AWG (1.31mm^2) Stranded Copper Wire or better.

    ***DISCLAIMER:** The wire distances and voltage drop calculations shown here are for general reference only and is not intended as a guarantee that an installation per these calculations will assure proper operation of the iCAM. It is the responsibility of the installer or system architect to provide their own calculation of voltage drop with all installation considerations to assure that the proper voltage and amperage is applied to each iCAM.

    ****DISCLAIMER REFERENCE:** Change in wire gauge or material will affect the voltage drop calculation shown below. 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 iCAM7000 Series 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 iCAM.

    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 iCAM:
    - *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 .33mm^2) Solid Copper – Twisted Pair Wire or better.
        - 4 Conductors (RxD -, RxD +, TxD -, TxD +).
        - Maximum Length: 304 Meters (1000 Feet).
    - *GPI wiring:*
        - 16 AWG (1.31mm^2) Stranded Copper Wire or better.
        - 2 Conductors (Input, Ground).
        - Maximum Length: 60 Meters (190 Feet).
    - *RS232 (External Smart Card Reader) wiring:*
        - 22 AWG (0 .33mm^2) Solid Copper – Twisted Pair Wire or better.
        - 4 Conductors (Power-12VDC, RxD, TxD, Ground).
        - Maximum Length: 7.6 Meters (25 Feet).
    - *External Speaker*
        - 22 AWG (0 .33mm^2) 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).

iCAM7000 & 7100 Series Hardware Installation
The iCAM7000 series unit can be fitted to a surface mount (available out-of-the-box), recess mount (with optional recess mounting kit), or optional desktop stand.

13.3 iCAM7000 & 7100 Series Mounting & Stand Solutions

Surface Mounting

The iCAM can be surface mounted with standard equipment provided with the contents of your unit. Review the following procedure for instruction on how to surface mount your iCAM7000/7100 series camera unit.

1. Open each cap at both sides of unit, and loosen the captive screws (with included L wrench) to release the interface panel.
2. After opening the interface panel, loosen the screw. Unscrew the installation plate screw to separate from the installation plate.
3. Separate the installation plate by sliding the plate downward.
4. Place the installation plate on the desired wall and screw into wall. Feed any needed wiring through the installation plate hole (i.e.: Power, Ethernet, etc). Attach the installation plate to the wall surface using the appropriate fastener (recommended #10 screws) and anchors for the wall material. Another option is to mount and fasten the installation plate to a previously installed electrical gang box.
5. Slide the iCAM7000 series camera unit into the installation plate and fasten the installation plate with a screw.
6. Remove protective film from RTC battery.
7. Before wiring unit, confirm the power is in the off position. Route and connect the Power and Ethernet wires to iCAM7000 series.

   ***NOTE**: If connecting any other wiring such as Wiegand, GPI/O to the iCAM, review the following section "Wire Connection Details" before closing interface panel and fastening screws.*

8. Turn on power source and switch the power switch of the iCAM7000 series unit to the ON position.
9. After wiring the unit and switching it to the ON position, close the interface panel and fasten the screws (with screw caps placed back into closed position).

Recess Mounting (optional)

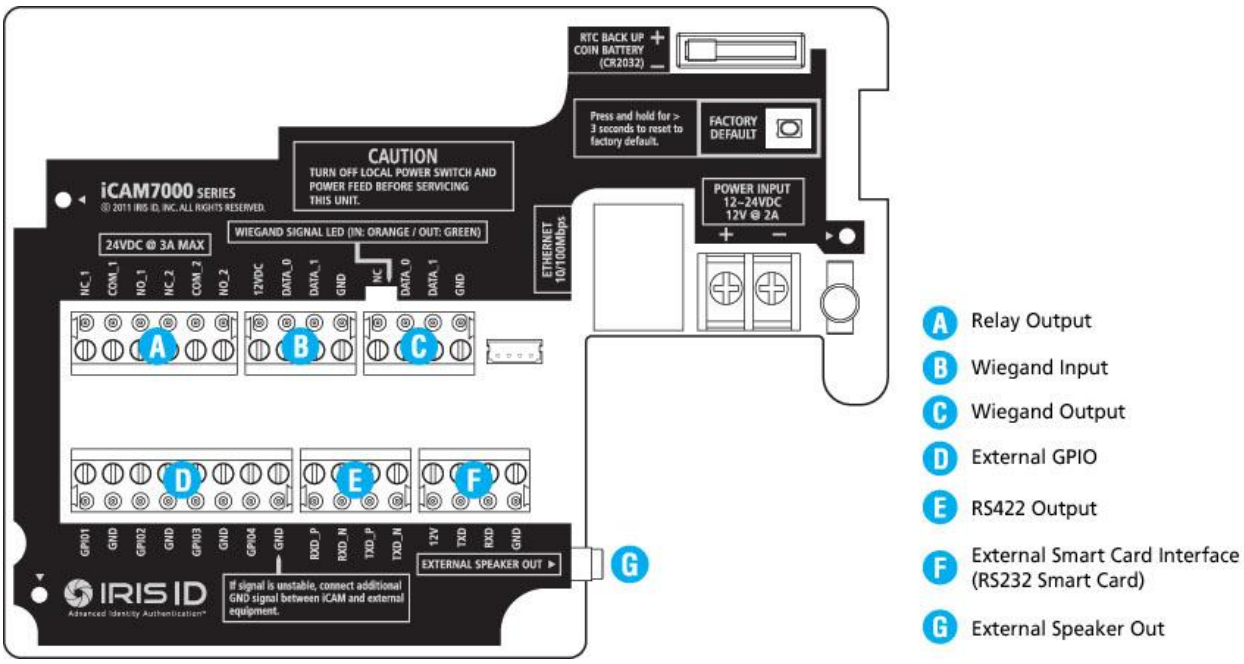
The iCAM can be used with an optional recess mount kit. The Recess mount kit is compatible with both the iCAM7000 and iCAM7100 model camera units. Contact Iris ID for details on purchasing and availability.

