Iris ID

IrisAccess® EAC v.3.05x Software

Installation Guide – For iCAM Series

January, 2012

IrisAccess® EAC Installation Guide – For iCAM Series

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

Document Number: IRISIDEAC-26-0100-0112

Table of Contents

1. Introduction

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

Traditional Notions of Establishing Identity

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

Biometric Appeal of Iris Recognition

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

Benefits:

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

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

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

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

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

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

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

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

1.1 Product Overview

Iris Access EAC software is an application suite designed specifically for use with applicable Iris ID Hardware. The software suite consists of eight programs specially created to assist with installation, configuration, monitoring, Database backup/merge/recovery, time and attendance, reporting tools, user enrollment/modification and much more.

What is the IrisAccess® EAC exactly? Iris ID's IrisAccess® EAC software is an application suite that provides a solution to Iris ID recognition equipment in a full featured, easy to setup, expandable and manageable product suite. The EAC software when paired in conjunction with an iCAM4000 series Camera Unit can be used for the purposes of Door Access Control, time and attendance, identification verification and privacy control, enrollment, reporting, system status monitoring, and door entry status monitoring. Capable of integrating with almost any environment, the EAC application has been optimized to function with our products in such a way that it lends itself to ultimate convenience and manageability for the user.

1.2 Purpose and Audience for this Guide

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

This Guide is intended to be used as a reference for your product and its accessories. This document includes detailed background on the product technology, setup instruction, additional recommended accessories, Troubleshooting-frequently asked questions, 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, as well as installing all Iris ID products.

1.3 Reference Materials

In addition to this guide, your software CD should contain a "EAC User manual Guide" 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. What's In The Box

The IrisAccess EAC software should contain the following items:

- Software CD: IrisAccess EAC v.3.05x
- Software CD-Key on CD Case Cover

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

Required Equipment (not included)

- Iris Camera (iCAM)
- Ethernet Switch (Ethernet hub is not acceptable)
- Ethernet Wiring (Ethernet hub is not acceptable)
- FGB (required for use with OU3000 unit(s) only)
- IBM Compatible PC

Recommended Equipment (not included)

- Uninterruptible Power Supply

Minimum Computer requirements (for Initial Setup)

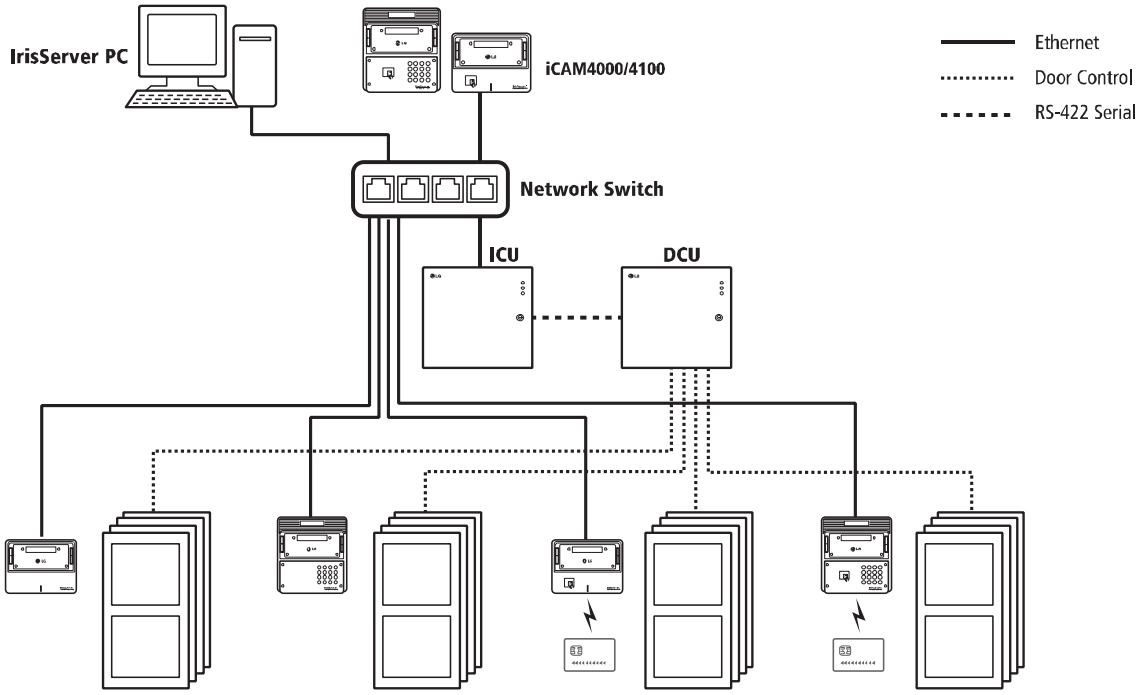
- Windows 2000, XP Pro, Server 2003, Vista or Window 7 Operating System
- Internet Browser (such as Internet Explorer)
- Pentium 4 compatible 1.6GHz Processor
- 512MB Memory (RAM)
- 10 GB Harrd Disk Drive
- CD-Rom Drive (for software installation)
- Ethernet Port (100 Mbps recommended)
- Mouse, SVGA Monitor, Keyboard
- Optional – Sound Card and speakers for audible monitoring alarms

