Iris ID

IrisAccess® Web Configuration Interface Guide

– For iCAM Series

June, 2010

IrisAccess® Web Configuration Guide – For iCAM Series

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

Document Number: IRISIDEAC-12-0100-0610

Table of Contents

1. Introduction

Since 1997, IRIS ID has been the key developer and driver of the commercialization of iris recognition technology. Iris IDAccess®, now in a third generation, is the world's leading deployed iris recognition platform. Found on 6 continents, in thousands of locations, authenticating the identities of millions and millions of persons, more people in more places authenticate with Iris IDAccess 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. Iris IDAccess® 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

Your IrisAccess ™ system is designed to work with the iCAM4000/4100 camera units. Each iCAM contains an internal configuration web interface. A multitude of configurations and options are available through this interface.

The configuration web interface for your iCAM is accessible directly through an internet browser that is connected your network.

1.2 Purpose and Audience for this Guide

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

This Guide is intended to be used as a reference for 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 this device.

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

1.3 Reference Materials

In addition to this guide, your software CD should contain an “EAC Software User Guide, 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.Iris IDiris.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)

- Iris Camera (iCAM)
- Ethernet Switch (Ethernet hub is not acceptable)
- Ethernet Wiring
- Uninterruptible Power Supply
- IBM Compatible PC

Minimum Computer requirements (for Initial Configuration)

- 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. The iCAM Configuration Interface

From a PC with an internet browser connected to the network (that the iCAM is connected to), type the IP address of the iCAM. For example, if the IP address of an iCAM is 192.168.5.100 (default IP), you would access the configuration web interface by typing http://192.168.5.100 from an internet browser.

To login, the User ID required when prompted is **iCAM4000**. The Password is **iris4000**

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

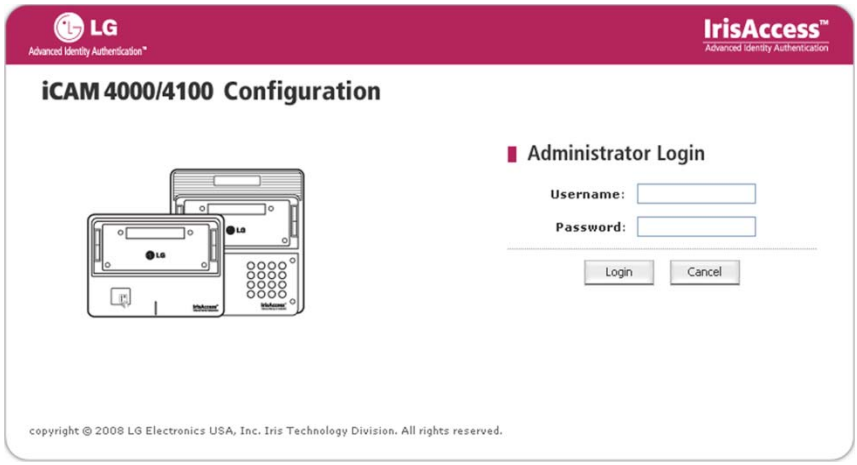
Once you have connected to the Web Configuration Interface of the iCAM, a wide variety of in depth setting configurations, information, and options become available to further resource your system.

