



IrisAccess® Software User Manual

Version 3.09x

March 28, 2013

Copyright © 1999-2012 Iris ID, Inc. All rights reserved.

IrisAccess EAC User Manual

If this manual is distributed with software that includes an end user agreement, this guide, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. Except as permitted by any such license, no part of this manual may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Iris ID Incorporated. Please note that the content in this manual is protected under copyright law even if it is not distributed with software that includes an end user license agreement.

The content of this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Iris ID, Incorporated. Iris ID, Incorporated assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this manual.

Please remember that existing images or drawings that you may want to include in your document may be protected under copyright law. The unauthorized incorporation of such material into your work could be a violation of the rights of the copyright owner. Please be sure to obtain any permission required from the copyright owner.

LG, LG Iris, the LG logo, LG Iris logo and IrisAccess are either registered trademarks or trademarks of Iris ID Incorporated in the United States and/or other countries.

The HASP®HL system and its documentation are copyrighted © 1985 to present by Aladdin Knowledge Systems Ltd. All rights reserved. HASP and Hardlock are registered trademarks of Aladdin Knowledge Systems Ltd. SRM, HASP®SRM, HASP® Business Studio, Cross-Locking, License on Chip, LoC, HASP®HL Basic, HASP®HL Pro, HASP®HL Max, HASP®HL Time HASP®HL Net, HASP®HL NetTime, and HASP®HL Drive are trademarks of Aladdin Knowledge Systems Ltd.

RSA is trademark of RSA Security Inc. IrisAccess, IrisCode are registered trademarks of Iridian Technologies, Inc. Windows 2000, Windows XP are trademark of Microsoft Corporation. All other trademarks are properties of their respective holders.

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

Document Number: IRISIDEAC-28-0305-0313

Table of Contents

TABLE OF CONTENTS	1
1. INTRODUCTION TO THE USER MANUAL.....	7
1.1 Installation Pre-Requisites	7
1.2 Scope	8
1.3 Overview	8
1.4 Network & DB Security.....	8
2. IRISACCESS™ IRISSERVER.....	10
2.1 IrisAccess™ IrisServer	10
2.1.1 How to Run IrisServer	10
2.1.2 How to View the IrisServer Window	13
2.1.3 Registration of IrisManager or Modification of IrisManager Information.....	15
2.1.4 Connecting to MS-SQL Server 2000 Database.....	15
2.1.5 Connecting to Oracle Server 2000 Database.....	16
2.1.6 Generating and Registering Encryption Keys for Smart Card Operation	17
2.1.7 Upgrading License	18
2.2 IrisAccess™ IrisManager	21
2.2.1 How to Run IrisManager.....	21
2.2.2 How to Login to IrisManager.....	21
2.2.3 Display when the Server DB is being Updated.....	26
2.2.4 Display when the Remote Database in ICU is being Updated.....	28
2.2.5 Display when IrisServer is Busy.....	29
2.2.6 Program Management	29
2.2.6.1 Register New iCAM4000/4100 series Remote Unit.....	29
2.2.6.2 Register New iCAM7000/7100 series Option 3 Remote Unit	31
2.2.6.3 Register New iCAM7000/7100 series Option 1 Remote Unit with ICU7000	32
2.2.6.4 Modify Remote Unit Information.....	33
2.2.6.5 Delete Remote Unit	34
2.2.6.6 Registering IrisEnroll.....	35
2.2.6.7 Modification of IrisEnroll Information	37
2.2.6.8 Delete IrisEnroll	38
2.2.6.9 Registration of IrisManager.....	40
2.2.6.10 Modify IrisManager Information.....	42
2.2.6.11 Delete IrisManager	43
2.2.6.12 Register IrisMonitor	44
2.2.6.13 Modification of IrisMonitor Information	46
2.2.6.14 Delete IrisMonitor.....	48
2.2.7 Group Management	49
2.2.7.1 Add Remote Group.....	49
2.2.7.2 Modify Remote Group.....	52

2.2.7.3	Delete Remote Group	55
2.2.7.4	Add Time Group	57
2.2.7.5	Modify Time Group	60
2.2.7.6	Delete Time Group	63
2.2.7.7	Add Holiday List	65
2.2.7.8	Modify Holiday List	68
2.2.7.9	Delete Holiday List	70
2.2.7.10	Prioritized ICU DB sync	72
2.2.8	<i>Administration</i>	72
2.2.8.1	Administrator/Operator	73
2.2.8.2	Modification of the Administrator/Operator	76
2.2.8.3	Deletion of the Administrator/Operator	78
2.2.8.4	Operator Log Report	79
2.2.8.5	Security Setting	81
2.2.9	<i>Administer User Access Control</i>	82
2.2.9.1	Add New Users	82
2.2.9.2	Modify User Information	90
2.2.9.3	Delete User Information	96
2.2.9.4	Multi-Assignment for Users	96
2.2.10	<i>Reports</i>	99
2.2.10.1	Enroll Report	99
2.2.10.2	Access Reports	102
2.2.10.3	Time & Attendance Reporting / Filtering	105
2.2.10.4	System Reports	108
2.2.11	<i>Door Control</i>	110
2.2.11.1	Opening Door(s) Once	110
2.2.12	<i>Tool Operation</i>	111
2.2.12.1	Options	111
2.2.12.2	Auto Update	114
3.	ICAM7000 UPDATE	114
3.1	iCAM7000 Update	114
3.1.1	<i>Minimum System Requirements</i>	115
3.2	Standard usage for Installation / Updating iCAM	115
3.3	Full Description Use of IrisAccess™ iCAM7000 Update	117
3.3.1	<i>Add</i>	117
3.3.2	<i>Modify</i>	118
3.3.3	<i>Clear</i>	118
3.3.4	<i>Delete</i>	118
3.3.5	<i>Find iCAM7000s</i>	119
3.3.6	<i>Update</i>	119
3.3.7	<i>New Installation</i>	120

3.3.8	Save List to File	121
3.3.9	Load List From File	122
3.3.10	Exit.....	122
4.	IRISACCESS™ OPTION3ADMIN	123
4.1	IrisAccess™ Option3Admin.....	123
4.1.1	Minimum System Requirements.....	123
4.1.2	Version Compatibility.....	123
4.2	How to Use IrisAccess™ Option3Admin	124
4.2.1	Add.....	124
4.2.2	Modify.....	125
4.2.3	Remove	126
4.2.4	Clear	126
4.2.5	Delete List	126
4.2.6	Update IrisServer IP / Security ID.....	127
4.2.7	Save to File.....	127
4.2.8	Load from File	128
4.2.9	Exit	128
5.	IRISACCESS™ ENROLL4000.....	128
5.1	IrisAccess™ IrisEnroll4000	128
5.1.1	How to Run IrisEnroll4000	128
5.1.2	How to Login to IrisEnroll4000	130
5.1.3	Enroll.....	134
5.1.4	Identify.....	152
5.1.5	Verify.....	154
5.1.6	Live View.....	160
5.1.7	Option Settings	161
5.1.7.1	iCAM Setting.....	161
5.1.7.2	IrisServer IP Address	162
5.1.7.3	Program Lock.....	163
5.1.7.4	Fake Eye Detection.....	164
5.1.7.5	Display.....	166
5.1.7.6	Smart Card	166
5.1.7.7	Eye Selection.....	169
6.	IRISACCESS™ IRISMONITOR.....	170
6.1	IrisAccess™ IrisMonitor	170
6.1.1	How to Run IrisMonitor	170
6.1.2	How to Login to IrisMonitor.....	171
6.1.3	Other Program Launch	175
6.1.4	System Status.....	176
6.1.5	Option Settings	177

6.1.5.1	Setting the IP Address of IrisServer	178
6.1.5.2	Selecting the Display of User ID	180
6.1.5.3	Specifying the Warnings	181
6.1.6	Password.....	183
6.1.7	Time & Attendance Display information	183
6.1.8	Remote Unit Created for iCAM7100 – Option 3	184
7.	IRISACCESS™ IRISDBADMIN.....	186
7.1.1	<i>IrisAccess™ IrisDBAdmin</i>	186
7.1.2	<i>How to Run IrisDBAdmin</i>	186
7.1.3	<i>IrisDBAdmin for MS ACCESS Database</i>	187
7.1.3.1	Upgrading Database	188
7.1.3.2	Importing Database.....	189
7.1.3.3	Database Backup	194
7.1.3.4	Log Backup.....	195
7.1.3.5	Merging User Data.....	197
7.1.4	<i>IrisDBAdmin for MS SQL Server</i>	203
7.1.4.1	Upgrading Database	206
7.1.4.2	Creating Database	207
7.1.4.3	Dropping Database.....	209
7.1.4.4	Importing Database.....	210
7.1.4.5	Database Backup	216
7.1.4.6	Log Backup.....	218
7.1.4.7	Administrator	219
7.1.4.8	User.....	220
7.1.4.9	Merging User Data.....	223
7.1.5	<i>IrisDBAdmin for Oracle</i>	224
7.1.5.1	Upgrading Database	225
7.1.5.2	Creating Database	227
7.1.5.3	Dropping Database.....	229
7.1.5.4	Importing Database.....	230
7.1.5.5	Database Backup	234
7.1.5.6	Log Backup.....	234
7.1.5.7	Administrator	234
7.1.5.8	User.....	235
7.1.5.9	Merging Database.....	239
8.	IRISICUADMIN4000	240
8.1	<i>IrisICUAdmin4000</i>	240
8.1.1	<i>IrisICUAdmin40000 Program usage</i>	240
8.1.2	<i>How to open IrisICUAdmin4000</i>	240
8.1.3	<i>Description of Menu items in IrisICUAdmin4000</i>	241
8.1.4	<i>The ICUAmin4000 New Installation Window</i>	241

8.1.5	The ICUAmin4000 Upgrade Window.....	247
8.1.6	The ICUAmin4000 Configuration Window.....	260
8.1.7	The ICUAmin4000 Change Password Window	278
9.	IRISICUADMIN7000	281
9.1	IrisICUAdmin7000 Information	281
9.1.1	About IrisICUAdmin7000	281
9.1.2	IrisICUAdmin7000 Purpose and Technical Details.....	282
9.1.3	Minimum System Requirements.....	282
9.1.4	Version Compatibility.....	282
9.2	How to Use IrisAccess™ ICUAdmin7000	283
9.2.1	Add.....	283
9.2.2	Update	284
9.2.3	Clear.....	285
9.2.4	Delete All.....	285
9.2.5	Delete Selected	286
9.2.6	Find ICU7000s	286
9.2.7	Get ICU7000 Info.....	287
9.2.8	New Installation.....	287
9.2.9	Update	288
9.2.10	Get ICU Config	289
9.2.11	Set ICU Config.....	290
9.2.12	Save List to a File	290
9.2.13	Load List to a File.....	291
10.	TECHNICAL SUPPORT.....	291
10.1	Technical Assistance	291
10.1.1	How to receive Technical Support	291
11.	APPENDIX	292
11.1	IrisAccess™ IrisEnroll3000.....	292
11.1.1	How to Run IrisEnroll3000.....	292
11.1.2	How to Login to IrisEnroll3000	293
11.1.3	Enroll.....	295
11.1.4	Add	312
11.1.5	Identify.....	314
11.1.6	Verify	316
11.1.7	Live View.....	321
11.1.8	Option Settings.....	322
11.1.8.1	EOU Setting.....	322
11.1.8.2	IrisServer IP Address.....	323
11.1.8.3	Program Lock.....	324
11.1.8.4	Fake Eye Detection	325

11.1.8.5	Display	326
11.1.8.6	Smart Card.....	327
11.1.9	Password	329
11.1.10	Security ID.....	330
11.2	IrisICUAdmin30000	331
11.2.1	How to open IrisICUAdmin3000	331
11.2.2	Description of Menu items in IrisICUAdmin3000	332
11.2.3	The ICUAmin3000 New Installation Window	332
11.2.4	The IrisICUAdmin3000 Upgrade Window.....	338
11.2.5	The ICUAdmin3000 Configuration Window	349
11.2.6	The ICUAdmin3000 Change Password Window.....	368

1. Introduction to the User Manual

1.1 Installation Pre-Requisites

Supported Computer Hardware Recommendations:

- Operating system - Windows 2000/XP, Windows Vista, Windows 7
- Pentium Compatible 1.8 (or higher) GHz Processor
- 1 GB (or higher) Memory
- 10 GB Hard Disk space (or greater)
- CD-Rom
- Ethernet Port (100 Mbps recommended)
- 1 Serial Port for ICU configuration OR 1 USB 2.0 (or higher) port (for use with USB to Serial adapter)
- Speakers (if sound warnings are used)

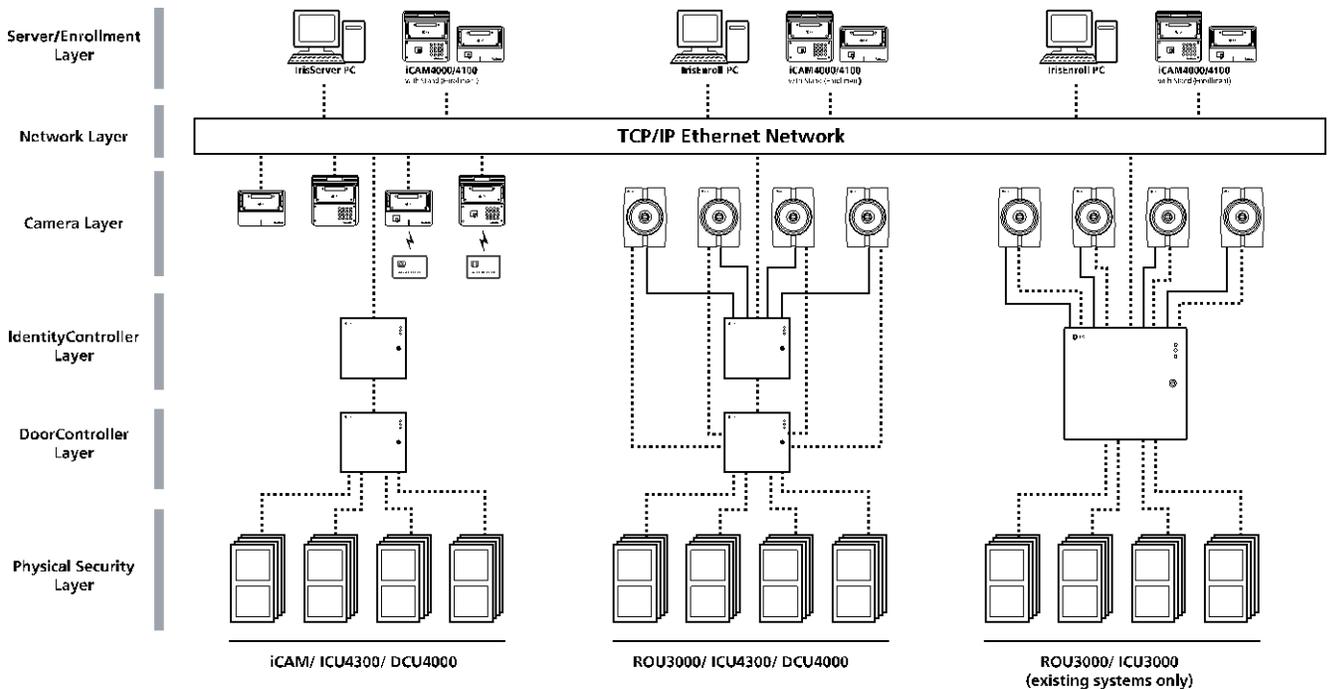
- Administrative rights are required to install or uninstall the IrisAccess EAC Software.
- Power user rights or above is required to run the IrisAccess EAC Software.
- Microsoft Window 2000 Professional (Service Pack 3) or Microsoft Windows XP Professional (Service Pack 1) or Windows Vista, or Windows 7.
- It is required that a network card and network configuration be completed before installing the IrisAccess software.
** Note: All computers in the IrisAccess EAC system should be set to static IP addresses.*
- It is strongly recommended that the IrisAccess software be connected through a 100Mbps network.
- It is recommended that the monitor resolution be at least 1024x768 pixels at 16-bit color.
- For windows to display correctly in Microsoft Windows XP, please set the DPI setting as “Normal size (96DPI)”. You can see the “DPI setting” on Start > Control Panel > Appearance and Themes > Display > Setting > Advanced > General > Display in Windows XP.
- In order to use Oracle as the database type, the OO4O (Oracle Objects For OLE) must be installed on the IrisServer PC.
** Note: OO4O has been included in EAC S/W package CD.*
- In order to run the IrisDiagnosis program, the .Net Framework version 1.1 must be installed. You may install it though the EAC S/W package CD.

- It is recommended that all IrisAccess system components (PCs, ICUs, ROUs, EOU) be powered through Uninterruptible Power Supplies (UPSs). This will help prevent damage by power fluctuations and increase uptime.

1.2 Scope

This document explains about various applications in IrisAccess™ system and explains how these applications are used. The applications that are explained in this document are IrisServer, IrisManager, IrisEnroll, IrisMonitor and IrisDBAdmin.

1.3 Overview



1.4 Network & DB Security

The IrisCode™ is encrypted by AES when it is stored in the database. The server and each remote unit have a unique Secret Key that is generated during initial installation.

If you select the high security option (the first option in the section “2.2.8.5 Security Setting” in this document), the Secret Key is not stored in the ICU - the ICU will get the Secret Key from the server when it is restarted. If the ICU fails to connect to the server after a restart, it will not identify any user until it succeeds in connecting to the server. The Secret Key exchange is protected by the RSA public-key cryptosystem, using the Security ID typed in during ROU/ICU configuration and the ROU registration in IrisManager. Please refer to section 2.2, item 4 in the document IrisAccess™ Software Installation Manual (Document No.DV002S501) and section 2.2.6.1 in this document, respectively.

If you select the low security option (the second option in the section “2.2.8.5 Security Setting” in this document), the Secret Key is stored in the ICU - so the ICU will not need to get the Secret Key from the server when it is restarted. If you select the low security option, the remote unit will be activated without connecting to the server after being restarted, and be capable of identifying enrolled users.

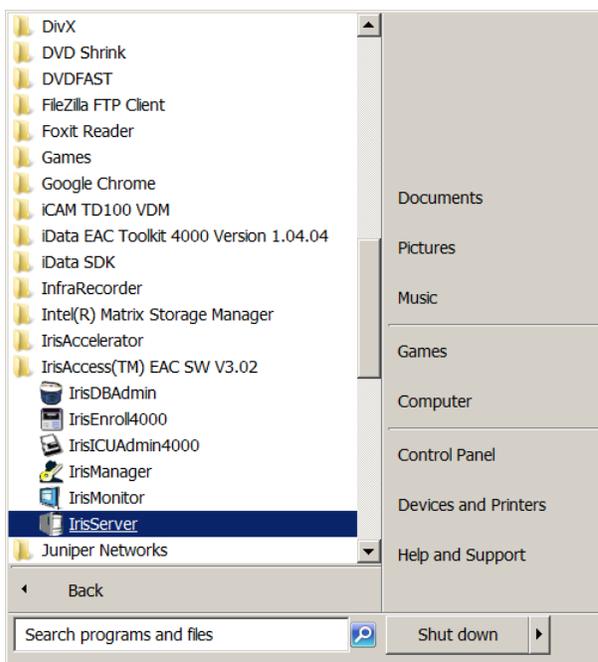
2. IrisAccess™ IrisServer

2.1 IrisAccess™ IrisServer

The IrisServer is an application within the iData Entry Access Control (EAC) Software suite that is used to communicate with the ICU units and other applications within the EAC Software available for use. *Note: This application is not a running service, and is required to be opened when desired to be used. As an application the program will be in the closed state if the PC was rebooted or has been placed in a sleep mode. This program can only run with a windows login user with administrative rights.*

2.1.1 How to Run IrisServer

To start the IrisServer, click on the IrisServer menu item. The location of the program is shown in the figure below:

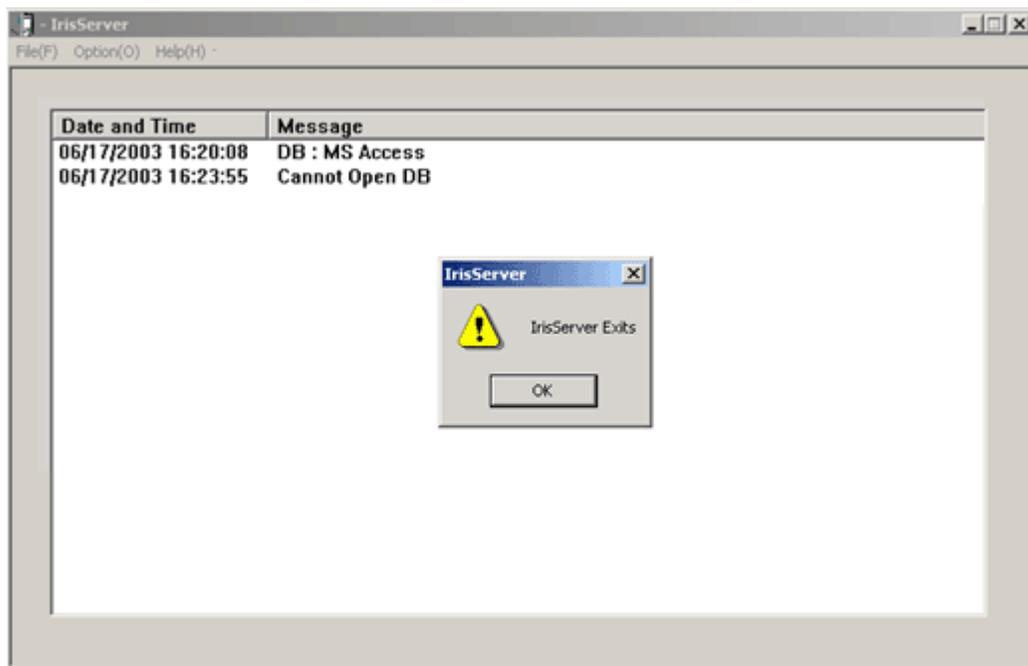
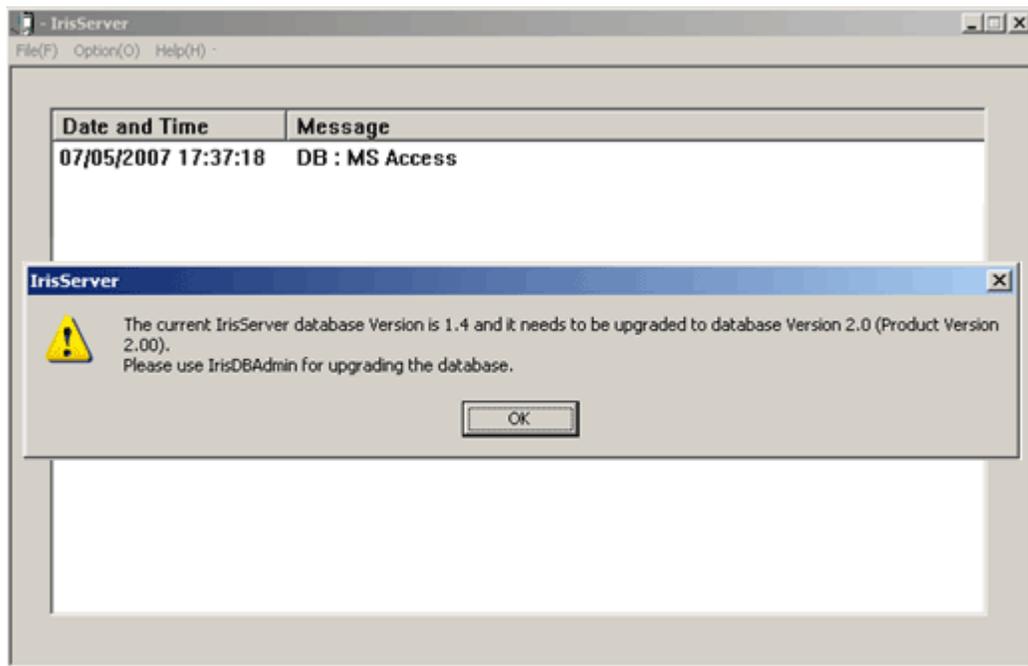


After starting, IrisServer will minimize to the system tray, as illustrated below:



1. When a MS Access Database is used, the Database is automatically created (**Note: It is **not** required that MS Access be installed.*)

2. If the Database already exists on the Server PC, and it is a previous version, the Database may need to be upgraded (Refer to 2.6.2.1, UPGRADING DATABASE). IrisServer will display the message below and exit.