Desktop Stand Kit (optional)

The iCAM can be used with an optional desktop stand kit. The desktop stand allows the iCAM7000 Series to sit on a level surface and an incline for usage without the need for mounting. The Desktop Stand kit is compatible with both the iCAM7000 and iCAM7100 model camera units. Contact Iris ID for details on purchasing and availability.

14. Connection Details for Wiring iCAM7000 Series (iCAM7000/7100)

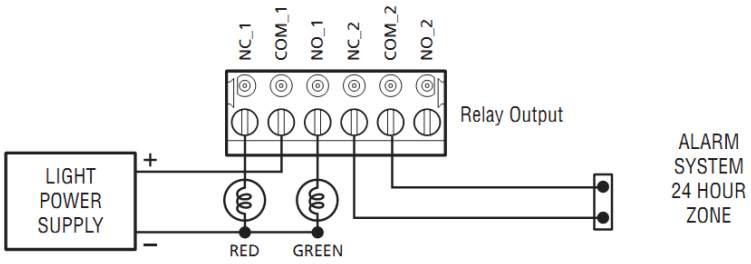
The iCAM7000 Camera units contain six connectors located on the interior of the unit. These connectors are surrounded by a wiring legend guide (black with white writing). This legend guide provides specific details for connection details for each connector. Below Each connector (when the connector is removed) displays the function for the connector port. The six connector parts are for relay input, Wiegand input, Wiegand output, external GPI/O, RS422 Output, External Smart Card Interface (RS232 Smart Card), 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.

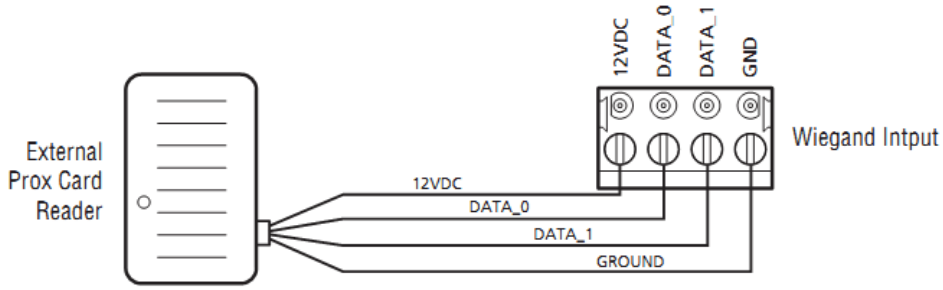
14.1 Relay Output

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 typically used to indicate iCAM tamper. 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.



14.2 Wiegand Input

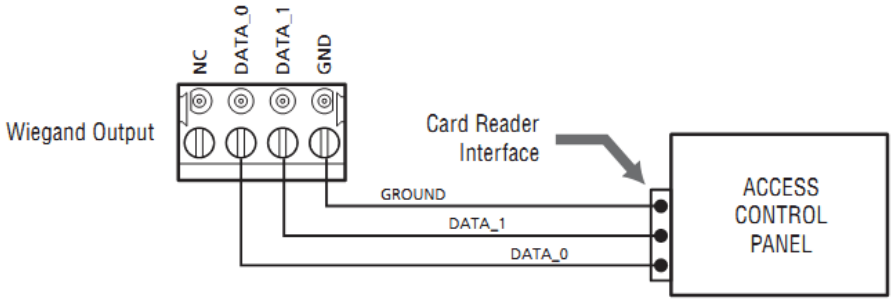
Wiegand input is available on the iCAM for connection from 3rd party proximity card readers. This connection can provide 12VDC and a maximum 500mA current to a proximity card reader.



14.3 Wiegand Output

The Wiegand Output from the iCAM7000 series camera 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:

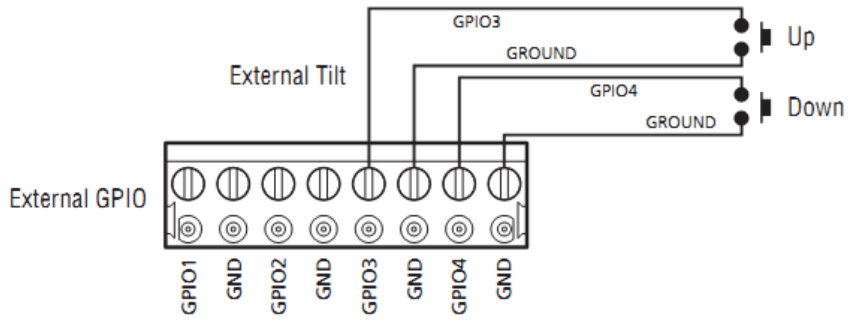
- Wiegand output uses 3 wire interface (Data0, Data1, and Ground),
- Maximum wire length from iCAM to Access Control Panel is 500feet (152m).