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

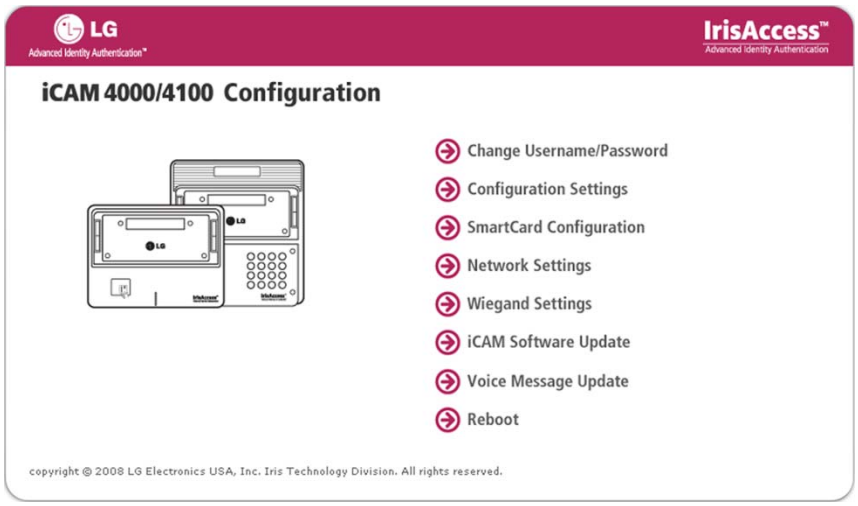
3.1 Changing the IP address of an iCAM

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

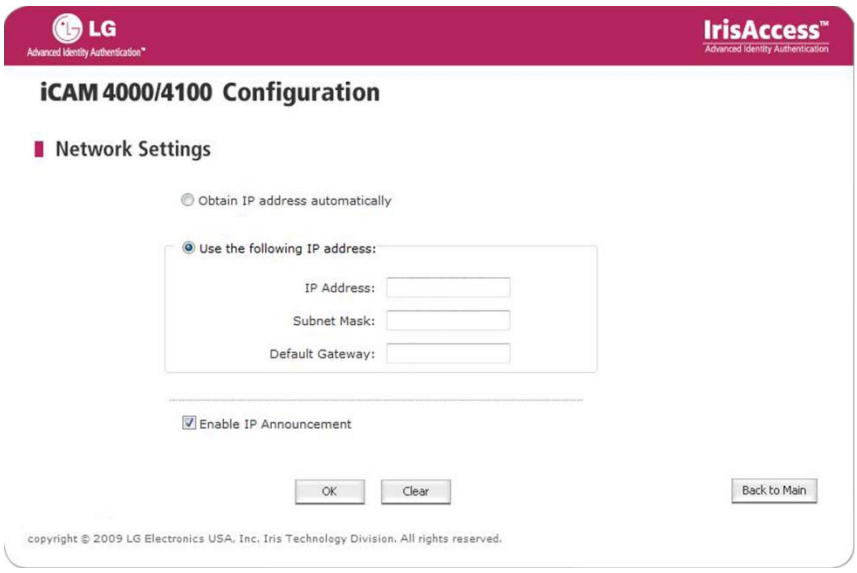
1. Set the computer to the static IP of 192.168.5.250 - subnet 255.255.255.0
2. Open the web browser and enter http://192.168.5.100 in the address bar then press ENTER. The iCAM login screen will appear.
3. Enter the default Username: **iCAM4000** and Password: **iris4000** (both are case sensitive)



4. The iCAM Configuration Main Menu will appear.



5. Select Network Settings.



6. Enter the new IP address for the iCAM (default = 192.168.5.100)

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

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

* 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.*

3.2 How to Test the IP Addess 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.

3.3 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.

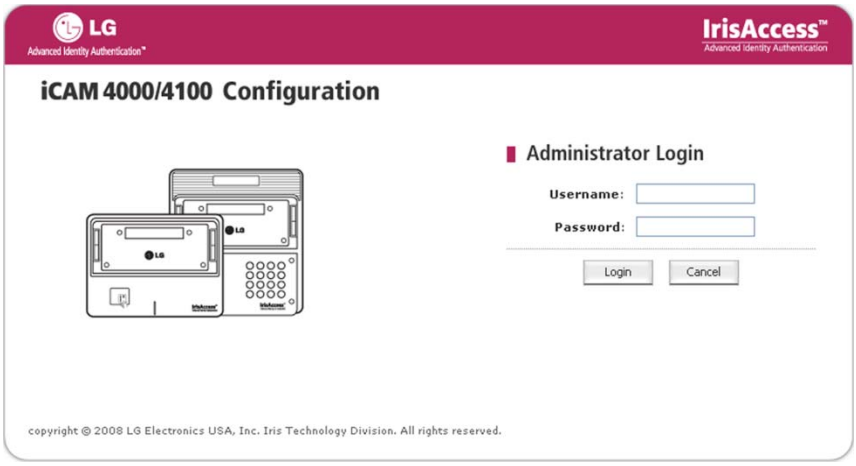
4. Understanding The iCAM Configuration Interface

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.

