

Information Technology Department

Government Of Sindh



IRIS Access

Configuration & Installation

Biometric Identification Electronic System

ADP: 1488

Year: 2009-2010

Prepared By:

INFOTECH

TABLE OF CONTENTS

<u>IRIS Access 4000.....</u>	<u>3</u>
<u>The IRIS Access 4000 EAC System</u>	<u>5</u>
<u>Intuitive User Interface.....</u>	<u>6</u>
<u>iCam4000 IRIS Camera.....</u>	<u>7</u>
<u>Inside iCam 4000.....</u>	<u>8</u>
<u>Use of Iris Access.....</u>	<u>10</u>
<u>Prepared Iris Server Pc.....</u>	<u>11</u>
<u>Preparing for Installation.....</u>	<u>16</u>
<u>Installing the EAC Software.....</u>	<u>17</u>
<u>Iris Server.....</u>	<u>23</u>
<u>Iris Manager.....</u>	<u>25</u>
<u>Iris Enroll 4000.....</u>	<u>27</u>
<u>Identifying User.....</u>	<u>31</u>
<u>Iris Monitor.....</u>	<u>35</u>
<u>Iris DBA Admin.....</u>	<u>51</u>
<u>Technical Support</u>	<u>56</u>

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 solution that works with many leading cards, card readers and or pin input devices for verification, the IrisAccess 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.

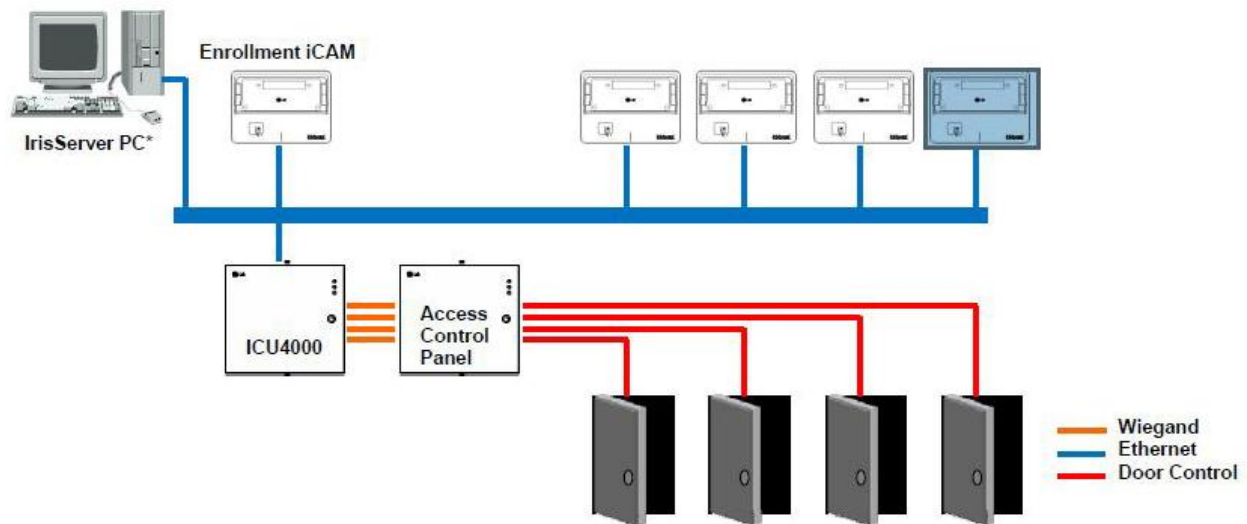
The IrisAccess® 4000 solution is versatile and flexible allowing easy integration and expansion into a range of applications. An intuitive user interface, with visual and audible prompts enables users to be enrolled and identified more easily and more quickly at an affordable price. A powered, auto-tilt 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.

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.

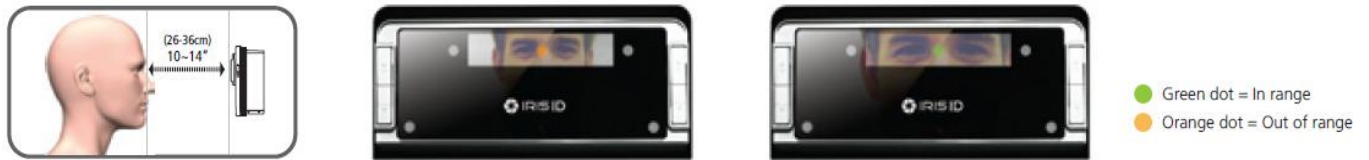
Every iris pattern is unique and stable for life barring direct trauma. Since there are more readily measurable characteristics in the iris, iris recognition is the most accurate, fastest, and scalable option for small and large scale biometric deployments. Finger, hand, voice, vein and facial characteristics 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	Power (Blue), Accept (Green), Reject (Red)
Range LED	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

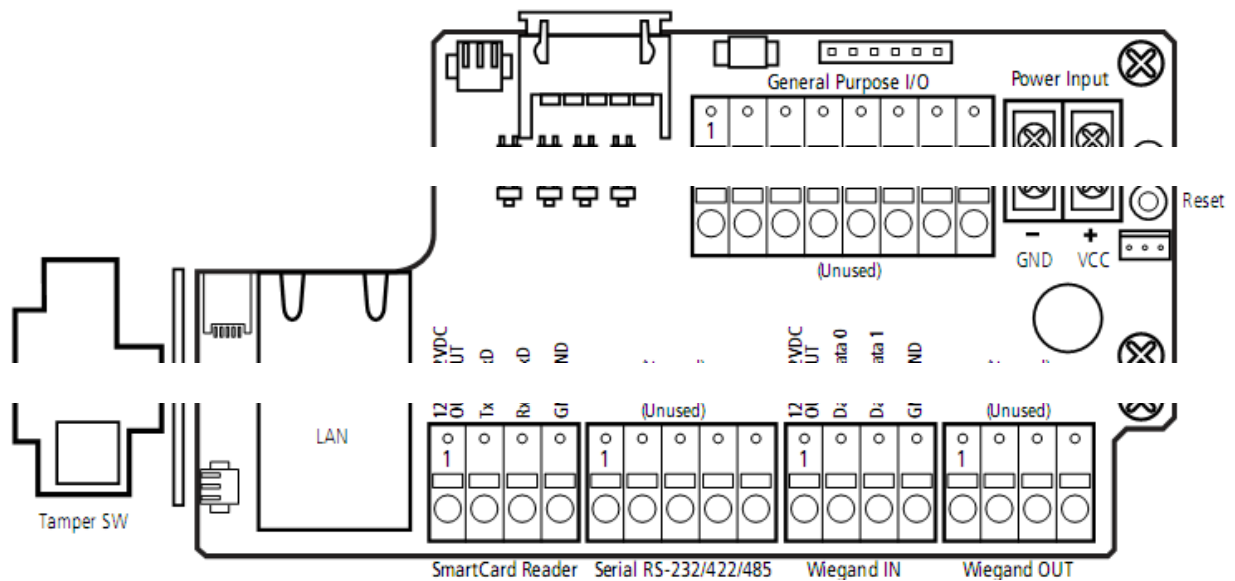
- AC Power Cord
- AC Power Adapter
- Straight Ethernet Cable

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



Training 3

Installation and Dimension

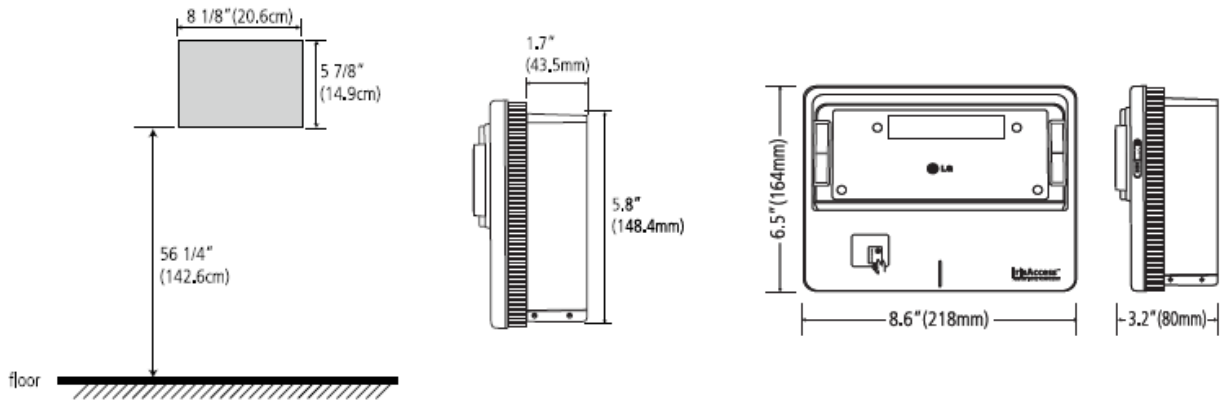


Illustration of mounting prep depth requirements with flush mount to wall.