14.4 External GPI/O

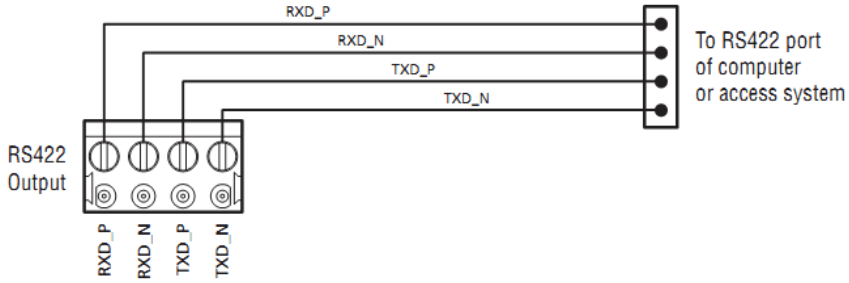
GPIO3 and 4 can be used to control the tilt position of the tilt unit of an iCAM7000. Use GPIO3 and GND for up tilting. Use GPIO4 and GND for down tilting.
GPIO Specifications:

- For output, the GPIO can provide 5VDC @ 20mA.
- For Input, the GPIO is selectable between active High & active Low.
- Assignment of GPIO is handled through Software.



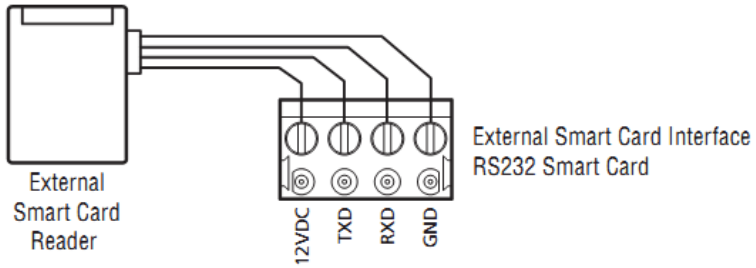
14.5 RS422 Output

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.



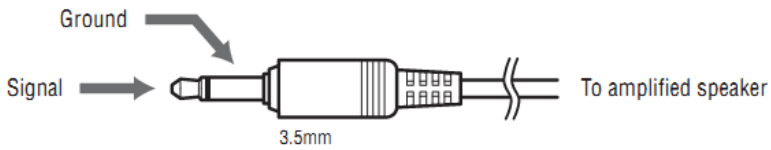
14.6 External Smart Card Interface (RS232 Smart Card)

Allows connection of internally (ex. HID OEM150) and externally installed smart card readers which utilize serial (RS232) communications. This connection can provide 12VDC and a maximum of 500mA current to a smart card reader.



14.7 External Speaker Out

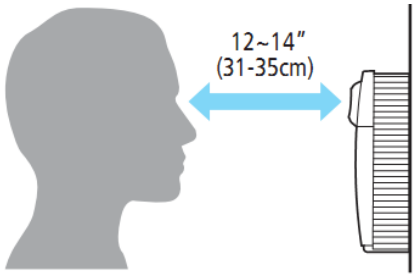
The External Speaker Out allows for a connection of an external amplified speaker. This port provides mono (single channel) audio of voice prompts and other unit sounds. Both the internal and external speakers can operate concurrently.



15. How to Operate iCAM7000 Series Camera Unit (iCAM7000/7100)

Operating the iCAM7000 Camera unit is very intuitive. This section covers operation usage, tilting angles and distance for general use, how to enroll a user, and identification at a remote iCAM7000 series camera unit.

15.1 Operation Range

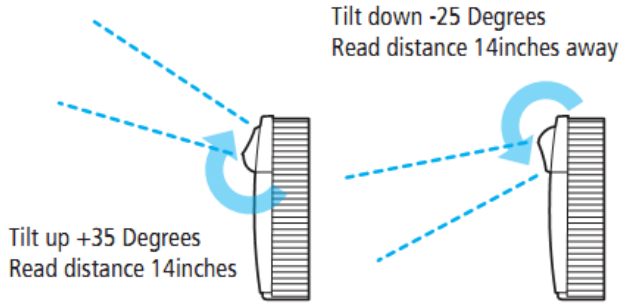


- iCAM activates when user approaches or when card is presented.
- Picture capture range is 12~14 inches (31-35cm) away.
- Self or auto/set height adjustment.
- Placing dot over the bridge of the nose easily helps alignment.
- Orange dot turns to green dot when user is at correct distance. (Green dot = In Range / Orange dot = Out of range.)
- Visual indication is amplified with friendly audio prompts.
- Right and left irides are acquired.
- A face picture can also be captured.

15.2 The Angles and Distance for General Use

The on-unit up/down tilt buttons can be used to adjust the tilt angle; or an external mounted switch can be wired to control up/down tilt via GPI.

- Tilt up +35 Degrees. Read distance 14inches.
- Tilt down -25 Degrees. Read distance 14inches away.