Optional Equipment

- Additional Iris Camera(s)
- ICU4000 or 3000 series
- DCU4000

*Note: *The computer with the EAC software installed and running the IrisServer application is considered the "irisServer".*

2.1 The IrisAccess EAC Software



About the Software

The EAC software version you received is designed to operate using both IrisAccess 3000 and IrisAccess 4000 series hardware. The IrisAccess EAC is a suite of applications used to configure the system, manage the user database, monitor the system and user activities, and enroll users.

** One computer can act as Enroll, Manager, and Monitor. These functions can also be split over different computers.*

Breakdown of EAC suite applications

IrisServer – Controls the IrisAccess database and communications to and from the ICU(s) and IrisAccess system. Only one IrisServer application per network is needed.

IrisManager – Manages the system configuration, system permissions, and user database. Up to 10 IrisManager applications can be placed on one network, however only one can be active at any time.

IrisMonitor – Allows for real-time monitoring of system status and user activities with optional audio alerts. Up to 10 IrisMonitor applications can be placed on one network

IrisEnroll3000 – Used with the IrisAccess 3000 series iris cameras for user enrollment. Up to 32 per network, total number shared with the number of IrisEnroll3000 on the network. (Although not shown by default, this application can be found in the C:\Program Files (x86)\Iris ID\IrisAccess\IrisEnroll3000.exe\ location of your PC when typical installations have been performed.)

IrisEnroll4000 - Used with the IrisAccess 4000 series iris cameras for user enrollment. Up to 32 per network, total number shared with the number of IrisEnroll3000 on the network.

IrisDBAdmin – Provides backup and other database utilities. For use with the IrisServer Only.

IrisICUAdmin3000 – Used to configure the ICU3000 and ICU4300 hardware for use with OU3000 iris camera units. (Although not shown by default, this application can be found in the C:\Program Files (x86)\Iris ID\IrisAccess\IrisICUAdmin3000.exe\ location of your PC when typical installations have been performed.)

IrisICUAdmin4000 – Used to configure the 4000 series ICU for use with the 4000 series iris cameras (iCAM).

** Refer to the software Manual and Users Manual located on the software CD for more information.*

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

3. Installation Requirements

- If upgrading an existing IrisAccess system to EAC v.3.05x software, please follow the upgrade documentation located on the EAC software CD; or the support web site www.Iris IDiris.com > Support & Service. Refer to the "Create Web Support Account.pdf" document included on the software CD to create an account on the support web site to access this information.

- Microsoft Access is the standard database type used in the IrisAccess system. MS SQL Server or oracle 9i can also be used but will require the appropriate DBMS software be installed prior to the installation of the EAC software.

- The Server and Enrollment computer should be placed within the protected area and in a location that is not accessible by the general staff or public.

- All system components including the Ethernet network should be powered through Uninterruptible Power Supplies (UPS). UPS will provide power line filtering as well as power back-up operation.

- Each device on the Ethernet network system must have a uniquely statically assigned IP address.

- IrisEnroll3000 and IrisEnroll4000 will not function simultaneously on the same computer.

- The ICU4300(-W) will support either iCAM (4000/4100) iris cameras or OU3000 iris camera units. The ICU4000R(-W) will support only iCAM (400/4100) iris camera units.

4. Preparing for Installation

1. Connect all System Components; follow the Hardware Guide included with each iCAM, ICU and DCU unit (when applicable) for the hardware connections.