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

6. Use of IrisAccess



Building Security



Transportation Security



Laboratory Security



Infrastructure Security



Public Safety & Justice



Time & Attendance



Border Control



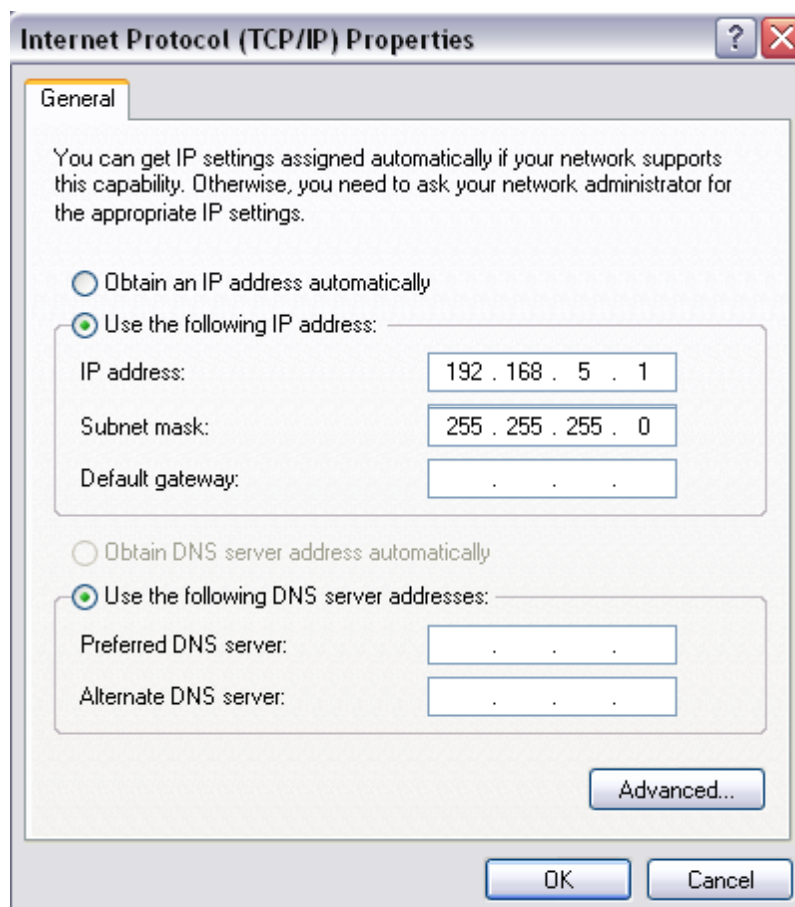
Data Center Security

System Configuration and Setup

7. Prepare the IrisServer PC

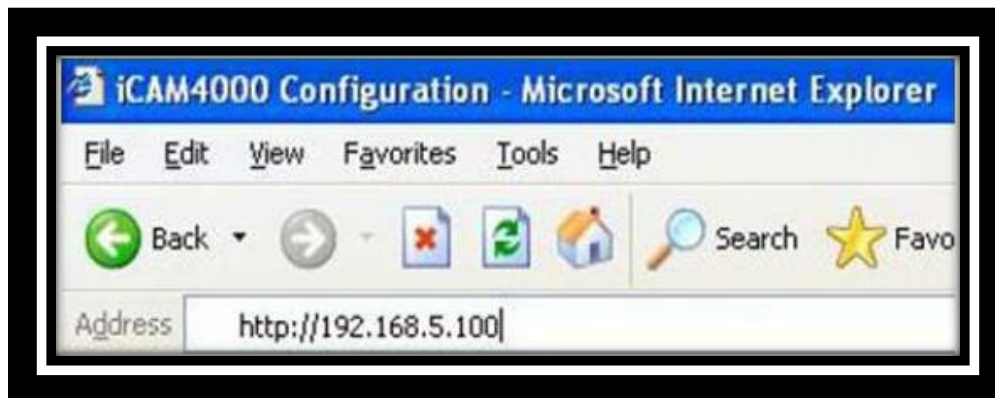
In order to configure the iCAM iris cameras, the IrisServer computer must be given the static IP Address of 192.168.5.1

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.



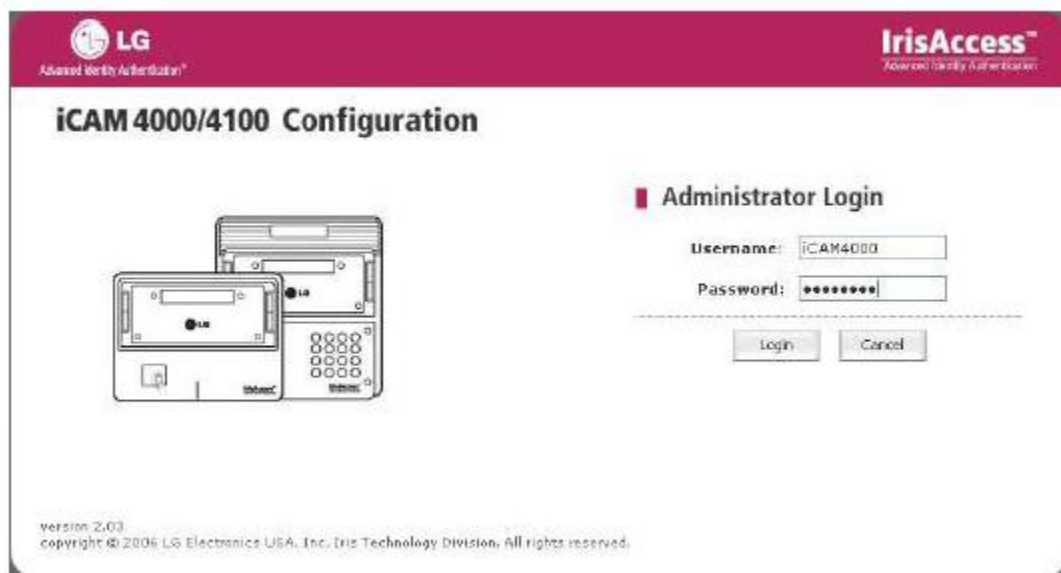
Configuring the iCAM IP Address

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>



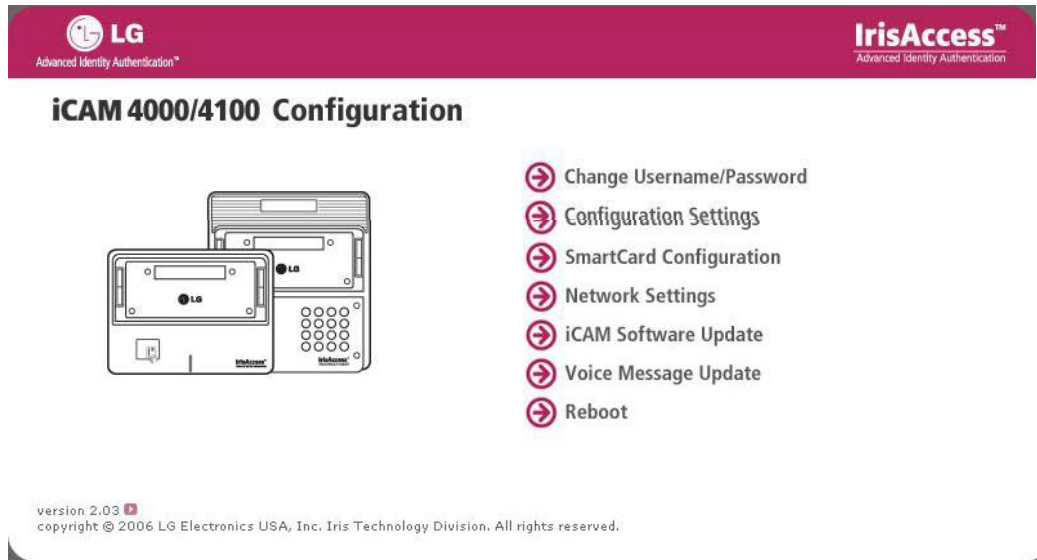
At the log in screen enter the

Username: iCAM4000 and the password: iris4000. Click Login



Steps for Changing iCAM IP Address

At the menu select “Network Settings”



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

The screenshot shows the 'iCAM 4000/4100 Configuration' screen with the 'Network Settings' option selected, indicated by a red square icon. The title 'iCAM 4000/4100 Configuration' is at the top. Below the title, the 'Network Settings' section contains four input fields:

- IP Address: 192.168.5.100
- Subnet Mask: 255.255.255.0
- Broadcast Address: 192.168.5.255
- Default Gateway: 192.168.5.254

Below the input fields are three buttons: 'OK', 'Clear', and 'Back to Main'. At the bottom left, the version information is shown: 'version 2.03' and 'copyright © 2006 LG Electronics USA, Inc. Iris Technology Division. All rights reserved.'

Steps for Changing iCAM IP Address (cont'd)

The IP Address is changed within seconds.

After each iCAM configuration the arp cache on the computer must 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 and perform the configuration to the next iCAM.

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

8. Preparing for Installation

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

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

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

Other documents such as the IrisAccess® 4000 and 3000 Hardware Manuals, User's Manual, Upgrade docs etc. Are available 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 from 192.168.5.1 please change 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

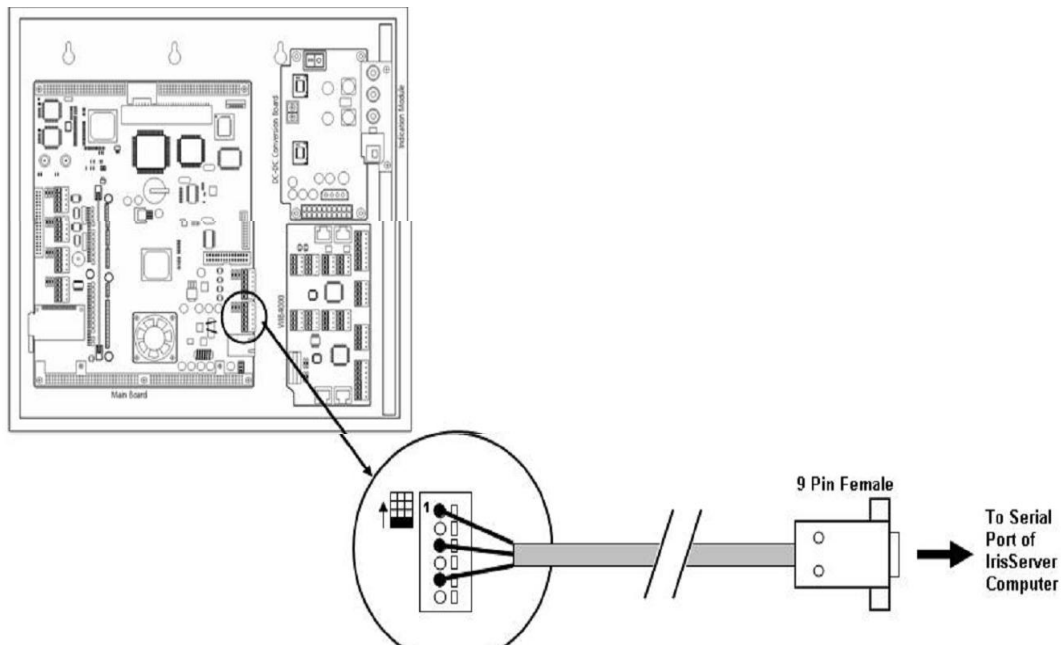
If required the EAC software can be installed on additional computers to serve as additional IrisEnroll, IrisManager, and IrisMonitor stations

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 not power 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.