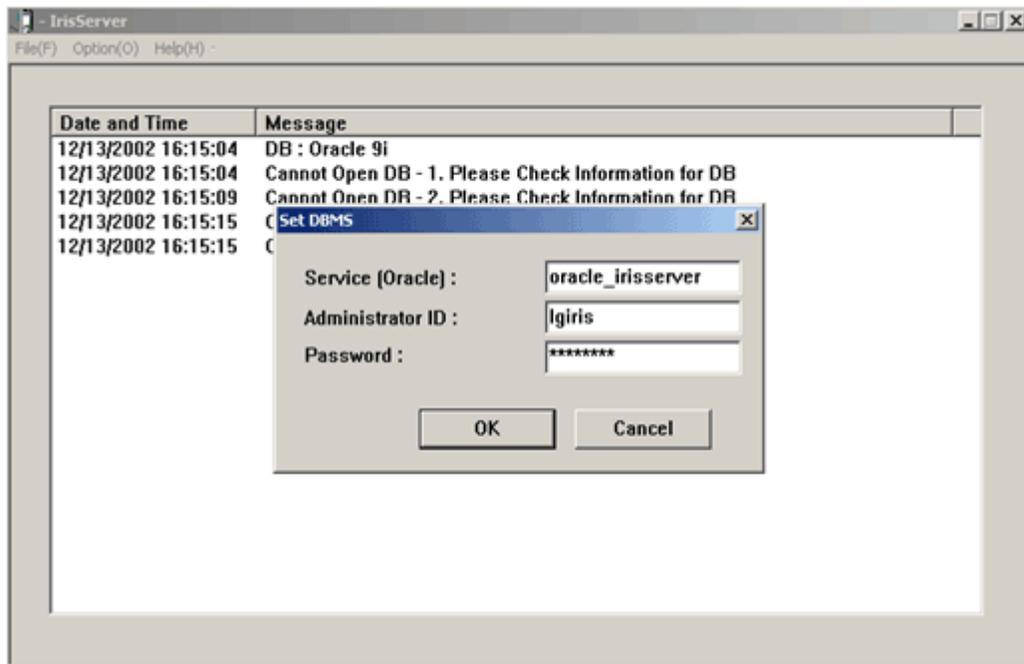
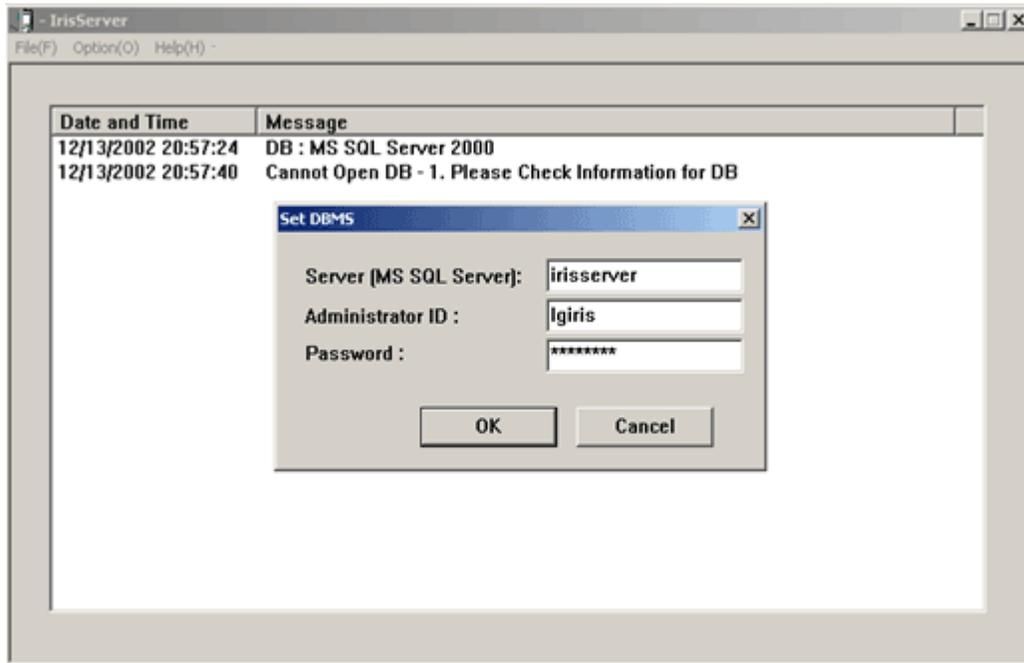


3. If using MS SQL Server or Oracle as the database, IrisServer will need to be configured when run for the first time. If IrisServer loses the network

connection to the MS SQL Server computer, the Administrator ID and password must be re-entered

4. To connect to a MS SQL Server database, enter the MS SQL Server name (or IP address), administrator ID and password in each field. To connect to an Oracle database, enter the Oracle Service name, administrator ID and password in each field.

5. Click the OK button.



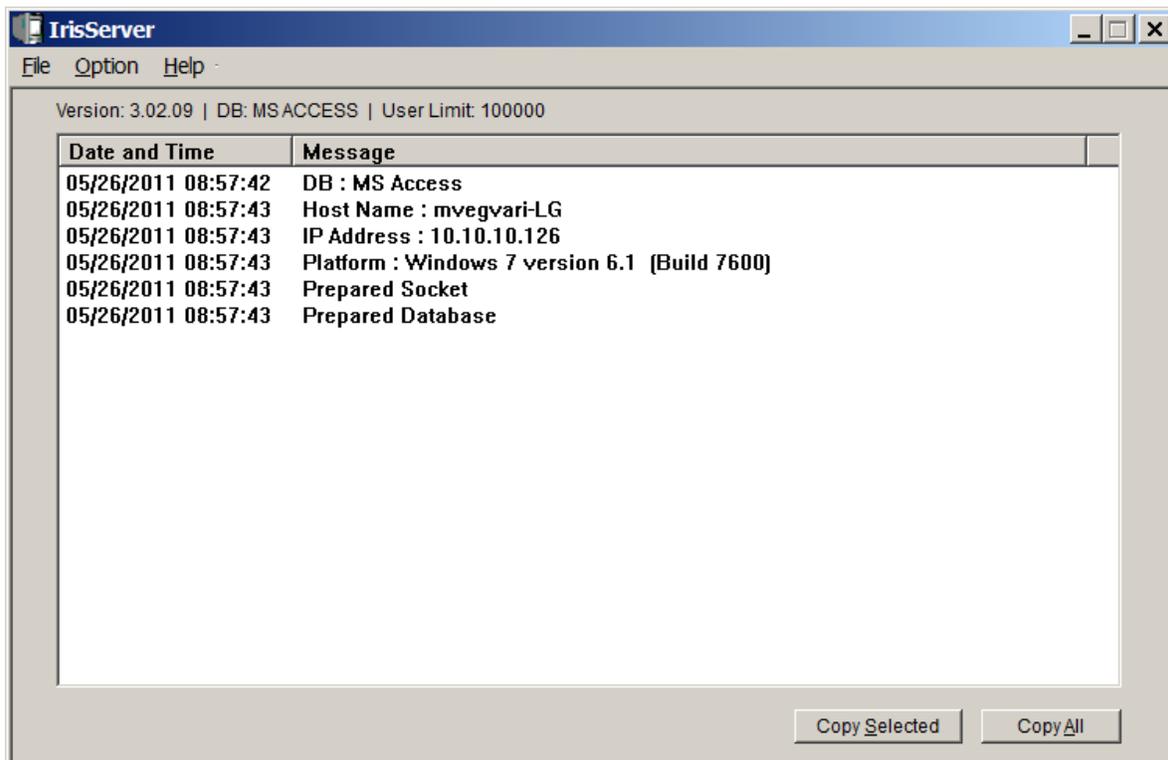
2.1.2 How to View the IrisServer Window

After double-clicking on the IrisServer icon in the taskbar, the following logon window is displayed on the screen.



1. Enter the ID and Password of an account with administrator-level privileges and click the OK button.
 - ▣ Only administrators may login to IrisServer. The default ID and password of the administrator is “**administrator**” and “**iris3000**” respectively. These may be changed by administrators. Refer to the section 2.2.8.2 Modification of the Administrator/Operator.

After successfully logging into IrisServer, you can see the IrisServer window as shown in the following figure:



Message Window

IrisServer log messages can be viewed in the IrisServer window.

2.1.3 Registration of IrisManager or Modification of IrisManager Information

IrisManager can be registered or IrisManager information can be modified using the following steps.

1. Select the Option > Set IrisManager ... item in the menu bar of the IrisServer main window. The following Set IrisManager dialog box is displayed.

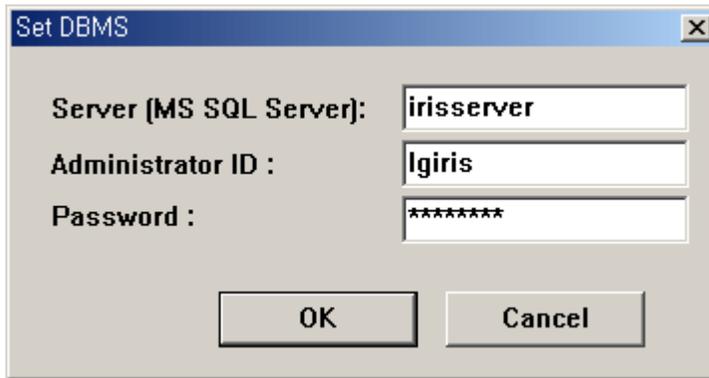


2. Enter IrisManager Name. This field can contain any name desired, however must contain a minimum of 1 character and a maximum of 20 characters.
3. Enter IP Address of the IrisManager. If IrisManager will be located on the same computer as IrisServer, we recommend entering the loopback address (127.0.0.1) as the IP Address.
4. Click OK button.

2.1.4 Connecting to MS-SQL Server 2000 Database

1. MS SQL Server must have been selected during installation to perform this operation. (MS SQL must have been installed prior to iData EAC software installation.)
2. Select the Option > Set DBMS item in the menu bar of the IrisServer main window.

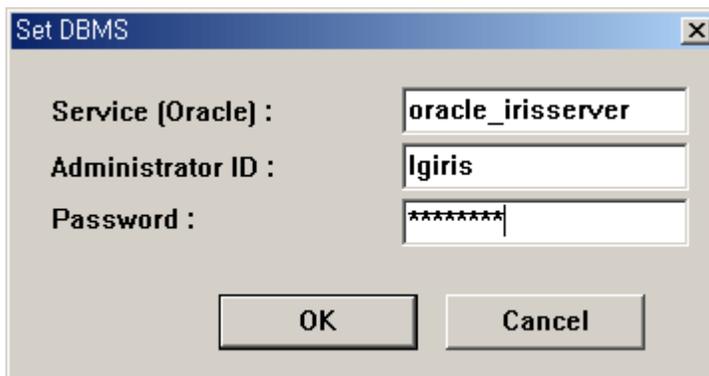
3. Enter the MS SQL Server name (or IP address), administrator ID and password in each field and then click the OK button to connect to the MS SQL Server database.



The screenshot shows a dialog box titled "Set DBMS" with a close button (X) in the top right corner. It contains three input fields: "Server (MS SQL Server):" with the value "irisserver", "Administrator ID :" with the value "lgiris", and "Password :" with the value "*****". At the bottom, there are two buttons: "OK" and "Cancel".

2.1.5 Connecting to Oracle Server 2000 Database

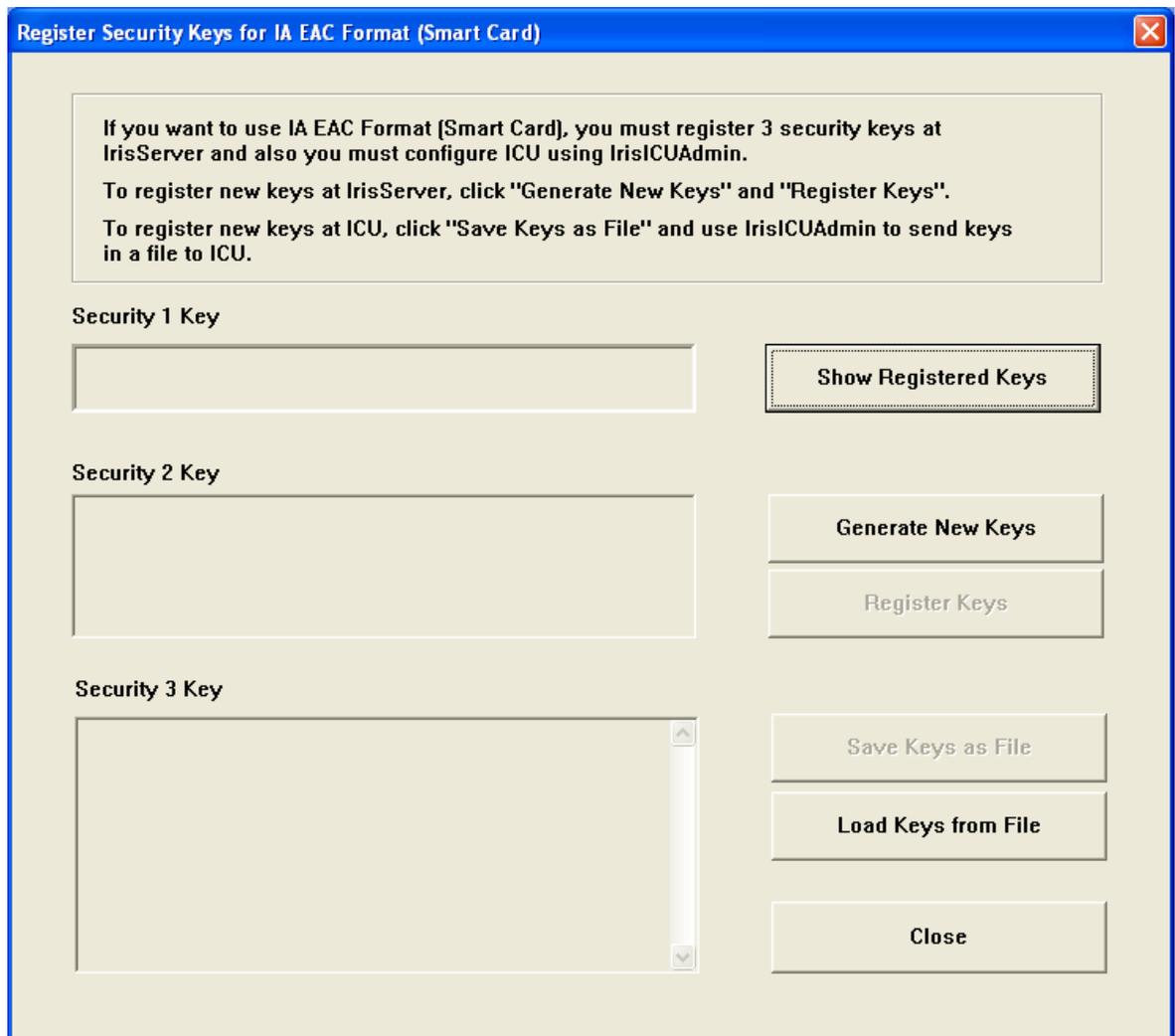
1. Oracle must have been selected during installation to perform this operation. (Oracle must have been installed prior to iData EAC software installation.)
2. Select the Option > Set DBMS item in the menu bar of the IrisServer main window.
3. Enter the Oracle Service, Administrator ID and Password in each field and then click the OK button to connect to Oracle Server database.



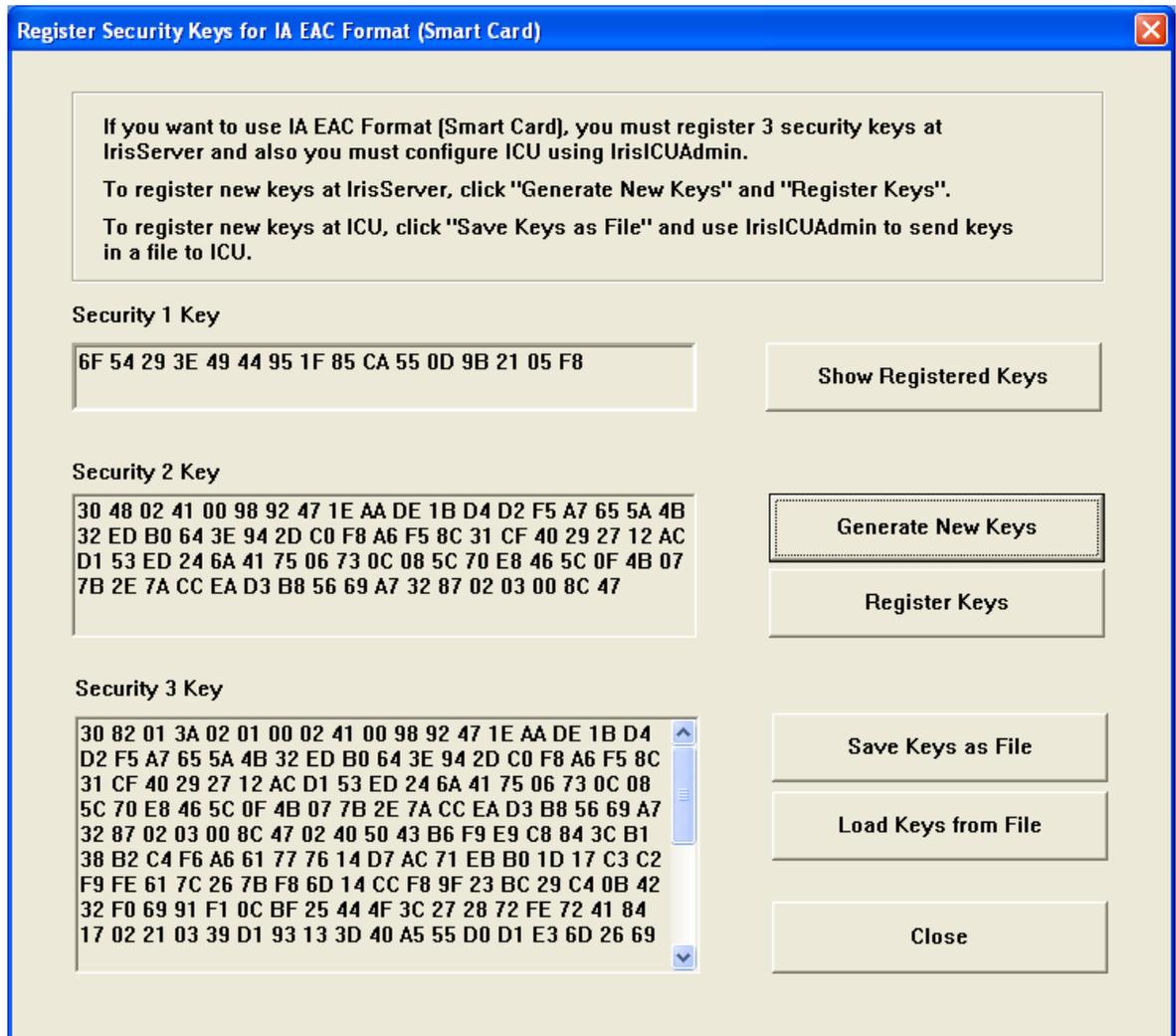
The screenshot shows a dialog box titled "Set DBMS" with a close button (X) in the top right corner. It contains three input fields: "Service (Oracle) :" with the value "oracle_irisserver", "Administrator ID :" with the value "lgiris", and "Password :" with the value "*****". At the bottom, there are two buttons: "OK" and "Cancel".

2.1.6 Generating and Registering Encryption Keys for Smart Card Operation

1. Select the Option > Set Smart Card (IA EAC Format)... item in the menu bar of the IrisServer main window and you will see the following window.



2. "Generate New Keys" button creates new keys for Smart Card encryption.



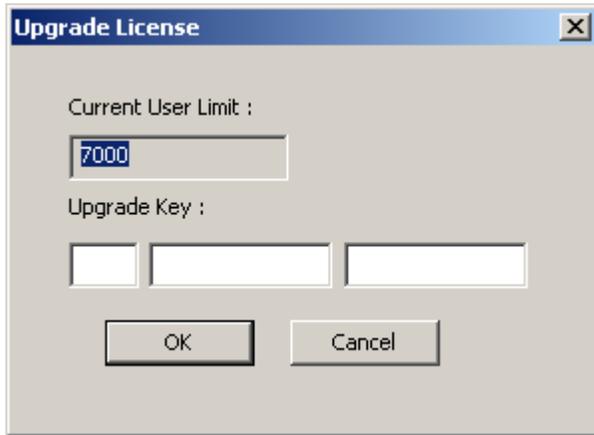
3. "Register Keys" Registers the displayed encryption keys into the database.

**Note: Keys must be registered before using IrisEnroll for the first time if using Smart Cards*

4. "Save Keys" Saves the encryption keys as a data file.
5. "Load Keys" Loads encryption keys from a file.

