Information Technology Department

Government Of Sindh

Govt of Sindh

IRIS Access

Configuration & Installation

Biometric Identification Electronic System

ADP: 1488

Year: 2009-2010

Prepared By:

INFOTECH

TABLE OS CONTENTS

1. IrisAccess® 4000

Iris ID's IrisAccess® 4000 sets the standard for performance and versatility for iris recognition.Whether you are looking for a single biometric identification solution or a multi-factor solutionthat works with many leading cards, card readers and or pin input devices for verification, theIrisAccess platform will meet your needs.

Iris ID Systems has been the key developer and driver of the commercialization of iris recognition technology for over 10 years. IrisAccess®, now in its third generation with even more features and flexibility is the world's leading deployed iris recognition platform. Iris ID's biometric solutions enabling non-contact and highly accurate identification by the iris of the eye, deliver security, convenience, privacy and productivity to millions around the world.

The IrisAccess® 4000 solution is versatile and flexible allowing easy integration and expansion into a range of applications. An intuitive user interface, with visual and audible prompts enables users to be enrolled and identified more easily and more quickly at an affordable price. A powered, auto-tilt capability further increases both speed and convenience by adjusting for height with a simple touch or if a card is presented when multi–factor authentication is chosen.

IRIS ACCESS SYSTEM CONFIGURATION AND INSTALLATION

The security of the IrisAccess® platform is also superior since no biometric templates are stored on the iCAMs. Experts also concede that the countermeasures built into the IrisAccess® suite set the standard for the industry. A new iData software suite for access control and a tool kit for building identity dependent applications support several different encryption alternatives is FIPS201 compliant and include PKI support.

Every iris pattern is unique and stable for life barring direct trauma. Since there are more readily measurable characteristics in the iris, iris recognition is the most accurate, fastest, and scalable option for small and large scale biometric deployments. Finger, hand, voice, vein and facial characteristics often vary and change over time.

2. The IrisAccess™ 4000 EAC System

• IP (Ethernet) based system

• Consists of Computers, Iris Cameras, and Control Units.

• Can operate in conjunction with 3rd party access control systems.
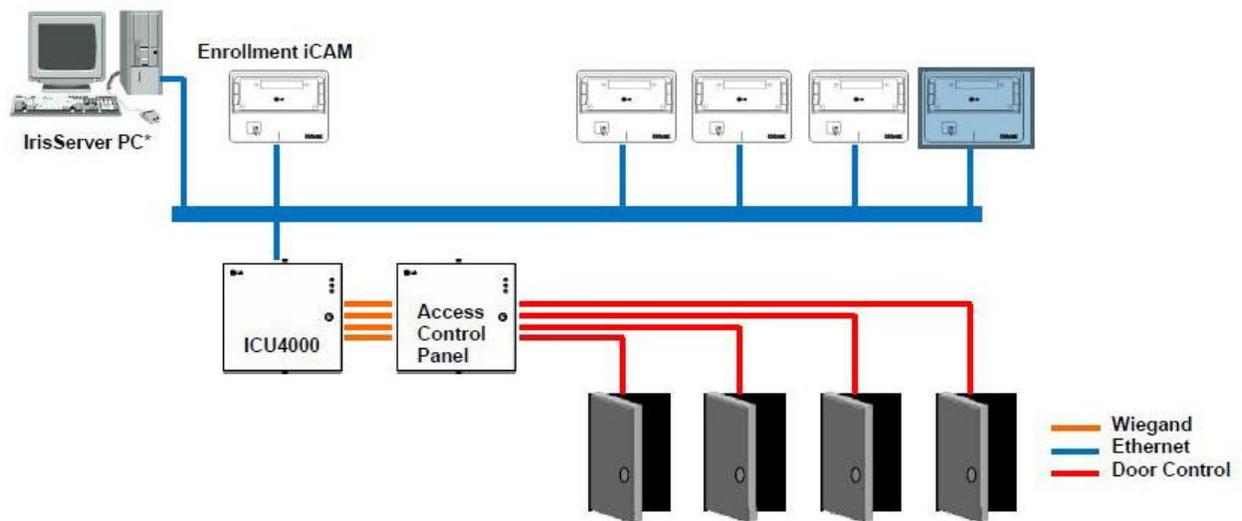
3. Intuitive User Interface

- iCAM activates when user approaches or when card is presented.

- Picture capture range is 10-14 inches (26-36cm) away.

- Self or auto/set height adjustment.

- Placing dot over the bridge of nose easily helps alignment.

- Orange (dot) turns to green (dot) 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.

4. iCAM4000 (IrisCamera)

Dimensions (W x H x D)	8.6" x 6.5" x 3.2" (218mm x 164mm x 80mm)
Weight	4.4lbs (2kg)
Power Input	12VDC, 2.5A
Power Consumption	30W
Status LED Range LED	Power (Blue), Accept (Green), Reject (Red) Operating Range (Green), Out-of-Range (Orange)
Voice Indication	Flexible Voice Message (English: standard, Other Language: downloading available)
Iris Capture Range	10.2" ~ 14.2" (26cm ~ 36cm)
Operating Temperature	32°F ~ 104°F (0°C ~ 40°C)
Storage Temperature	-4°F ~ 140°F (-20°C ~ 60°C)
Humidity	0% to 95% Non-condensing
Rotation Angle	+35°/-25°

Interface
• Ethernet • Proximity Card Reader (Wiegand In) • SmartCard Reader (Optional) • Wiegand Out • Dry Contact Relay

Equipment supplied with iCAM4000
• AC Power Cord • AC Power Adapter • Straight Ethernet Cable

IrisServer PC Requirement

Operating System	Windows® 7/Vista/XP (32-bit only)
Processor	Pentium® 4 1.6GHz or higher
Memory	512MB or higher (minimum 2GB for Windows 7 or Vista)
Hard Disk	10GB or higher
Ethernet	10/100Mbps Full Duplex
Other	CD-ROM

5. Inside iCAM 4000

• Power and Network are required connections

• Wiegand In and Smartcard are optional

• Reset button to reload default IP address and iCAMlogin

• Tamper switch on unit rear and front panel
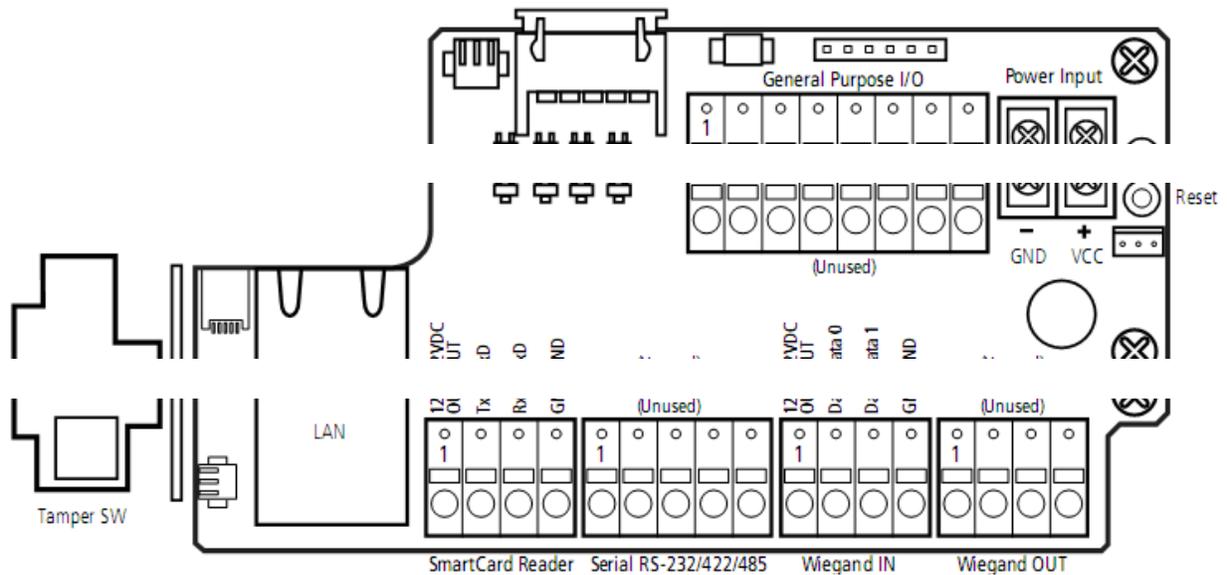
Installation and Dimension
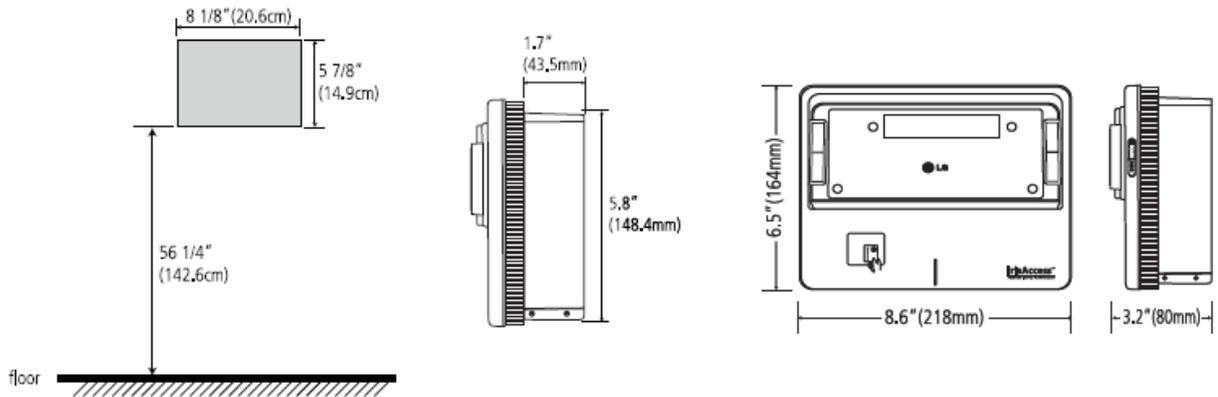
Illustration of mounting prep depth requirements with flush mount to wall.