Training 3

ICU4000 New Installation - Config Network IP/Security ID

 **Configure Network IP Address**

Setting for IrisServer


Server IP Address

Settings for ICU4000

ICU IP Address ex) 160.160.97.42

Gateway Address ex) 160.160.97.254

Subnet Mask ex) 255.255.255.0

 Disconnected

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.

Installed iCAM	Security ID
<input checked="" type="checkbox"/> iCAM 1	200a aaaa aaaa aaa1
<input checked="" type="checkbox"/> iCAM 2	200a aaaa aaaa aaa2
<input checked="" type="checkbox"/> iCAM 3	200a aaaa aaaa aaa3
<input checked="" type="checkbox"/> iCAM 4	200a aaaa aaaa aaa4

iCAM 3 and iCAM 4 are available for only 4-channel ICU4000.

Only select the iCAMs which are installed in this ICU. A unique security ID must be used for each iCAM connected in this system, this security ID can consist of numbers, upper and lower case letters and special characters. The security ID must be 16 characters long and is case sensitive. The security ID's should be recorded as these will need to be entered exactly into the IrisManager as a later time.

Disconnected Cancel < Back Next > Finish

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

Training 3

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.

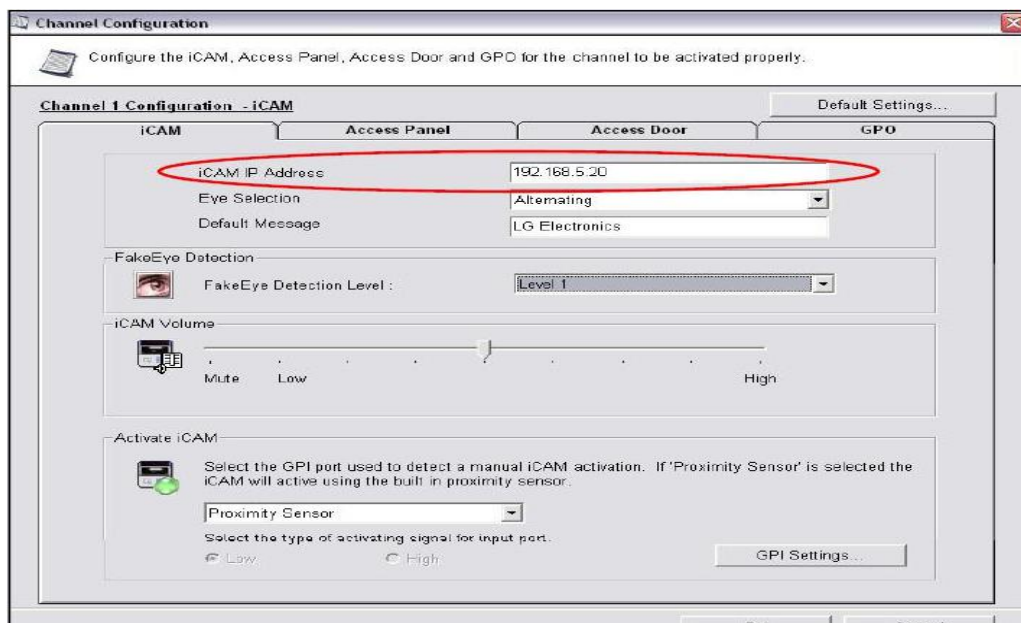
Continue the setup by entering the password for the ICU. The default password is iris4000.

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 click 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

Training 3

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.

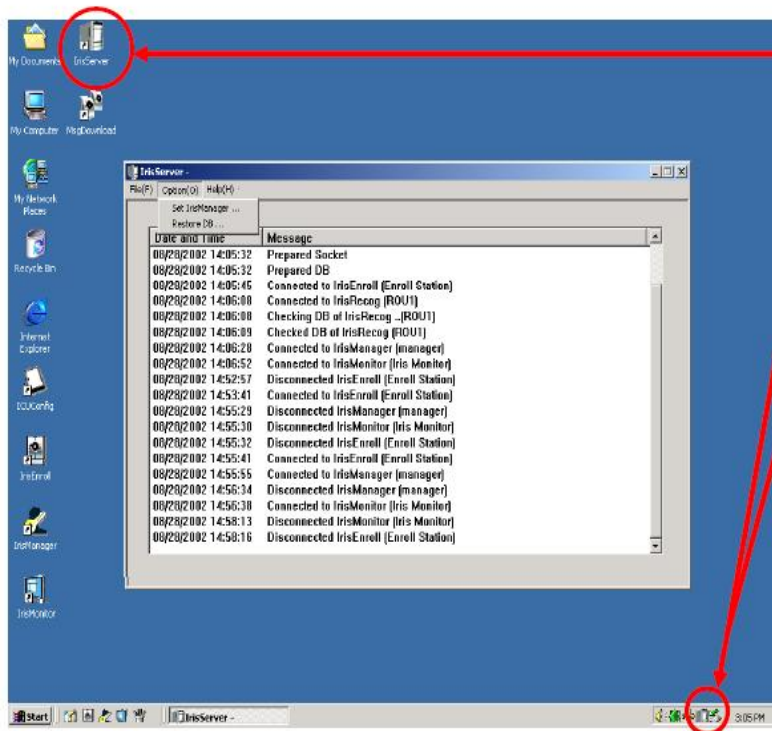
The remaining ICU's maybe configured at this time by following the same procedure.

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

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 14:05:50	Connected to IrisRecog (ROU1)
08/28/2002 14:05:50	Checking DB at IrisRecog - (ROU1)
08/28/2002 14:05:50	Checked DB at IrisRecog (ROU1)
08/28/2002 14:05:52	Connected to IrisManager (manager)
08/28/2002 14:05:52	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 14:53:29	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 14:55:34	Disconnected IrisManager (manager)
08/28/2002 14:55:38	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)

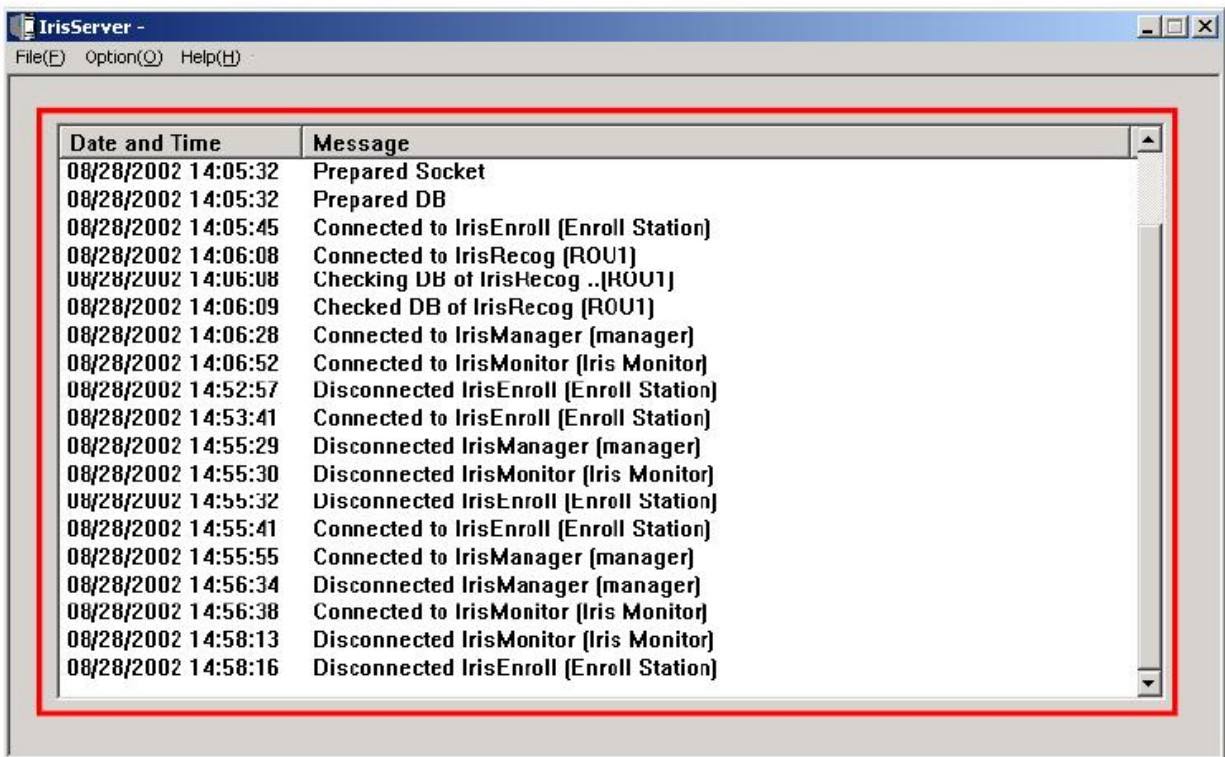
IrisServer Main Window

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



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 desktop icon.