2.1.7 Upgrading License

1. Select the *Option* > "Upgrade License..." item in the menu bar of the IrisServer main window and you will see the following window.



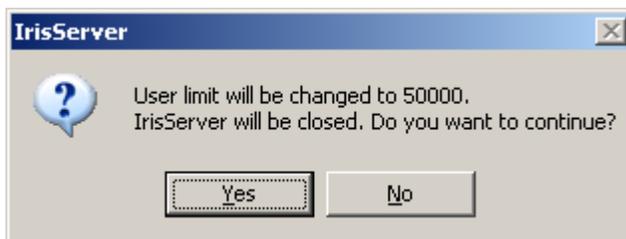
Current User Limit indicates the maximum number of users supported by current License Key.

2. Enter 18 digit upgrade key and click *OK*.
3. If the key is invalid the following dialog will be displayed.



Clicking *OK* button will display Upgrade License dialog to enter key again.

4. If the key is valid the following dialog will be displayed.



This is a sample UI on upgrading to 50000 users. License up-gradation requires a restart of IrisServer.

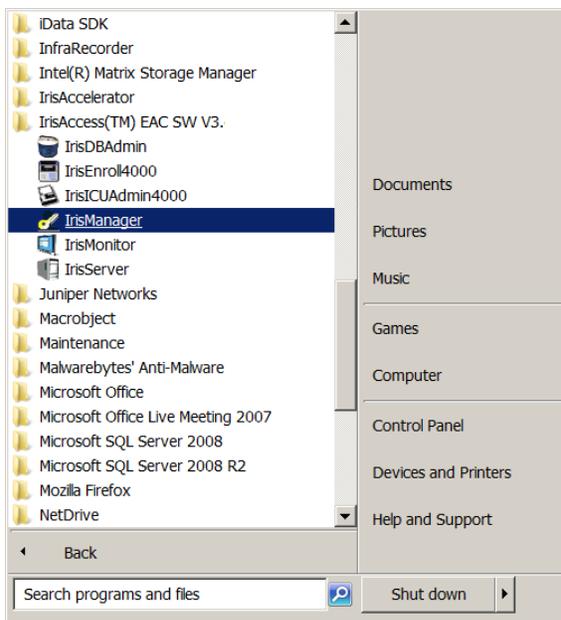
- (a) Click *Yes* to upgrade and IrisServer will exit.
- (b) Click *No* and License Key won't be upgraded.

2.2 IrisAccess™ IrisManager

IrisManager is used to manage the Users, Operators (Administrator-level only), Remote Units, Programs, and Groups, as well as Report generation.

2.2.1 How to Run IrisManager

To start the **IrisManager**, click on the **IrisManager** menu item. The location of the program is shown in the figure below.



2.2.2 How to Login to IrisManager

Clicking on the IrisManager icon will open the following login window.



To login to IrisManager:

1. Enter the ID and Password of an operator who has management rights. The default ID and password are “**administrator**” and “**iris3000**” respectively. These can be changed by the administrator. Refer to the section 2.2.8.2 Modification of the Administrator/Operator.
2. Click the *OK* button to login to the IrisManager.

To cancel, click on the *Cancel* button.

If the login to the IrisManager was successful, the following Notice window may appear (When you login with the default password “iris3000”).



Check the “Don’t open this window next time” option to avoid being notified next time you login.

Click on *No* to continue with the same password.

Click on *Yes* to get the following Operator information window used to change the password.

Operator information

Information

All fields marked with an asterisk (*) must be filled in completely.

* **Operator ID** administrator

User ID

First Name administrator

Last Name administrator

E-mail

Change password

Current Password

New password

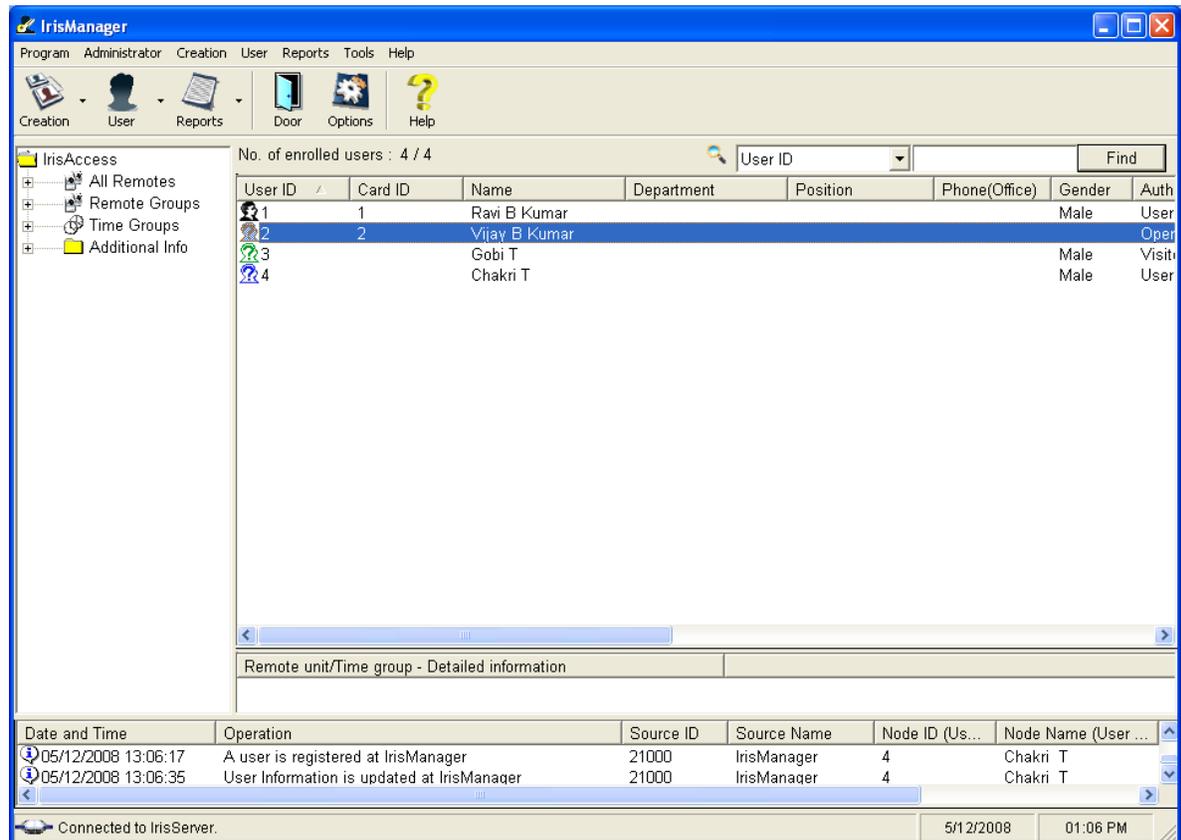
Confirm Password

Modify Cancel

Click on the “*Change Password button*” in the Operator information window. Enter the current password in the Current Password field, and enter the new password in the New Password and Confirm Password fields. Click the “*Modify*” button to change the password.

The main **IrisManager** window will be opened after changing the password successfully or aborting the password changing operation.

The same **IrisManager** window will be displayed without the Notice window, if the password is secured.



User Icon Key:

-  (Orange): Operator
-  (Orange): Operator whose iris not enrolled.
-  (Orange): Operator with no Remote/Time Group assigned.

-  (Black): General User
-  (Black): General User whose iris is not enrolled.
-  (Black): General User with no Remote/Time Group assigned.

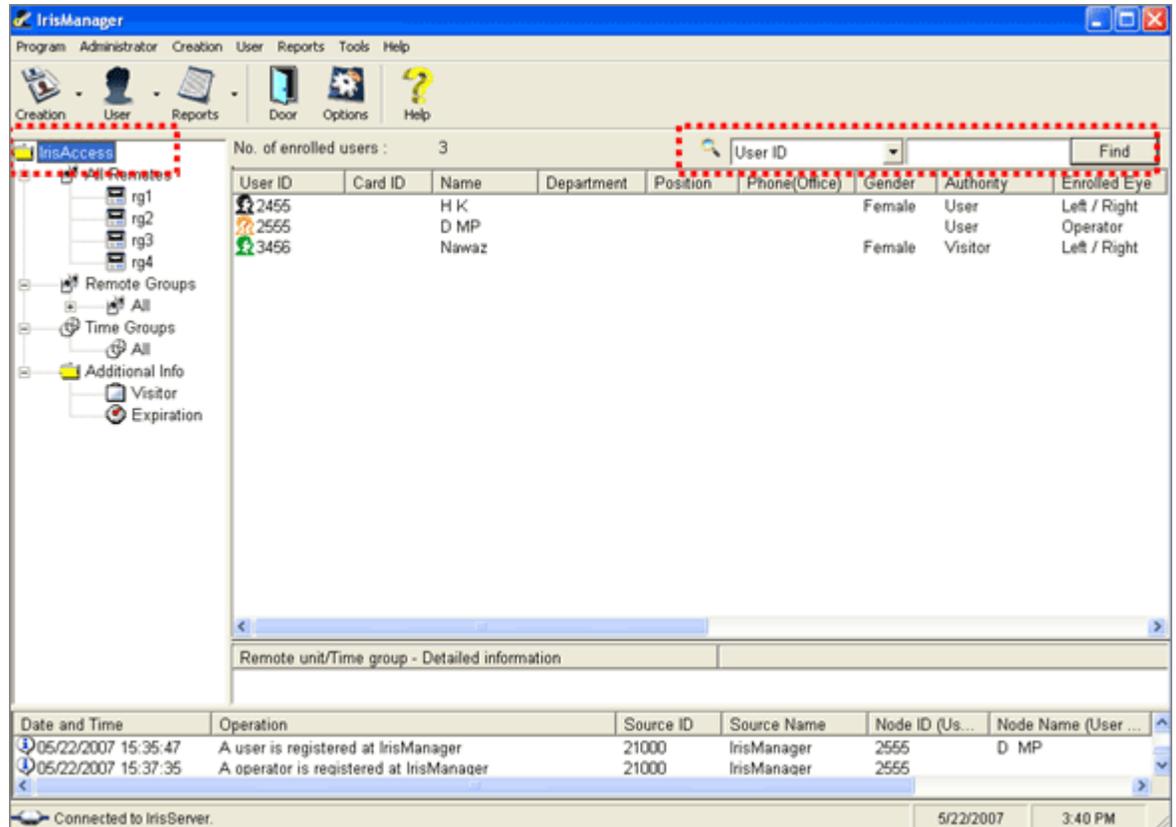
-  (Green): Visitor
-  (Green): Visitor whose iris is not enrolled
-  (Green): Visitor with no Remote Group or Reservation Time assigned.

-  (Blue): Operator/General User/Visitor whose term of validity is expired.
-  (Blue): Operator/General User/Visitor whose iris is not enrolled and term of validity is expired.

 (Blue): Operator/General User/Visitor with no Remote/Time Group assigned and whose term of validity expired.

In the **IrisManager** window, User Information (User ID, CardID, , Name, Department, Position, Telephone, Gender, Authority, Enrolled Eye, Warning Eye, Enrollment Date, Expiration Date, Reservation Time (Visitor only), and memos) can be viewed.

The user list may be filtered using the **Find** option. To use the find option, select either **User ID, First Name, Last Name, Gender, Department, Position,** or **Card ID** in the drop-down box highlighted below and enter or select the value in the next text box. Clicking the **Find** button will display all the user records that match the criteria selected in the **IrisManager** window. To reset **IrisManager** to display all user records, double-click the **IrisAccess** folder.



All **Remote Units** created in IrisManager may be viewed by clicking on

the **All Remote Units** item.

Remote Groups, Time Groups, Visitors, and Expiration Dates may be viewed using the items in the left pane.

2.2.3 Display when the Server DB is being Updated

When the following operations are performed in **IrisManager**, an entry is created in the **Status Frame** when **IrisServer** is updated.

- Registration of a user
- Modification or Deletion of user information
- Registration of a operator
- Modification or Deletion of operator information
- Registration of a remote unit, IrisEnroll, IrisManager or IrisMonitor
- Modification or Deletion of information about a remote unit, IrisEnroll, IrisManager or IrisMonitor
- Registration of a remote group, time group or holiday
- Modification or Deletion of information about a remote group, time group, holiday

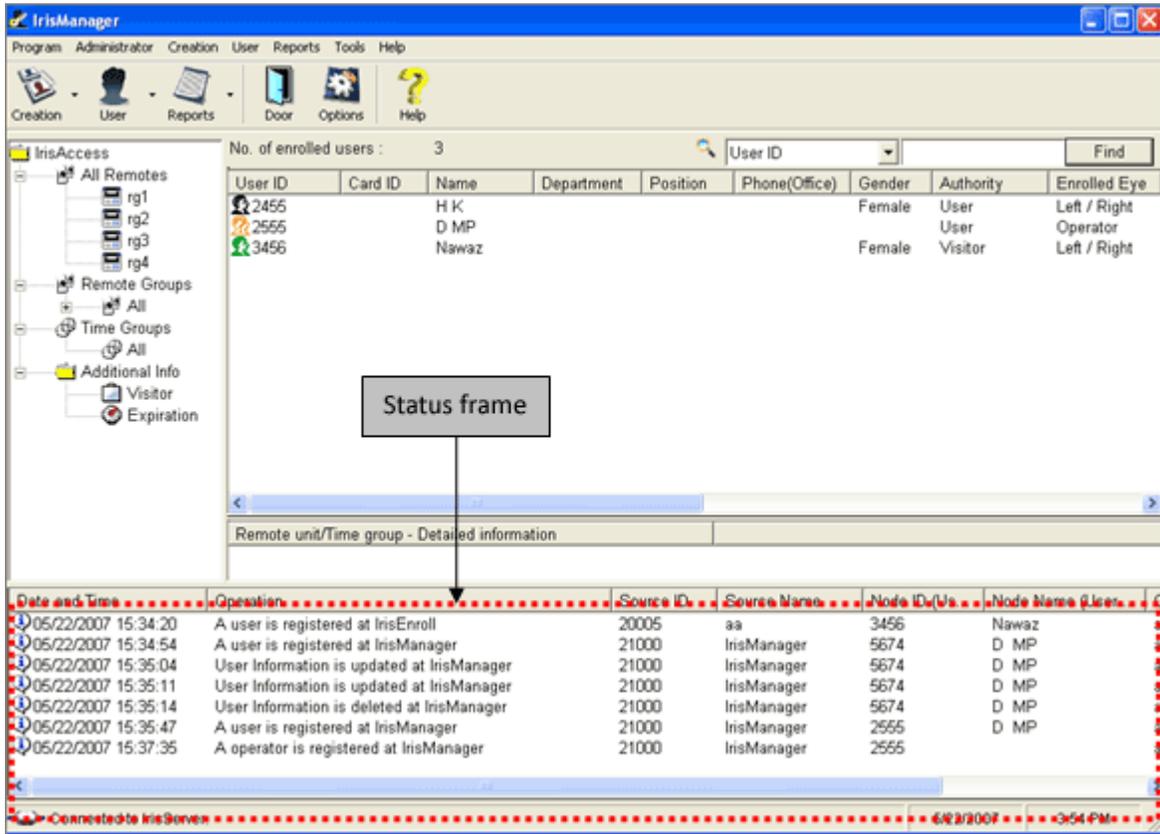
The screenshot shows the IrisManager application window. The title bar reads "IrisManager". The menu bar includes "Program", "Administrator", "Creation", "User", "Reports", "Tools", and "Help". Below the menu bar is a toolbar with icons for "Creation", "User", "Reports", "Door", "Options", and "Help".

The main interface is divided into several sections:

- Left Panel (Tree View):** Shows a hierarchy under "IrisAccess":
 - All Remotes (rg1, rg2, rg3, rg4)
 - Remote Groups (All)
 - Time Groups (All)
 - Additional Info (Visitor, Expiration)
- Top Right:** "No. of enrolled users : 3" and a search box for "User ID" with a "Find" button.
- Center Table:** A table listing enrolled users:

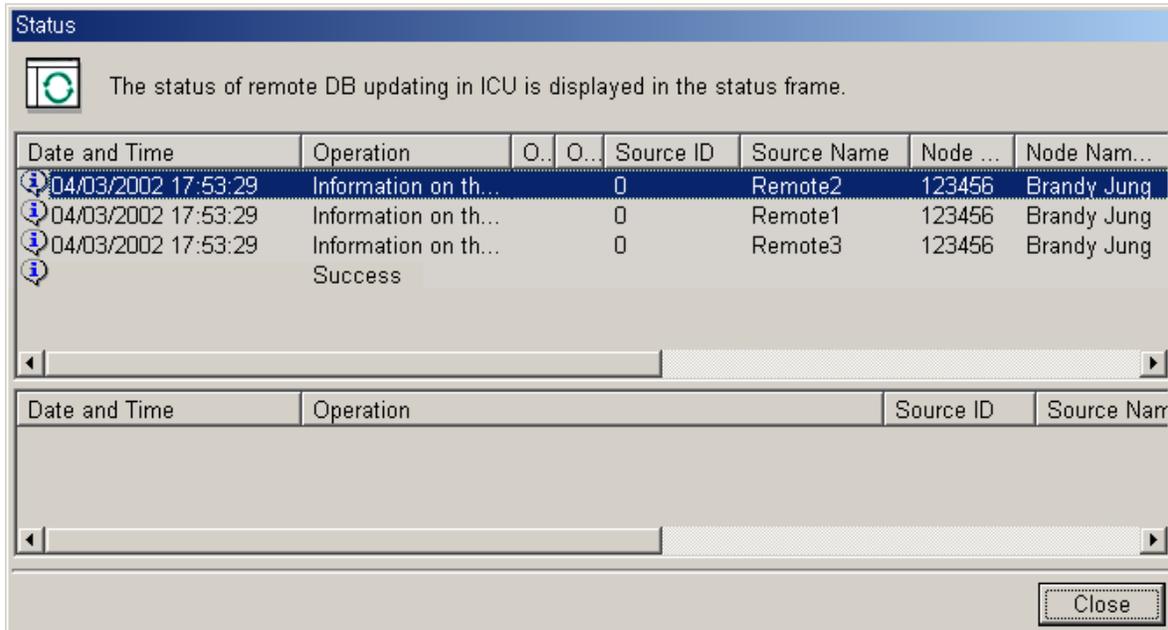
User ID	Card ID	Name	Department	Position	Phone(Office)	Gender	Authority	Enrolled Eye
2455		H K				Female	User	Left / Right
2555		D MP					User	Operator
3456		Nawaz				Female	Visitor	Left / Right
- Bottom Section:** A log of operations with columns: "Date and Time", "Operation", "Source ID", "Source Name", "Node ID (Us...", and "Node Name (User ...".

Date and Time	Operation	Source ID	Source Name	Node ID (Us...	Node Name (User ...
06/03/2005 10:08:13	User Information is updated at IrisManager	21000	Mgr1	1102	Brandy Park
06/03/2005 10:32:40	User Information is updated at IrisManager	21000	Mgr1	1102	Brandy Park
06/03/2005 10:32:57	User Information is updated at IrisManager	21000	Mgr1	1101	Ghali C G
06/03/2005 10:33:46	User Information is updated at IrisManager	21000	Mgr1	1102	Brandy Park
06/03/2005 10:34:04	A bio-Excel is registered at IrisManager	21000	Mgr1		Excel
- Bottom Right:** "Connected to IrisServer." and a timestamp "5/22/2007 3:40 PM".



2.2.4 Display when the Remote Database in ICU is being Updated

While the remote Database in the ICU is being updated, the following popup window is displayed in **IrisManager**. The status of update process is displayed in the status frame.



2.2.5 Display when IrisServer is Busy

If IrisServer is busy, the following window is displayed.

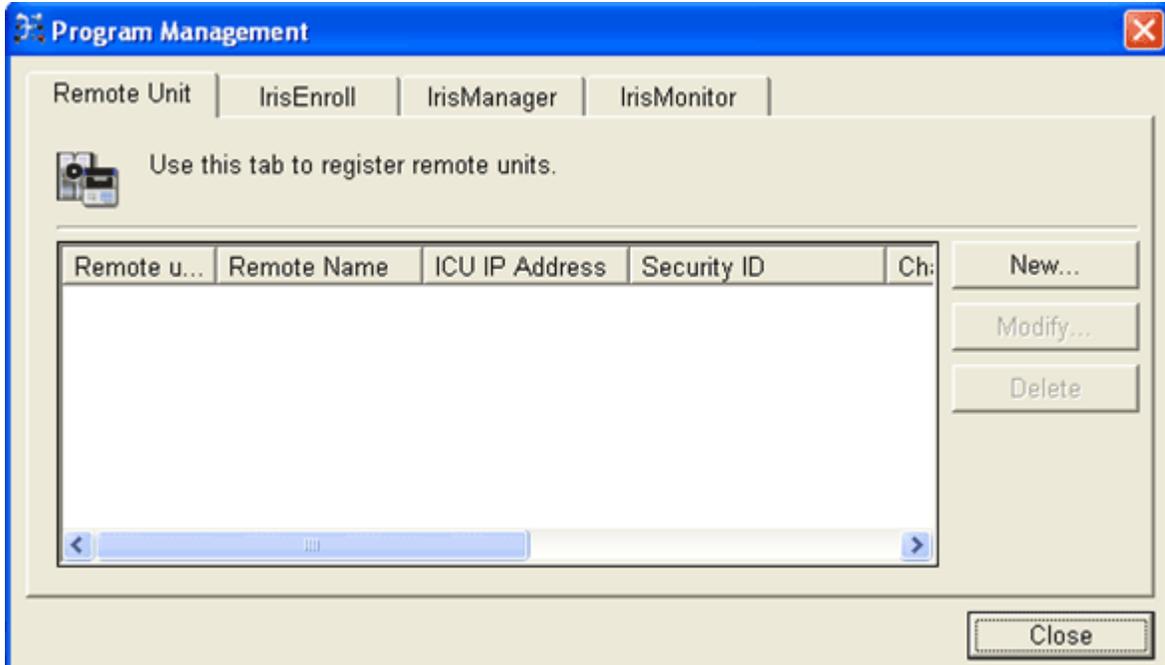


2.2.6 Program Management

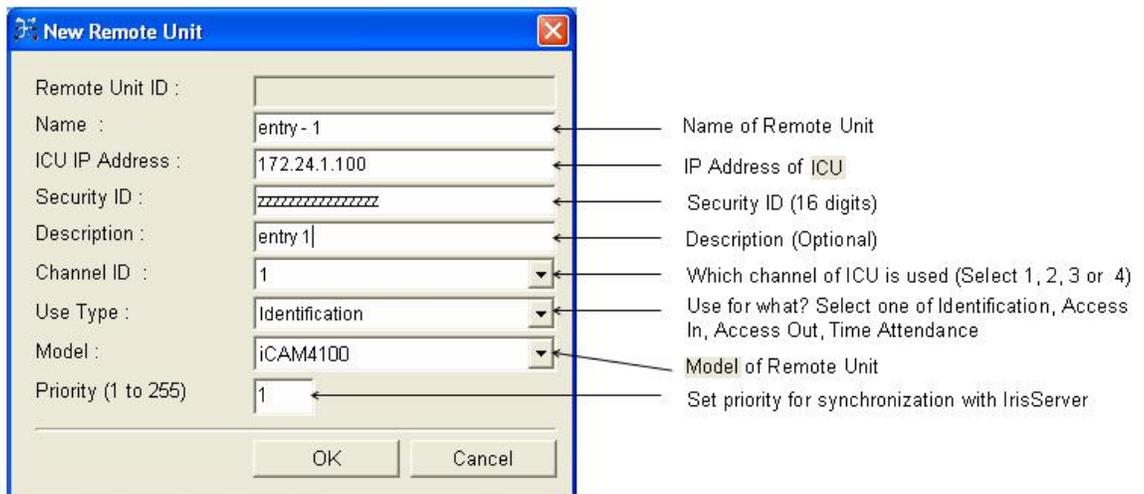
2.2.6.1 Register New iCAM4000/4100 series Remote Unit

New remote units may be registered in IrisManager by selecting the **Remote unit** item on the **Creation button** on the toolbar or from **Creation** on the menu bar.