4.1 Login and Main Menu Screen

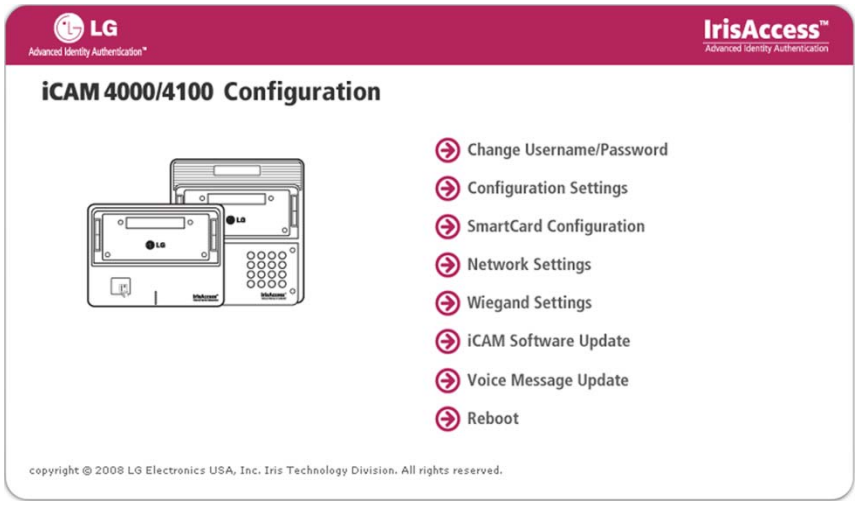
4.1.1 Login Screen

Enter the default Username: iCAM4000 and Password: iris4000 (both are case sensitive) if still set to default settings.



4.1.2 Main Screen

Once you have accessed the iCAM Configuration Main Screen (Menu screen), configurations such as changing of administrator password, date and time settings, SmartCard 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.



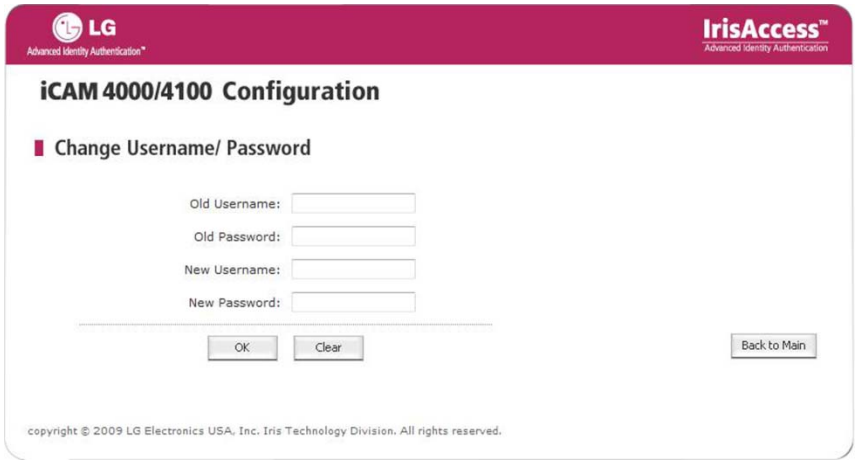
4.1.3 System Information Screen

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.

4.2 Breakdown of the Configuration Interface

4.2.1 Change Username/Password

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.