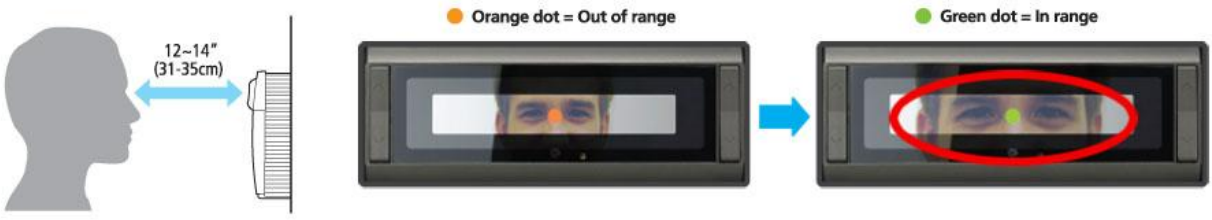


15.3 How to Enroll a User

The IrisEnroll4000 application (part of the iData EAC software suite) provides the capability to perform iris enrollment and recognition. An intuitive user interface with visual and audible prompts enables users to quickly enroll and verify using the Iris ID IrisAccess iCAM7000 series of camera units. When it comes to accurate and fast authentication, the IrisAccess solution is extraordinarily flexible and extremely accurate. It is recommended that the iCAM7000 Series camera unit is in operation mode "option 1" in order to allow the iCAM to get connected to the Enrollment application.
*NOTE: iCAM7000 Series camera units cannot connect to an enrollment application such as IrisEnroll4000 when in operational mode "option 3". To switch operational modes of the iCAM7000 Series camera unit, access the iCAM Configuration interface from an internet browser. For details on how to access and modify the Operational mode of an iCAM7000 Series camera unit – view the "Using the iCAM Configuration Interface sections of this document".

Please review the diagram below to understand the user interface before attempting to use the iCAM4000. When the iCAM is operational the colored dots will help with positioning.

- Look at and align eyes in the mirror from 10-14 inches away as pictured below.
- Align eyes so that the colored dot is on the bridge of the nose, between eyes.



- iCAM activates when user approaches or when card is presented.
- Picture capture range is 12~14 inches (31-35cm) away.
- Self or auto/set height adjustment.
- Placing dot over the bridge of nose, easily helps alignment.
- Orange turns to green when user is at correct distance.
- Visual indication is amplified with friendly audio prompts.
- Right and left irides are acquired.
- A face picture can also be captured.

**Note: Additional guides and instructions on how to properly enroll people and use the iCAM7000 are available in the "IrisAccess EAC User Manual".*

Enrollment Tips:

- Explain the use of the iris camera and positioning before attempting to use.

  a) Align eyes 10-14 inches away from camera.

  b) Position both eyes so they are visible in the mirror.

  c) Position both eyes so that the Orange or Green Dot is in between eyes.

  d) Open eyes wide for enrollment so good pictures are taken.

  e) When the Green Dot is visible then the user is in the correct position.

  f) Listen to iCAM voice tips from the camera. "Move closer" or "Move further back"

15.4 Identification at Remote Units (controlled by something other than an enrollment application)

When an iCAM7000 series camera will be used as a remote unit, it is required that something is properly controlling the iCAM7000 series unit in order for the device to function correctly. The iCAM7000 series camera must be controlled by something other than the IrisEnroll4000 application from the EAC application suite.

If the iCAM7000 Series unit is being controlled by the IrisEnroll4000 application, (or a proprietary enrollment application) the same iCAM7000 series device cannot be used for remote unit identification. This is because the iCAM7000 cannot be controlled by 2 processes at the same time.

Identification/Verification per Operational Mode:

Option 1

The iCAM7000 Series camera unit when used in *"option 1"* operation mode should be controlled by an ICU4000R in order to function as a remote unit when using IrisAccess iData EAC software. In the event that IrisAccess iData software is not used, the iCAM7000 series unit can function and perform iris matching by other network software or devices such as iData SDK software (iCAM4000 Series compatible).

Option 2

The iCAM7000 Series camera unit when used in *"option 2"* operational mode does not require any additional controller. This mode is designed to function as a stand-alone device for use with

verification (1:1) of iris templates on a Smart Card. This option requires that the iCAM be used in conjunction with a compatible Smart Card reader and iData CMA software (or pre-existing Smart Cards with iris Access EAC or 3rd party applications).

Option 3

The iCAM7000 Series camera unit when used in *"option 3"* operational mode can be setup to be controlled and iris matched inside the iCAM. This option provides the function of an ICU within the iCAM. This operational mode is only available with the use of IrisAccess iData EAC software.

16. Three Factor Authentication and PIN Only Options

To perform 3 factor authentication, the iCAM series hardware and Iris ID EAC enrollment/configuration software **must** be used in conjunction with a (PACS) third party access control/authentication panel. The PACS panel must support "Card + PIN" mode and accept a Wiegand input. (Please review the PACS manufacturer's documentation.)

To perform 2 factor authentication, various iCAM models with Iris ID EAC software can output a single wiegand output based on successful Card+Iris or Pin+Iris combinations. (The resulting wiegand output can be sent to a third party PACS system.)

a) Single Reader Solution – 3 Factor Authentication.
The iCAM7111 model iCAM with built in card reader and built in keypad can be configured to authenticate an individual using CARD + IRIS + PIN provided the cards used can be read by the optional HID readers available inside the iCAM and the PACs panel can interpret the "8 bit burst PIN Mode" commonly referred to as the "Dorado mode". (Please review the PACS manufacturer's documentation.)

b) Two Reader Solutions – 3 Factor Authentication.
The iCAM7xxx models can be combined with third party card readers and/or combination keypads to provide a 3 factor authentication solution when used in conjunction with a third party access control panel. The third party (PACS) must be configurable to receive and compare 1-2 inputs from different readers before granting access. (Please review the PACS manufacturer's documentation.)