Select **Remote Unit** after clicking on the **Creation** button from the toolbar or from the menu bar. The following **Program Management** popup window is displayed.



1. To register a new remote unit, click on the **New** button. The **New Remote Unit** window is displayed.



2. To add the Information of **New Remote Unit**,

- a. Enter the **Name** of the remote unit, **ICU IP Address** of the ICU it is attached to, **Security ID** and the **Description** (optional). You must also select the **Channel ID** that the remote unit is connected to in the ICU and **Use Type** from the combo boxes in the **New Remote Unit** window. The **Use Type** selection does not affect the operation of the remote unit. Remote unit use type specifies functionality. You must also select the **model** type being used. Enter the Priority number of camera type that will be used – By default, the priority level is set to 1, which is the highest priority.

***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.*

3. Once all the required fields are entered, click on **OK** button to complete the remote unit registration.
 - ◆ The **Security ID** must be identical to the **Security ID** typed in during ICU configuration. A different **Security ID** has to be assigned to each remote unit with 16 characters that are numbers, capital or lower case letters and special characters. Please refer to section 2.2, item 4 in the document **IrisAccess Software Installation Manual** (Document No. DV002S501).
4. The successful addition of the remote unit causes the **Status** window to pop up, explained in the section 2.2.4. Click on **Close** button in the **Status** window to close it.

2.2.6.2 Register New iCAM7000/7100 series Option 3 Remote Unit

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.

The image shows a 'New Remote Unit' dialog box with the following fields and values:

Field	Value
Remote Unit ID :	
Name :	23_43
ICU IP Address :	10.227.24.4
Security ID :	xxxxxxxxxxxxxxxx
Description :	Entry -1
Channel ID :	1
Model :	iCAM7100 + Matching
Priority (1 to 255)	1

2.2.6.3 Register New iCAM7000/7100 series Option 1 Remote Unit with ICU7000

IrisManager allows creation of remote unit for iCAM7000/7100 Option 1. Refer picture below.

The ICU7000 settings should be configured prior to performing the configuration setup procedures performed in this section. Follow this section to properly assign the ICU7000 settings into the IrisManager section of the iData EAC software (version 3.07.08 and above).

1. Open the IrisServer.exe application (if not open already).
2. Open the IrisManager application (default User ID = administrator / Password = iris3000).
3. Select > Creation > Remote Unit
4. Press > New
 - a. Fill in the Name field (any description desired can be entered).
 - b. Enter the ICU7000 IP address.
 - c. Enter the ICU7000 security ID.
 - d. Fill in the ICU channel description field (this can be left blank or entered with any description).
 - e. Select Channel ID 1 from the dropdown box.
 - f. Select the Model type of iCAM7000 series and ICU7000 from the dropdown box.

Remote Unit ID :

Name :

ICU IP Address :

Security ID :

Description :

Channel ID :

Model :

Priority (1 to 255) :

Model options:

- iCAM4000 + ICU
- iCAM4100 + ICU
- iCAM7000 + ICU4000
- iCAM7100 + ICU4000
- iCAM7000 + ICU7000
- iCAM7100 + ICU7000

2.2.6.4 Modify Remote Unit Information

The information about the existing **Remote Unit(s)** may be modified.

To modify the Remote Unit information:

1. Select **Remote unit** after clicking on **Creation** in the menu bar. The following window will appear on the screen.

Program Management

Remote Unit | IrisEnroll | IrisManager | IrisMonitor

Use this tab to register remote units.

Remote u...	Remote Name	ICU IP Address	Security ID	Ch:
5	Remote1	172.24.3.203	5555555555555555	1

Buttons: New..., Modify..., Delete, Close

Select the **Remote Unit** to be modified and click on the **Modify** button (shown with an arrow in the above figure). The following window appears on the screen.

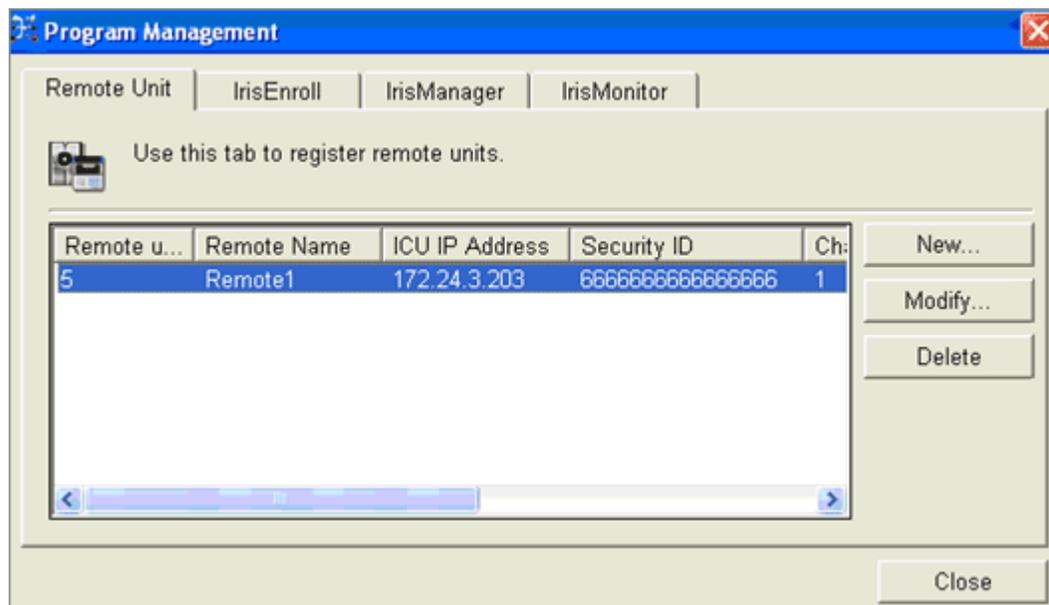
2. Modify the fields to be updated and then click on **Modify** button to register the modified values with the database.
3. The successful modification of the remote unit causes the **Status** window to pop up, explained in the section 2.2.4. Click on **Close** button in the **Status** window to close it.
 - ◆ If no **Remote Unit** was selected before clicking the **Modify** Button in Step 2, then the following window will pop-up.



2.2.6.5 Delete Remote Unit

The existing Remote Units may be deleted using the following steps:

1. Select **Remote unit** after clicking on **Creation** in the menu bar. The following window will appear on the screen.



2. Select the **Remote Unit** to be deleted and then click on the **Delete** button. The following **Confirmation** window will be displayed. This message prevents the accidental deletion of a **Remote Unit**.



3. Clicking on the **Yes** button to delete the **Remote Unit** will display the following window.



4. Click on **OK**. The successful deletion of the remote unit results in the **Status** window opening, explained in the section 2.2.4. Click on **Close** button in the **Status** window to close it.

2.2.6.6 Registering IrisEnroll

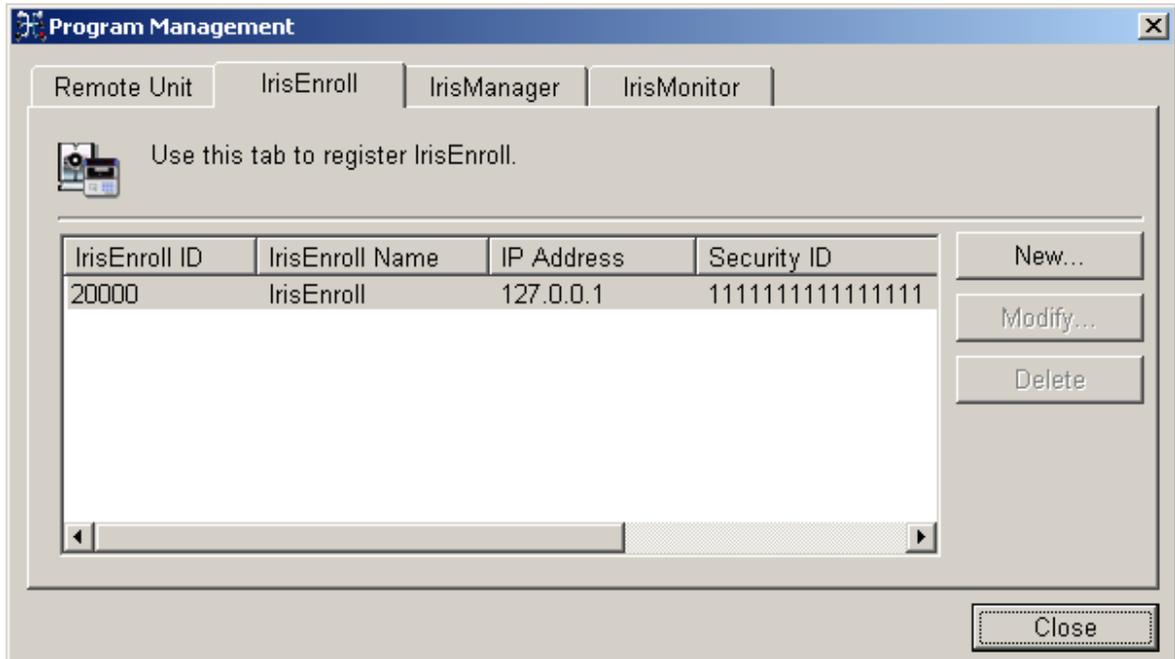
IrisEnroll is used to enroll the Iris of users into the system, and for identification or verification of the users.

- ✓ IrisEnroll Creation Count

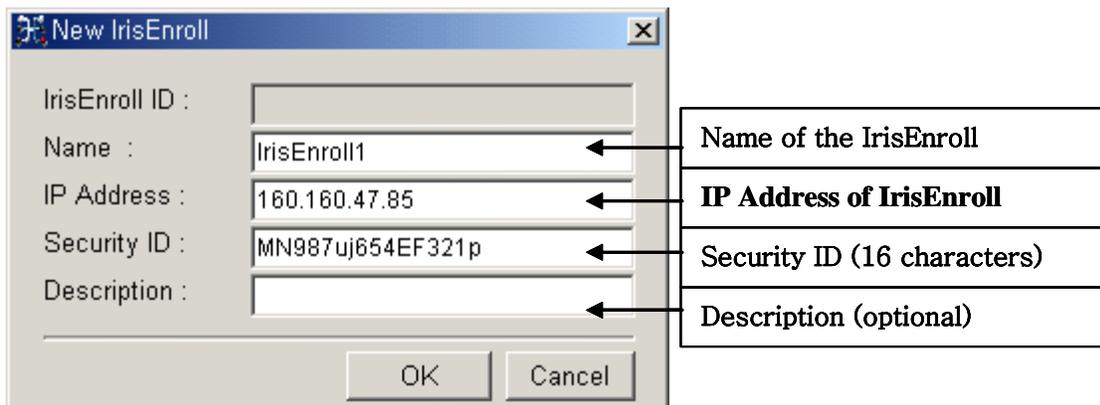
The maximum number of IrisEnroll that can be registered is 32

IrisEnroll can be registered using the following steps.

1. Select **IrisEnroll** after clicking on **Creation** in the menu bar.



- Click on the **New** button (which is shown with an arrow in the above figure) to get the following **New IrisEnroll** window used to enter the information for the New **IrisEnroll**.



- Fill the fields **Name**, **IP Address**, **Security ID*** and **Description** (optional) in the **New IrisEnroll** window. If **IrisEnroll** will be located on the same computer as **IrisServer** and **IrisManager**, we recommend entering the loopback address (127.0.0.1) as the IP Address.

- ◆ **Security ID** (You may create any **Security ID** at your disposal). **Security ID** must be identical to the **Security ID** entered when running IrisEnroll for the first time. **Security ID** must consist of 16 characters that are numbers,

capital or lower case letters and special characters. (These characters are case-sensitive). Click on the **OK** button to complete the registration.

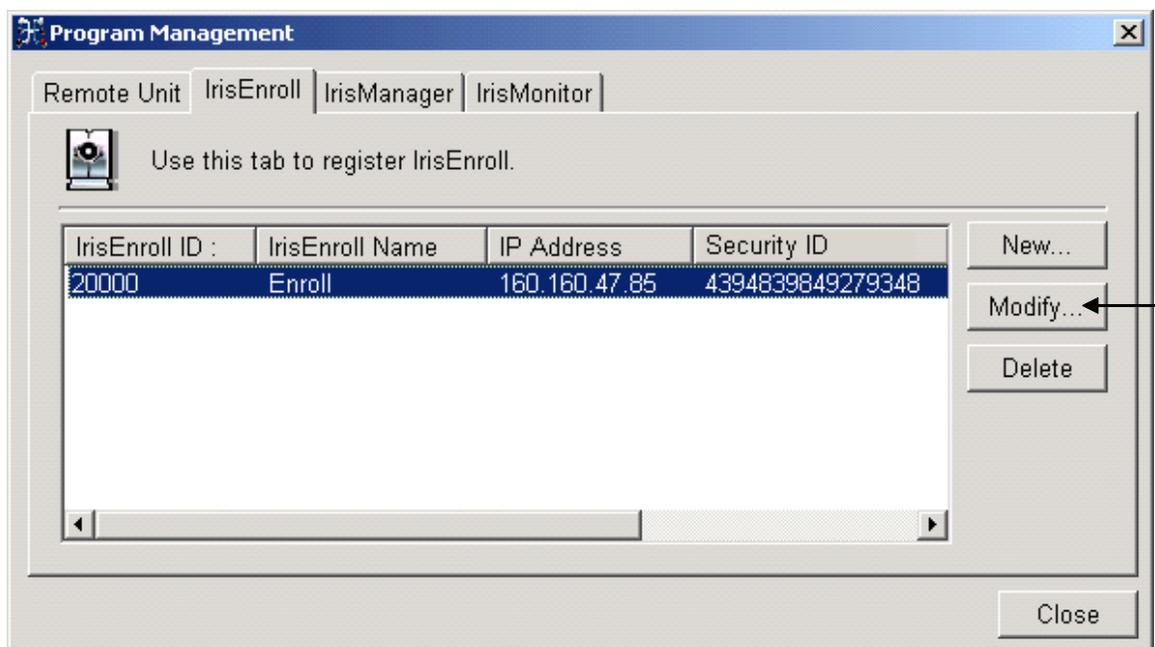
4. Registration of IrisEnroll may be cancelled by clicking on **Cancel** button.

2.2.6.7 Modification of IrisEnroll Information

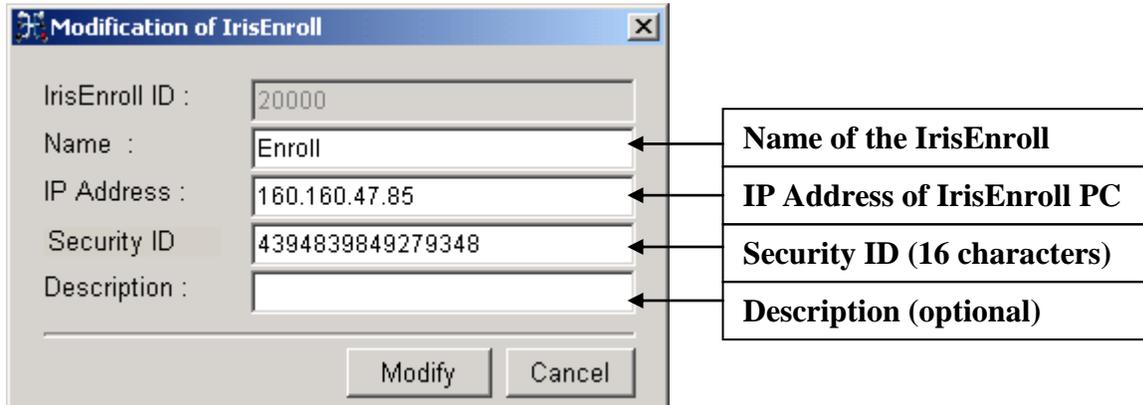
The information about the existing IrisEnroll(s) may be modified.

The steps to modify IrisEnroll information are:

1. Select **IrisEnroll** after clicking on **Creation** from the menu bar. The following **Program Management** window will open.



2. Select the **IrisEnroll** entry to be modified from the list of existing **IrisEnroll(s)**.
3. Click on the **Modify** button (which is shown with an arrow in the above figure). The following **Modification of IrisEnroll** window is displayed.



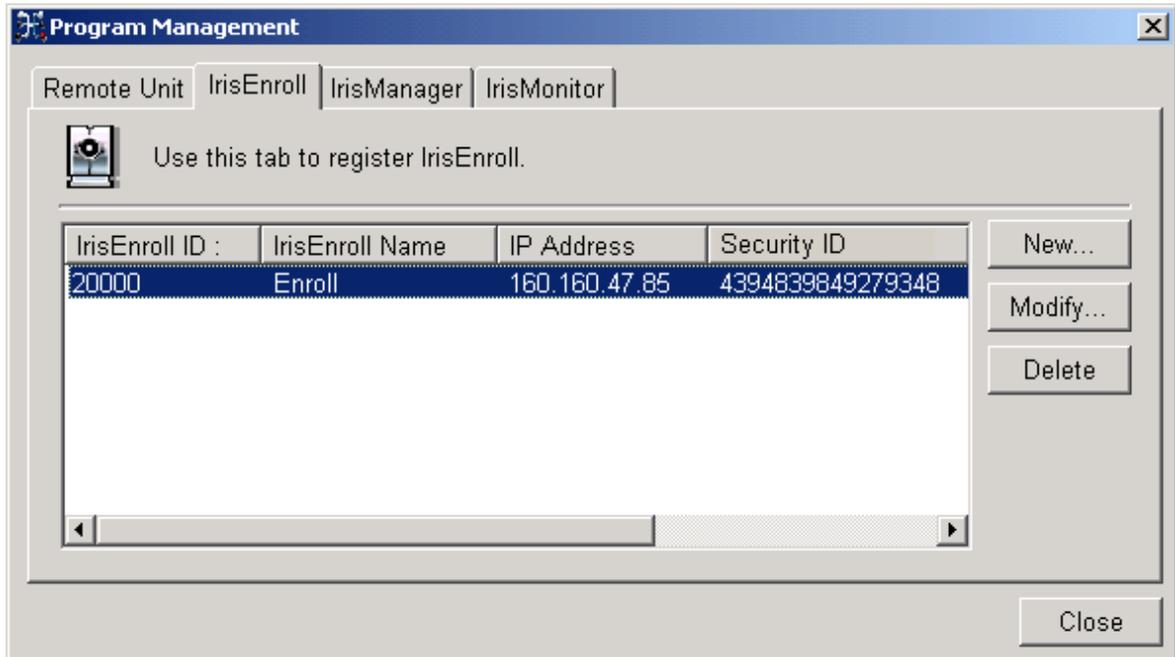
4. Change the fields to be updated and click on Modify to register these updated values.
5. To cancel the modification of the IrisEnroll, click on Cancel button.

2.2.6.8 Delete IrisEnroll

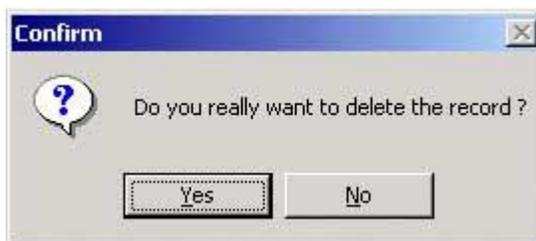
Existing **IrisEnroll(s)** may be deleted using this feature.

To **delete** an **IrisEnroll(s)** entry:

1. Select **IrisEnroll** after clicking on **creation** from the menu bar to get the **Program Management** window.



2. Select the **IrisEnroll entry** to delete from the list of existing **IrisEnroll(s)**.
3. Click on the **Delete** button (which is shown with an arrow in the above figure). A confirmation window opens on the screen as shown in the figure below.



4. Click on the **Yes** button in the **Confirm** window to delete the **IrisEnroll** entry.
5. Accidental removal of the **IrisEnroll** can be avoided by clicking on the **NO** button.
6. If no **IrisEnroll** was selected before pressing the **Delete** button, then the following **warning** window appears on the screen.