Recess mount kit available for iCAM4000 - Order iCAM-RM Mount kit.

6. Use of IrisAccess

System Configuration and Setup

7. Prepare the IrisServer PC

In order to configure the iCAM iris cameras, the IrisServer computer must be given the static IP Address of 192.168.5.1

If a different static IP Address is required for the IrisServer computer, this can be changed after all of the iCAM's have been configured.
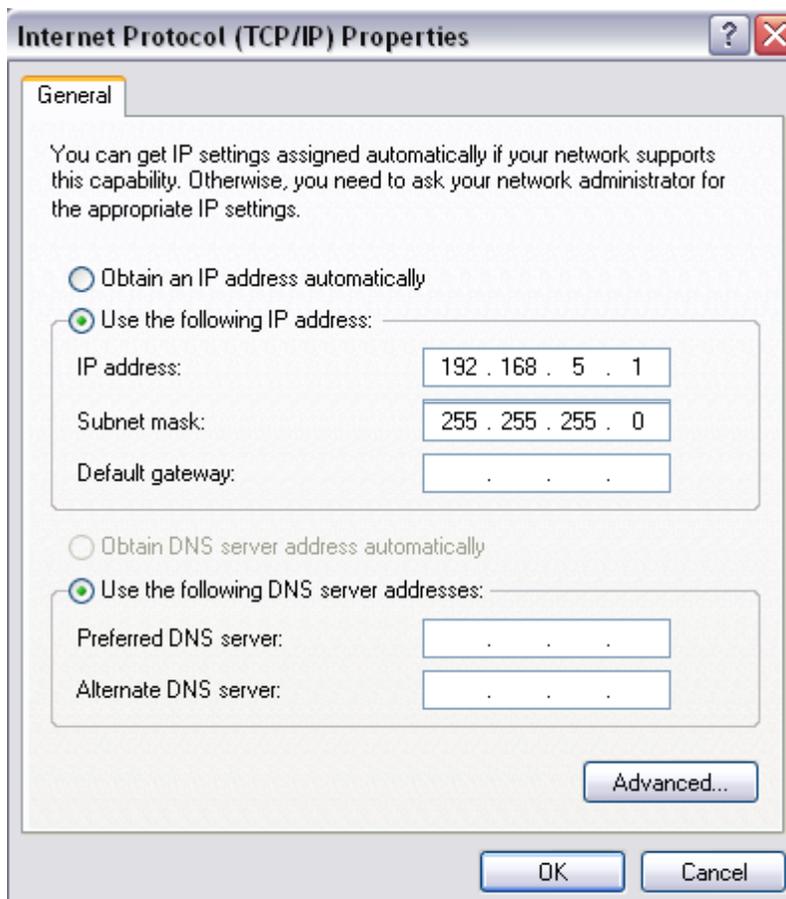
Configuring the iCAM IP Address

With the iCAM connected and powered on, enter in the URL for the iCAM in the computer's web browser address bar. http://192.168.5.100
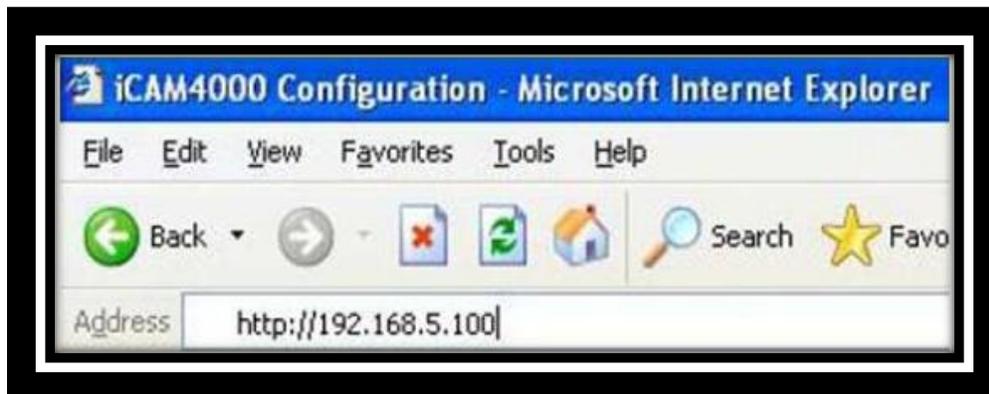
At the log in screen enter the

Username: iCAM4000 and thepassword: iris4000. Click Login
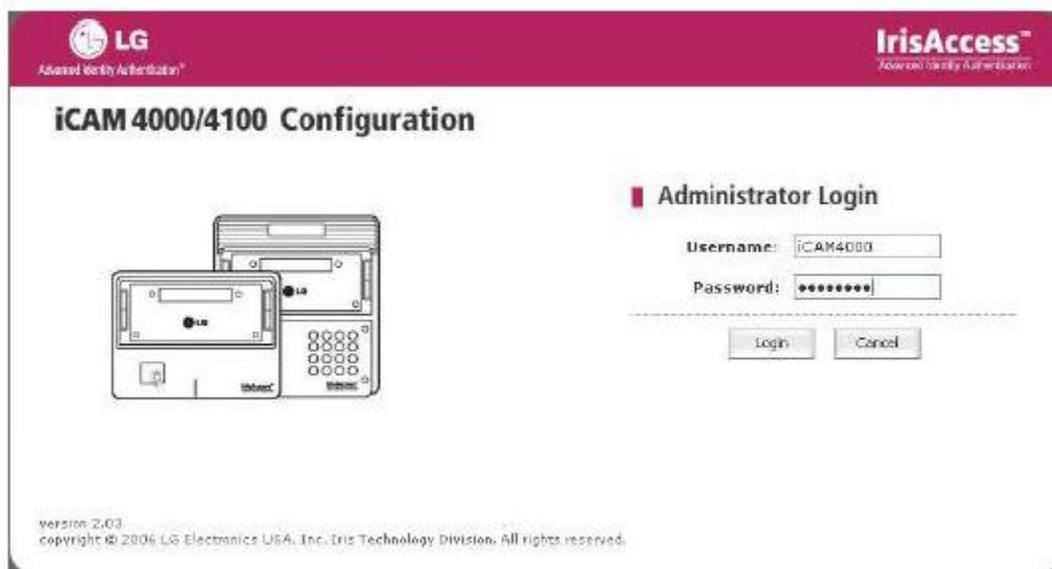
Steps for ChangingiCAM IP Address

At the menu select "Network Settings"

Enter the desired IP information then click OK to save and change the address values.

Steps for Changing iCAM IP Address (cont'd)

The IP Address is changed within seconds.

After each iCAM configuration the arp cache on the computermust be deleted.

Click on Start (in the Windows task bar)

Select Run

Type cmd

Press Enter

At the command prompt type: arp –d

Close the command prompt window.

Connect the next iCAM to be configured on the network andperform the configuration to the next iCAM.

To avoid confusion you may want to remove the configurediCAMs until all are completed.

8. Preparing for Installation

Software Disk Insert – Starting point for all installations. Identifies the documentation needed for installation and otherdocuments to refer to as needed.

Hardware Guides – Steps for hardware installation and unit setupintegration with other hardware.

Software Installation Guide – Step by step procedure forinstallation of the EAC software.

Other documents such as the IrisAccess® 4000 and 3000Hardware Manuals, User's Manual, Upgrade docs etc.Areavailable on the software CD.

Technical support web site knowledgebase is available 24/7

9. Installing the EAC Software

If the IP Address of the IrisServer computer is to be different from192.168.5.1 please changes the address at this time.

Install the IrisAccess® EAC Software on the IrisServer computer.

Follow the IrisAccess® EAC Software Installation Guide for software installation and configuration.— CD Key is printed on the CD case label

If required the EAC software can be installed on additional computers to serve as additional IrisEnroll, IrisManager, and IrisMonitor stations

Configuring the ICU

Configuration of the ICU requires a serial connection between the IrisServer computer and the ICU.

The ICU Serial Configuration Cable is included with each ICU. This has a 9 pin female serial connector on one end and a 6 pin Wieland connector on the other.