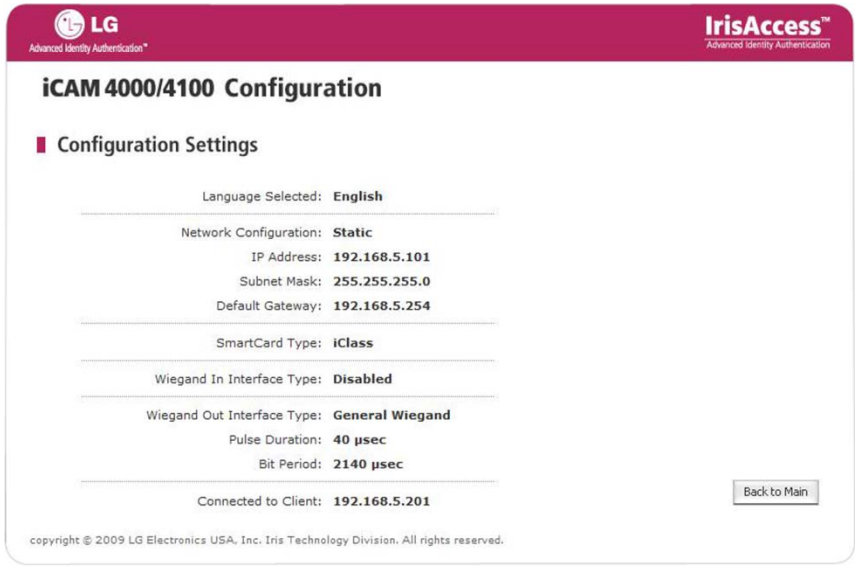


**Note: The iCAM reset button will reset customized the User ID / Password to the default factory settings.*

4.2.2 Configuration Settings

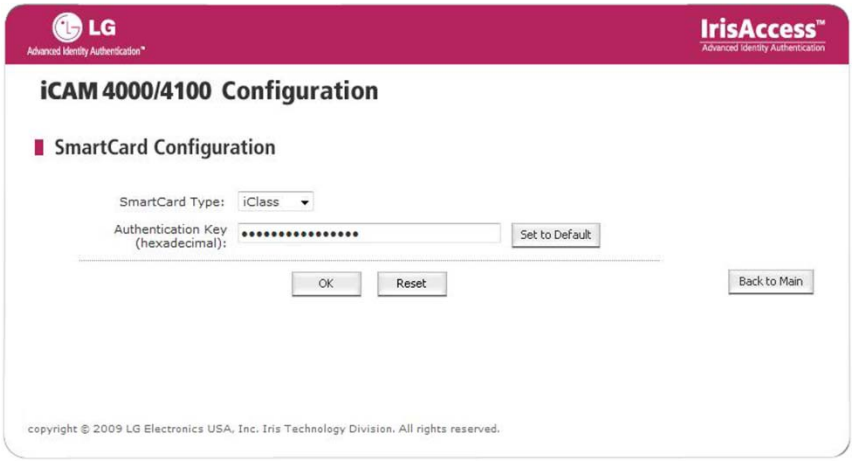
These settings are viewable only, and indicate the specific currently configured general settings which include Language type, Network configuration type, IP address settings, smart card setting, and connected client. Please see below for detailed information for each item.

- Language Type – The Language voice file selected.
- Network configuration type – Static or dynamic (DHCP) addressing.
- IP address – The specific IP address, Subnet mask, and default gateway currently assigned.
- SmartCard Type – Optional SmartCard reader Type (iClass, MiFare, DesFire, or NONE).