7. In this case, click on **OK** and continue from step 2 to delete the **IrisEnroll** entry.

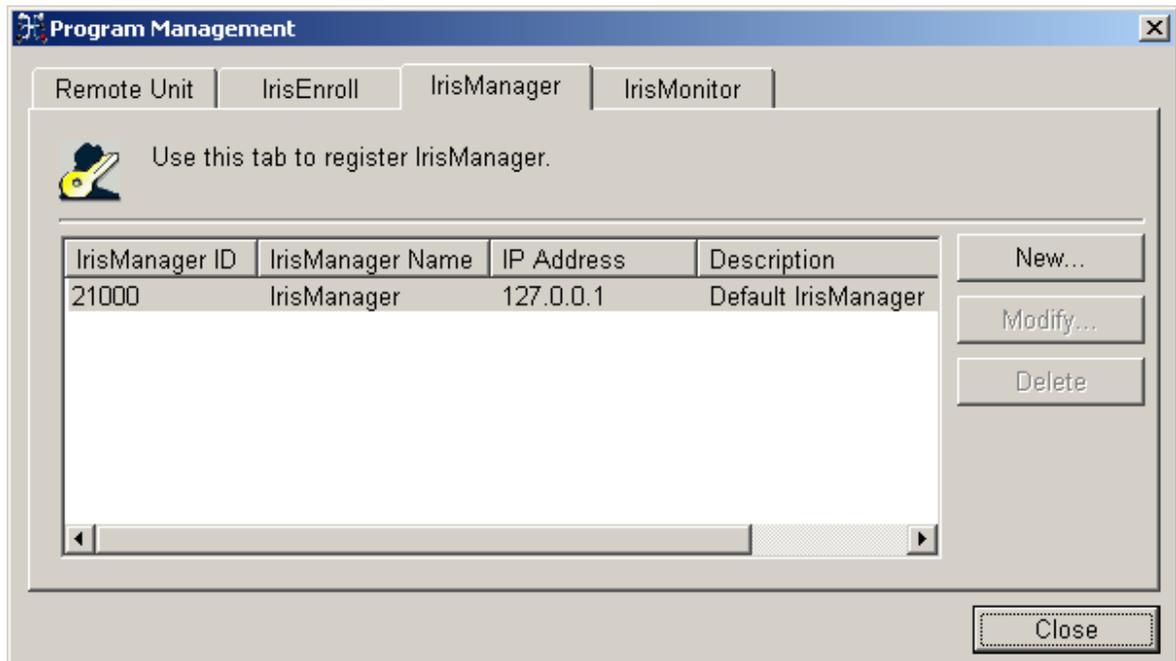
2.2.6.9 Registration of IrisManager

You can register up to 10 **IrisManager(s)**, but only **1** IrisManager may be connected to IrisServer at any time. The initial IrisManager registration must be performed through IrisServer. Please refer to the Section 2.1.3 **REGISTRATION OF IrisManager** in this manual for details.

- ✓ If an IrisManager is already connected to IrisServer and a second IrisManager attempts connection, the second IrisManager will receive “**Another IrisManager(Manager_1) is already connected to server**” message.

IrisManager can be registered using the following steps.

1. Select **IrisManager** after clicking on **Creation** in the menu bar.



2. Click on the **New** button (which is shown with an arrow in the above figure) to open the following **New IrisManager** window.



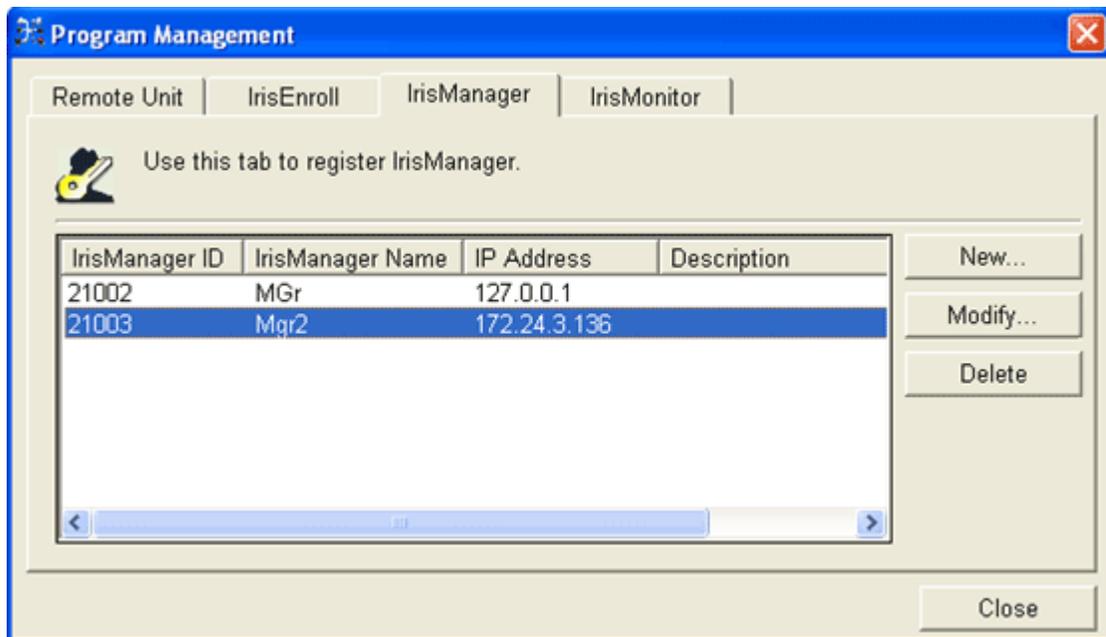
3. Fill in the fields **Name**, **IP Address**, and **Description** (optional) in the **New IrisManager** window.
4. Click on the **OK** button to complete the registration of the **IrisManager**.
5. The registration of the **IrisManager** can be cancelled by clicking on **Cancel** button.

2.2.6.10 Modify IrisManager Information

The information about an existing IrisManager may be modified.

The steps to modify IrisManager information are

1. Select **IrisManager** in the **Creation** item, from the toolbar or from the menu to open the following **Program Management** window.



2. Select the **IrisManager** entry to be modified.
3. Click on the **Modify** button (which is shown with an arrow in the above figure). The following window is displayed.



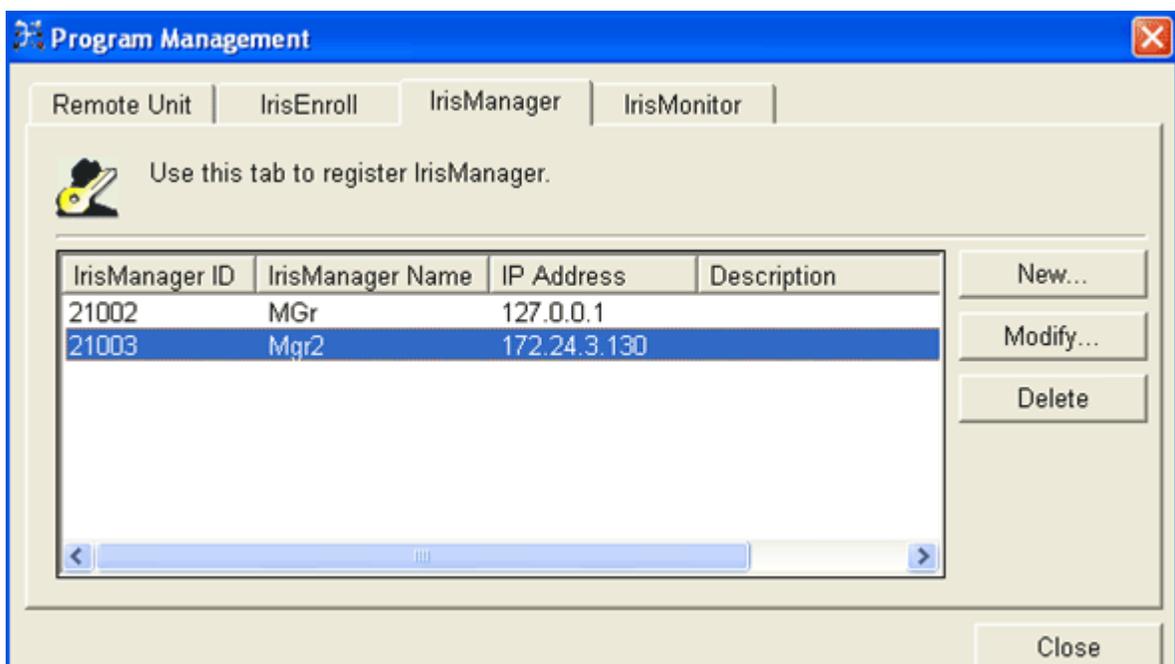
A dialog box titled "Modification of IrisManager" with a close button (X) in the top right corner. It contains four text input fields: "IrisManager ID" with the value "21003", "Name" with the value "Mgr2", "IP Address" with the value "172.24.3.130", and "Description" which is empty. At the bottom, there are two buttons: "Modify" and "Cancel".

4. Change the fields to be updated and click on the **Modify** button to register the updated values.
5. The **Cancel** button may be used to cancel the modification of the IrisManager entry.

2.2.6.11 Delete IrisManager

An existing IrisManager entry may be deleted using the following steps:

1. Select **IrisManager** after clicking on **Creation** from the menu bar to open the following **Program Management** window.



A window titled "Program Management" with a close button (X) in the top right corner. It has four tabs: "Remote Unit", "IrisEnroll", "IrisManager", and "IrisMonitor". The "IrisManager" tab is selected. Below the tabs, there is a key icon and the text "Use this tab to register IrisManager." Below this is a table with four columns: "IrisManager ID", "IrisManager Name", "IP Address", and "Description". The table contains two rows: one with ID "21002", Name "MGr", and IP "127.0.0.1"; and another with ID "21003", Name "Mgr2", and IP "172.24.3.130". The second row is highlighted. To the right of the table are three buttons: "New...", "Modify...", and "Delete". At the bottom right of the window is a "Close" button.

IrisManager ID	IrisManager Name	IP Address	Description
21002	MGr	127.0.0.1	
21003	Mgr2	172.24.3.130	

2. Select the **IrisManager** entry to be deleted.
3. Click on the **Delete** button (which is shown with an arrow in the above figure). The following **Confirm** window opens up.



4. Click on the **Yes** button to **delete** the **IrisManager** entry.
5. Accidental deletion of an **IrisManager** entry may be avoided by clicking on the **No** button.

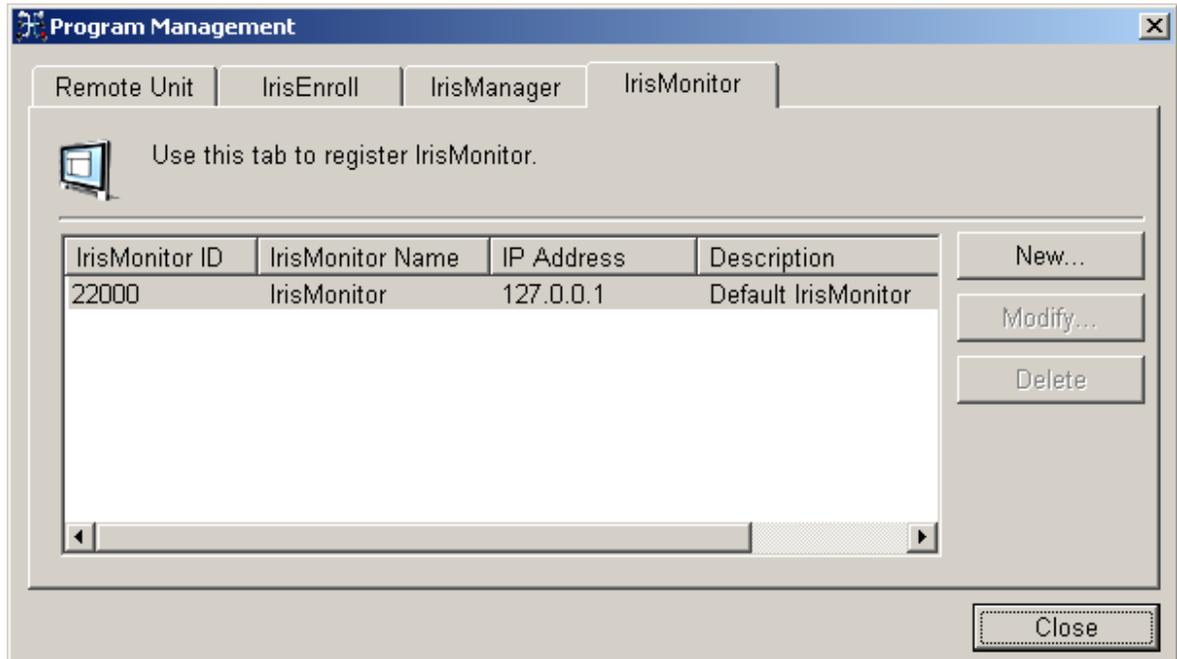
2.2.6.12 Register IrisMonitor

IrisMonitor is used to monitor the IrisAccess system.

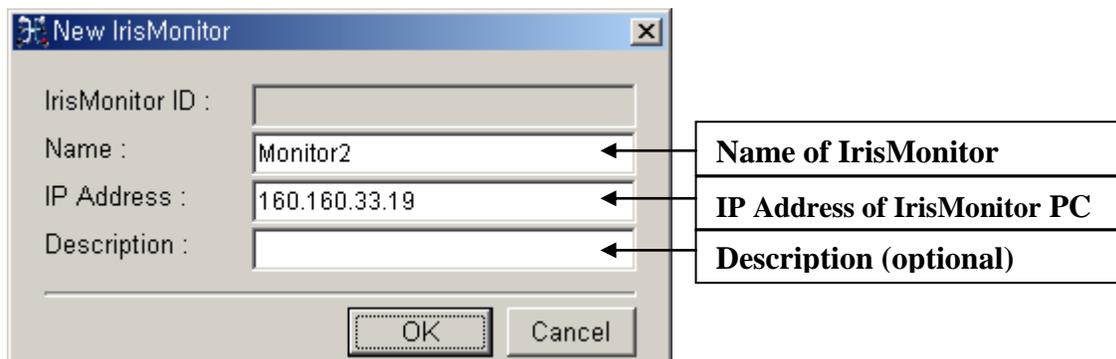
- ✓ IrisMonitor Creation Count
The maximum number of **IrisMonitor(s)** that may be registered is 10

Below is the process for registering an instance of **IrisMonitor** with the **IrisManager**.

1. Select **IrisMonitor** after clicking on **Creation** in the menu bar, to get the following **Program Management** window.



2. Click on the **New** button (Which is shown with an arrow in the above figure).
3. The **New IrisMonitor** window opens. This window is used to enter the information for the **New IrisMonitor**.



4. Enter the Name, IP Address and Description. The Description field is optional. If IrisMonitor will be located on the same computer as IrisServer, we recommend entering the loopback address (127.0.0.1) as the IP Address.
5. Click on the OK button to complete the registration of the new IrisMonitor with the IrisManager. If any of the required field were not filled, an error message box appears. For example, if the name field is not filled, the following window appears.



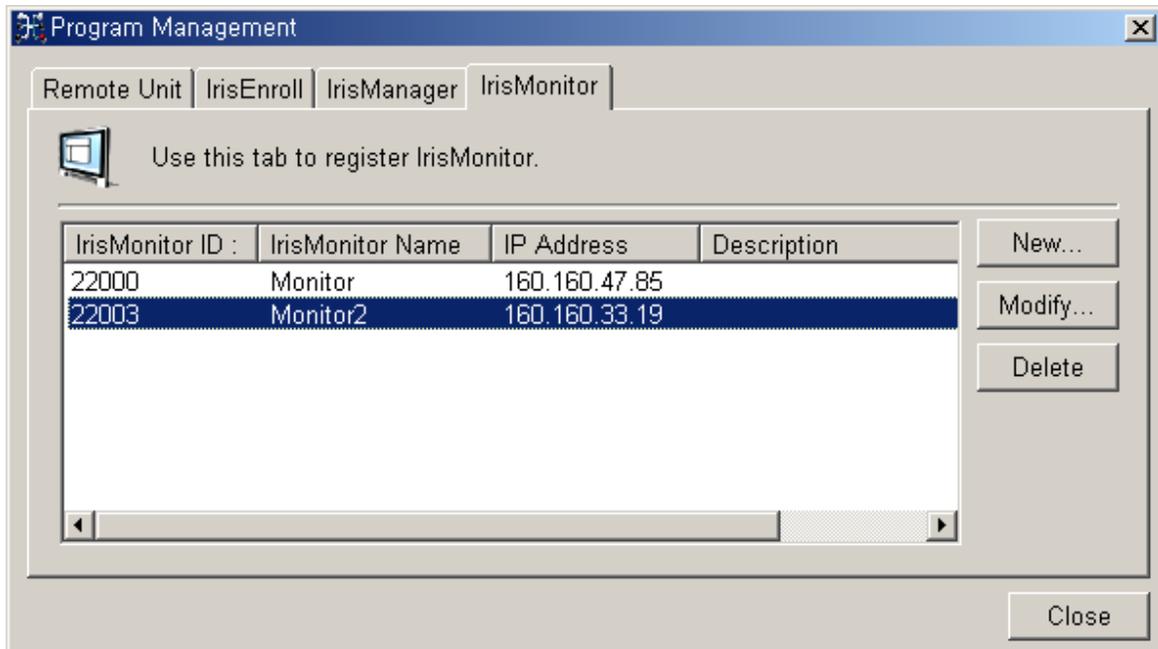
6. In this case, click on **OK** button, to return to the **New IrisMonitor** window and continue from step 2.
7. The addition of **New IrisMonitor** may be cancelled by clicking on the **Cancel** button in the **New IrisMonitor** window.

2.2.6.13 Modification of IrisMonitor Information

The information about the existing **IrisMonitor(s)** may be modified using this feature.

The steps to modify **IrisMonitor** information are:

1. Select **IrisMonitor** after clicking on **Creation** from the menu bar to get the following **Program Management** window:



2. Select the IrisMonitor entry to be modified from the list.

3. Click on the Modify button (which is shown with an arrow in the above figure), to open the Modification of IrisMonitor window, used to view/edit the IrisMonitor information.



The image shows a dialog box titled "Modification of IrisMonitor". It contains four text input fields: "IrisMonitor ID" with the value "22003", "Name" with the value "Monitor2", "IP Address" with the value "160.160.33.19", and "Description" which is empty. At the bottom right, there are two buttons: "Modify" and "Cancel".

4. Change the fields to be updated and click on Modify to register these updated values.
5. If any of the required fields (Name and IP Address) are blank, then a message will be displayed. For example, if the Name field is not filled then the following message will open on the screen.



6. In this case, click on the **OK** button to return to the **Modification of IrisMonitor** window
7. To cancel the modification of the **IrisMonitor** entry click on the **Cancel** button in the **Modification of IrisMonitor** window.
8. If no **IrisMonitor** entry was selected before clicking on the Modify button in the **Program Management** window, a **warning** window is displayed as shown below.



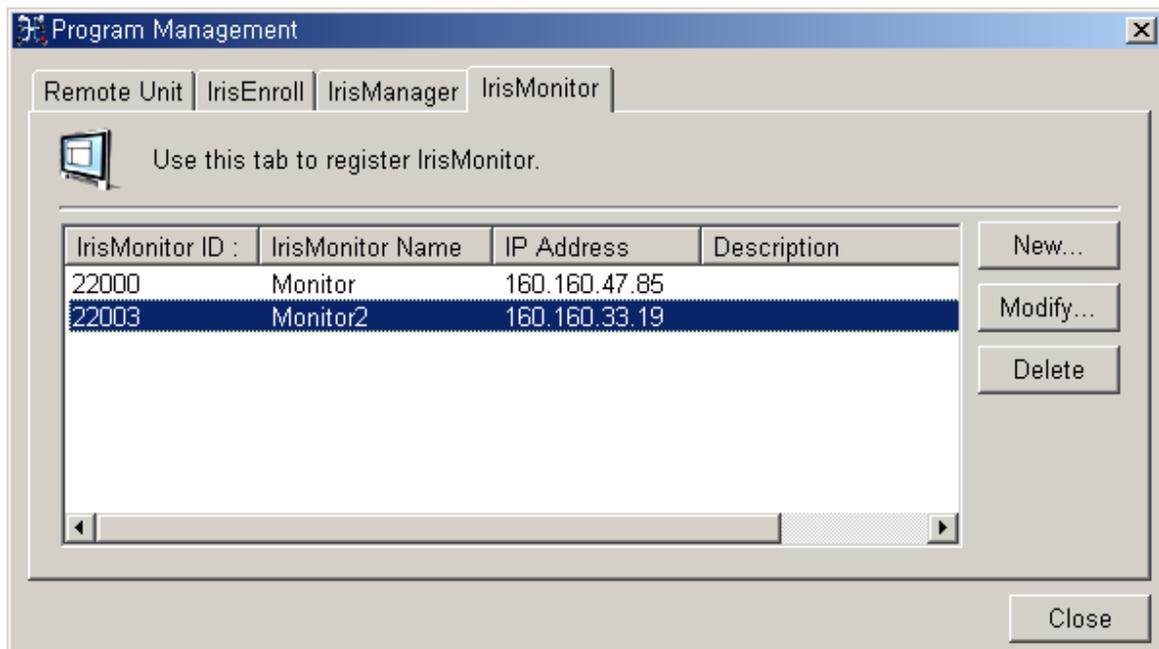
9. In this case, click on **OK** and continue from step 2 to **modify** the **IrisMonitor** successfully.

2.2.6.14 Delete IrisMonitor

The existing **IrisMonitor(s)** can be deleted using this feature.

The steps to delete an existing **IrisMonitor** entry are:

1. Select **IrisMonitor** after clicking on **Creation** from the menu bar to get the following **Program Management** window:



2. Select the **IrisMonitor** entry to be deleted.

3. Click on the **Delete** button (which is shown with an arrow in the above figure). The following **Confirmation** window is displayed on the screen.



4. Click on the **Yes** button to delete the **IrisMonitor** entry.
5. Accidental removal of the IrisMonitor may be avoided by clicking on the **NO** button.
6. If no IrisMonitor was selected in **Program Management** window, during step2, before executing step3, the following **warning** window appears on the screen.



7. In this case, click on **OK** button to return to the **Program Management** window and continue from step2 to delete the **IrisMonitor** entry successfully.