2. Set a static IP Address for the Iris Server computer in Windows, refer to the tech Bulletin TB-0121 for details. As an example, we will be using the IP address 192.168.5.250

3. Only power on one iCAM at a time to avoid any potential IP conflicts.

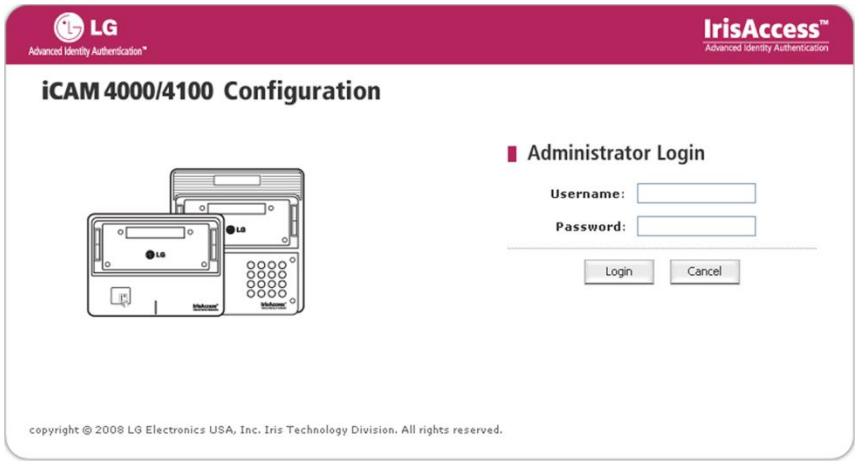
4. Assign a unique IP address for each iCAM to be used in the system. Refer to the below "iCAM Configuration" section for the iCAM IP address configuration procedure.

5. iCAM Configuration

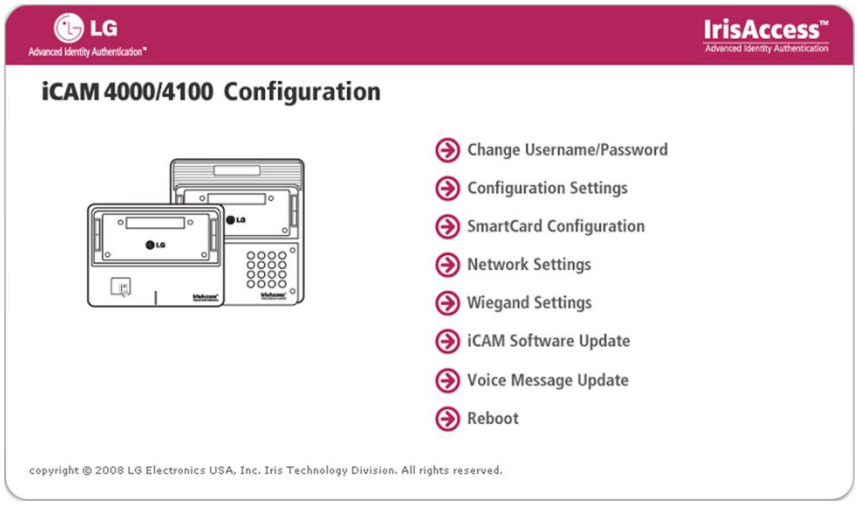
5.1 Changing the IP Address of an iCAM4000 Series Unit

** 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.*

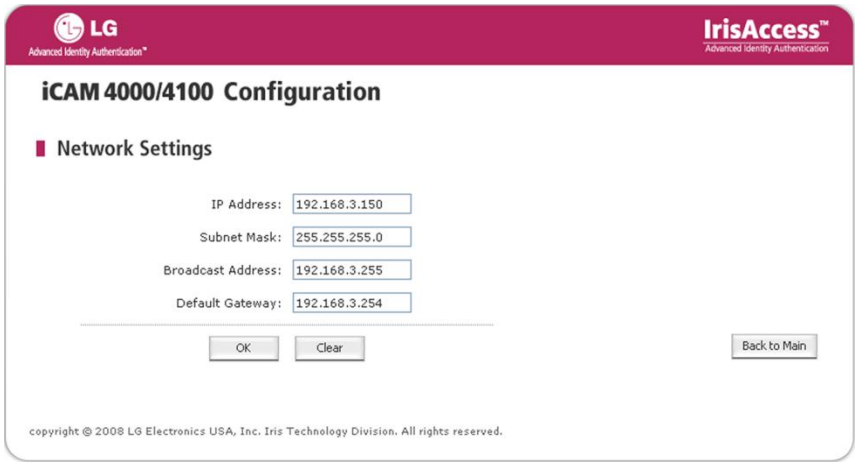
1. Set the computer to the static IP of 192.168.5.250 - subnet 255.255.255.0
2. Open the web browser and enter http://192.168.5.100 in the address bar then press ENTER. The iCAM login screen will appear.
3. Enter the default Username: iCAM4000 and Password: iris4000 (both are case sensitive)



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.*

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.

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.

* Note: *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.*

5.2 Changing the IP Address of an iCAM7000 Series Unit

Note: To avoid IP Address conflicts: 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. Any computer with a web browser which supports graphics (ex. Internet Explorer) can be used to configure the iCAM7000series cameras.. (Default IP settings are used for reference.)