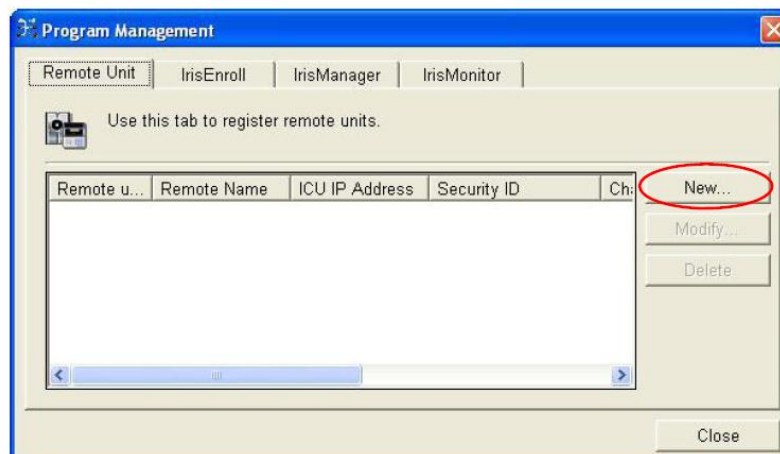
The system configuration is performed in IrisManager / Creation menu.

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

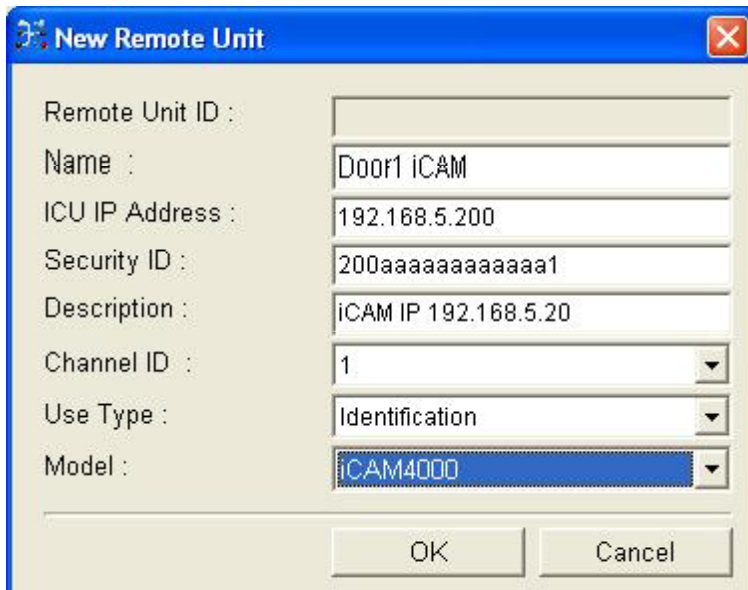
Since we are using only the IrisServer computer for IrisEnroll, IrisManager, and IrisMonitor we do not need to modify the default settings. If we did want to change settings we could click on the New... button to add computers or Modify... to change existing settings.

When the applications are started for the first time, the loopback IP 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.



New Remote Unit

Remote Unit ID :

Name :

ICU IP Address :

Security ID :

Description :

Channel ID :

Use Type :

Model :

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.

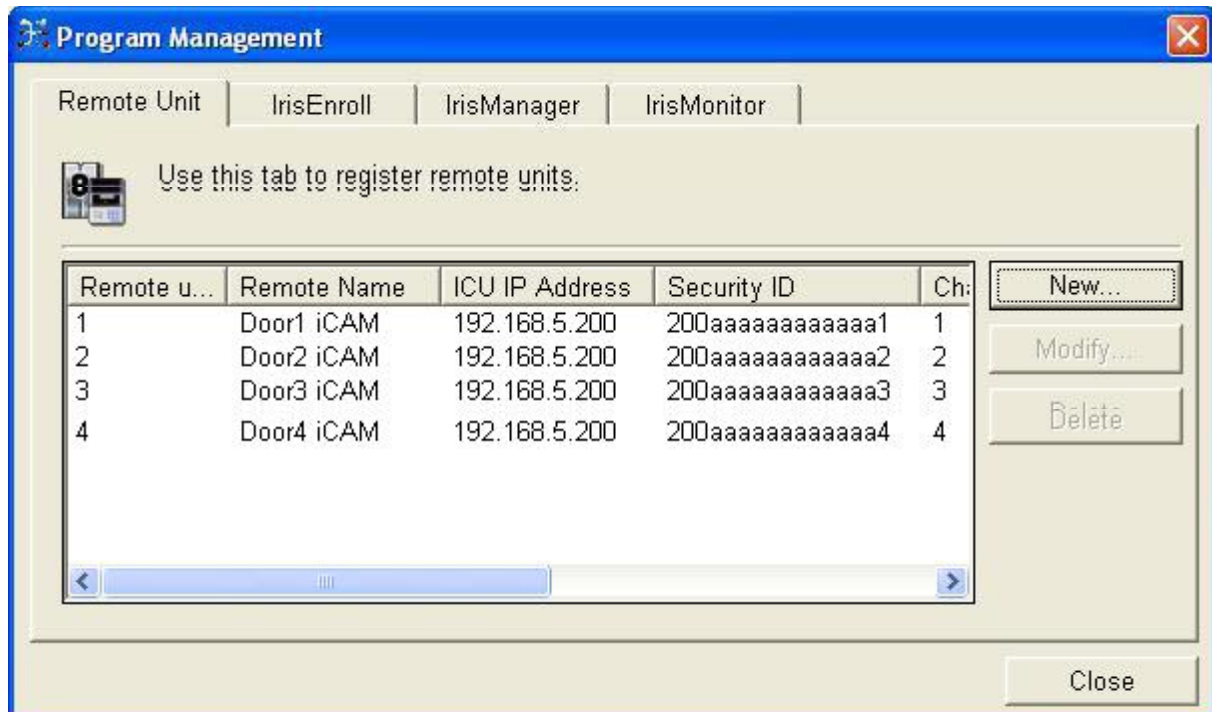
Description: Optional field for other information. Putting the iCAM IP Address here will assist in troubleshooting.

Training 3

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.

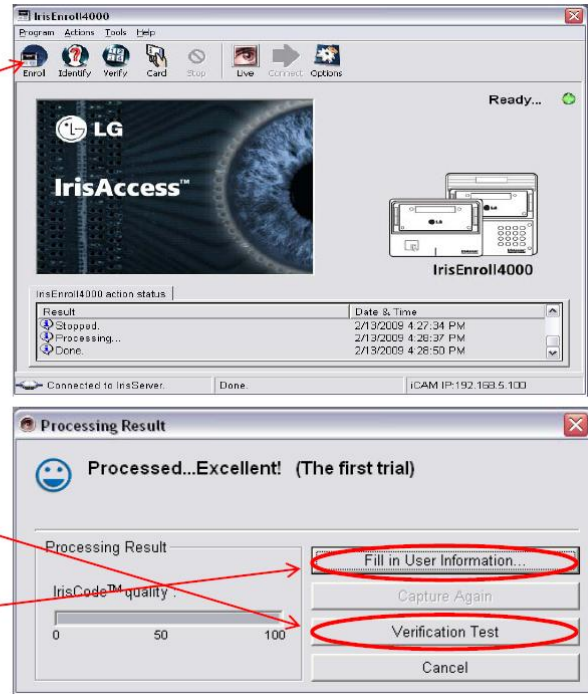
12.IrisEnroll4000



- 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.



Training 3

- 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.)

User Information

Type user ID and then click 'Get user information' button. If user information is not found, click OK, to enable user information fields. If the user information already exists in the server DB, the information will be displayed.

* User ID: test Get user information

Basic information of the user - All fields marked with an asterisk (*) must be filled.

Name
First Name: Test
MI:
Last Name: Test

Card
Prox card
None
Smart Card
Prox card
* Card Number:
Get From Card

Photo
Capture Image
Select Photo...
Delete photo

Gender
☐ Female
☒ Male

Eye
☒ Left ☒ Right
Use warning eye - ☐ Left ☐ Right

Click the 'Next' button to continue.

< Back Next > Cancel

- 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.)

User Information

Type user ID and then click 'Get user information' button. If user information is not found, click OK, to enable user information fields. If the user information already exists in the server DB, the information will be displayed.

* User ID: test Get user information

Basic information of the user - All fields marked with an asterisk (*) must be filled.