2.2.7 Group Management

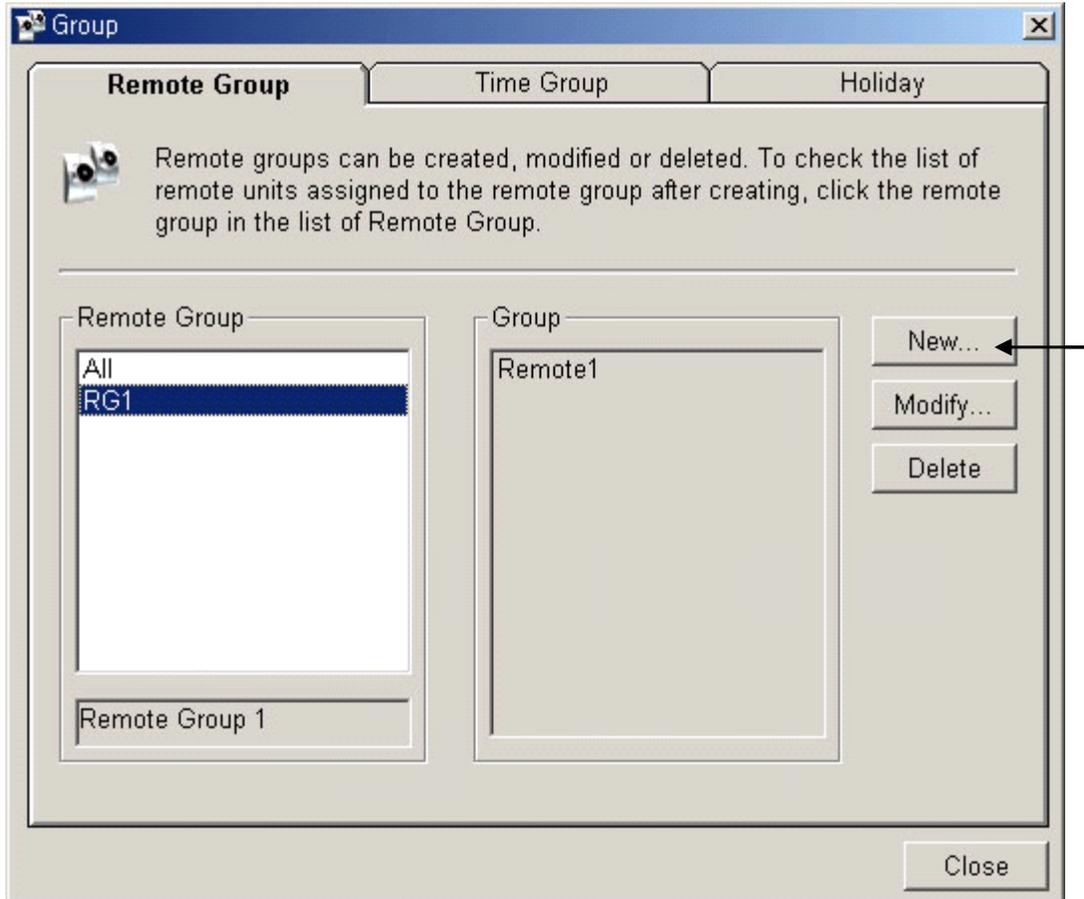
2.2.7.1 Add Remote Group

This feature is used to add a **New Remote Group** to the **IrisManager**.

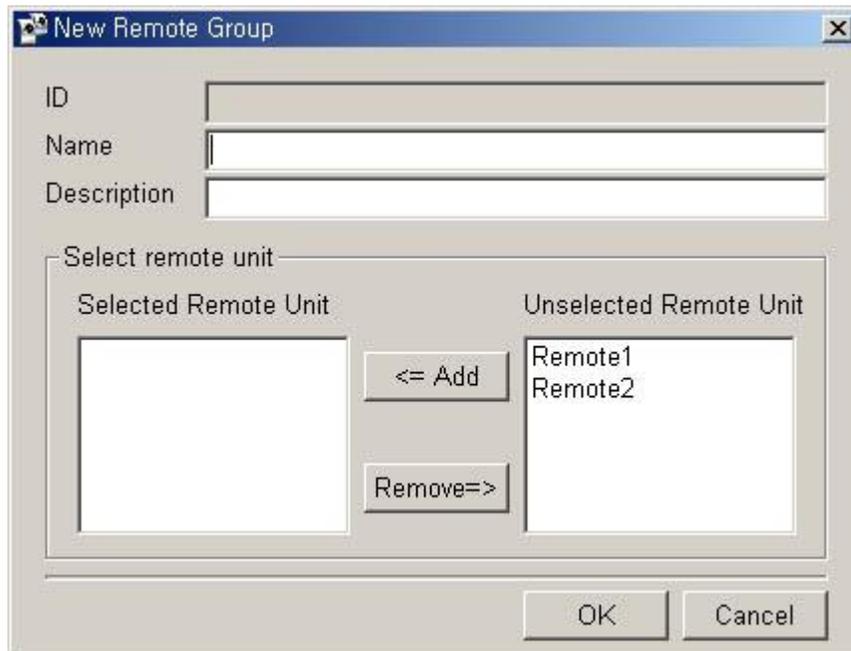
The maximum number of Remote Groups that may be registered is 255 in Basic and Extended version.

Below is the process to add a new remote group to the existing system.

1. Select **Remote Group** after clicking on **Creation** in the menu bar, to open the following **(Group)** window.



2. Click on the New button, to open the following New Remote Group window.



3. Select the **Remote Units** for the new **Remote group** from the listed Remote Units in the right side of the window, labeled **Unselected Remote Unit**.
4. After selection, the **Remote Units** may be added to the new **Remote Unit Group** by clicking the **Add** button. The added **Remote units** can be seen in the window labeled **Selected Remote Unit**.
5. Selecting the Remote Unit from the window labeled **Selected Remote Unit** and then clicking on the **Remove** button removes the selected Remote Units.
6. Click on the **OK** button to complete the addition of the new **Remote Group**. Click on the **Cancel** button to cancel the addition of the new **Remote Group**.

The successful addition of the **Remote Group** causes the **Status** window to open, explained in section 2.2.4. Click on the **Close** button in the **Status** window to close it.

If the **Name** field is blank for the New **Remote Group**, then clicking on **OK** in **New Remote Group** window will open the following **warning** window on the screen.

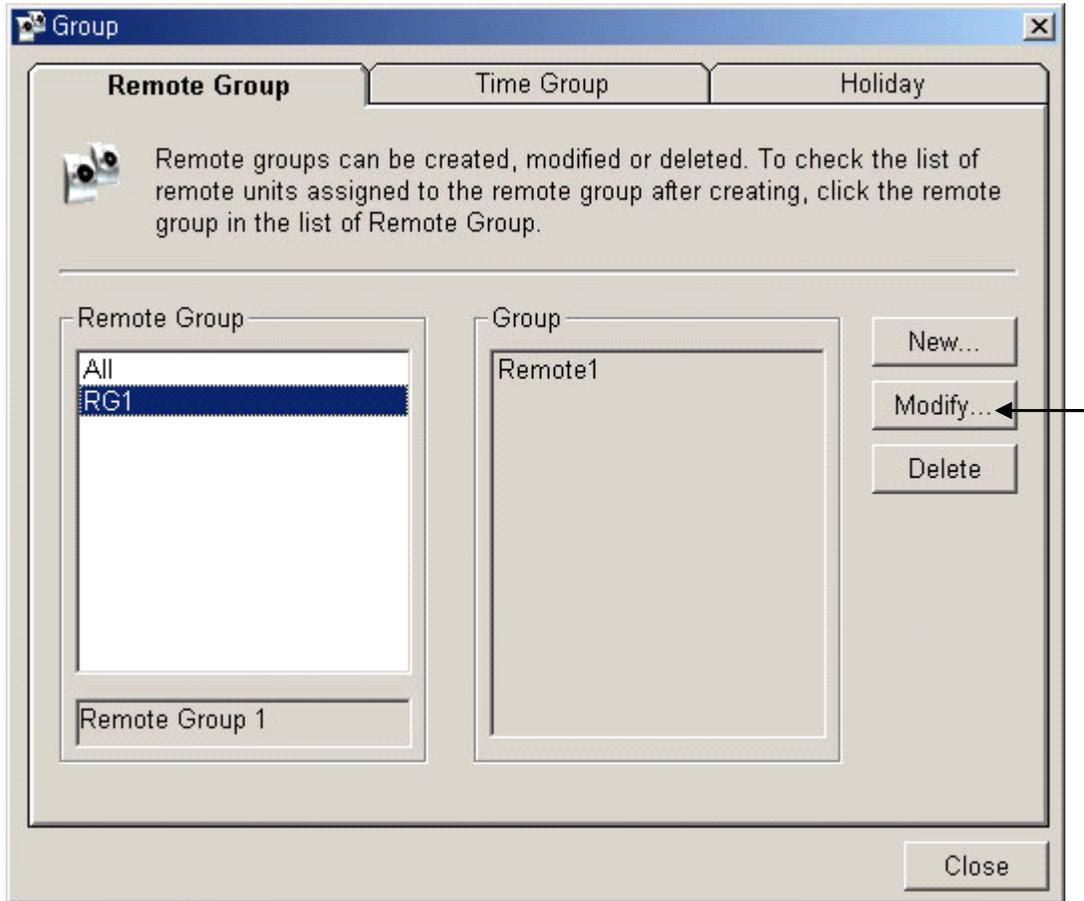


In this case, click on the **OK** button, to get the **New Remote Group** window. Then enter the required fields to successfully add the new **Remote Group**.

2.2.7.2 Modify Remote Group

Below are the steps to modify an existing **Remote Group**.

1. Select Remote Group after clicking on Creation in the menu bar, to open the following (Group) window used to Modify the existing Remote Group.



2. Select the Remote Group to be modified from the Remote group list.
3. Click on the Modify button (shown with an arrow in the figure above) to modify the selected Remote Group. The following Modification of Remote group window is displayed as shown in following figure:

4. New Remote Unit(s) can be added to the Remote Group by selecting the Remote unit from the list of Remote Units in the list Unselected Remote Units and then clicking on the button Add.
5. Existing Remote Unit(s) may be removed from the Remote Group by selecting the Remote Unit(s) from the list labeled Selected Remote Unit and clicking on the button Remove
6. The Name and Description of the Remote Group may be modified by entering the new Name and Description respectively.
7. Click on the Modify button to update the Remote group with these changed values. Click on the Cancel button to cancel the modifications.

The successful modification of the **Remote group** results in the opening of the **Status** window, explained in the section 2.2.4. Click on the **Close** button in the **Status** window to close it.

If the Name field is blank or the list of the **selected Remote Units** is empty, then clicking on **Modify** button will open the following **warning** window.



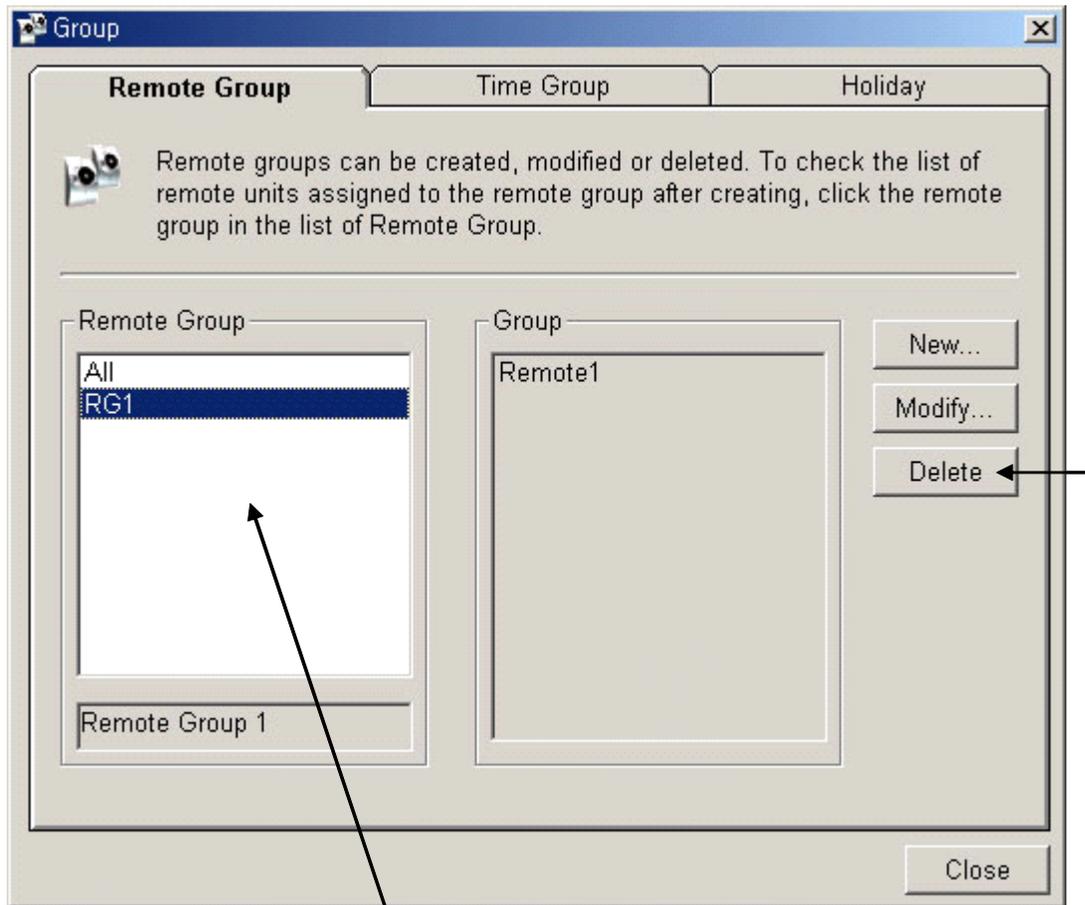
In this case, click on **OK**, to return to the **Modification of Remote Group** window and enter the necessary information before clicking on **Modify** button.

2.2.7.3 Delete Remote Group

Existing **Remote Group(s)** may be deleted using this feature.

Below is the process for deleting the **Remote Group**:

1. Select **Remote Group** after clicking on **Creation** in the menu bar, to open the following **(Group)** window.

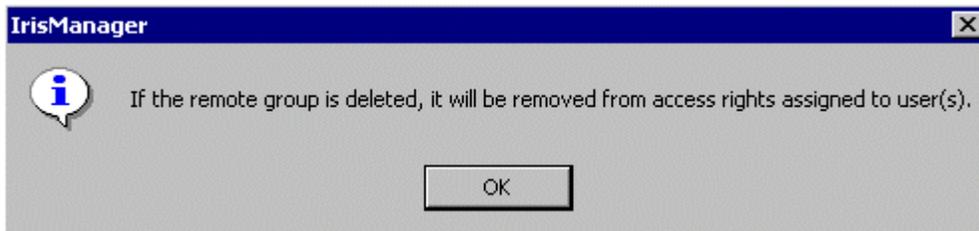


Existing Remote group List

2. Select the **Remote Group** to be deleted from the **Remote group list** (shown with an arrow in the figure above).
3. Click on the **Delete** button to delete the selected **Remote Group**. The following **confirmation window** is displayed.



4. Clicking on the **Yes** button will open the following window.



5. Click on **OK** to delete the **Remote Group**.

The successful deletion of the **Remote Group** results in the **Status** window opening, explained in the section 2.2.4. Click on the **Close** button in the **Status** window to close it.

6. Click on **No** in the **Confirm** window to avoid the accidental deletion of the **Remote Group(s)**.

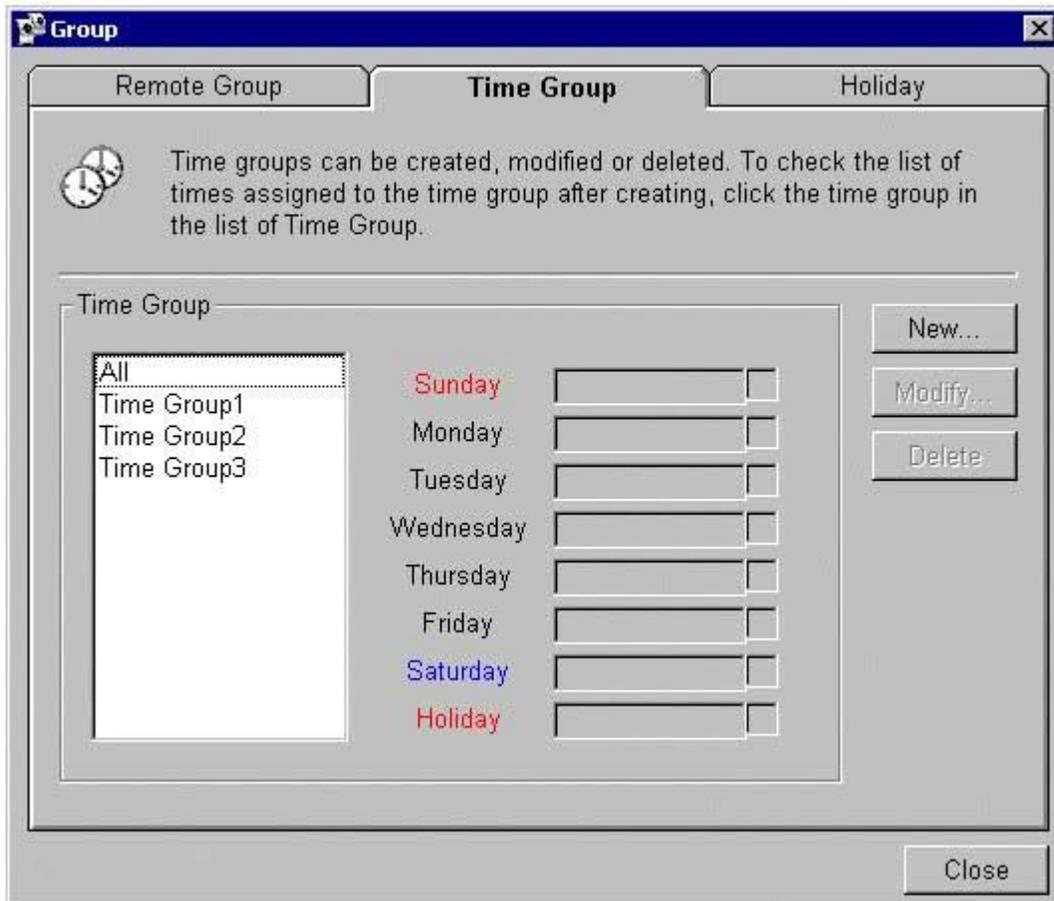
2.2.7.4 Add Time Group

The **Time Groups** are used to specify valid use times for the **Remote Units**.

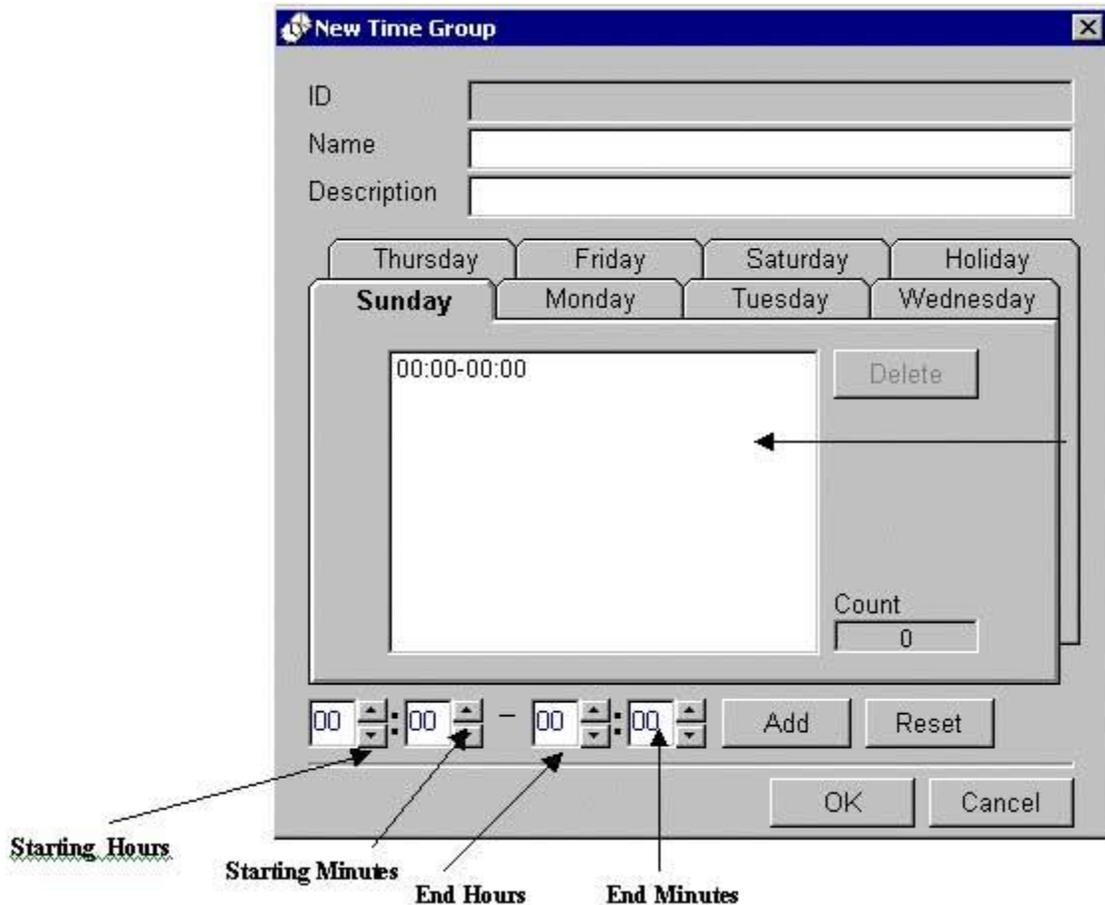
The maximum number of Time Groups that may be registered is 255 in Basic and Extended versions.

Below are the steps to add a New Time Group in **IrisManager**:

1. Select the **Time Group** item under **Creation** in the menu bar to open the following **(Group)** window.



2. Click on the **New** button to add a new **Time group**, which will open the following window titled **New Time Group**.



3. Enter the **Name** and **Description** of the new Time Group in the fields labeled Name and Description respectively. **Description** is an optional field.
4. **Time lists** can be added to the weekdays individually by clicking on the respective tabs. The Time can be adjusted with the up and down arrows near the Starting Hours, Starting Minutes, End Hours, and End Minutes.
5. Once the time values are specified (**start time** should be earlier than **end time**), click on the **Add** button to add this time list for that day.
6. Repeat the steps 4 and 5 to add the time for all the weekdays or the holiday.
7. It is possible to add more than one time list for a given day by repeating step 6, for the given day. Maximum 10 time lists may be added.

8. Clicking on **Reset** will reset the Starting Hours, Starting Minutes, End Hours, End Minutes boxes to zeros.
9. Click on the **OK** button to add the new **Time Group**. Addition of the new **Time Group** may be cancelled by clicking on the **Cancel** button.

The successful addition of the **Time Group** causes the **Status** window to open, explained in the section 2.2.4. Click on the **Close** button in the **Status** window to close it.

During step 5, if the **start time** is not earlier than the **end time**, after clicking the **Add**, the following **error message** will open.