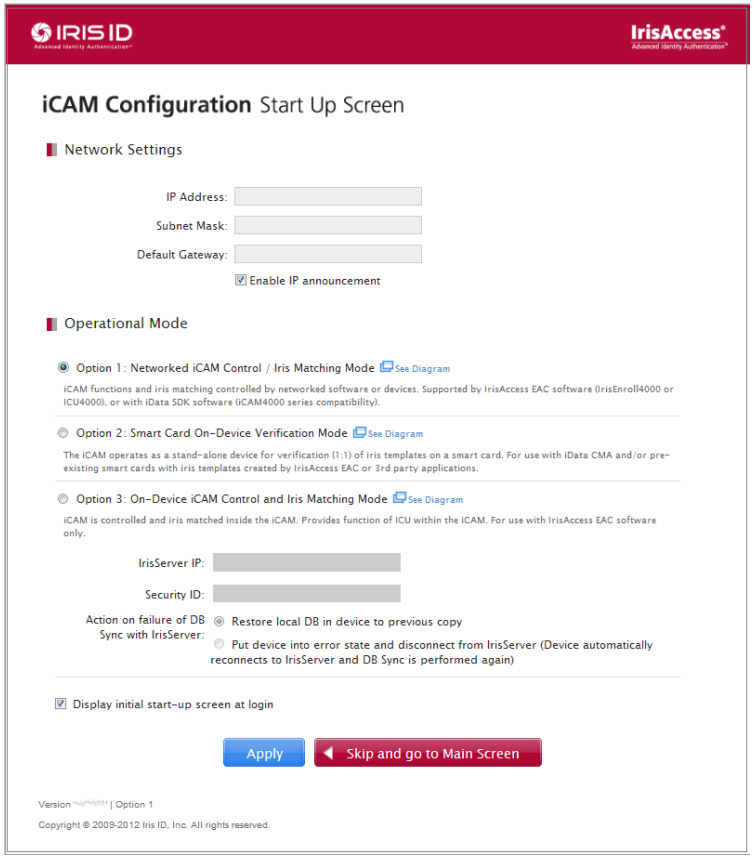
Additional Note: An Internet connection is not required to access or use the iCAM web configuration. Only a network connection between the computer and iCAM is required.

To login to iCAM, the Default *User ID* is: iCAM7000 / *Password* is: iris7000.

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

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".*



iCAM IP Address Settings:

4. 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)

5. 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:

6. Select Operational Mode: Option 3 for the iCAM. (See following data for details.)

   - "Option 1: Networked iCAM Control / Iris Matching Mode" – This document does not provide instructions for this option. Refer to the iCAM7000 User Guide for additional details. *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" - This document does not provide instructions for this option. Refer to the iCAM7000 User Guide for additional details.

   - "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 IrisAccess EAC software version 3.03.x and above.

**Note: If attempting to use an iCAM7000 series unit in operational mode "Option 3", compatible IrisAccess EAC software version 3.03.x 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).

7. 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.

8. Write down in the below fields the iCAM7000 Series IP address, IrisServer IP, and Security ID for each iCAM7000 that is to be used in Operational mode: Option 3

Note details for each iCAM being set up and save this data in a secure location.

iCAM7000 Series

IP Address: _____ . _____ . _____ . _____
Subnet Mask: _____ . _____ . _____ . _____
Gateway: _____ . _____ . _____ . _____
IrisServer IP: _____ . _____ . _____ . _____
Security ID (16 characters): _____

9. Press Apply to confirm changes and allow camera to reboot when prompted.

- 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.

> Resetting the iCAM if needed: The iCAM FACTORY DEFAULT button is located on the iCAM7000 interface board below the RTC battery. With the unit powered on, press and hold the FACTORY DEFAULT button for at least 5 seconds. This will reset the iCAM IP Address to the factory default of (192.168.5.100) .The default login ID for the iCAM (User ID= iCAM7000 / Password= iris7000).

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

A. Click on Start (in the Windows task bar of the connected PC)
B. Select: Run
C. Type: CMD
D. Press: Enter
E. At the command prompt type: ping <new IP> (ex. ping 192.168.5.120)
F. Close the command prompt window.
G. Write down in the below fields the iCAM7000 Series IP address, IrisServer IP, and Security ID for each iCAM7000 that is to be used in Operational mode: Option 3

6. Software Installation

Install the IrisAccess EAC v.3.05x software:

*Note: This procedure is for "Typical" installation using a MS Access database. The IrisServer will also function as the Enrollment, Manager, and Monitor computer. If the installation requires different setup, refer to the IrisAccess EAC v.3.05x software installation manual which is located on this software CD.