16.1 General Information for Three Factor Authentication

When the 3rd party PACS system is configured properly in (card + pin) mode, it can be set to "wait" for a PIN after a card number is received. The number of Pin digits is decided by the PACS system, thus Iris ID refers to this as "PACS Pin" mode. The successful 2 factor authentication of Card + Iris generates one wiegand output to the PACs system and the successful PIN output generates the 3rd factor of authentication from the iCAM7111.

Operation: After Card + Iris is completed on iCAM 7111 the user presses the keypad (F3) on the iCAM. When the keypad function it set to "8 bit burst" mode each key press will output the corresponding number to the PACS panel via Wiegand protocol.

The following information provides detail for configuring operational modes: Option 1 and Option 3. Determine the model of operation the iCAM71xx series will be used, and follow the appropriate setup process.

16.2 iCAM7100 Series 3 Factor Setup Procedure

- **Operational Mode - Option 1 Setup Procedure:**

  Follow these steps for general setup of iCAM7100 setup with 3 factor usage when in operational mode – *Option 1*.

  1. Open the option 1 iCAM Configuration settings screen.
  2. Set the ICU4000 channel that is controlling the iCAM7100 series camera unit:
     a. Set recognition mode to: *iCAM + Card (smartcard or Prox card).*
     b. Set External Hardware interface to: *iCAM*
     c. Select Ok and apply/send changes to the ICU - reboot as needed.
  3. Go to "Function Key & LCD Settings (7100 only). Under the iCAM Settings Menu select "8 bit burst" and press OK. Reboot as needed.
  4. Using a PACS panel that is capable of supporting 2 factor (Card ID + PIN), set a Pin for the user ID that is to be used (like that of an HID RK400 card reader).
  5. Verify that Wiegand output is correctly setup directly out of the iCAM to the PACS. Make sure that Data 0, Data 1, and Ground connections have been made.

- **Operational Mode - Option 3 Setup Procedure:**

  Follow these steps for general setup of iCAM7100 setup with 3 factor usage when in operational mode – *Option 3*.

  1. Open the option 3 iCAM Configuration settings screen.
  2. Set the iCAM7100 series camera unit recognition mode to to iCAM + Card (smartcard or Prox card). Select Ok and reboot as needed.
  3. Go to "Function Key & LCD Settings (7100 only). Under the PIN Pad Settings select "8 bit burst" and press OK. Reboot as needed.
  4. Using a PACS panel that is capable of supporting 2 factor (Card ID + PIN), set a Pin for the user's credential or card number that is to be used (like that of an HID RK400 card reader).
  5. Verify that Wiegand output is correctly setup directly out of the iCAM to the PACS. Make sure that Data 0, Data 1, and Ground connections have been made.

- **Three Factor Usage:**

  After successfully setting up the system to allow for three factor authentication, the camera can be used to function in 3 factor as needed. View the following usage process to determine the proper usage method.

  1. Enroll user in IrisAccess EAC system with a card
  a. Make sure that the Card ID field is filled in – as this is that number that is output to the PACS through the Wiegand output of the iCAM. (Wiegand Bypass)
  2. Present card to the iCAM card reader at the door
  3. Once card is read, present your eyes to the iCAM when prompted
  4. Once identity has been verified, press the F3 Function button on the iCAM (lower right button) to initiate the pin-pad to be opened on the iCAM7100 series LCD display.
     a. Enter the pin digits for the user as configured in the PACs system. (In 8 Bit Burst mode each key press will send data to the panel. In Galaxy format the enter button will need to be pressed to send all digits to the panel.

Note: The following is the responsibility of installers and the 3rd party Access Control Panel System hardware (PACS):

16.3 PIN Only Mode

Many PACS system panels can have a card reader port set to Pin or Card. If the system can accept Pin only as an authentication method, the keypad on the iCAM71x1 can be used to send digits to the PACS system. Since most PACS systems can accept a one time, or limited use PIN it is a convenient feature to allow access to users which are not enrolled into the iris biometric system. This does reduce the security required to gain access. (Please review your 3rd party PACS manufacturer's documentation.)

The following chart may be helpful in assessing the options available and necessary components required. Please consult with the manufacturer's documentation for more detail.

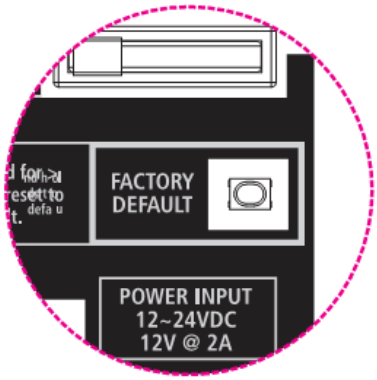
Components:	3 Factor / 2 Factor Authentication with 3rd Party PACS			2 Factor Authentication with IrisID EAC only	
Iris Enrollment / Configuration Software	IrisID EAC SW			IrisID EAC SW	
PACS: Access Authorization Software	3rd Party PACS: with available (Card + Pin) mode*			IrisID EAC SW	
Method	***A***	***B***	***C***	***D***	***E***
Authentication Mode	(Card + Iris + Pin)			(Card +Iris)	(Pin + Iris)
Iris Reader	iCAM7111	iCAM7101	iCAM7010	iCAM7xxx	iCAM7xxx
3rd Party Card or Pin Reader	NA	Card Reader	Pin Reader	Optional **	Optional **

*Please review the PACS manufacturer's documentation for details and support.