The serial cable is only required when programming the IP Address and the Security ID's on the ICU.
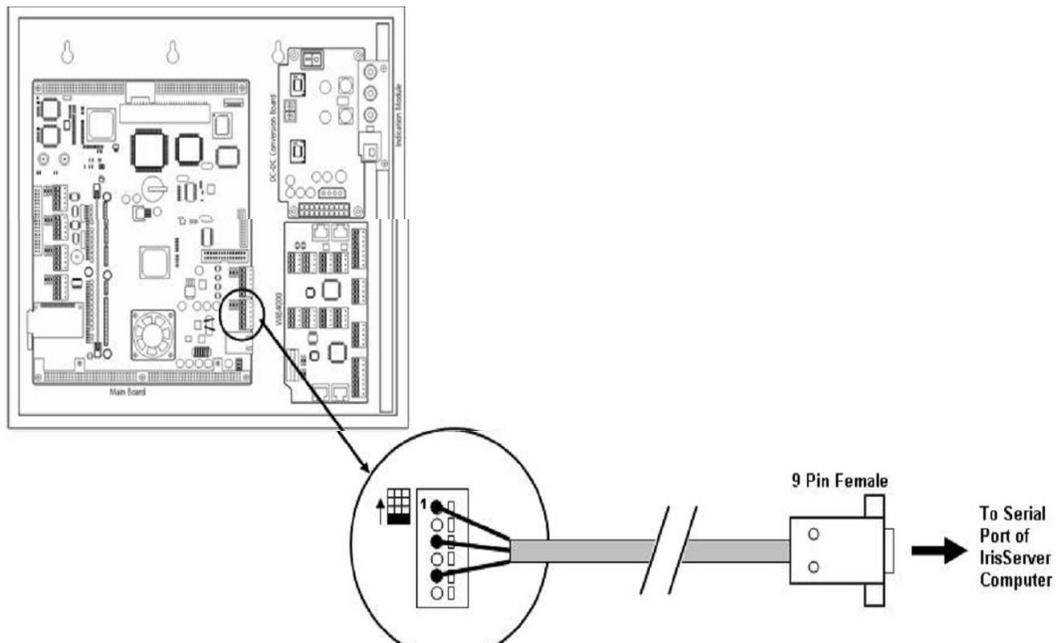
Configuring the ICU (cont'd)

The ICU is configured using the IrisICUAdmin utility.

When configuring the ICU with iCAMs use the IrisICUAdmin4000 program only.

Connect the ICU, but do notpower on the unit.

Double click on the IrisICUAdmin4000 icon. Select "New Installation" from the menu.

Enter the Server IP Address (the address entered here will be the only computer which will be allowed to communicate with the ICU) This must be the computer which will have the IrisServer program running.

ICU4000 New Installation - Config Network IP/Security ID

Configure Network IP Address

Setting for IrisServer

Server IP Address   192.168.5.1

Settings for ICU4000

ICU IP Address   192.168.5.200   ex) 160.160.97.42

Gateway Address   192.168.5.254   ex) 160.160.97.254

Subnet Mask   255.255.255.0   ex) 255.255.255.0

Disconnected   Cancel   < Back   Next >   Finish

Enter the SIDs for all four channels.

Be sure to record what has been entered for SIDs. They will need to be entered in IrisManager later and must match exactly.
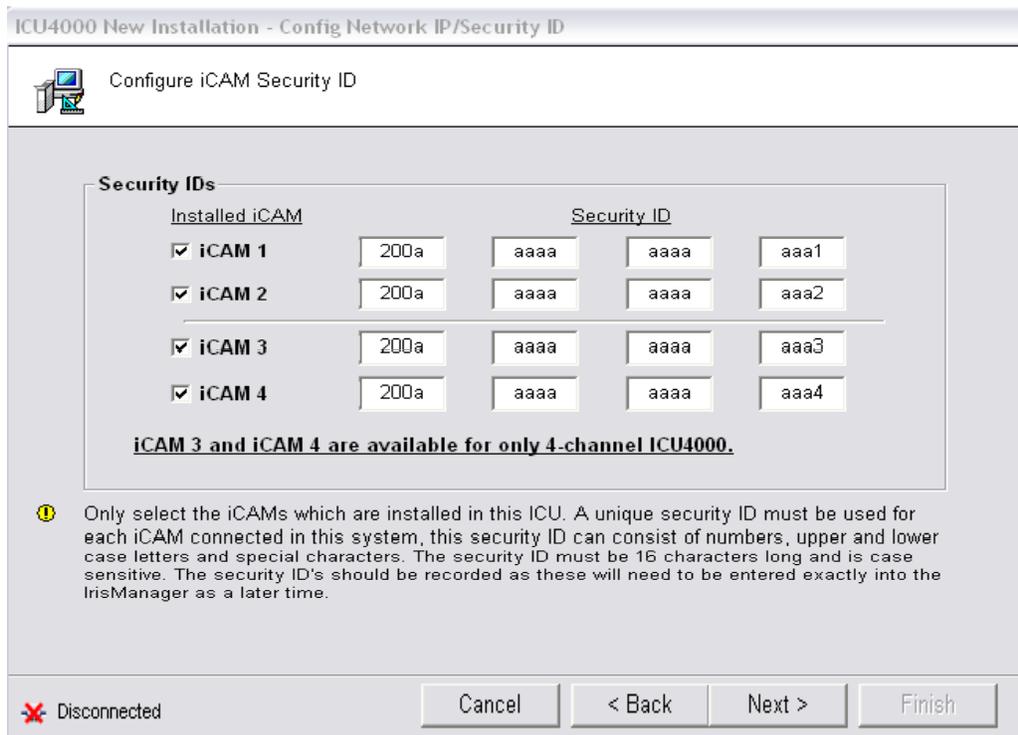
Select the COM port of the IrisServer to which the Configuration cable is connected.

Click Start, then Start and turn on the ICU.

During boot-up the ICU will look for the serial connection and will automatically start to download the configuration from the computer.

Connection and transfer should be complete within 80 seconds.

After the transfer is complete the serial cable may be removed .The rest of the ICU configuration will use the network.

Before proceeding, connect the DCU or WIB to CH1 of the ICU main board. If

using the DCU be sure that the DIP switches are in the down position. If using a WIB the DIP switches may be left in the up position.

Continue the setup by entering the password for the ICU. The default password is iris4000.

The ICU will connect over the network. Click Next to download the software into the ICU.

After the configuration files have been downloaded from the ICU c lick on configuration to modify the setting

The IP Address of the iCAM is entered into each channel of the ICU.

In this case channel 1 of this ICU will control the iCAM with the IP Address of 192.168.5.20
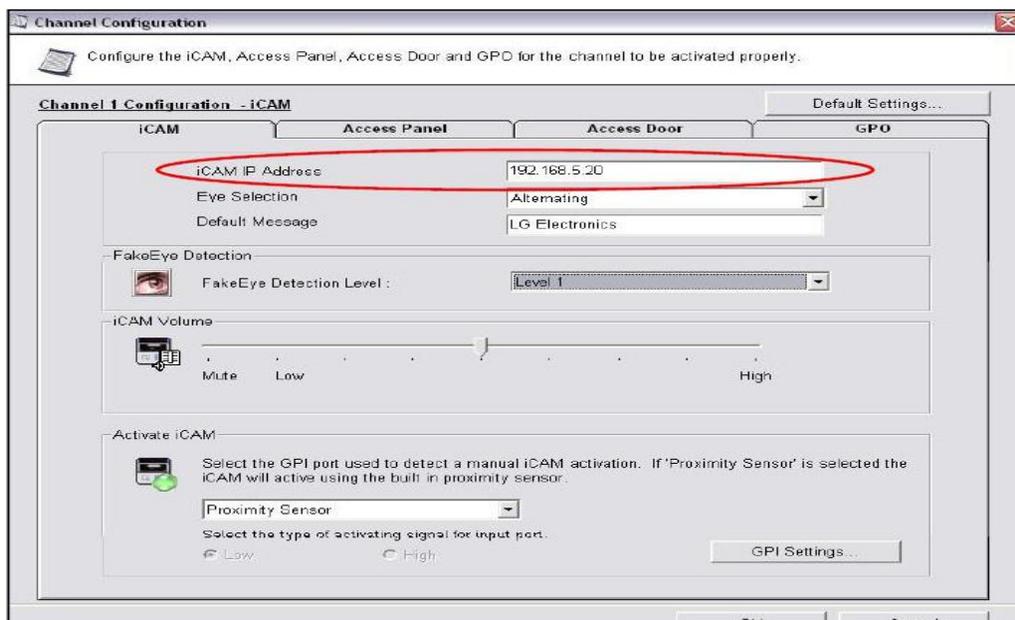
Repeat the IP Address entry for each channel of the ICU. If the channel is not

being used you may disable it by un-checking the Channel check mark.

Click next for the remaining configuration, and click Yes to reboot the ICU.

The remaining ICU's maybe configured at this time by following the same procedure.

Each ICU must have a unique IP Address and SIDs.

Do not connect more than one un-configured ICU to the network at the same time. This will cause an IP Address conflict on the network.