Name
First Name: Test
MI:
Last Name: Test

Card
Prox card
None
Smart Card
Prox card
* Card Number:
Get From Card

Photo
Capture Image
Select Photo...
Delete photo

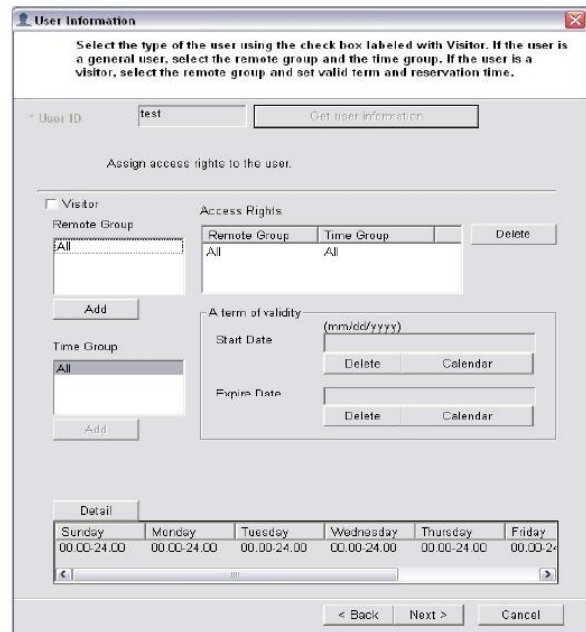
Gender
☐ Female
☒ Male

Eye
☒ Left ☒ Right
Use warning eye - ☐ Left ☐ Right

Click the 'Next' button to continue.

< Back Next > Cancel

- 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.



User Information

Select the type of the user using the check box labeled with Visitor. If the user is a general user, select the remote group and the time group. If the user is a visitor, select the remote group and set valid term and reservation time.

User ID:

Assign access rights to the user.

☐ Visitor

Remote Group:

Time Group:

Access Rights

Remote Group	Time Group	Delete
All	All	<input type="button" value="Delete"/>

A term of validity (mm/dd/yyyy)

Start Date:

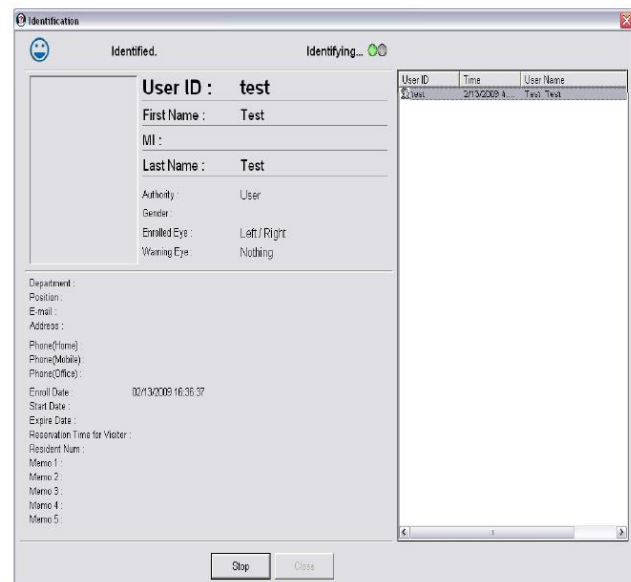
Expire Date:

Detail

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday
00:00-24:00	00:00-24:00	00:00-24:00	00:00-24:00	00:00-24:00	00:00-24:00

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)



Identification

Identified.

User ID:

First Name:

MI:

Last Name:

Authority:

Gender:

Enrolled Eye:

Wearing Eye:

Department:

Position:

E-mail:

Address:

Phone(Home):

Phone(Mobile):

Phone(Office):

Enroll Date:

Start Date:

Expire Date:

Reservation Time for Visitor:

Resident Num:

Memo 1:

Memo 2:

Memo 3:

Memo 4:

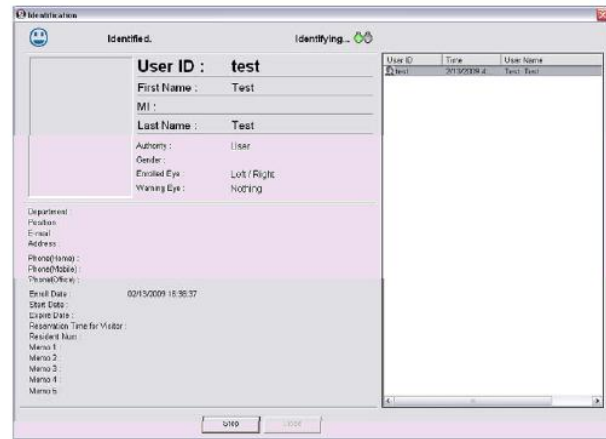
Memo 5:

User ID Time User Name

22 test	2013/2009-4	Test Test
---------	-------------	-----------

Verifying a User

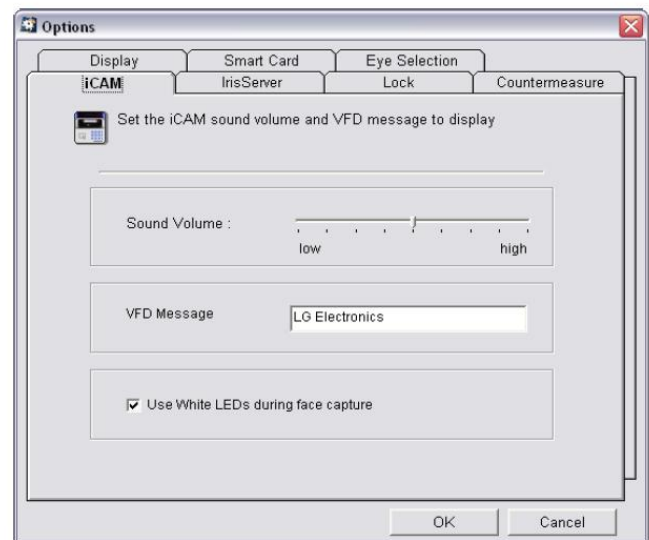
- Select verify from the tool bar on the main screen.
- Enter the User ID and click Verify to begin the Iris image capture process.



Once the Iris image is captured the results will display in a verification window.

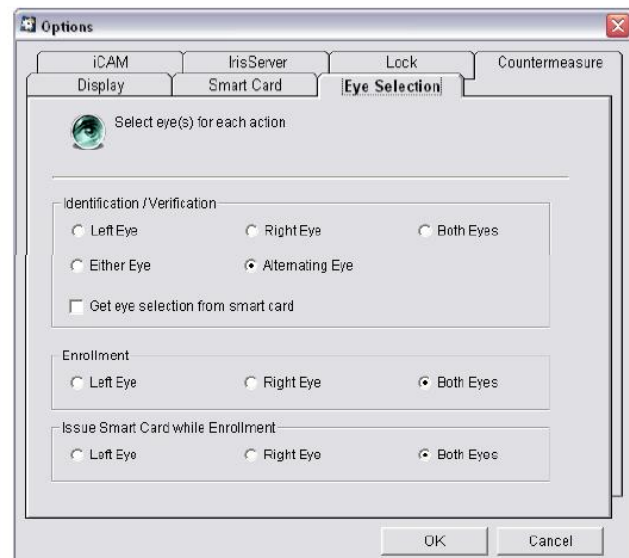
IrisEnroll4000 Options

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

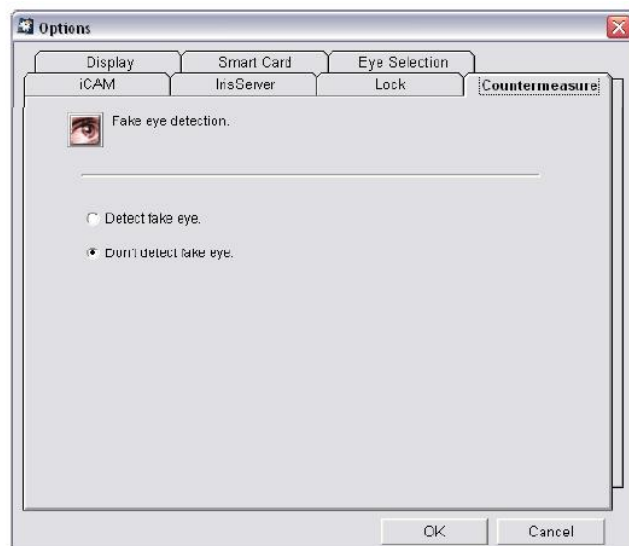


IrisEnroll4000 Options (cont'd)

- 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

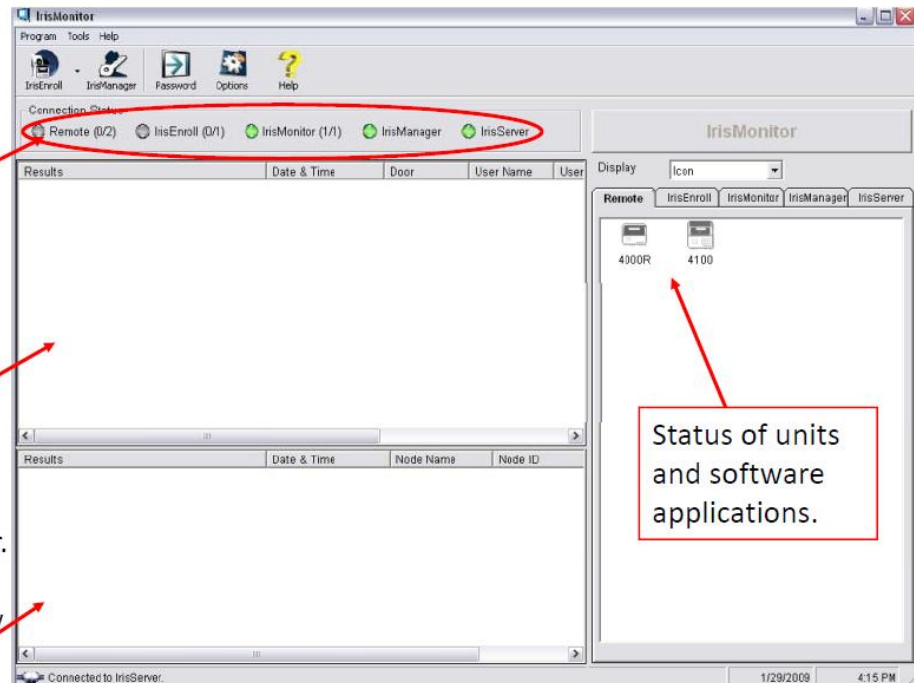
IrisMonitor Screen

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.