**Optional: Depends on iCAM model chosen which may include built in card reader and/or pin reader.

17. Restoring the Unit to Factory Default

The Factory Default can be used to restore settings of an iCAM7000 series camera 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.



17.1 IP Address Default

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

Note:
Default IP Address = 192.168.5.100, Subnet Mask = 255.255.255.0, Gateway = 192.168.5.254
Default User ID / Password = User ID: iCAM7000 / Password = iris7000

Hold the factory default button down for at least 3 seconds while the unit is already powered-on to reset the unit IP address information back to the default settings.

17.2 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 iCAM7000 series unit, hold the factory default button down for at least 5 seconds to restore the entire unit back to all factory default settings.

18. Fuse Replacement

The iCAM7000 series camera unit(s) contains a replaceable fuse which protects the unit(s) from excessive current consumption. In the event that the iCAM7000 series unit(s) 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 iCAM7000 Series camera unit. Contact IRIS ID Systems, Inc. for assistance with acquiring additional fuse parts as needed.

18.1 Fuse Specifications

Manufacturer: Littlefuse

Part No.: 0451 004. MRL

Ampere Rating: 4A

18.2 How to Test and Replace the Fuse

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

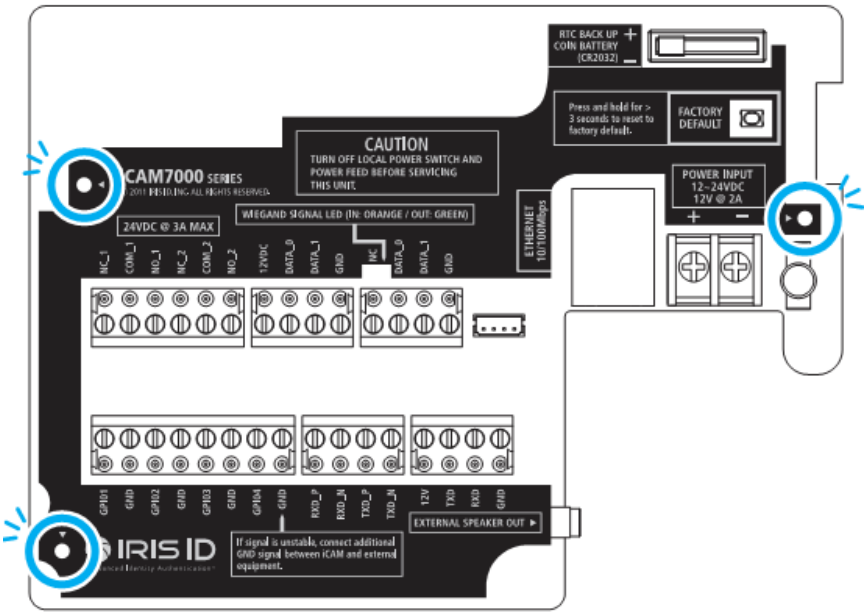
Before replacing the fuse, it is recommended to test the fuse and determine whether the fuse is actually faulty.

How to Test the Fuse:

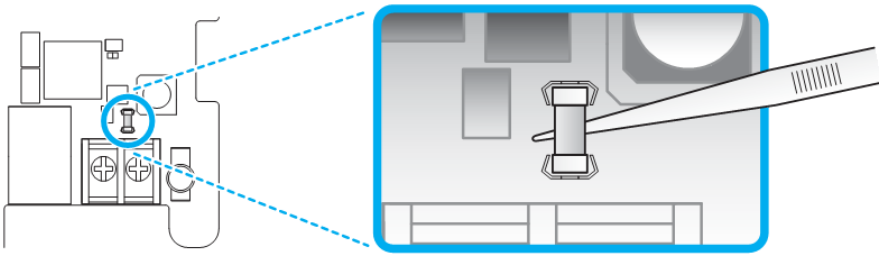
The fuse can be tested by checking the continuity across both sides of fuse with a multi-meter. If no continuity is measured, the fuse must be replaced.

How to Replace the Fuse:

1. Turn the unit to the OFF (down) position using the ON/OFF Switch.
2. Disconnect power from the unit.
3. Remove the screws to release the Wiring Legend Guide.



4. Use tweezers, and replace the Fuse.



19. Troubleshooting

The iCAM7000 camera unit series has many features and functions of operation. This section provides information on common misconceptions about the product and usage, and frequently asked questions.

19.1 Frequently Asked Questions (FAQs)

Q: Does the iCAM7000 Series require software to properly use the camera unit?

A: Yes. The iCAM7000 Series camera unit requires the use of software. Whether using IrisAccess EAC, iData CMA, or a version of SDK, the iCAM7000 Series units are designed to work in conjunction with software.

Q: Does the iCAM7000 Series provide native 3 factor modality out of the box?