10. IrisServer

Starting IrisServer
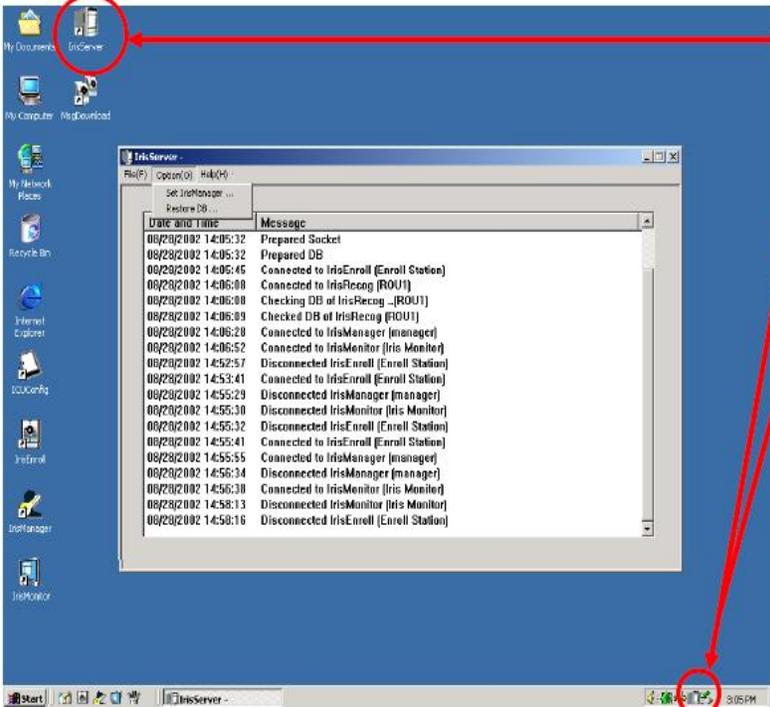
1. Double Click on the IrisServer Icon

2. IrisServer will open, then minimize to the task bar

3. Double click on the IrisServer icon to open.

4. Login with the information below when prompted.

ID: administrator
Password: iris3000

IrisServer Main Window

IrisServer should always be left running in the background (minimized).

Only one IrisServer per network.

Displays real-time database and remote unit connection status.

Helpful for troubleshooting iCAM / ICU connection problems

Date and Time	Message
08/28/2002 14:05:32	Prepared Socket
08/28/2002 14:05:32	Prepared DB
08/28/2002 14:05:45	Connected to IrisEnroll (Enroll Station)
08/28/2002 14:06:08	Connected to IrisRecog (ROU1)
08/28/2002 14:06:08	Checking DB of IrisRecog ..(ROU1)
08/28/2002 14:06:09	Checked DB of IrisRecog (ROU1)
08/28/2002 14:06:28	Connected to IrisManager (manager)
08/28/2002 14:06:52	Connected to IrisMonitor (Iris Monitor)
08/28/2002 14:52:57	Disconnected IrisEnroll (Enroll Station)
08/28/2002 14:53:41	Connected to IrisEnroll (Enroll Station)
08/28/2002 14:55:29	Disconnected IrisManager (manager)
08/28/2002 14:55:30	Disconnected IrisMonitor (Iris Monitor)
08/28/2002 14:55:32	Disconnected IrisEnroll (Enroll Station)
08/28/2002 14:55:41	Connected to IrisEnroll (Enroll Station)
08/28/2002 14:55:55	Connected to IrisManager (manager)
08/28/2002 14:56:34	Disconnected IrisManager (manager)
08/28/2002 14:56:38	Connected to IrisMonitor (Iris Monitor)
08/28/2002 14:58:13	Disconnected IrisMonitor (Iris Monitor)
08/28/2002 14:58:16	Disconnected IrisEnroll (Enroll Station)

11.IrisManager

Configuring IrisManager

This part of the setup is also covered in the EAC Software QuickInstallation Guide.

Open the IrisManager program by double clicking the desktopicon.

The system configuration is performed in IrisManager / Creationmenu.

A default configuration is created for IrisEnroll, IrisManager, andIrisMonitor. The system is configured to be able to run all programs from the IrisServer computer using the loopback IPAddress (127.0.0.1)

Since we are using only the IrisServer computer for IrisEnroll, IrisManager, and IrisMonitor we do not need to modify the default settings. If we did want to change settings we could click on the New… button to add computers or Modify… to change existing settings.

When the applications are started for the first time, the loopbackIP address (127.0.0.1) may need to be entered.

IrisEnroll4000 may require the SID to be entered:111111111111111.
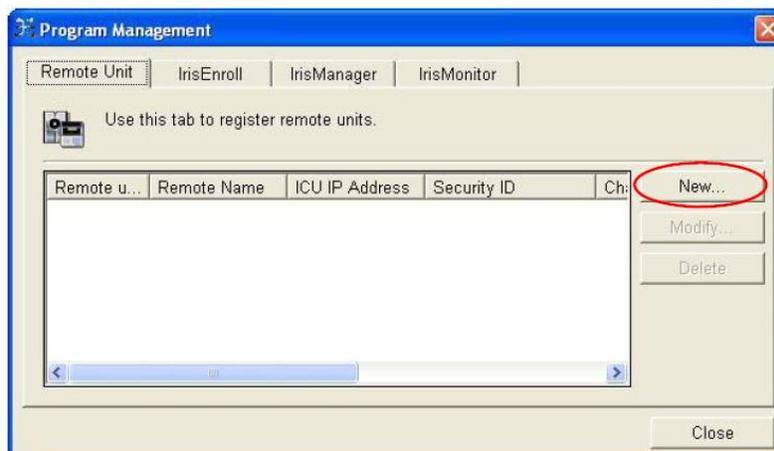
- Since we will have "Remote Units" (iCAMs protecting a door) we need to configure these in IrisManager. Click on the Remote Unit tab then the "New" button to add the configuration of the ICUs and their channels into IrisManager.

Name: Short descriptive name for the iCAM

ICU IP Address: The IP Address of the ICU which is controlling the iCAM.

Security ID: The Unique SID entered for the ICU channel during ICU configuration.

Description: Optional field for other information. Putting the iCAM IP Address here will assist in troubleshooting.

Channel ID: Channel of ICU which is controlling the iCAM.

Use Type: no effect

Model: Selects the icon type shown for this remote unit.
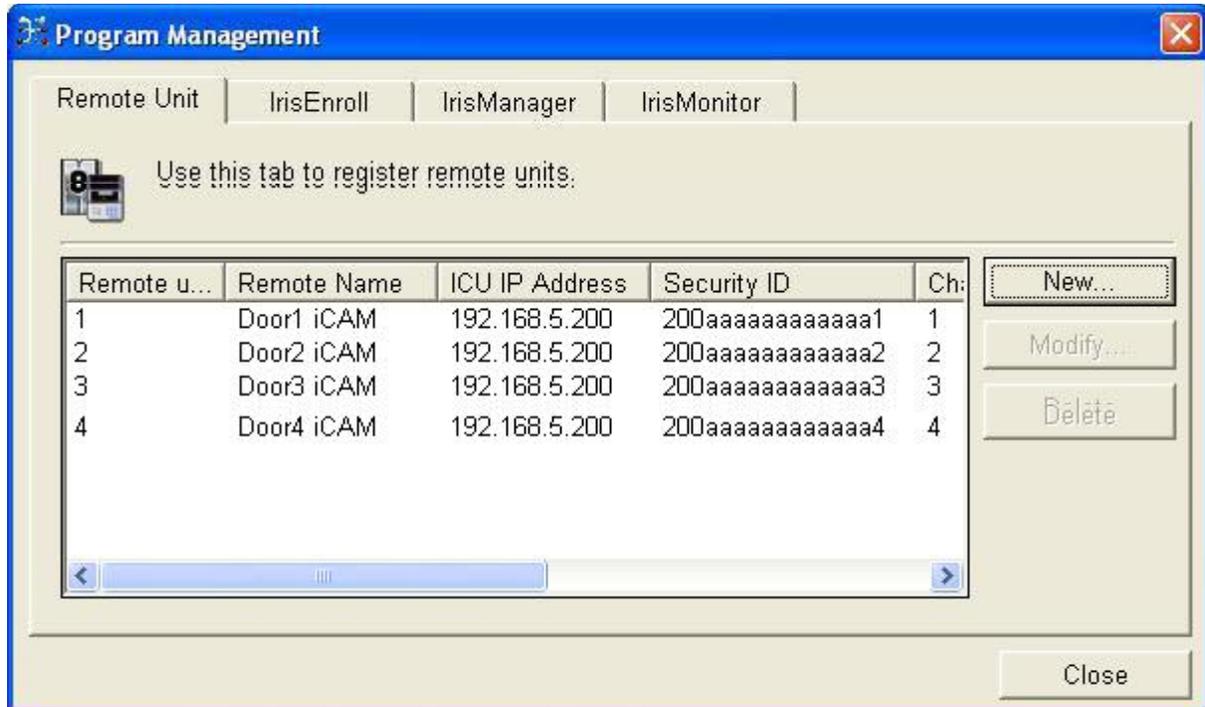
Complete the entries for each ICU and ICU channel that will make up the system.

12. IrisEnroll4000

• Enrollment

• Identification

• Verification

• Card

• Live

• Options

- When enrolling a user you will select Enroll from the main screen.
- The user will be prompted to present their iris to the iCAM.
- Upon successful iris capture you will receive a window indicating the quality of the image.
- Verification of the user is then required.
- Once the user is verified you can continue by filling in user information.

- Enter the **User ID** and then click the **Get user information** button.

- Optional entries:
  - First name, MI and Last name
  - Card reader ID and Card Number
  - Gender (Male/Female)
  - Photo (allows an image to be associated with the user being enrolled)

- Click Next to enter additional user information. (department, position, phone, email, address, etc.)

- Enter the **User ID** and then click the **Get user information** button.

- Optional entries:
  - First name, MI and Last name
  - Card reader ID and Card Number
  - Gender (Male/Female)
  - Photo (allows an image to be associated with the user being enrolled)

- Click Next to enter additional user information. (department, position, phone, email, address, etc.)