A. Right click on Start (on the task bar) and select Explore.
B. Click on the CD ROM drive containing the EAC v3.05x CD.
C. Double click on the setup folder.
D. Double click on the Setup.exe Icon (Setup Launcher Iris ID electronics)
E. Click Next on welcome screen
F. Enter the Serial Key. The Serial key can be found on the EAC software CD case label. Click Next.
G. Read License agreement, select "I accept all the terms…", and then click Next.
H. Enter Name and Company Name (Must have both username and company field filled in.)
I. Select "anyone who uses this computer" or "only the current logged in user can use the IrisAccess software". Click Next.
J. Click Next to install the software in the default location
K. Select "Typical" installation and click Next.
L. Click Next to the System screen.
M. Click OK to the disk space screen.
N. Select database type as "Microsoft Access…", click Next.
O. Click Next for default folders.
P. Click Next to install software.
Q. After the software is finished loading, click Finish.

*Note: *If running a software or hardware firewall product, disable and or "allow" all access of the IrisAccess EAC application and installation.*

*Note: Unlike some previous versions of EAC software, EAC v.3.05x has standard configurations for irisManager, IrisEnroll, and iris Monitor automatically entered.

The default configurations are:

IrisManager:	127.0.0.1	
IrisMonitor:	127.0.0.1	
IrisEnroll3000:	127.0.0.1	SID: 1111111111111111
IrisEnroll4000:	127.0.0.1	SID: 1111111111111111

*Note: *Determine and write down a compatible set of IP addresses to be used later for:*

Server PC – Example: 192.168.5.250

ICU4000 – Example: 192.168.5.200

ICAMs – Example: Enrollment iCAM: 192.168.5.10,

4 Remote iCAMs: 192.168.5.20, 192.168.5.21, 192.168.5.22, 192.168.5.23.

Refer to iCAM 4000 / 4100 Quick Start Guides to configure IP address in the iCAMs.

*Note: *IrisEnroll3000 and irisEnroll4000 will not function simultaneously on the same computer.*

7. Testing the Iris Server Software

*Note: For all EAC software, the default *username/ID* is: administrator and the *password* is iris3000 (this is case sensitive).

*Important: If Windows security prompts to block/unblock, choose "unblock".

1. Double click on the IrisServer icon on the desktop, a small icon near the windows clock will appear in the task bar.
2. Double click on the IrisManager icon to open, if prompted for the IP address; enter the configured address (127.0.0.1 in this example). If 127.0.0.1 is displayed – Click OK. Login to IrisManager to be sure that this application is operational. Enter username and password. Respond Yes or No to "do you want to change password now?". Minimize IrisManager.
3. Double click on the irisMonitor icon to open, if prompted for an IP address; enter the configured address (127.0.0.1 in this example). IF 127.0.0.1 displayed – Click OK. Login to IrisMonitor to be sure that this application is operational. Enter username and Password. Respond Yes or No to "Do you want to change the password now?". Minimize IrisMonitor.

If using an IrisAccess® 4000 series iris camera (iCAM) for enrollment:

1. Double click on the IrisEnroll4000 icon to open. Click OK, Exit.
2. Double Click on IrisEnroll4000 again. If prompted for an IP Address, enter the configured address. (127.0.0.1 in this example). If 127.0.0.1 is displayed – Click OK. If a dialog requesting a Security ID displays, enter the SID set in IrisManager (in this example 1111111111111111). Enter Username and Password.

> * Note: The software will automatically detect the iCAM software version. If the iCAM is not at the latest software, the system will automatically upgrade the iCAM.

3. Respond Yes or No to "Do you want to change the password now?"
4. Login to IrisEnroll4000 application.
5. A dialog will prompt of the IP Address of the Enrollment iCAM the address and click Connect. Enter IP address of iCAM – Example: 192.168.5.18
6. If "Notice" window pops up, Click Close.
7. In the IrisEnroll4000 action status window, the message should read "iCAM is normal". Exit Enrollment screen.

If using an IrisAccess® 7000 series iris camera (iCAM) for enrollment:

1. Double click on the IrisEnroll4000 icon to open. Click OK, Exit.
2. Double Click on IrisEnroll4000 again. If prompted for an IP Address, enter the configured address. (127.0.0.1 in this example). If 127.0.0.1 is displayed – Click OK. If a dialog requesting a Security ID displays, enter the SID set in IrisManager (in this example 1111111111111111). Enter Username and Password.

> * Note: In order to connect the iCAM7000 Series unit to IrisEnroll4000, the iCAM7000 series unit MUST be in Operational Mode: Option 1. (For details on how to change the operational mode of an iCAM, refer to the "*iCAM7000 Series User Guide*".