4.2.3 SmartCard Configuration

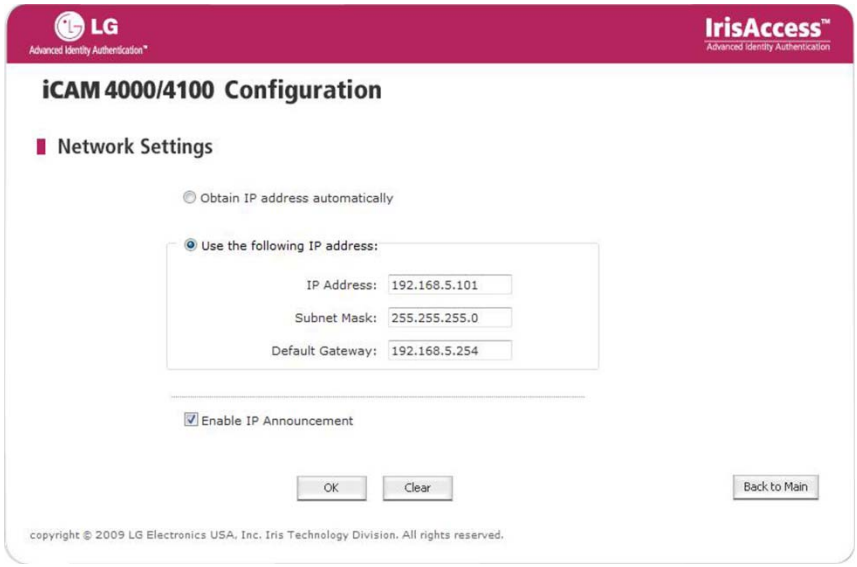
This screen allows for the modification and selection of a SmartCard type, and further allows for the input of an authentication key (hexadecimal), as well as the ability to restore back to the default settings of the iCAM.



***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.*

4.2.4 Network Settings

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

- If the new iCAM IP address is still on the same subnet as the computer: after 10 seconds the web browser will resolve to the new IP address and the login screen will appear again.
- If the new iCAM IP Address is on a different subnet: the web browser will display the standard "The page cannot be displayed" message.

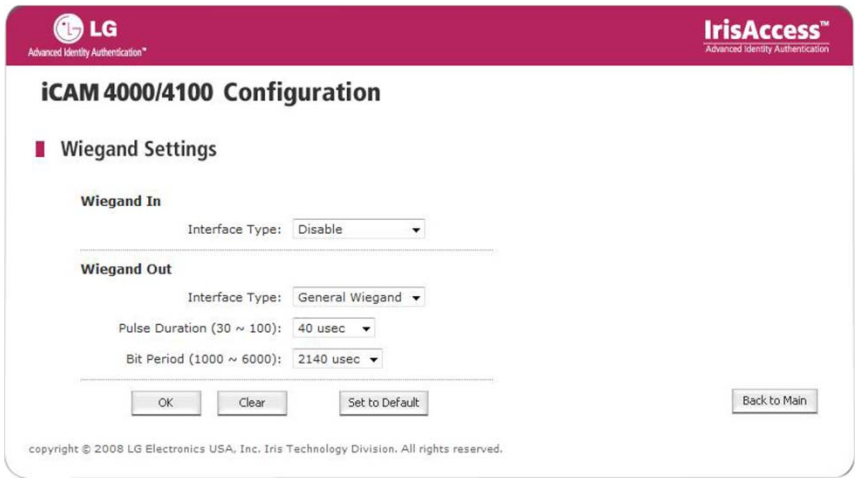
** Note: Pressing and holding the up tilt button for 12 seconds will cause the iCAM to announce the iCAM configured IP Address (Unless de-selected in this menu screen).*

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.

4.2.5 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.



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 "General Wiegand" 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 Pulse Duration (30-100 micro-seconds) for purposes of associating the correct time interval which makes up each bit.
6. If Wiegand Out is set to be enabled, select the Bit Period (1000-6000 micro-seconds) for purposes of associating the correct interval between Wiegand bits.