- Users should be assigned a remote group and time group.
- Visitors (users with temporary access rights) should be assigned to a remote group with set terms and reservation times. Select the Calendar button to select dates the user will be granted access.
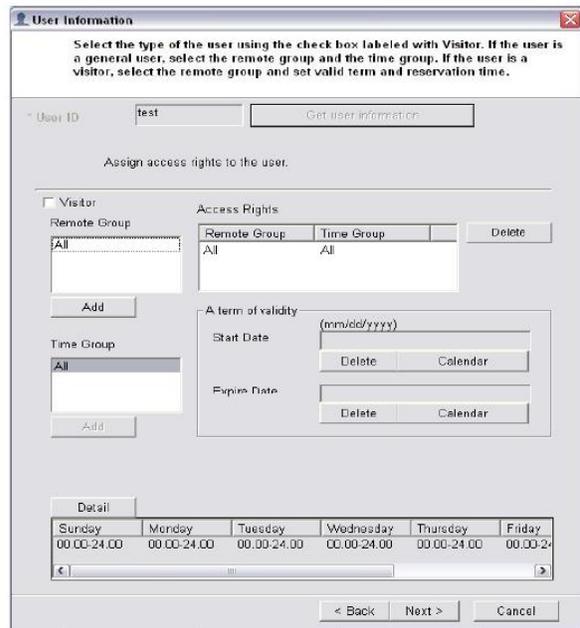
13. Identifying a User

- Select the **Identify** icon from the tool bar on the main screen.
- Click the start button and have the user present their iris to the iCAM. (the process of identifying will continue until the operator hits the stop button)
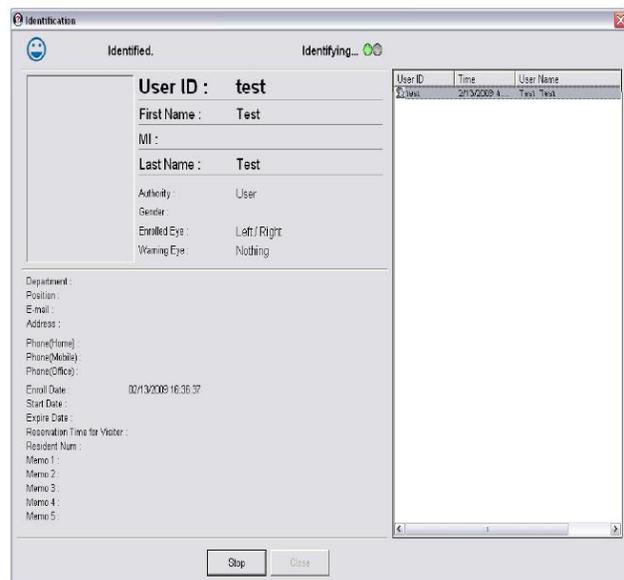
Verifying a User

- Select verify from the tool bar on the main screen.
- Enter the User ID and click Verify to being the Iris image capture process.
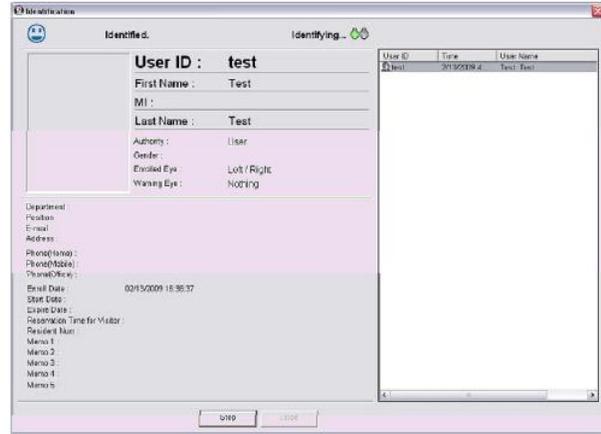
Once the Iris image is captured the results will display in a verification window.

IrisEnroll4000 Options

- This screen provides the function of changing iCAM settings such as:
  - Sound Volume
  - VFD Message
 - Using white LED's during image capture.

IrisEnroll4000 Options (cont'd)

- In this tab a user can set which eye should be considered when identifying and verifying, Left, Right, Both or Either. The user can also set which eye should be enrolled Left Right or both.
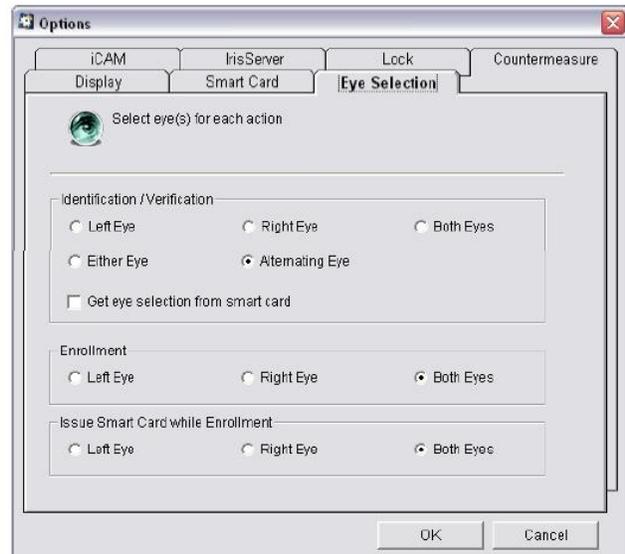
- When selecting the "Detect fake eye." option, fake eyes will be detected when a user tries to enroll, identify or verify.
- When selecting "Don't detect fake eye" no countermeasures will be considered when a user tries to enroll, identify or verify.
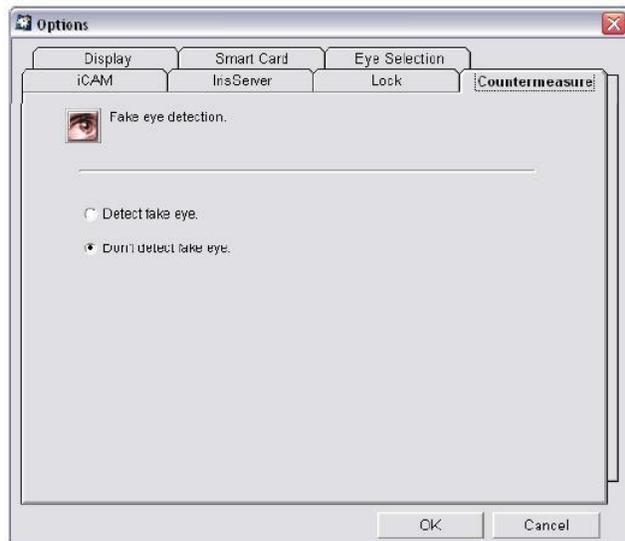
Testing the System

- At this point the IrisServer and ICUs should be able to communicate. Open IrisServer (double click on icon near taskbar clock), and view the messages in IrisServer for errors.
- Open the IrisEnroll4000 application, when prompted for an IP Address, enter the IP Address for the iCAM which will be used for enrollment.
- Perform a self enrollment, to test IrisEnroll and iCAM operation. Set permissions to All time, All remotes.
- Perform a recognition on an iCAM controlled by the ICU.
- If a DCU is connected listen for the relay click when a recognition is performed.

14.IrisMonitor

IrisMonitor Screen

The status of units and software applications.

Example: Remote(0/2) means that 2 Remote units are configured and neither is connected to the IrisServer.

User Activity monitor. Provides real time status of user activity and warnings.

System Activity monitor. Provides real time status of system activity and warnings.
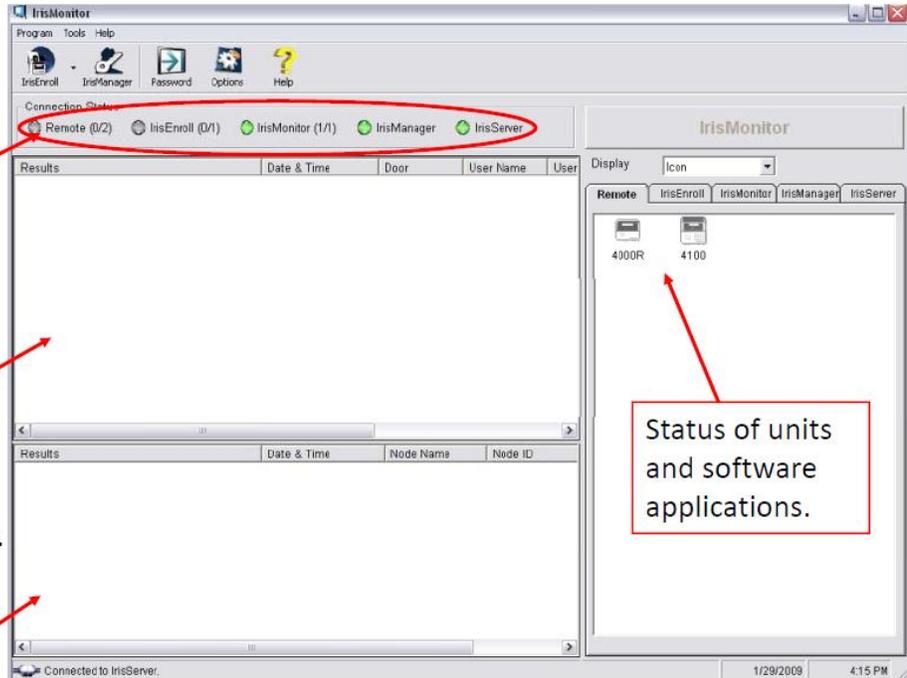
Status of units and software applications.