3. Respond Yes or No to “Do you want to change the password now?”
4. Login to IrisEnroll4000 application.
5. A dialog will prompt of the IP Address of the Enrollment iCAM the address and click Connect. Enter IP address of iCAM – Example: 192.168.5.18
6. If “Notice” window pops up, Click Close.
7. In the IrisEnroll4000 action status window, the message should read “iCAM is normal”. Exit Enrollment screen.

8. Configuring a Remote unit

This configuration is for an ICU to be used with iCAMs only.

*Note: *All iCAMs must have a unique IP address before continuing.*

Configure the remote unit in IrisManager (at Server):

A. Open IrisManager and login.
B. Click no to "…want to change the password now?"
C. Click on Creation on the menu bar.
D. Click on the Remote Unit tab, Click New.
E. Enter the Name: iCAM1 (for this example).
F. Enter the ICU IP address 192.168.5.200 (for this example)
G. Enter a Security ID (must be 16 characters – case sensitive) Example: aaaaaaaaaaaaaaa

*Note: *The Security ID entered for the iCAM in the ICU configuration and IrisManager-Creation must match exactly (they are case sensitive). Write down and keep track of the Security ID used for each iCAM, they will need to be entered later in this procedure.*

H. Select the Channel ID: 1 (in this example, the iCAm will be controlled by Channel 1 of the ICU).
I. Select Use Type: identification

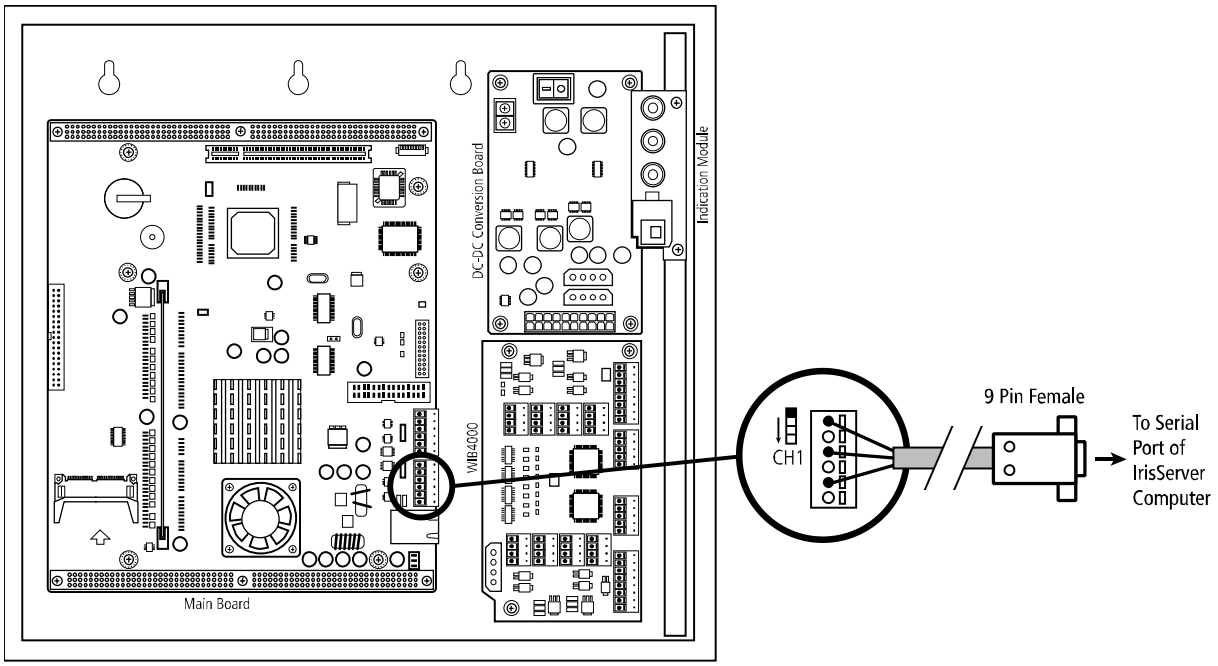
*Note: *The Use type field must be selected but does not have a function in v3.05x*

J. Select the Model: iCAM4000 or iCAM4100 (depending on unit type)
K. Set priority level (from 1-255. 1 Has highest priority level).
L. Click OK.
M. Click Close.
N. Close the IrisManager by clicking the Program menu and selecting Exit.
O. Click Yes to confirm exit.
P.