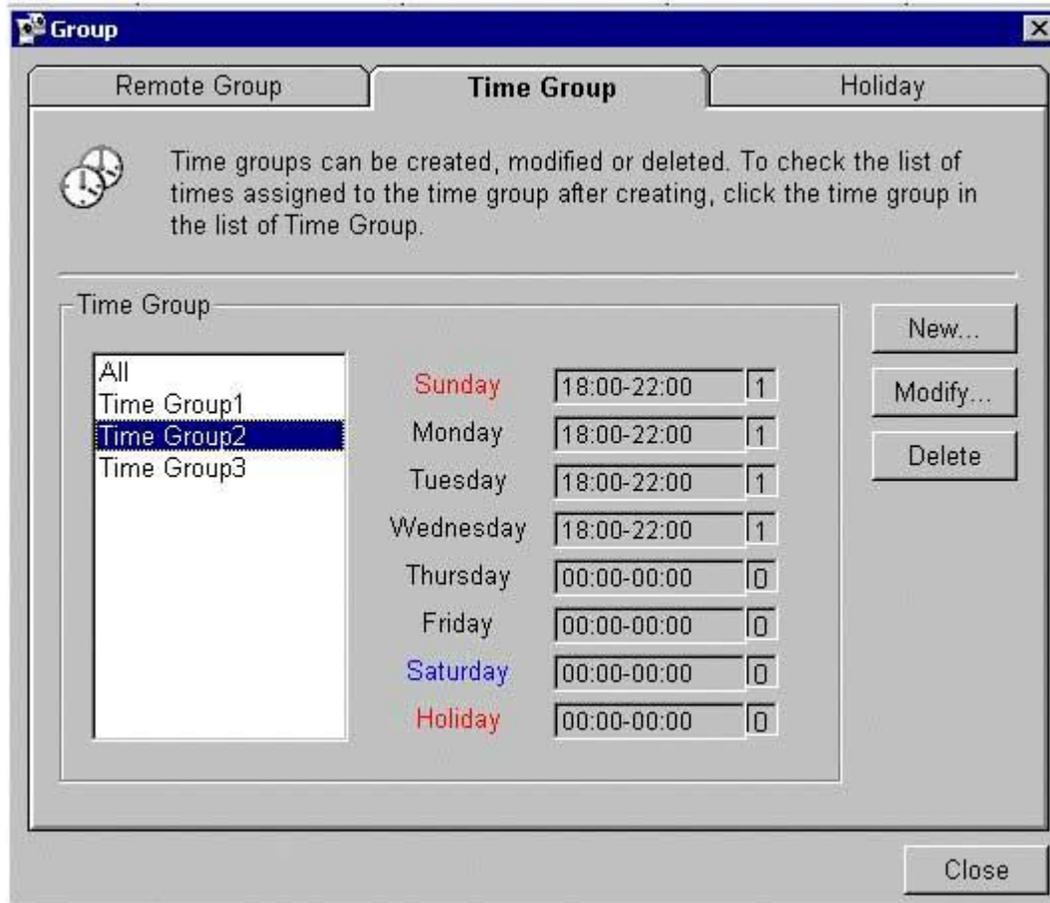


In this case, click on the **OK** button to get the **New Time Group** window, and set the **start time** earlier than the **end time** in the **New Time Group** window.

2.2.7.5 Modify Time Group

Existing **Time Group(s)** may be modified using the following steps:

1. Select **Time Group** after clicking on **Creation** in the menu bar, to open the following **Group** window used to modify an existing **Time Group**.



2. Select the **Time Group** to be modified from the list of existing **Time Groups** in **Time Group**, and then click on the **Modify** button to modify the existing **Time group**. This will open the following window titled **Modification of Time Group**.

Modification of Time Group

ID: 3

Name: Time Group2

Description:

Thursday Friday Saturday Holiday

Sunday Monday Tuesday Wednesday

18:00-22:00

Delete

Count: 1

00:00 - 00:00

Add Reset

Modify Cancel

Starting Hours Minutes End Hours Minutes

3. If the **Name and/or Description** is to be modified, then enter the Name and/or Description in the respective fields.
4. **Accessible periods** in the Time list for the weekdays/holiday can be updated individually by clicking on the respective tabs and selecting the accessible period to be modified.
5. Delete the accessible period to be modified by selecting it from the list and clicking on delete button.
6. Specify the **start time** and **end time** with hours and minutes in the time boxes below.
7. Once the time values are specified (**start time** should be earlier than the **end time**), click on the **Add** button to add the time list for that day.
8. Repeat steps 6 and 7 to add the time for all the weekdays or the holiday.

9. It is possible to add more than one time list for a given day by repeating step 8.
10. Click on the **Modify** button to modify the **Time Group**. Modification of the **Time Group** may be cancelled by clicking on **Cancel** button.

The successful modification of the time group causes the **Status** window to open, explained in the section 2.2.4. Click on the **Close** button in the **Status** window to close it.

During step 6, if the **start time** is not earlier than the **end time**, then after clicking the **Add** button during step 7, the following **Error message** will open.



In this case, click on the **OK** button to return to the **Modification of Time Group** window, and set the proper values in the **Modification of Time Group** window.

During step 2, if the **modify** button was clicked without selecting a **Time Group** then the following window will open.

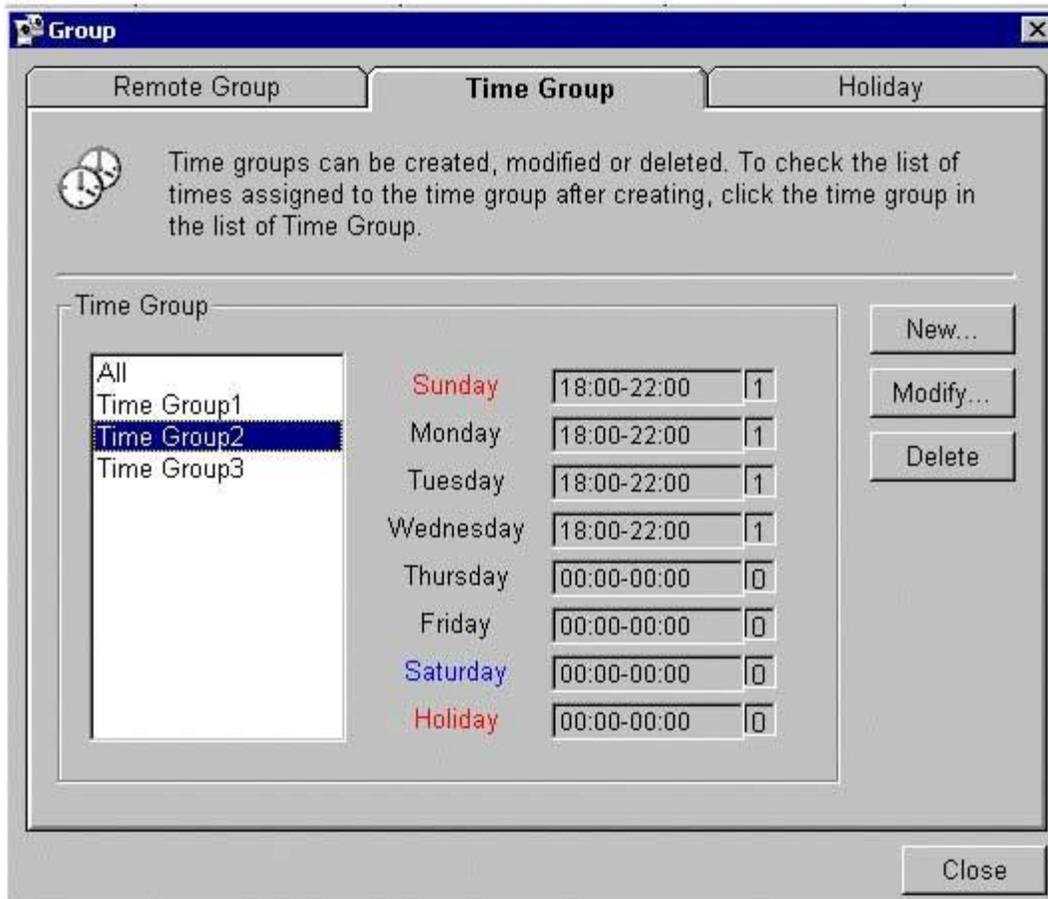


In this case, click on the **OK** button and continue from step 2, after selecting the time group.

2.2.7.6 Delete Time Group

Existing **Time Groups** may be deleted from the system using the following steps:

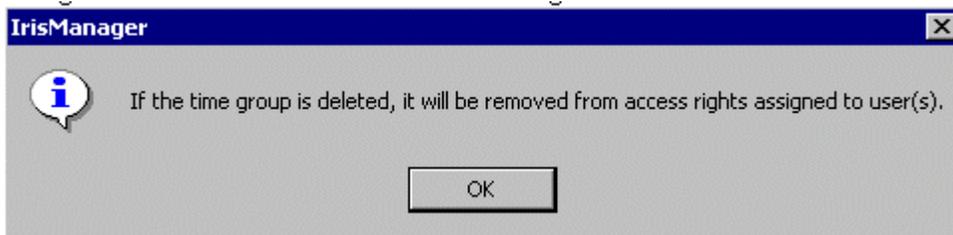
1. Select **Time Group** after clicking on **Creation** in the menu bar, to open the following **Group** window used to delete an existing **Time Group** in the system.



2. Select the **Time Group** to be deleted and click on the **Delete** button to delete an existing **Time Group**. A **confirmation** window is displayed as shown below.



3. Clicking on the **Yes** button will open the following window.



4. Click on the **OK** to delete the **Time Group**. Clicking on the **No** button in the **Confirm** window will avoid the accidental deletion of the **Time Group**. The successful deletion of the time group results the **Status** window to open, explained in section 2.2.4. Click on the **Close** button in the **Status** window to close it.

In step 2, if a Time Group was not selected before clicking on the **Delete** button, then the following warning message will open on the screen.



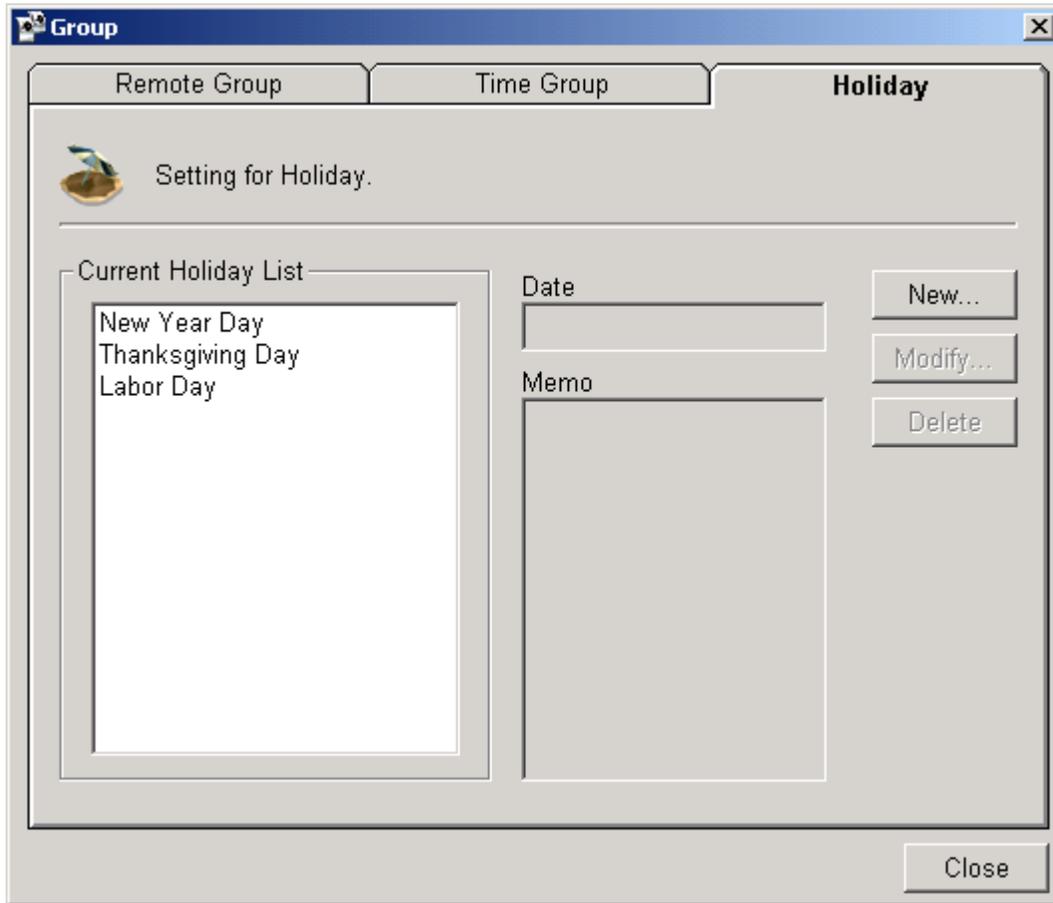
In this case click on **OK** to return to the **Group** window, and continue from step 2 to delete the **Time Group** successfully.

2.2.7.7 Add Holiday List

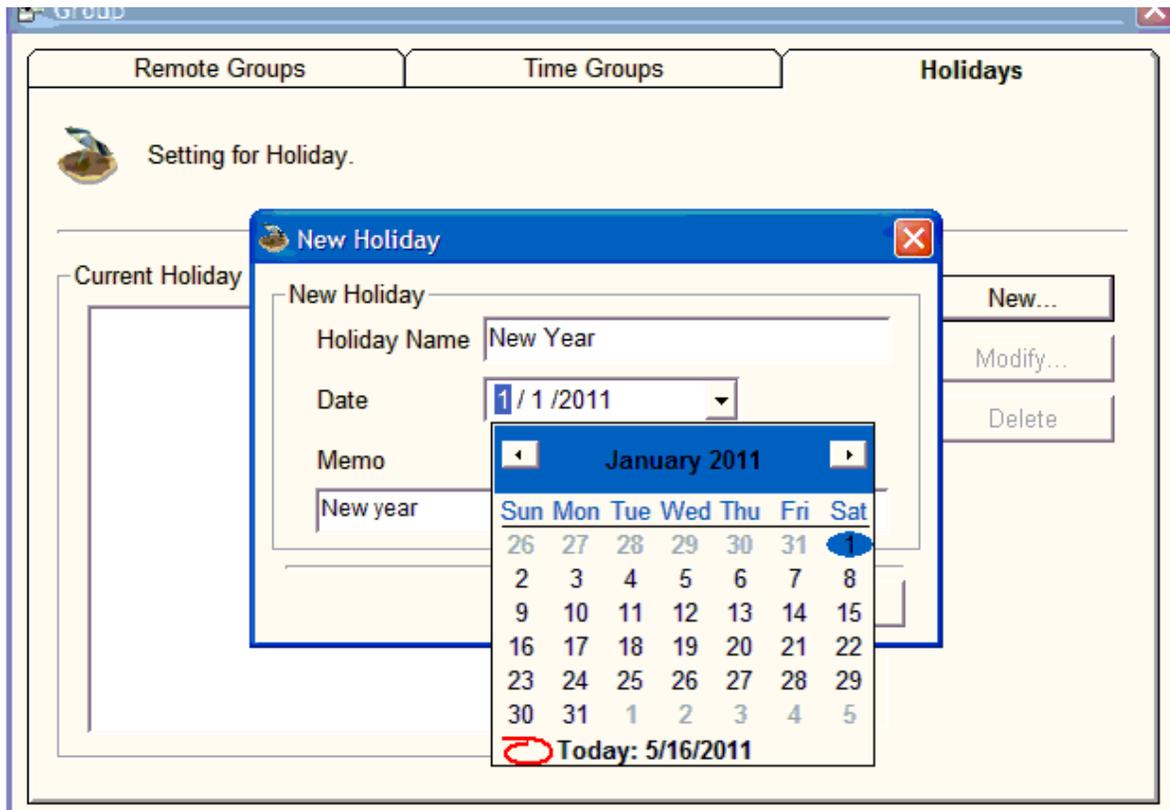
The **Current Holiday list** contains a list of Holidays created in the system. The maximum number of **Holiday** that may be registered is 255 in Basic and Extended version.

A new holiday may be added to the list using the following steps:

1. Select **Holiday** after clicking on **Creation** in the menu bar. The following **Group** window is displayed.



2. Clicking on the **New** button will display the following window.



3. Enter the **Name** of the Holiday, in the text box labeled Holiday Name.
4. Select the **Month** and **Year** of the Holiday from the combo boxes shown by the arrow in the illustration above.
5. Select the **Date** from the calendar.
6. The description of the **Holiday** may be entered in the text box labeled **Memo**.
7. Click on the **OK** button to add the Holiday to the current Holiday list. Click on the **Cancel** button to cancel the addition of the new Holiday to the current Holiday list.

The successful addition of the holiday causes the **Status** window to open, explained in section 2.2.4. Click on the **Close** button in the **Status** window to close it.

If the Holiday name is not specified, the warning message shown below will be displayed. In this case, click on **OK** and then add the Holiday name.



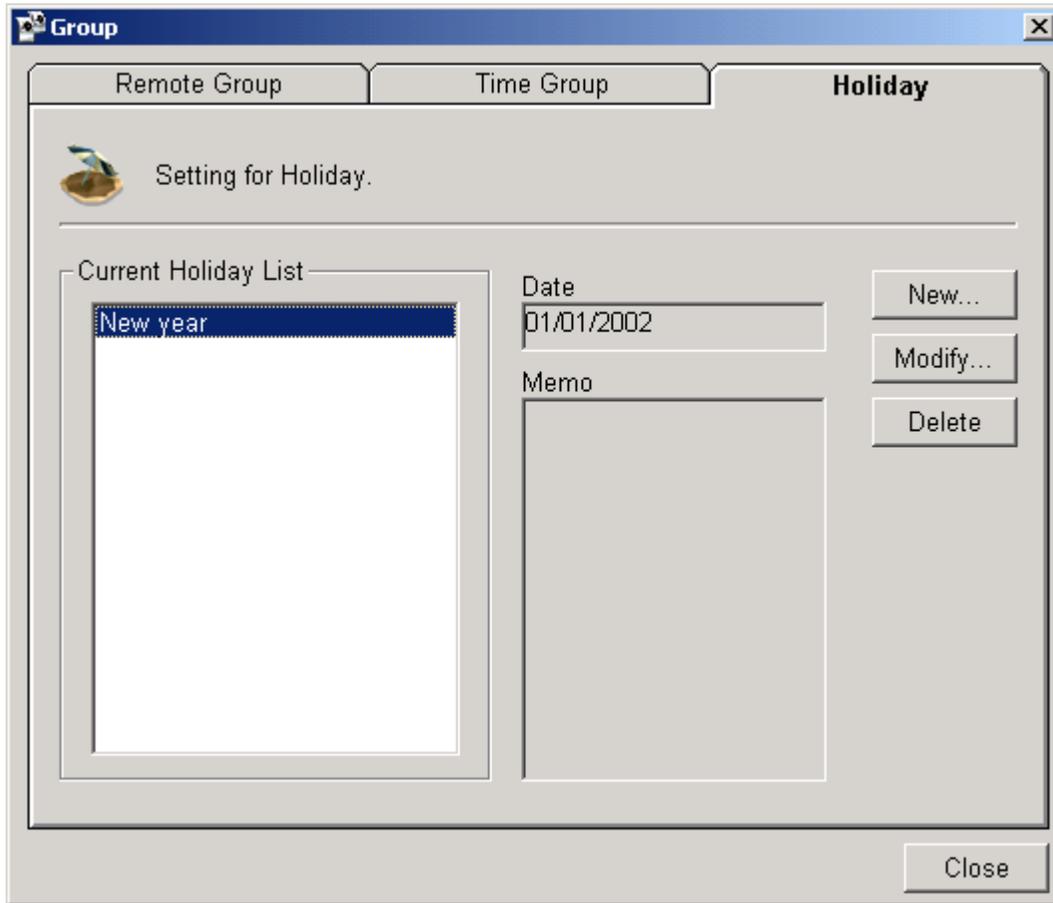
- ✓ If you want to set consecutive holidays, each day must be set individually. For example,

Holiday name	Date
New year day 1	01/01/2002
New year day 2	01/02/2002
New year day 3	01/03/2002

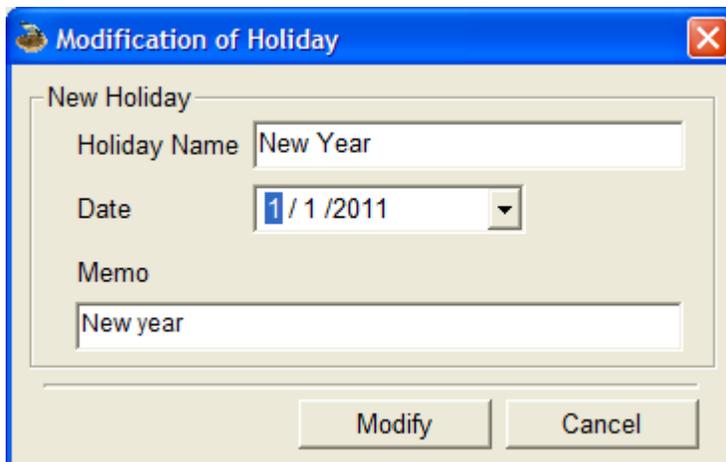
2.2.7.8 Modify Holiday List

Below are the steps used to modify the existing holiday list.

1. Select **Holiday** after clicking on **Creation** in the menu bar to get the following **Group window**.



2. Select the Holiday to be modified from the **Current Holiday list**, and then click the **Modify** button to modify the existing **Holiday**. The following window will open, titled **Modification of Holiday**.



3. Modify the fields to be updated and click on the **Modify** button.
4. Click on the **Cancel** button to cancel the modification.

The successful modification of the holiday causes the **Status** window to open, explained in section 2.2.4. Click on the **Close** button in the **Status** window to close it.

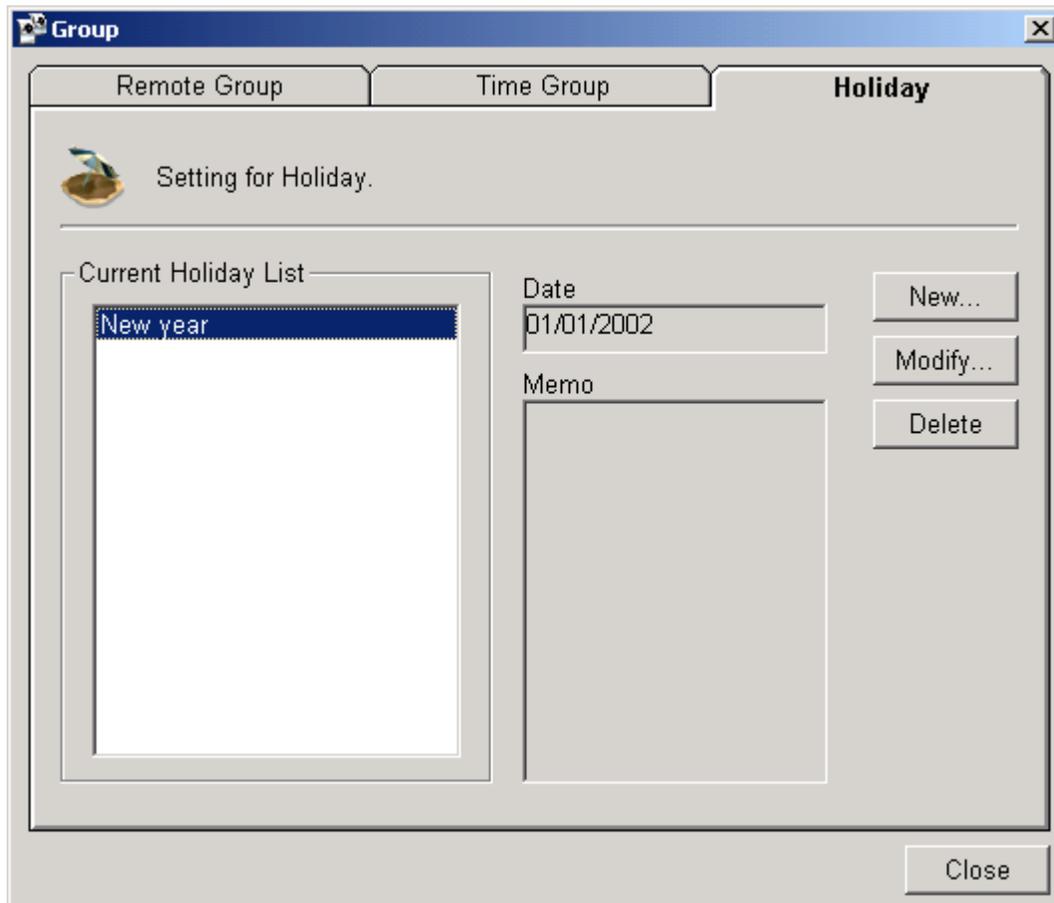
If the **Holiday Name** is not specified when the **Modify** button is clicked, the warning message shown below will be displayed. In this case, click on **OK** and then update the **Holiday Name**.