IrisMonitor Warning

IrisMonitor provides visual and audible alerts for user and system conditions.

The Warning button will flash Red on the IrisMonitor main screen and provide audible alarm using the computer sound output.

Alert conditions are selectable in the IrisMonitor – Options screen.
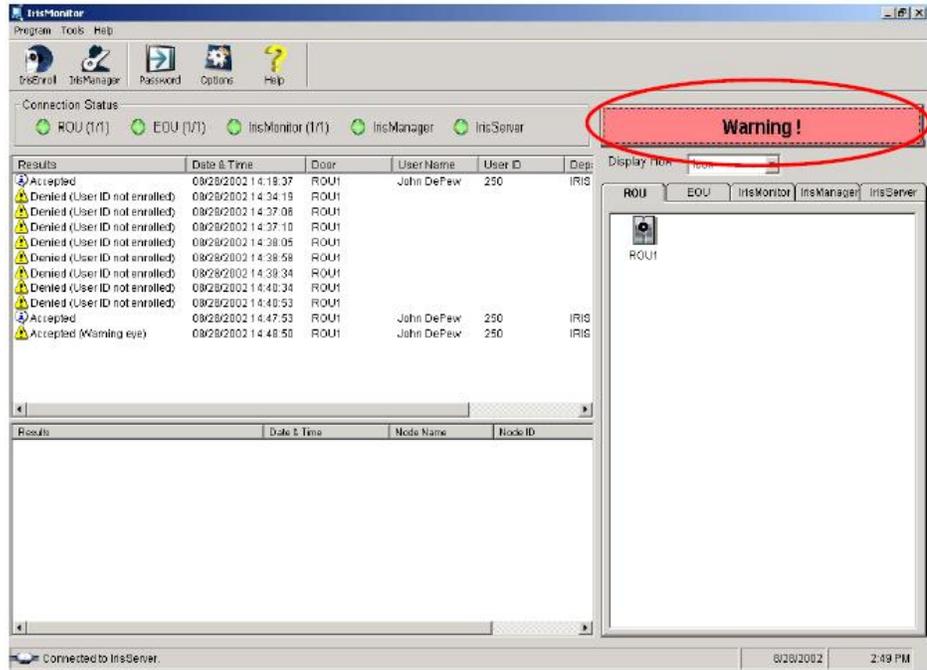
IrisMonitor Options
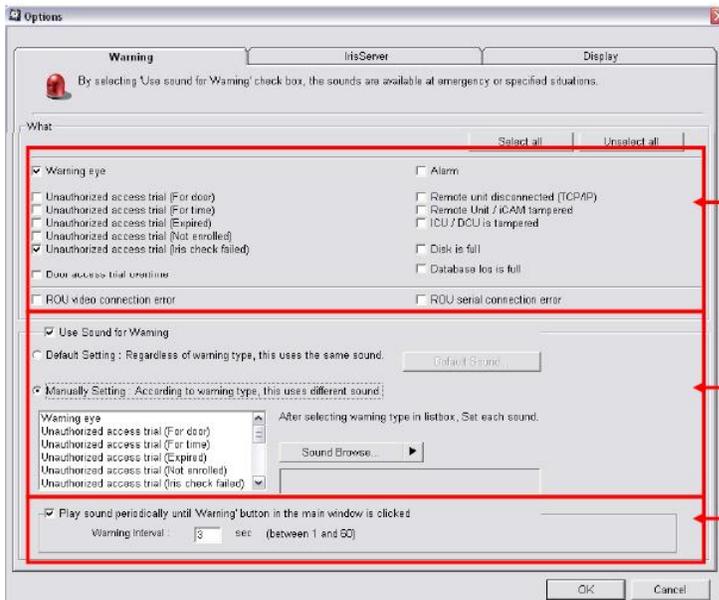
Select which events will trigger an alert.

Sound file to play for each different condition. Allows to browse and test the sound file.

Duration of the Sound file played and whether it will be continuous.

IrisManager

IrisManager

To start IrisManager, Double click on the IrisManager icon on the desktop. Enter ID: administrator, Password: iris3000

User Icons

(Orange): Operator

(Orange): Unauthorized Operator because iris is not enrolled.

(Orange): Unauthorized Operator because Remote or Time Group is not assigned to this user.

(Black): General User

(Black): Unauthorized general user because iris is not enrolled.

(Black): Unauthorized general user because Remote or Time Group is not assigned to this user.

(Green): Visitor

(Green): Unauthorized visitor because iris is not enrolled

(Green): Unauthorized visitor because remote group or reservation time is not assigned to this user.

* Note: Starting in EAC v3.0 a Blue user icon is available. This blue icon indicates that the users term of validity is expired.

Setting Users Access Rights
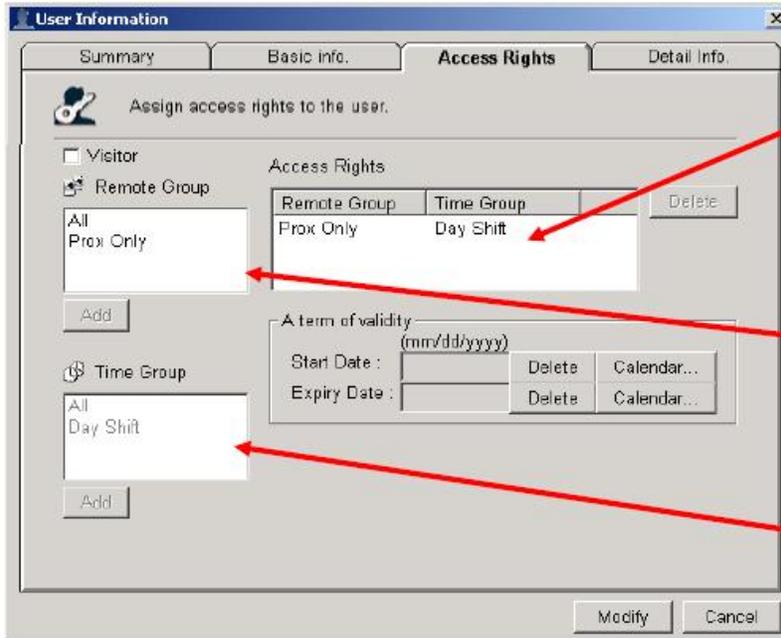
The selected Remote and Time group will be listed here. You can assign multiple groups to one user.

Select the Remote Group the user will have permission too. Click Add

Select the Time Group the user will have permission too. Click Add

The term of validity can also be set so that the users permission will automatically expire.

Setting Visitor Access

Select Visitor to set user active on a temporary basis.

Access Rights Assigned

Validity Settings

Start and Expire Dates

Start and Expire Times

Users Multi-Assignment

- Changes to multiple user accounts can be made at one time.
- Multiple users in the list can be selected by selecting the top user then hold shift key and click on bottom user.
- Multiple users can be individually selected by holding down the CTRL key while selecting
- While the users are selected click User – Multi-assign on menu bar.
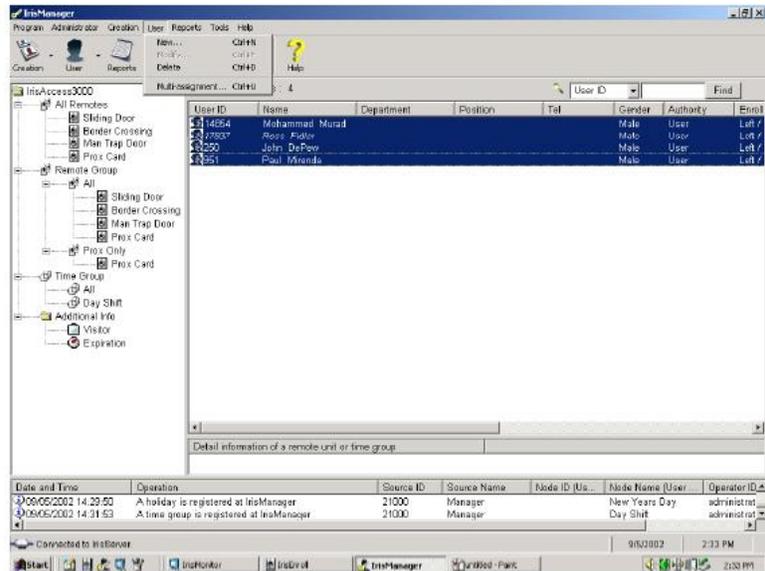
Edit Multi-Assignment

- In Multi-assign mode you can change access rights to several users at one time.

The list of users that have been selected.