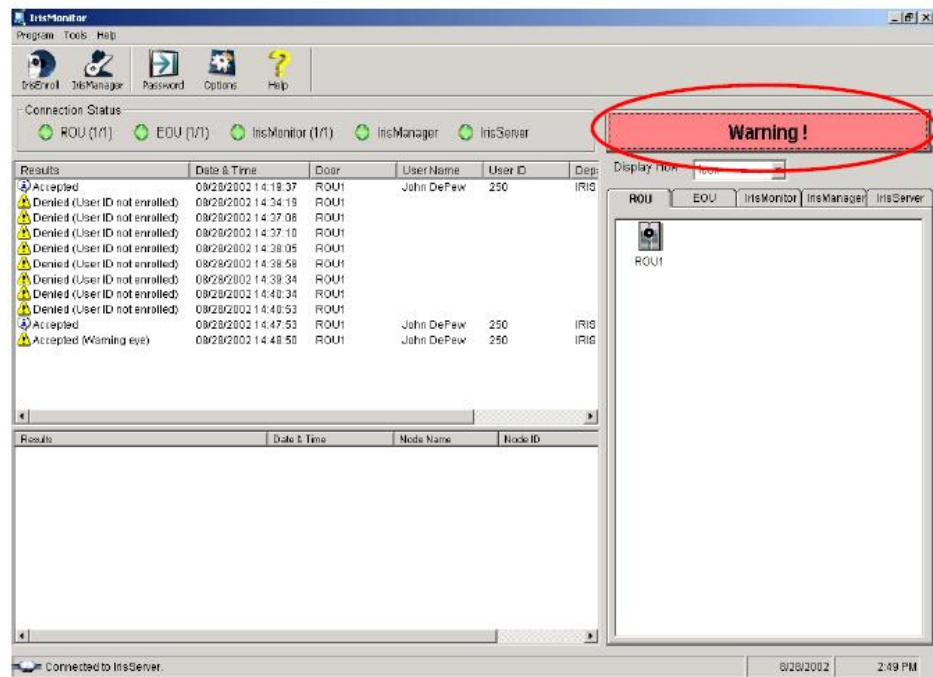


IrisMonitor Warning

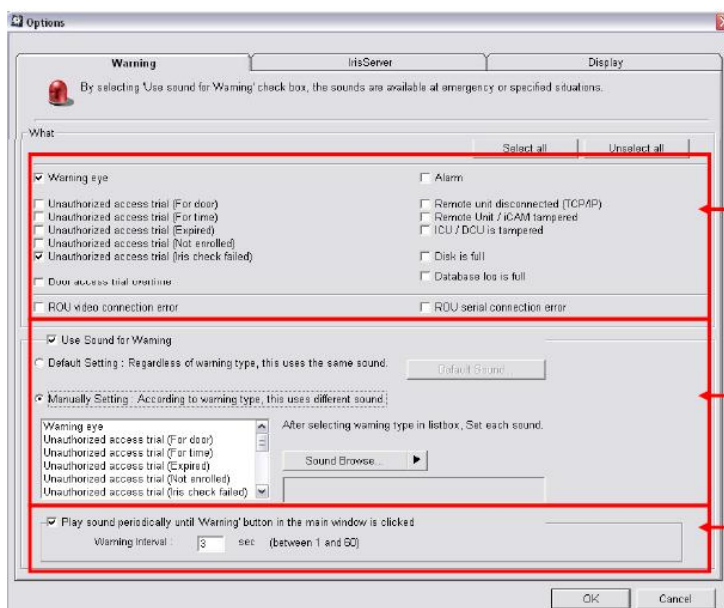
IrisMonitor provides visual and audible alerts for user and system conditions.

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

The screenshot shows the IrisManager application window. On the left is a tree view labeled "Device, Users, Groups Tree" containing folders like "All Remotes", "4000R", "4100", "Remote Groups", "Time Groups", "Additional Info", "Visitor", and "Expiration". The main area displays a table of "Enrolled Users" with columns: User ID, Card ID, Name, Department, Position, Phone(Office), Gender, and Auth. The table lists three users: Daria G. Dostine, Sohail M. Haque, and Mike Viegari. A red oval highlights the "Enrolled Users" table, and a red box highlights the entire table area. At the bottom, a "Real time System Activity" section shows a log of operations. The status bar at the bottom indicates "Connected to IrisServer" and the date/time "1/28/2008 11:58 AM".

User ID	Card ID	Name	Department	Position	Phone(Office)	Gender	Auth
0186		Daria G. Dostine				Male	User
4733		Sohail M. Haque				Female	User
4741		Mike Viegari				Male	User

Date and Time	Operation	Source ID	Source Name	Node ID (Us...	Node Name (User ...
Connected to IrisServer					

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

User Information

Summary Basic Info. **Access Rights** Detail Info.

Assign access rights to the user.

☐ Visitor

☒ Remote Group

All
Prox Only

Add

☒ Time Group

All
Day Shift

Add

Remote Group	Time Group	Delete
Prox Only	Day Shift	

A term of validity (mm/dd/yyyy)

Start Date : Delete Calendar...

Expiry Date : Delete Calendar...

Modify Cancel

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.

The image shows a 'User Information' dialog box with four tabs: Summary, Basic info., Access Rights, and Detail Info. The 'Access Rights' tab is selected. Inside this tab, there is a section titled 'Assign access rights to the user.' with two sub-sections: 'Visitor' and 'Remote Group'. The 'Visitor' checkbox is checked. Below it, there is a list box containing 'All' and 'Prox Only'. To the right of this list box is an 'Add' button. Further right, there is a section titled 'Access Rights' with a list box containing 'Remote Group' and 'Prox Only', and a 'Delete' button. Below this, there is a section titled 'A term of validity' with a '(mm/dd/yyyy)' label. It contains two rows: 'Start Date : 09/05/2002' and 'Expiry Date : 09/05/2002'. Each row has 'Delete' and 'Calendar...' buttons. Below this, there is a section titled 'Reservation time for visitor' with a time range selector showing '14:00 ~ 16:00'. At the bottom of the dialog box are 'Modify' and 'Cancel' buttons.

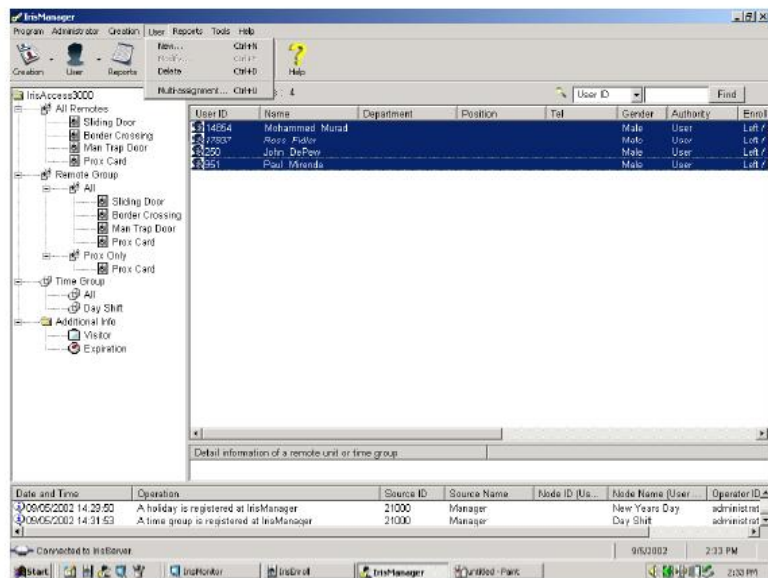
Access Rights Assigned

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.

Multi Assign

Same access rights can be assigned to the selected users. Select the remote groups to be assigned and click <Add> button. And then select the time groups to be assigned before clicking <Add> button.

Selected Users	
User ID	Name
10399	Jonathan D. Ja...
14954	Mohammed M...
17837	Ross Fidler
250	John DePew
951	Paul Mirenda

☐ Visitor

☒ Remote Group

Remote Group: All, Prox Only

☒ Time Group

Time Group: All, Day Shift

Access Rights

Remote Group	Time Group	
		<input type="button" value="Delete"/>

A term of validity (mm/dd/yyyy)

Start Date:

Expiry Date:

Administrators and Operators



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).

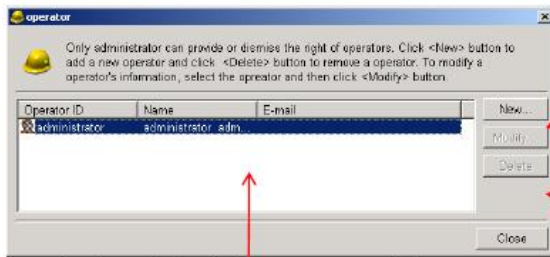
This screen is used to create other administrators and operators that will be able to log in and use the IrisAccess applications.