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

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

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

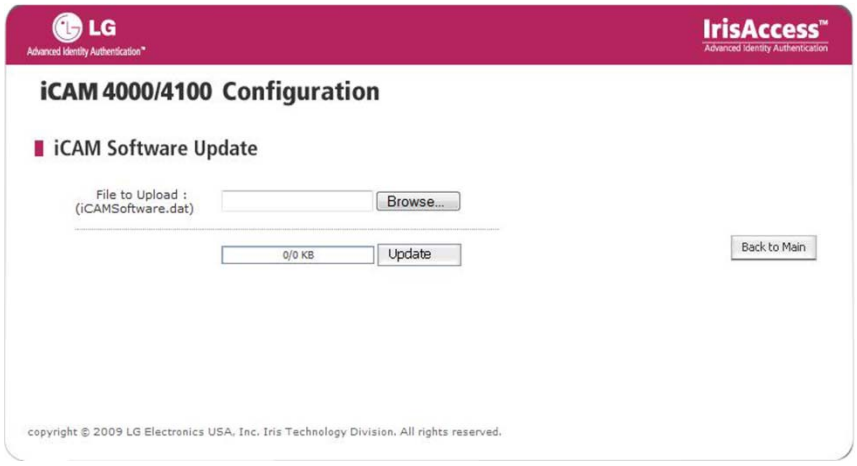
Note: *The Total Wiegand Bits, Facility Code, and Valid Bits are determined by the card or Access system configuration.*

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.*

4.2.6 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 Electronics, IRIS Technology Division 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.)*



Manually upgrading iCAM:

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 "iCAMsoftware.dat", make a new folder on the c: drive and place the file in that new folder.

Updating the iCAM Software:

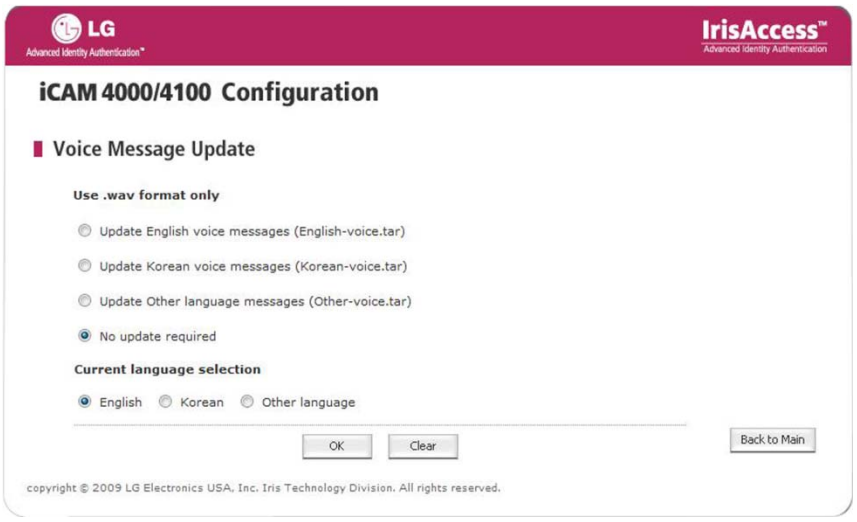
- Log into the iCAM (web browser interface)
- From the main menu select iCAM Software Update
- Select Browse
- Select the path to the iCAMsoftware.dat file
- Double click on the "Update" button. (Files will transfer and iCAM software will update, this may take several minutes)
- When complete a summary screen will display
- Click Yes to reboot the iCAM
- Enter the username (iCAM4000) and password (iris4000)
- 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.

4.2.7 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 an ftp server the iCam can access.
2. Log into the iCam web interface using 'iCAM4000' as the username and 'iris4000' as the password.
3. Select 'Voice Message Update'.
4. Select 'Update Other language messages (Other-voice.tar)' and set the 'Current language selection' to 'Other language'.
5. Press 'Ok'.
6. Enter the ftp server details and press 'Ok'.
7. 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 Update English voice message (English-voice.tar) 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 'iCAM400' for username and 'iris4000' 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.

4.2.8 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.

5. 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.