Administrators and Operators

Administrator	
Operators...	Ctrl+O
Operation log...	Ctrl+L
Security Setting...	
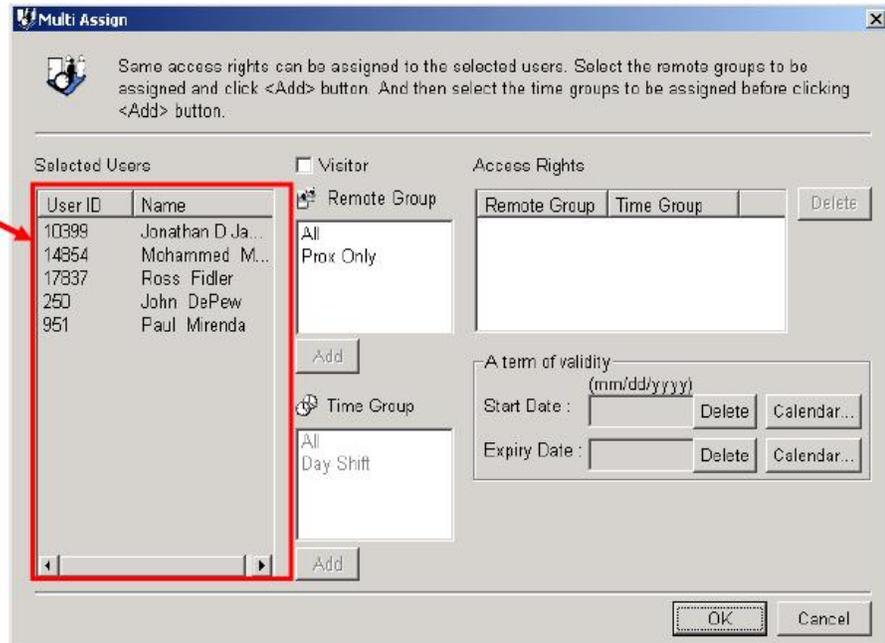
From menu bar select Administrator then click operators.

By default there is an administrator option called "administrator" (This is the account used to log into the IrisAccess applications).

This screen is used to create other administrators and operators that will be able to log in and use the IrisAccess applications.

Administrator Vs. Operator

Administrators can control all options available in the IrisAccess software, including system configuration.

Operators have limited access to applications and reduced available functions within IrisManager (set by an administrator).

Setup Operators

New – Create Admin/Operator

Modify – Modify existing Admin/Operator

Delete – Delete existing Admin/Operator
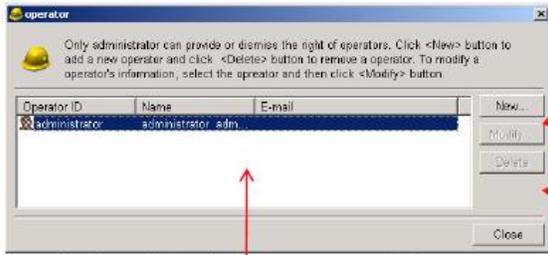
The existing Administrators and Operators

Operator ID – The username used to open the IrisAccess applications.

Optional User ID – The user ID that the operator uses for iris access.

Password – Password used to access application.

Operator Authority
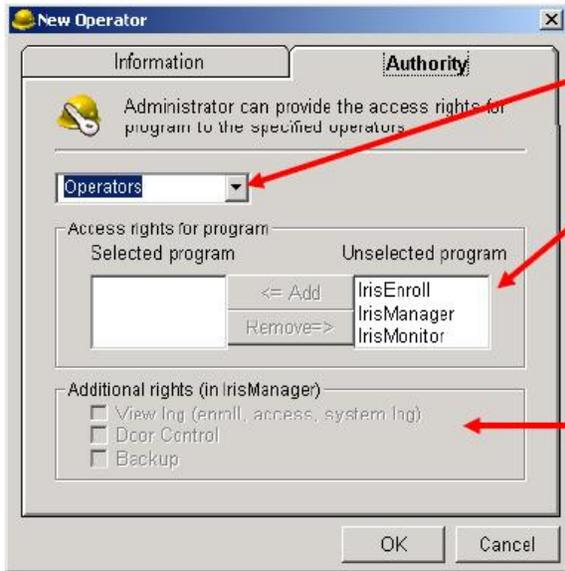
Operator or Administrator privileges

Programs that operator not able to access. Click Add to give operator access.

Functions within IrisManager that operator will be able to access.

View log (view reports)   Door Control (able to open doors) Backup(can run database backup)

Operator Level IrisManager
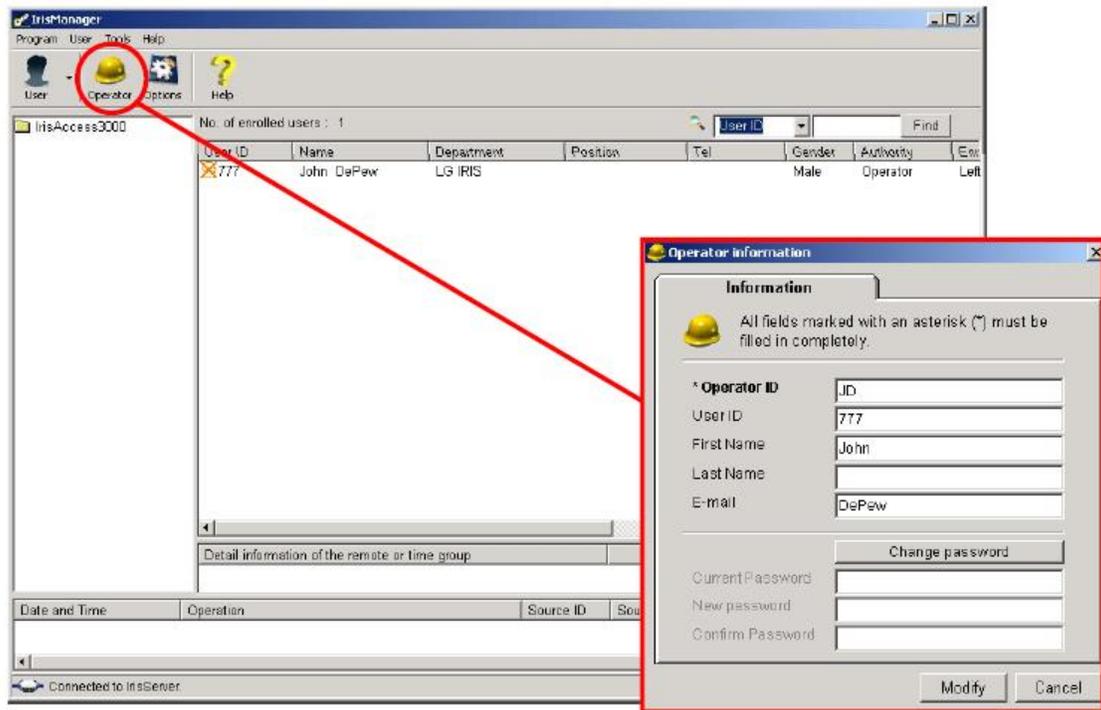
This is a restricted operator screen (no configuration or report permissions)

Setup Remote Groups
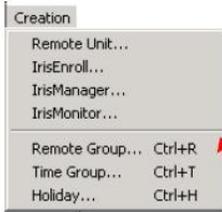
Click on Creation in the menu bar and select Remote Group

New – Create new group.

Modify – Modify existing remote group.

Delete – Delete existing remote group.

IRIS Access System Configuration and Installation

Setup Remote Groups

Creation
Remote Unit...
IrisEnroll...
IrisManager...
IrisMonitor...
Remote Group...   Ctrl+R
Time Group...   Ctrl+T
Holiday...   Ctrl+H

Click on Creation in the menu bar and select Remote Group

Group

| Remote Group | Time Group | Holiday |

Remote groups can be created, modified or deleted. To check the list of remote units assigned to the remote group after creating, click the remote group in the list of Remote Group.

Remote Group

Group

New...

Modify...

Delete

Close

New – Create new group.

Modify – Modify existing remote group.

Delete – Delete existing remote group.

Making Remote Groups

New Remote Group

ID

Name :

Description

Select remote unit

Selected Remote Unit

<= Add

Remove=>

Unselected Remote Unit

Border Crossing
Man Trap Door
Prox Card
Sliding Door

OK   Cancel
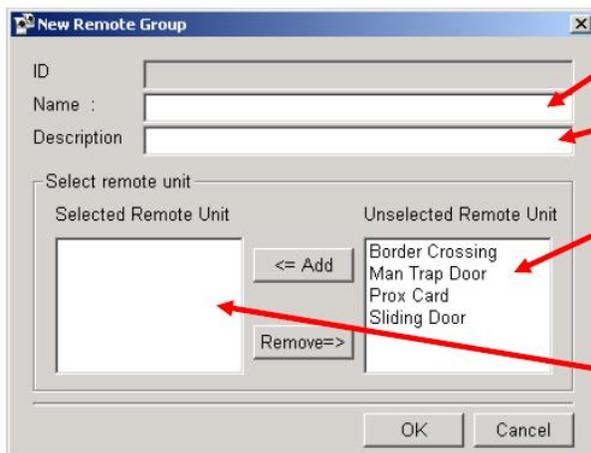
Enter Remote Group name

Description is optional

Select the iris cameras which you want to add to the group.

Selected iris camera will appear here.

Setup Holidays
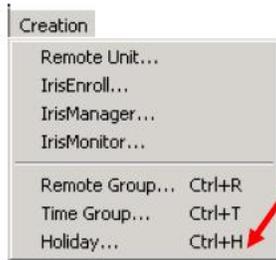
Click on Creation in the menu bar and select Holiday.
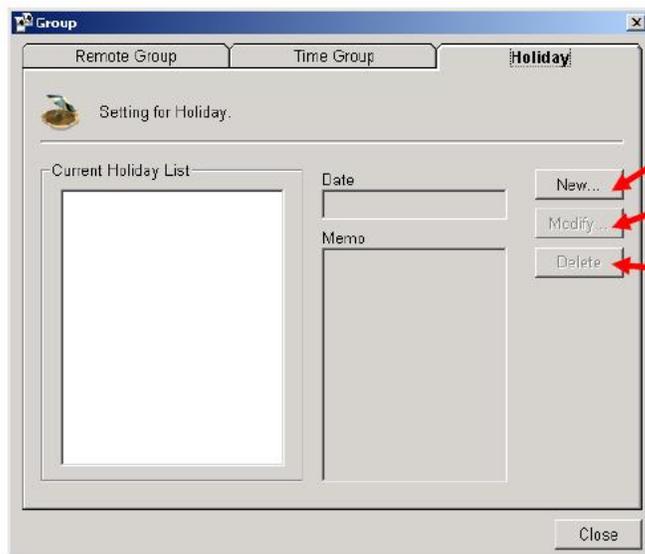
New – Create new Holiday.