A: The iCAM allows for the ability of Iris + Pin (local), or Iris + Card (Smart card or Prox Card) which are native to an iCAM7100 unit. As a result, 2 factors are available when one thinks of the Iris ID IrisAccess EAC software as a component. However, with the use of a PACS (Physical Access Control Systems) , three factor authentication is possible.

Recognize the iCAM7100 PACS "8 bit burst PIN Mode" is an emulation of what is commonly referred to as "Dorado" mode for commonly available card readers (Ex: HID card readers with a keypad) .

Most PACS systems support Card + Pin as an authentication mode. Recall iCAM can deliver two factors with the standard Iris Access System software configuration (ex: Card + Iris).

Now let's consider the use case for three factor authentication. After successful Card + Iris authentication (2-factor) on the 7100 device itself, the card number is output on the Wiegand output of the iCAM 7100. When the PACS system is configured properly (card + pin) it can be set to "wait" for a PIN after a card number is presented. Keep in mind the number of Pin digits is decided by the PACS system, and not the Iris Access System; hence Iris ID refers to this as PACS Pin mode. Operation: After Card + Iris is completed on iCAM 7100 the user calls up the keypad (F3) on the iCAM 7100. When the keypad function it set to 8 bit burst mode each key press with output the corresponding number to the PACS panel.

Alternately many PACS system panels can have a card reader port set to Pin or Card. If the system accepts Pin only as an authentication method, the iCAM 7100 keypad can be used at any time to gain access through the PACS system. Since most PACS systems can accept a one time, or limited use PIN it is a convenient feature to allow access to users which are not enrolled into the Iris biometric system.

Q: Does every iCAM7000 Series camera unit come with a standard LCD display?

A: No. Two lines of iCAM7000 Series camera units are available. The iCAM7000 and iCAM7100 models are both available for purchase. Although the iCAM7000 does not contain an LCD display, Pop-up LCD Pin Pad, or Function Keys, the iCAM7100 model comes standard with such options.

Q: Does the iCAM7000 Series camera unit require a network/LAN connection?

A: Generally Yes. For initial setup a LAN connection is required regardless of Operational Mode option that will be used. Our device requires a physical network connection when in Operational Modes 1, and 3. However, after setup of Operational Mode 2, the iCAM does not require connection to a network.

Q: Is the iCAM7000 Series a compatible replacement to an iCAM4000/iCAM4100?

A: Yes. The iCAM7000 Series camera units can function as if it is an iCAM4000 unit. Consult your authorized IRIS ID reseller for additional information and details on compatibility.

Q: Can the iCAM7000 Series camera unit use legacy software such as EAC software 3.00.14 or below?

A: No. The iCAM7000 series camera units (operational modes 1 and 2) can work with IrisAccess EAC software version 3.01.35 P1 or higher. Additionally, the iCAM7000 series camera units that are going to use operational mode 3 will require the IrisAccess EAC software version that matches compatible EAC software available with Operational Mode Option 3. (For example: If using EAC software version 3.05.02 P1, the compatible software version of iCAM Software in Option 3 must be 7.05.02 P1).
**Note: When using Operational mode "option 3", the EAC version must be a compatible match the iCAM software version. (For example: If using EAC software version 3.05.02 P1, the compatible software version of iCAM Software in Option 3 must be 7.05.02 P1).*

Q: Is the iCAM7000 Series camera unit weather and/or water-resistant?

A: No. Our products are NOT weather resistant or water-proof. As a result, it is recommended that the iCAM7000 series camera unit be used for indoor use for best results and hardware longevity. However, if exterior use is required, our products can be used with a 3rd party enclosure for weather-resistance. Contact an IRIS ID authorized reseller for additional information.

Q: Does the iCAM7000 series camera unit come with a power supply?

A: No. The package of the iCAM7000 Series camera does not include a power supply, however for short distance installations (ex. Enrollment Station, Kiosk, ATM, etc.) a 12VDC power supply is available through Iris ID (Part number *iCAM7-PWR*). This external power supply is a "brick" style with an attached 1.52 meter (5 foot) low voltage cable. Any modification to the Iris ID power supply is not recommended. To purchase a power supply directly from IRIS ID, please contact an IRIS ID authorized reseller for additional information.

For building installations, a 3rd party power supply is recommended to power each iCAM on the system. Please note power requirements found in the "General Wiring and Electrical/Power Requirements" section of this document.

Q: Does the iCAM7000 series require a Windows XP (or above) computer to perform setup and installation?

A: Yes. A computer running Windows XP or higher operating system is required for installation.

Q: Does the iCAM7000 series come with a CCTV module out of the box?

A: No. At this time, the iCAM7000 Series camera unit has an opening where a 3rd party CCTV camera module can be placed. However, IRIS ID does not *currently* provide such a module for our product. Please contact an IRIS ID authorized reseller for additional information.

Q: What are the differences between an iCAM7000 and the iCAM7100 models?

A: Some differences do exist between an iCAM7000 series and iCAM7100 models. An iCAM7100 model camera unit contains a different front panel – The 7100 model front panel includes a touch LCD Display, Pop-Up Pin Pad, and 6 function keys. However, both the iCAM7000 models and iCAM7100 models can be ordered with an internal card reader.

Q: When I plug in my iCAM, why is it not powering on?