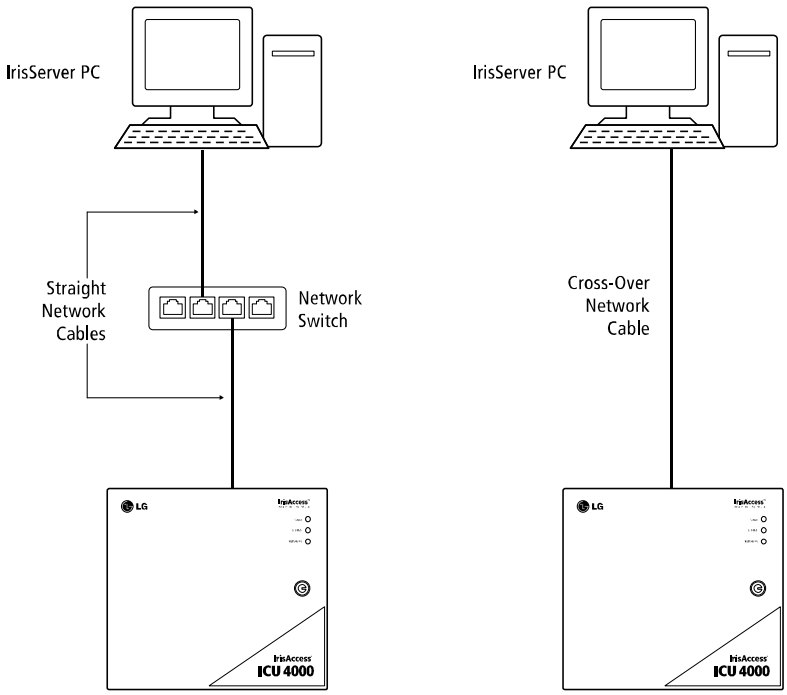
9. Configuring an ICU

Setup and configure the ICU:

A. Turn the ICU power off.
B. Connect the ICU Configuration cable included with the ICU and a Cat5 crossover cable (or Ethernet switch) between the ICU and the Server. (Details below.)



< ICU Configuration Cable connection Diagram >



< Ethernet Connection Diagram >

- Connect the ICU configuration cable between COM port 1 or 2 of the IrisServer computer and Serial Connection (CH1) on the ICU main board. (Remove existing connector as needed).
- Set the CH1 communication type switch on the ICU main board to the RS232 position (down).
- Use the IrisICUAdmin4000 application (new installation) to configure the ICU4000R

* Note: If the IrisServer is too far from the installed location of the ICU, the EAC software can be installed on a laptop. From the laptop IrisICUAdmin4000 can be used to set the IP Addresses and Security IDs on the ICU. Software updates and ICU configurations then can be performed over the network from the IrisServer.

C. Open the IrisICUAdmin4000 program by double clicking the icon ion the desktop.
D. Click on New Installation
E. Click Next
F. Enter the following information:
   -Enter Server IP address: 192.168.5.250 (for this example)
   -Enter ICU IP address: 192.168.5.200 (for this example)
   -Enter Gateway address: 192.168.5.254 (for this example)
   -Enter Subnet: 255.255.255.0 (for this example)
G. Click Next, Click OK.
H. Checkmark iCAM 1 (installed iCAM) and enter the Security ID (in this example: 200aaaaaaaaaaa1).

*Note: *In a full installation a Security ID should be filled in for each iCAM being configured. A Security ID can be assigned even if the iCAM will not be connected at this time. Checkmark the other iCAMs and enter in the Security ID (each unique), then uncheck the iCAM if not being used at this point. Be sure to record the security ID for future reference. Once entered the Security ID cannot be viewed at a later time. The Security ID can only be changed by the ICU serial connection running New installation in from the IrisICUAdmin application.*

I. Click Next.
J. Select the COM port of the server that will be used for the serial communication to the ICU.
K. Click Next.
L. Click Start, Start.
M. Turn on the ICU power.

*Note: *In approximately 120 seconds, files will transfer. If the file fails to transfer within 160 seconds, turn off the ICU, check the serial connection and the COM port, which was selected.*

N. Click Close on the Success window that appears.
O. Click Next.
P. Click Next.

*Note:

- *After configuration, set the CH1 communication switch on the ICU main board back to the original position ICU4000R-W (WIB-RS232) unless connecting to the ICU to a DCU requiring a RS-422 connection.*
- *Replace the original communication cable to the WIB or connection to the DCU.*

Q. Enter the ICU *password*: iris4000.

R. Click Next.
S. If the default password was used, click to close the warning.
T. Click Next.
U. Click Start installation.