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



The existing Administrators and Operators

New – Create Admin/Operator

Modify – Modify existing Admin/Operator

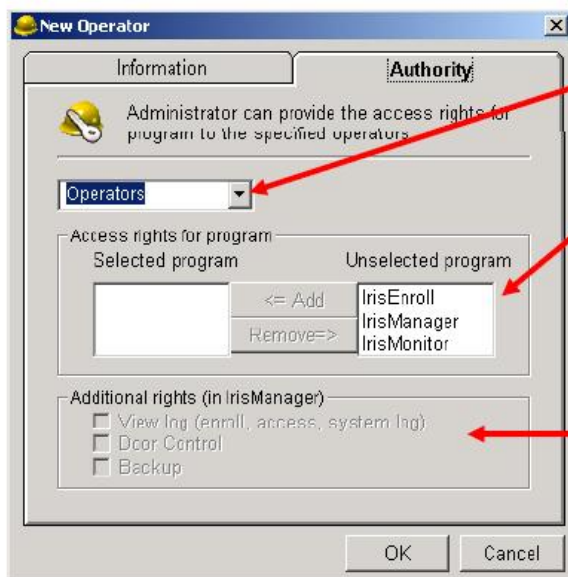
Delete – Delete existing Admin/Operator

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



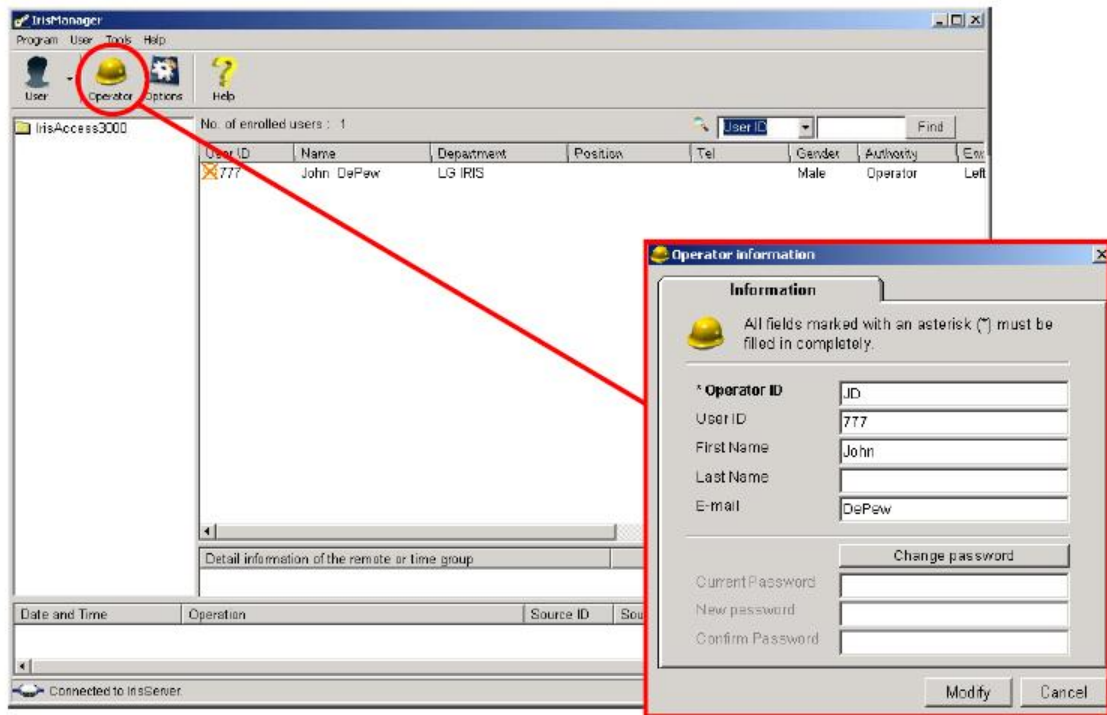
Operator or Administrator privileges

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

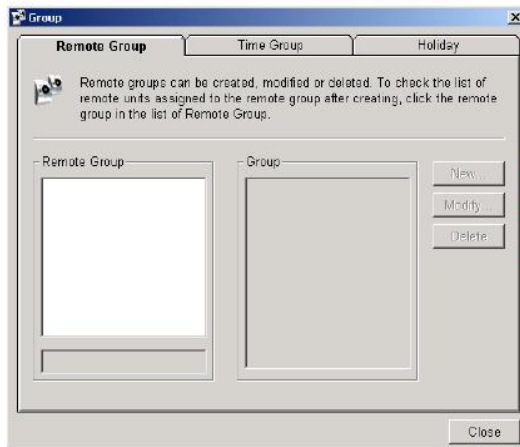


This is a restricted operator screen (no configuration or report permissions)

Setup Remote Groups



Click on Creation in the menu bar and select Remote Group

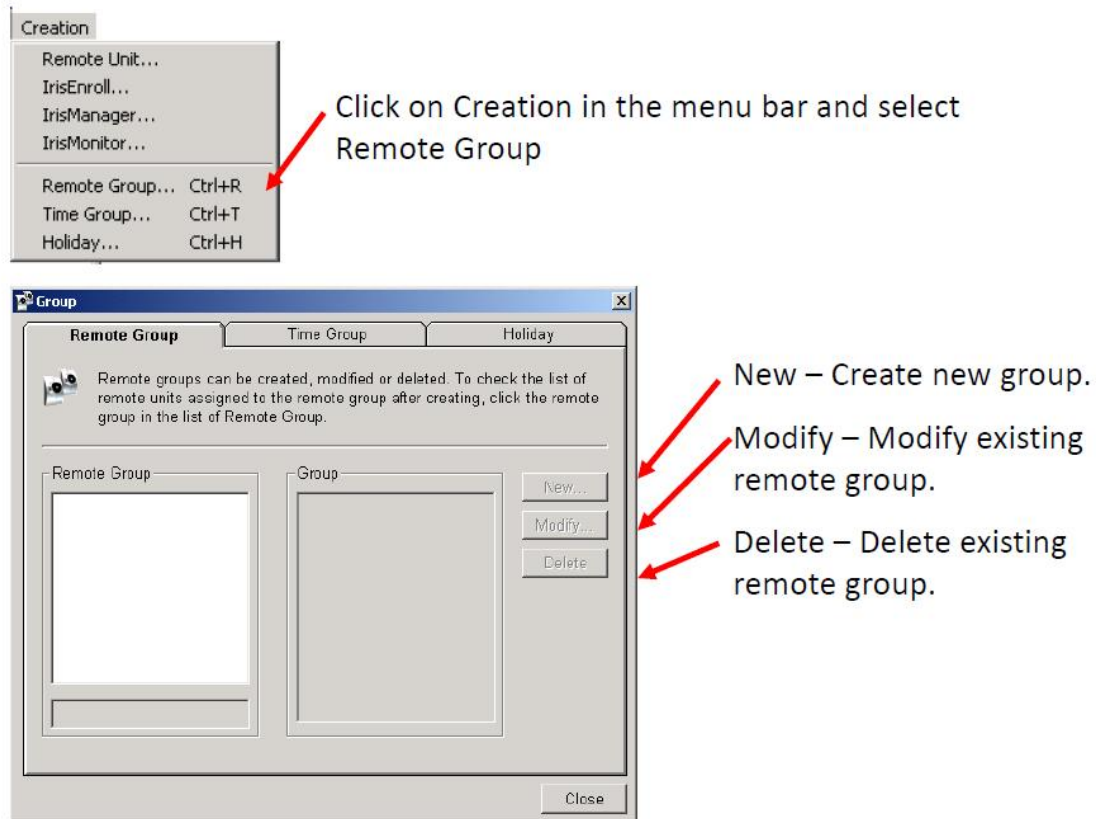


New – Create new group.

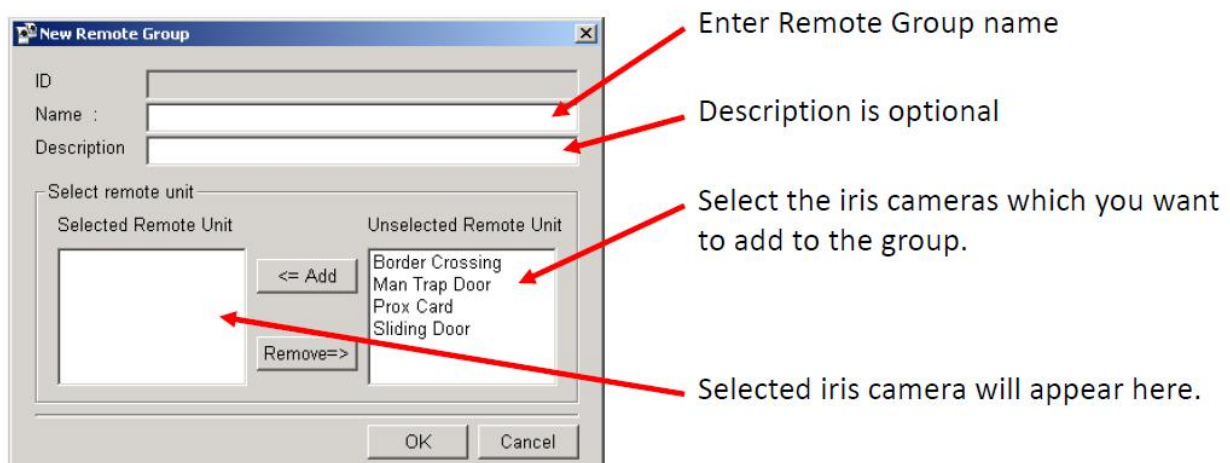
Modify – Modify existing remote group.

Delete – Delete existing remote group.