A: If your iCAM is not powering on, verify the following:

a. Verify that the correct power is being supplied to the unit. The recommended power requirements are: 12-24VDC +/- 10% / Minimum 24W (12VDC @ 2AMPS). The use of a stable power supply and proper gauge wire is required.
b. Verify that the Positive and negative connectors are correctly positioned and fastened to the screw down connections of the iCAM power connection.
c. Confirm that the On/Off Switch is placed to the ON position (UP).
d. Verify that the fuse is not blown in the iCAM unit. The fuse can be tested by checking the continuity across both sides of the fuse with a multi-meter.

***Note:** One additional replacement fuse is included with the iCAM7000 series located on the back of the Wiring Legend Guide.*

Q: How do I determine the IP address of an iCAM7000 Series camera unit?

A: An iCAM7000 series camera unit can audibly announce the IP address (if the setting from iCAM configuration is not disabled). To hear the IP address of the iCAM, press any of the tilt buttons for ~10 seconds.

Q: What are the differences between an iCAM4000 Series unit and an iCAM7000 Series unit?

A: View the following chart for differences, similarities and specifications for each of the iCAM models:

Features	 iCAM4000 Models	 iCAM7100 Models	 iCAM7000 Models
Dimensions	8.6"x6.5"x3.2"	7.01" x 8.31" x 2.52"	7.01" x 8.31" x 2.52"
Weight	4.4 lbs.	3.5lbs	3.5lbs
Power Input	12 VDC @2A	12~24 VDC, @2A	12~24 VDC, @2A
Voice Indication	English standard, others available	English standard, others available	English standard, others available
Iris Capture Range	10.2" ~ 14.2"	12" ~ 14"	12" ~ 14"
User Input	X	6 definable function keys	X
Touch Screen LCD	X	4.3" (iCAM7100 models)	X
Pin Pad	External Only	Pop-up on screen (iCAM7100 models)	External Only
Flash	X	Flash for face capture	Flash for face capture
Face Image Camera	.03 MP	5MP	5MP
Communications	Ethernet, RS422, RS232	Ethernet, RS422, RS232	Ethernet, RS422, RS232
Operating Temperature	32F ~ 104F	32F ~ 113F	32F ~ 113F
Storage Temperature	0 ~ 140F	0 ~ 203F	0 ~ 203F
Inputs/Outputs	Proximity Card Reader (Wiegand In), Embedded Smart Card reader (optional), Wiegand In, Wiegand Out, Relay x 2	Proximity Card Reader (Wiegand In), Embedded Smart Card reader (optional), Wiegand In, Wiegand Out, Relay x 2, Programmable GPIO x 4	Proximity Card Reader (Wiegand In), Embedded Smart Card reader (optional), Wiegand In, Wiegand Out, Relay x 2, Programmable GPIO x 4

Q: Can I buy an iCAM7000 model unit and then later upgrade its hardware to an iCAM7100 model unit, or add an internal card reader?

A: No. Once the unit is purchased, modifications are unable to be made. Please contact an IRIS ID authorized reseller for additional information.

Q: If an iCAM7100 unit (which contains an LCD screen) is purchased, can I disable the screen?

A: Yes. The LCD Display can be turned On or Off from the iCAM Configuration > iCAM Settings screen.

Q: Can an iCAM7100 model unit have custom images/pictures/logos on the LCD screen?

A: No. At this time, the ability to modify or upload logos to the LCD screen is not available. However, it is possible to place a 20 character message/statement that can appear on the LCD Display. To make these changes, login to the iCAM Configuration screen and change the "LCD Message" for your iCAM.

Q: How do I properly use the Factory default button on the iCAM7000 series units?

A: The Factory Default Button is located on the iCAM interface board below the RTC battery. It can be used to restore settings of an iCAM7000 series camera 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.

- IP Address Default:

- Restores the IP address and User ID/Password of the iCAM to the factory default values. **(IP= 192.168.5.100 / User ID = iCAM7000 / Password = iris7000)**

Hold the factory default button down for at least 3 seconds while the unit is already powered-on to reset the unit IP address information back to the default settings.

- Factory Default:

- This factory default resets ALL settings to the factory default.

***NOTE:** Any information, uploaded information (including firmware 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 iCAM7000 series unit, hold the factory default button down for at least 5 seconds to restore the entire unit back to all factory default settings.

Q: Can the Physical MAC Address of an iCAM7000 Series unit be determined without powering on the unit?

A: Yes. To determine the Physical MAC address, you can open the front panel of the iCAM unit to view a sticker which contains a serial number of the unit and the physical MAC address of the iCAM. Additionally, you can determine the physical MAC address by logging into the iCAMs iCAM Configuration screen and

selecting the arrow located on the left hand side of the main screen (next to the version number). This System Information screen will display the iCAM S/N as well as the iCAM MAC Address.

Q: Is a dedicated iCAM7000 series camera required for enrollment purposes?

A: Although not required, a dedicated iCAM is recommended as an enrollment unit for best practice usage. Keep in mind, an iCAM7000, iCAM7100, or even an iCAM4000/4100 series unit can be used as enrollment regardless of whether the system is primarily 4000 series or 7000 series specific. Additionally, if using only 1 iCAM for enrollment and for recognition, modifications to settings will most likely be required each time the iCAM is switched from identification to enrollment.

20. Warranty Information

20.1 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.*

20.2 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.*

21. 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.

21.1 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.

21.2 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.