Modify – Modify existing Holiday.

Delete – Delete existing Holiday.

Entering a Holiday

The date selected as a Holiday will use the defined holiday time schedule set up in the time group.

Reports

IrisAccess® EAC software has four different reports. All reports are filterable, printable, and exportable to Microsoft Excel (Excel must be installed on system)

- Enroll report – All enrollment activity
- Access report – All door access history including rejection, warning eyes, etc.
- System report – All system operations, including remote unit connection / disconnection.
- Operator log – Operator and Administrator activity. What operations were performed while operator was logged on.

15.Iris DBAdmin

IrisDBAdmin

- The IrisDBAdmin utility is used to manage the IrisAccess® Database.
- The options available in IrisDBAdmin is determined by the DBMS type used for the IrisAccess® Database.
- With a MS Access DB only Upgrade, Import, or Backup DB functions are available.
- MS SQL and Oracle 9i have all IrisDBAdmin functions available.
- For upgrade, import, backup, and merge the IrisServer program must first be stopped.

- To open the program double click on the IrisDBAdmin icon located on the desktop.
- When IrisDBAdmin is started the program will prompt for the location of the DB to be administered.
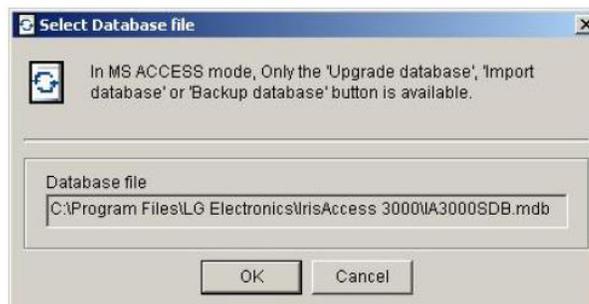
IrisDBAdmin Main Menu

Create Database – Creates DB in SQL and Oracle.

Drop Database – Erases DB in SQL and Oracle.

Upgrade Database – Upgrades a older IrisAccess DB to the v1.241 format.

Import Database – Import DB from previous stored DB
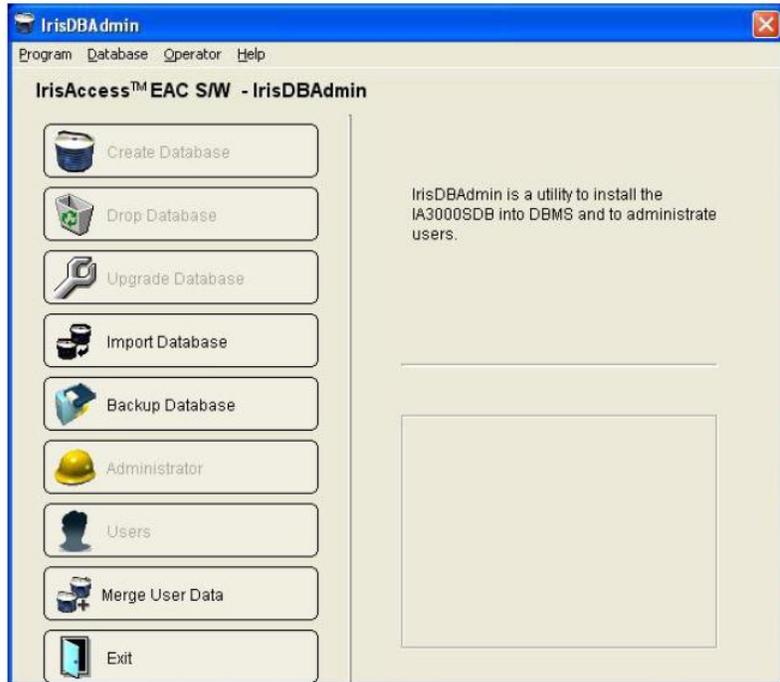
Backup Database – Backup current DB and Log files.

Administrator – SQL and Oracle DB administration.

Users – SQL and Oracle user access.

Merge User Data – To merge an existing IrisAccess DB into the active IrisAccess DB.
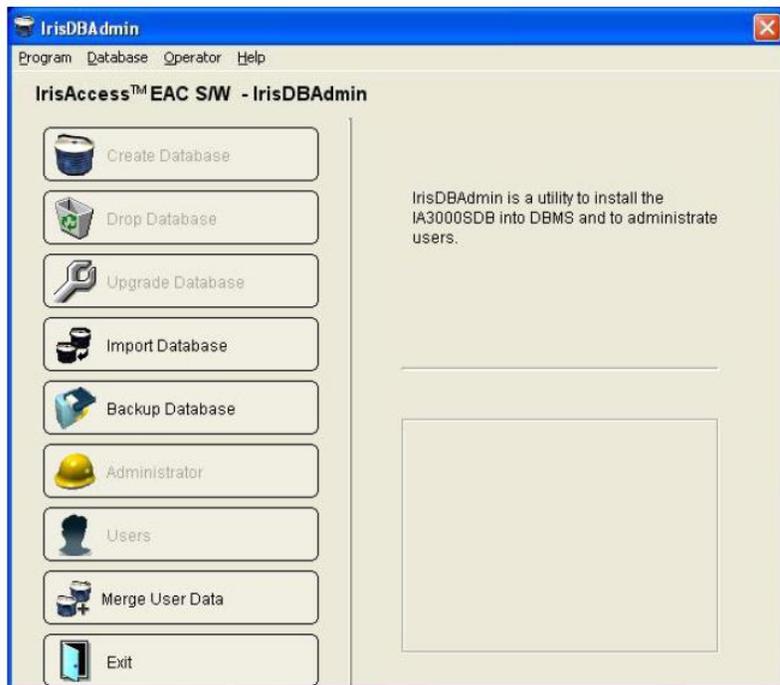
IrisDBAdmin - Backup

Backup creates a backup copy of the IrisAccess database to the specified location. This backup must be initiated manually.

Enter destination path

Enter destination filename

We recommend backing up the DB after new enrollments or at least once a month. IrisMonitor will report if DB allocation is reaching its limit and needs to be backed up immediately.

Backup Log copies and cleans up the system log file database to the specified location. This backup must be initiated manually.

Enter destination path

Filename is created automatically

IrisDBAdmin - Merge

Merge allows an existing IrisAccess® DB to be merged with the active IrisAccess® database

Access Rights of users when imported ⟶

Overwrite existing users if matched ⟶

Location of merge log files ⟶

Type of database being merged and location. ⟶
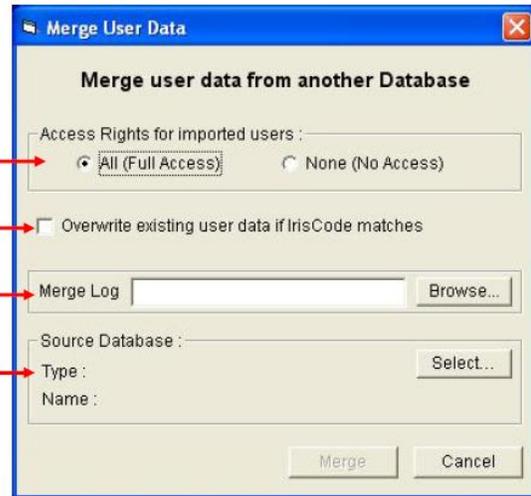
Select the database type and DB location.
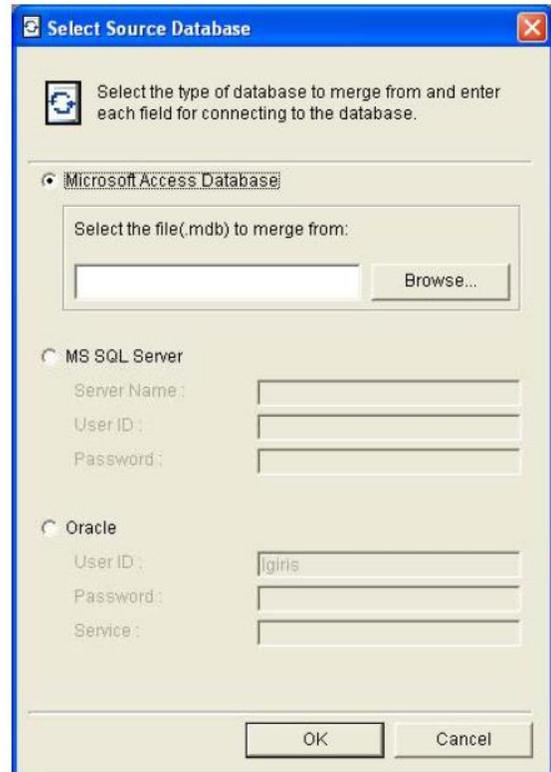
16. Technical Support

Iris ID support web site: www.irisid.com, click on Support &Service. Knowledgebase answers available 24 x 7 x 365.