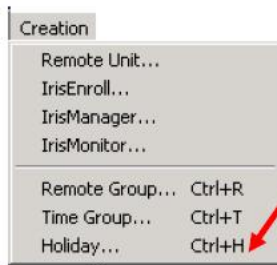
Setup Remote Groups



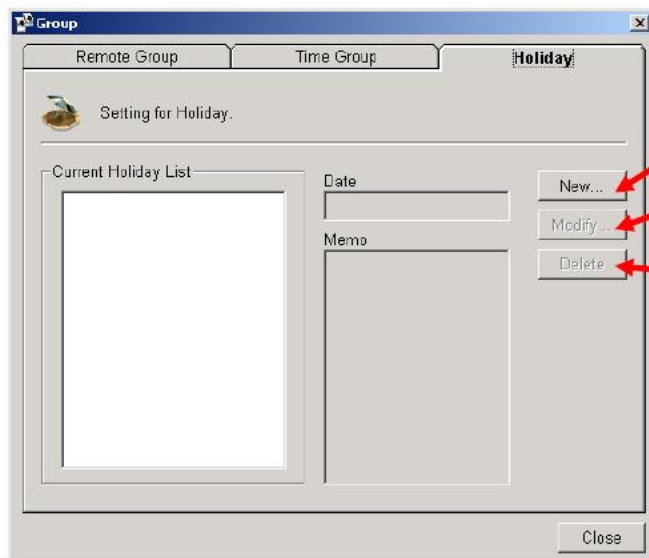
Making Remote Groups



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 'New Holiday' dialog box contains the following fields and controls:

- Holiday Name:** A text input field with an annotation: "Enter Holiday name".
- Date:** Includes a month/year selector (currently 'Aug' and '2002') with an annotation: "Select month and year", and a calendar grid below it. An annotation: "Select the day of the week which you want to add as a holiday." points to the calendar grid.
- Memo:** A text input field with an annotation: "Memo is optional".
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

S	M	T	W	T	F	S
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

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

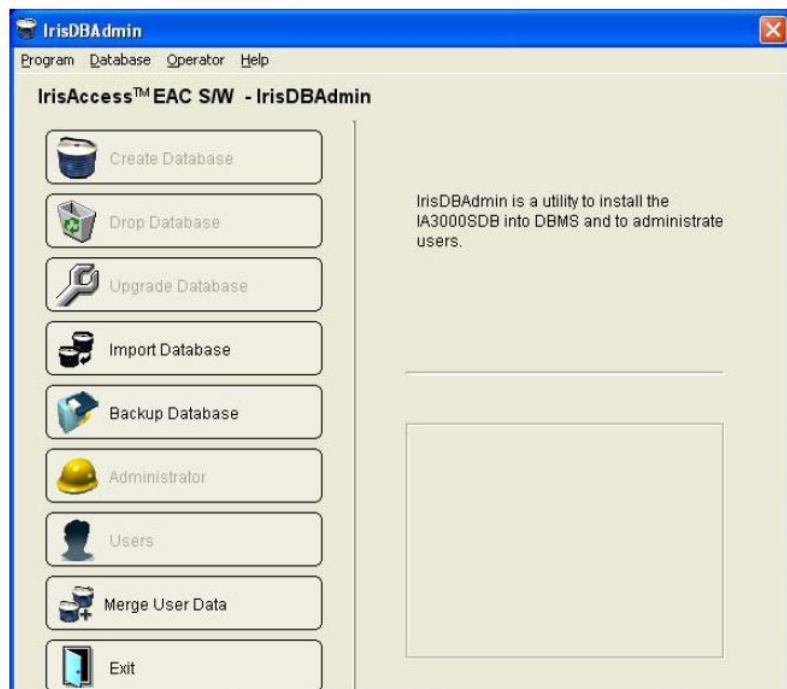


Backup Database – Backup current DB and Log files.

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.



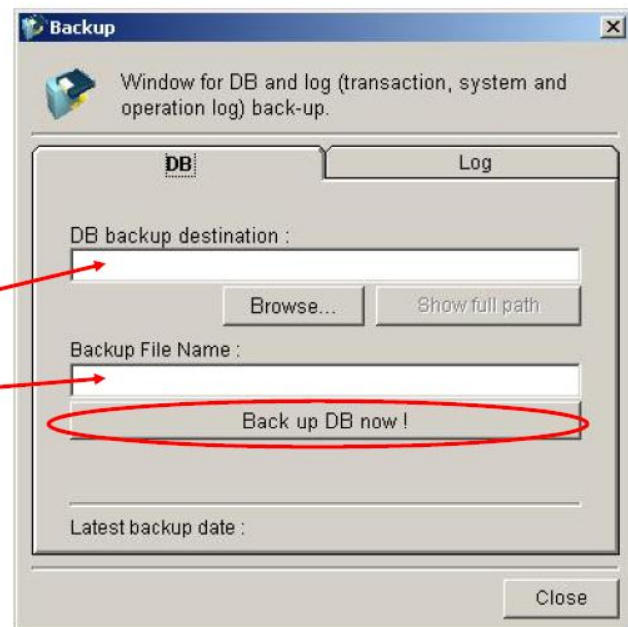
IrisDBAdmin - Backup

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

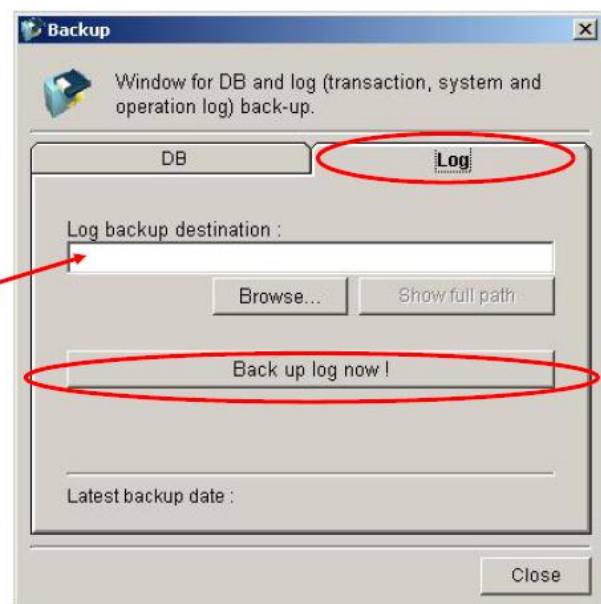
We recommend backing up the DB after new enrollments or at least once a month. IrisMonitor will report if DB allocation is reaching its limit and needs to be backed up immediately.



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

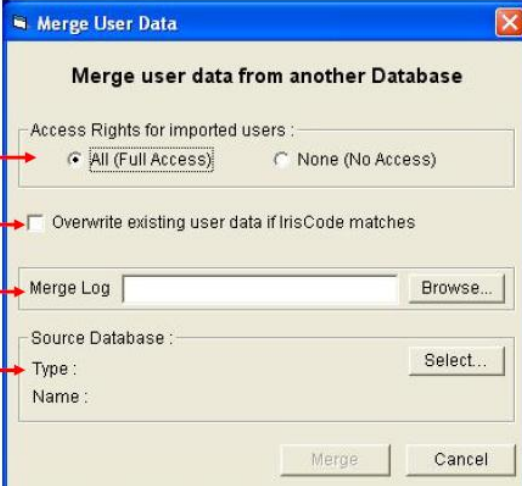
Merge allows an existing IrisAccess® DB to be merged with the active IrisAccess® database

Access Rights of users when imported

Overwrite existing users if matched

Location of merge log files

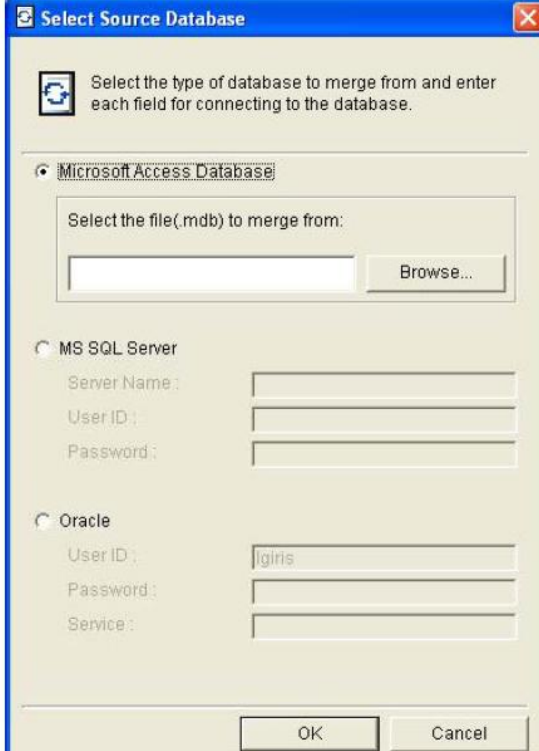
Type of database being merged and location.



The 'Merge User Data' dialog box is titled 'Merge user data from another Database'. It contains the following fields and controls:

- Access Rights for imported users :** Two radio buttons: ☒ All (Full Access) and ☐ None (No Access).
- Overwrite existing user data if IrisCode matches**: A checkbox that is currently unchecked.
- Merge Log**: A text input field followed by a 'Browse...' button.
- Source Database :** A section with 'Type :' and 'Name :' labels, and a 'Select...' button.
- Buttons**: 'Merge' and 'Cancel' buttons at the bottom right.

Select the database type and DB location.



The 'Select Source Database' dialog box is titled 'Select the type of database to merge from and enter each field for connecting to the database.' It contains the following fields and controls:

- Database Type Selection**: Three radio buttons: ☒ Microsoft Access Database, ☐ MS SQL Server, and ☐ Oracle.
- Microsoft Access Database**: A section with 'Select the file(.mdb) to merge from:' label, a text input field, and a 'Browse...' button.
- MS SQL Server**: A section with 'Server Name:', 'User ID:', and 'Password:' labels, each followed by a text input field.
- Oracle**: A section with 'User ID:', 'Password:', and 'Service:' labels, each followed by a text input field.
- Buttons**: 'OK' and 'Cancel' buttons at the bottom right.

16. Technical Support

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