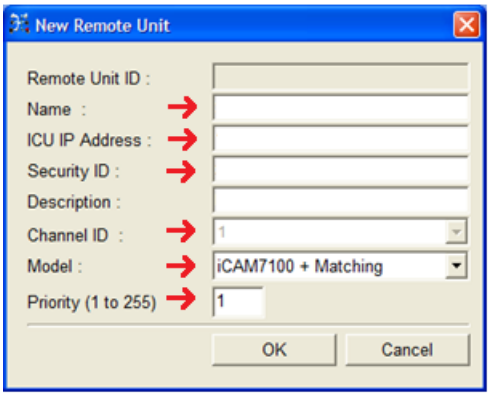
*Note: *Files will transfer from the server to the ICU over the Ethernet connection. This will install the new software to the ICU. However, if the dialogue box appears with a message "Cannot initialize connection with the ICU4000, please confirm the ICU4000 is online", click on the internet explorer. Click on File, and uncheck "work offline".*

V. Click OK. Click Next, Next, Next.
W. The current ICU configuration will download from the ICU to the IrisICUAdmin screen. Click OK.
X. Click OK.
Y. Click Configure.
Z. Enter the IP address of the iCAM.
AA. Verify ad modify the configuration as needed.
BB. Click OK.
CC. If prompted, click yes in the warning window.
DD. Click Next
EE. Click Send. Configuration changes will be sent to the ICU.
FF. At "ICU Configuration is completed" message, Click OK.
GG. Click Next, Click Finish. The ICU will reboot automatically.
HH. Click OK, Click OK.
II. Exit the IrisICUAdmin4000 program.

*Note: *In an actual installation the setup and configuration must be completed for each ICU in the system. Unique IP address information must be used for each ICU; a unique Security ID must be used for each ROU or iCAM in the system. In order for each component to communicate to the IrisServer, it must be defined in irisManager under Creation.*

10. Registering an iCAM7000 Series in Option 3 Mode

IrisManager allows creation of remote unit for iCAM7000/7100 Option 3. Refer picture below. Enter the iCAM IP address in the ICU IP Address box. Selecting iCAM7000 + Matching or iCAM7100 + Matching option from the Model drop down menu will automatically set Channel ID to 1 and its control will be disabled.



Step Process:

1. Install EAC Software version 3.03.x (or above) if not already installed. -Refer to the *"iData EAC User Manual"* for complete software information instructions.
2. Open the IrisServer.exe application (located on the desktop)
3. Open the IrisManager application (located on the desktop)
4. Select the Creation button in IrisManager and select Remote unit tab (if not already selected).
5. Click on the New Button. The *New remote unit window* will be displayed.
    a. Enter a Name of the remote unit – this can be descriptive, (ex: FrontDoor 1)
    b. Enter the ICU IP Address - which is the same IP address as the iCAM7000 series in Option 3 mode. (Option 3 implies that ICU matching functions are performed inside the iCAM.)
    c. Enter the Security ID (16 characters) which is the security ID that is setup when configuring the iCAM for option 3 mode.
        - The Security ID must be identical to the Security ID typed in during the setup of the iCAM setup when configuring it with option 3. (step 6 above)
    d. Enter a Description - this can be whatever you wish.
    e. You must also select the Channel ID as 1
    f. Select the Model – Make sure to select "iCAM7xxx + Matching"
    g. Set the Priority – generally this is set to 1.

    Note: More than one camera unit can have the same priority (from 1 – 255. 1 is the highest priority and 255 is the lowest). When the priority level is set, the iCAM will function and receive/send update information for the highest priority iCAM unit(s) first.
6. Once all the required fields are entered, click OK button to complete the remote unit registration.
7. The successful addition of the remote unit causes the Status window to pop up.

- *Repeat these steps to configure each iCAM7000 series camera unit for option 3 as needed.*

11. Testing the System

How to Test the System

A. Enroll a user using IrisEnroll, assign the enrollment to the "ALL" Remote Group and the "ALL" Time Group. If a user was previously enrolled, their permissions may be changed through IrisManager.
B. Open the IrisServer program by double clicking on the IrisServer icon near the clock in the task bar and login.
C. View the messages in IrisServer. There should be a message "Updated the database of irisRecog [iCAM1]" (iCAM1 is the name assigned to the iCAM in creation, if a different name was used; the other name will appear instead).
D. If an error message continues to appear, check the Security ID, and IP address entered in the IrisManager to be sure it matches what was assigned in IrisICUAdmin4000, or check the network connections between the iCAM and ICU. Check that the iCAM is powered on.
E. Have the enrolled user present their eyes to the iCAM. A successful identification should take place.
F. If the user fails to be identified, recheck their permissions in IrisManager.

*Note: *If required the ICU configurations can now be changed using irisICUAdmin4000 Configuration. Refer to the User's manual located on the EAC software CD for details.*

12. 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.