2.2.7.9 Delete Holiday List

Deletion of an existing Holiday can be done by the following steps:

1. Select **Holiday** after clicking on **Creation** in the menu bar to open the following **Group Window**.



2. Select the **Holiday** to be deleted from the **Current Holiday** list and click on the **Delete** button.
3. Clicking on the **Delete** button will display the following window for **confirmation**. Click on the **Yes** button to delete the **Holiday** from the holiday list. Click on the **No** button to cancel the deletion.



The successful deletion of the holiday results in the **Status** window opening up, explained in the section 2.2.4. Click on the **Close** button in the **Status** window to close it.

2.2.7.10 Prioritized ICU DB sync

When user information is added/modified/deleted from IrisEnroll / IrisManager, the IrisServer sends the changes to all channels (Remote Units) connected to IrisServer.

Earlier, IrisServer used to send changes to each connected recog channel (Remote Unit) in the order in which they were connected to IrisServer, and user had no control over it.

The new Prioritized ICU DB sync feature lets the user configure which channel (Remote Unit) has to be synchronized first, second, third and so on.

User can set / modify the priority for DB sync for any Remote Unit from the IrisManager (Creation->Remote Unit).

- Priority field is added to New Remote Unit and Modification of Remote Unit dialogs.
- Priority field column is also added to the list control that displays the list of registered Remote Units.
- Priority value can be set as any value from 1 to 255.
- A priority value of 1 is assigned to Remote Unit if the priority is not defined.
- If all channels have the same priority value, then this feature has no effect.
- Remote Unit with priority 1 is synchronized first and Remote Unit with priority 255 is synchronized last.
- Multiple Remote Units can have the same priority value.
- Multiple Remote Units having same priority are synchronized in the order of connection to IrisServer.

2.2.8 Administration

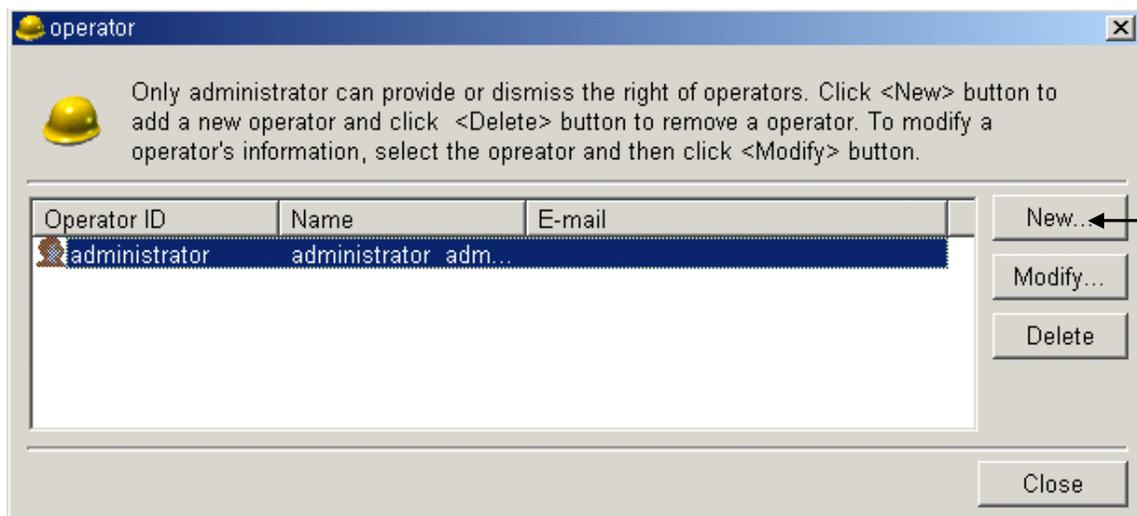
Only administrators can use these features to manage other administrators as well as operators. Operators cannot use this feature.

2.2.8.1 Administrator/Operator

Administrators have full access rights and the access rights of the operator are limited.

Below is the process for adding a new **Administrator/Operator**:

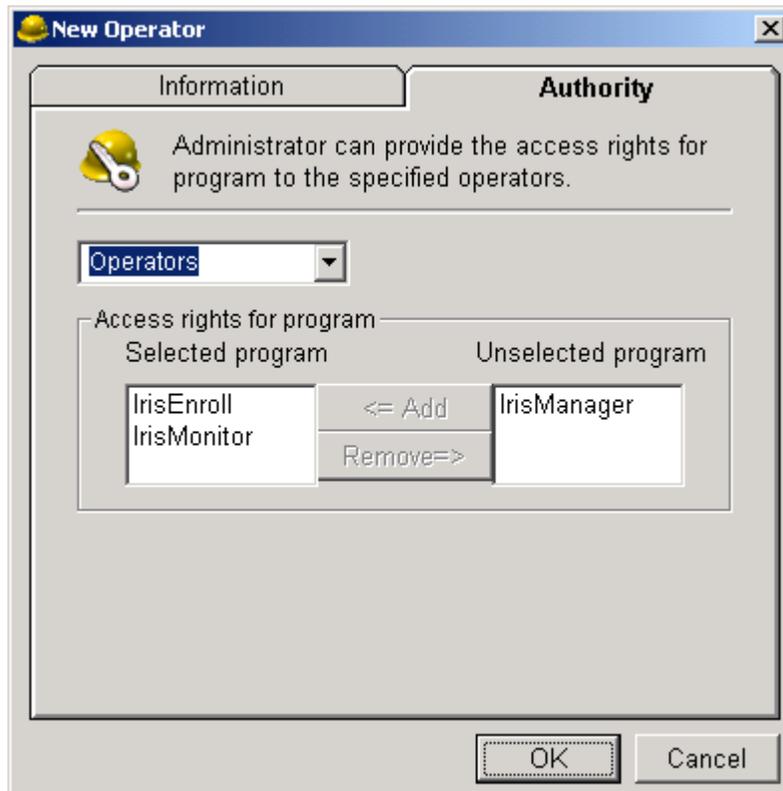
1. Select the **Operators** item in the **Administrator** button in the menu bar to get the following **Operator** window. The Administrator item is enabled only when logged into **IrisManager** as an Administrator.



2. Click on the button labeled **New** to open the **New Operator** window. This window allows you to specify the type of the operator (administrator level or operator level), **access rights** and the **information** about the **administrator/operator**.

The screenshot shows a 'New Operator' dialog box with two tabs: 'Information' and 'Authority'. The 'Information' tab is selected and contains a yellow bell icon and a message: 'All fields marked with an asterisk (*) must be filled in completely.' Below this message are several input fields: '* Operator ID', 'User ID', 'First Name', 'Last Name', 'E-mail', '* Password', and '* Confirm Password'. The 'Authority' tab is also visible but not selected. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

3. After filling the required information (marked in **bold**) in the above window, the type of operator and access rights can be added using the tab labeled **Authority**. This results in the following change in the **New Operator** window.
 - ◆ If the operator to be registered is already registered as a user of this system, enter the User ID. If the operator is not registered as a user, leave the "User ID" field blank.



4. The type of the operator can be specified by selecting either Administrator or Operator in the combo box pointed to with an arrow.
5. The rights for the operator can be specified as follows:
 - a. Select an item on the right to be added from the list of rights under **Unselected program**.
 - b. Click on the **Add** button to add this **right** to the operator.
 - c. The **selected rights** can be viewed on the list of **rights** labeled with **Selected program**.
6. Specification of rights for the **administrator** is not required, since the administrator has all rights by **default**.
7. Click on **OK** after entering all the information.
8. If any of the necessary information was not entered, a window with an **error message** will open on the screen after clicking the **OK** button. For example, if the **operator ID** is not entered, the following window is displayed on the screen. In this case click on the **OK** button, and enter the required information in the **New Operator** window, with the **information** tab selected.



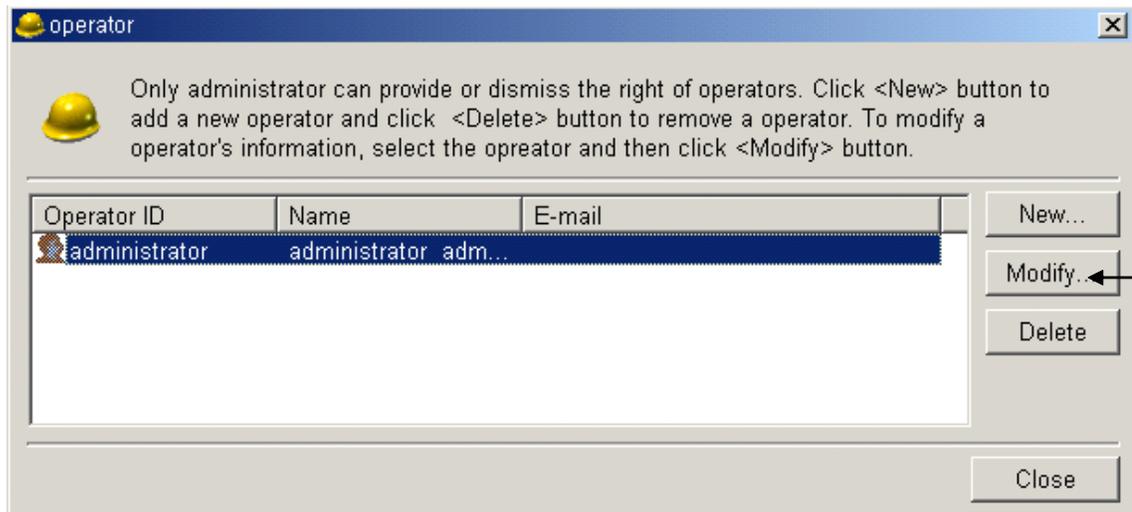
9. If the **access rights** are not specified for the **operator**, then after entering the required operator information, clicking on the **OK** button in the **New Operator** window will open the following **error** window. Click on **OK** to return to the **New Operator** window and assign the access rights and click on the **OK** button in the **New Operator** window.



2.2.8.2 Modification of the Administrator/Operator

Below is the process for **Modification** of the **Administrator/operator**

1. Select the **Operators** item in the **Administrator** button in the menu bar to open the following **Operator** window. The Administrator item is enabled for Administrators only.



2. Select the **Operator** entry to be modified and click on the **Modify** button, shown with an arrow in the window above. A window titled **Operator Information** will be displayed.

The screenshot shows a window titled "Operator Information" with a yellow hard hat icon. Below the title bar is a message: "All fields marked with an asterisk (*) must be filled." Below the message is a form with the following fields:

- * Operator ID: administrator2
- User ID: (empty)
- First Name: administrator2
- Last Name: administrator2
- E-mail: (empty)

 Below the form is a "Change password" button. Below that are two password fields: "New password" and "Confirm Password". At the bottom of the window are "Modify" and "Cancel" buttons.

3. Update the fields to be modified.

- ◆ Note: If the operator is already registered as a user of this system, enter the user ID. If the operator is not registered as a user, leave “User ID” field blank.
4. Click on the **Change Password** button to change the Operators password. The Change Password button will change to **Cancel to change** as shown below.
 5. To cancel the password change, click the **Cancel to change** button.

Operator Information

Information | Authority

All fields marked with an asterisk (*) must be filled in completely.

* Operator ID: administrator2

User ID:

First Name: administrator2

Last Name: administrator2

E-mail:

Cancel to change

* New Password:

* Confirm Password:

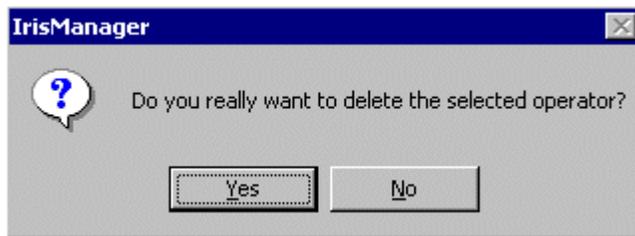
Modify | Cancel

6. Enter the **New Password** in the **New Password** field and confirm the password in the **Confirm Password** field.
7. Click on the **Authority** tab field to review and update the operator type and access rights.

2.2.8.3 Deletion of the Administrator/Operator

1. An existing Administrator/Operator may be deleted using the following procedure:

2. Click on the **Delete** button in the **Operator** window to open the following confirmation window.

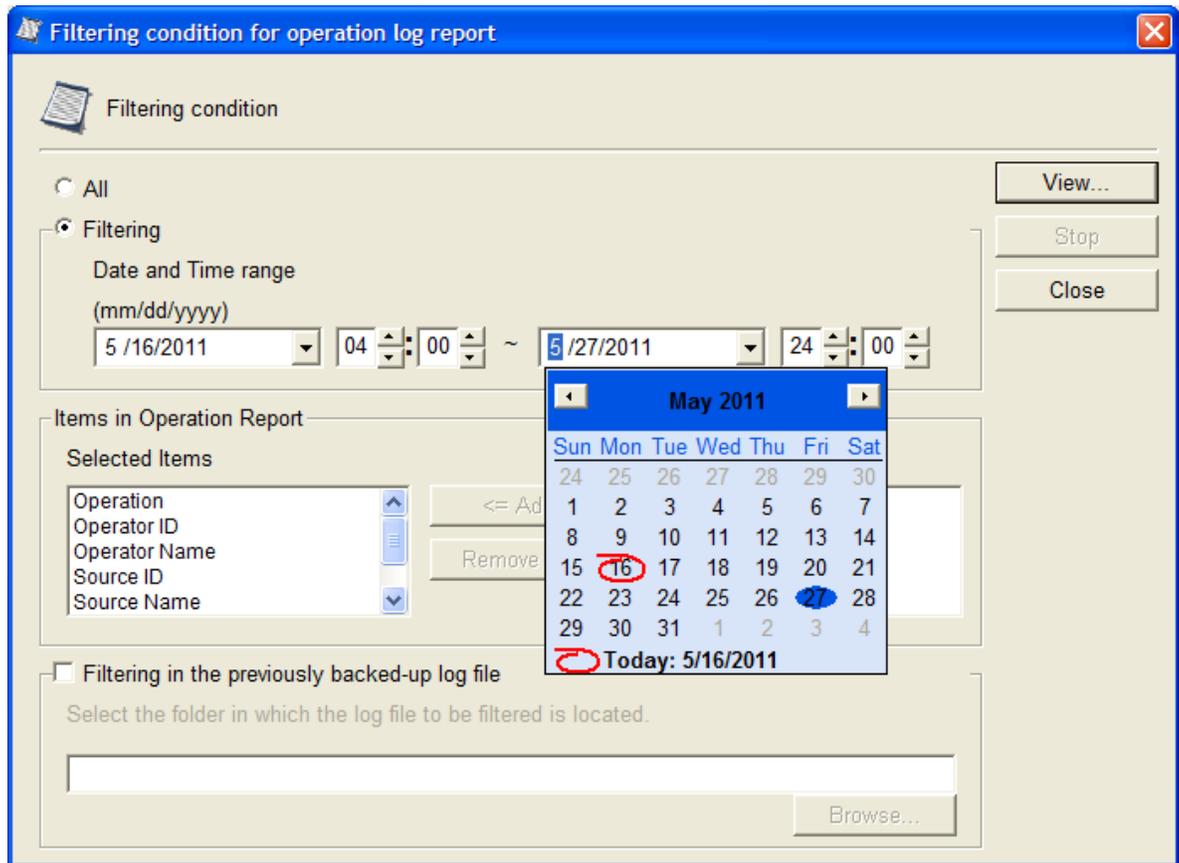


3. Click on **YES** to delete the **Administrator/operator**.
4. Click on the **No** button to avoid the accidental deletion of the **Administrator/Operator**.

2.2.8.4 Operator Log Report

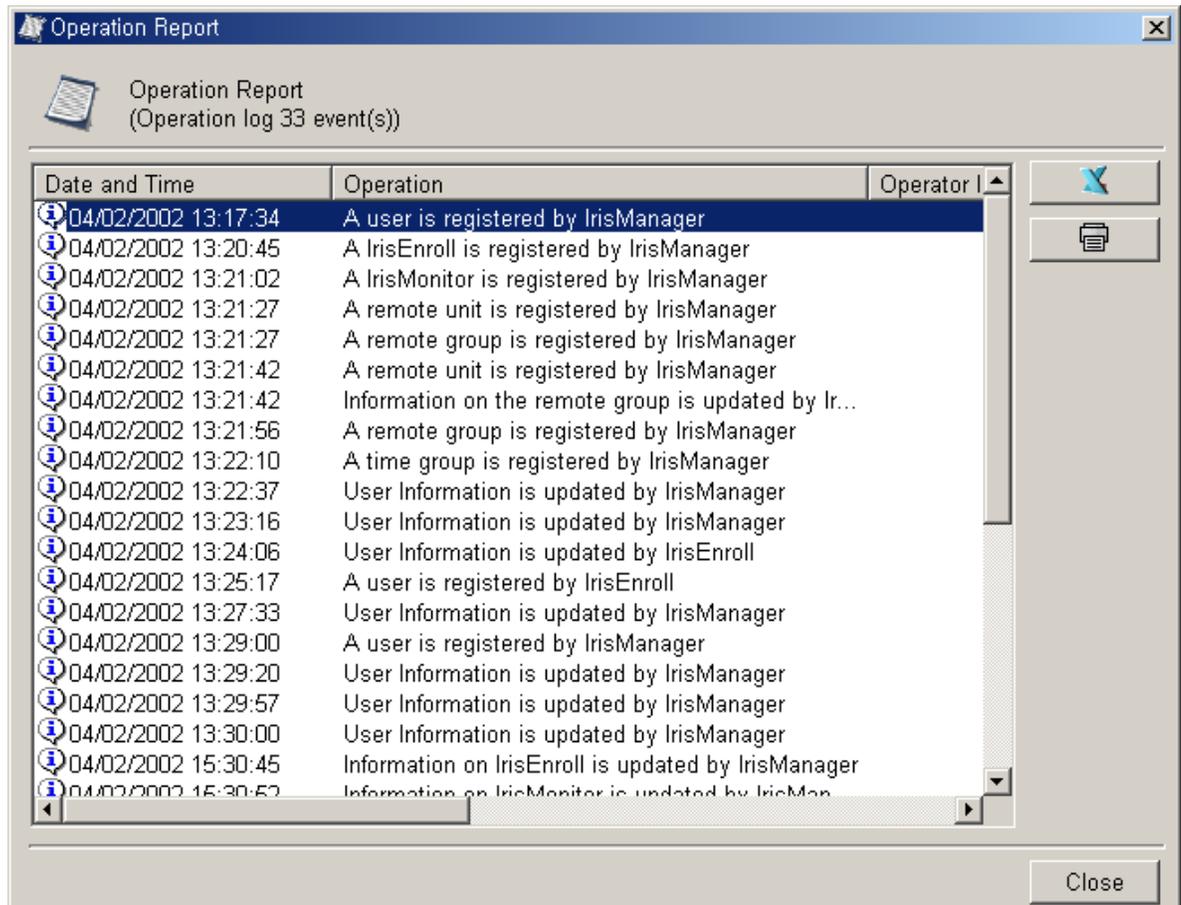
Administrators may run reports detailing all actions performed by Operators on the system.

1. Select **Administrator** from the menu bar.
2. Select the **Operation log item**.
3. The following **Filtering condition for operation log report** window will open.



4. Select **All** or **Filtering**. Select the **All** item for a report of all logs. Select **Filtering** to view the logs based on a **Date and Time range**.
5. If you select **Filtering**, select the date and time range in the **Filtering** frame, highlighted in the picture above.
6. Select the items to be included in the report from the **Items in System Report**. This may be done by selecting the items in the **Unselected Items** list and clicking on the **Add** button. Selected items may be removed by selecting the items in the **Selected Items** list and clicking on the **Remove** button.
7. If you want to view the logs stored in a backed-up log file, select the "**Filtering in the previously backed-up log file**" check box. Click on the **Browse** button to select the folder in which the log files to be included in the report is located. Refer to the section 2.6.2.4 LOG BACKUP. **The backup log file's name created after log back up should be not changed.** If this name is changed, information from the backup log files cannot be included in the report.
8. Click on the **View** button to view the results in the **Operation Report** window as shown below.

9. Click on the **Stop** button to stop the log reporting process. When you click the **Stop** button, logs that have been transferred from the server database will be displayed in the **Operation Report** window.



10. This information can be saved into an **Excel** sheet (Microsoft Excel must be installed) by pressing the button with the Excel icon on it, or printed by pressing the button with a printer icon on it, with the buttons pointed with the arrows, respectively.
11. Clicking on the **Close** button will close the **Operation Report** screen and return to the **Filtering condition for operation log Report** screen.

2.2.8.5 Security Setting

You can set the security level of the remote units. This setting determines if the

Remote Units will be operational after a restart without first connecting to the IrisServer. Only administrator(s) may set the security level.



If you select the first option, the Security IDs, registered in IrisManager and registered in the remote unit with ICU configuration, and are checked and compared in the IrisServer and the remote unit any time the remote unit is restarted. Because this security level can prevent the substitution of an unauthorized remote unit, it is more secure. It is recommended to use this feature.

If you select the second option, the remote unit will be activated after a restart without connecting to the IrisServer. The change of security level will be applied to the remote units only after the remote units are connected to IrisServer. This selection is enabled by default.

2.2.9 Administer User Access Control

2.2.9.1 Add New Users

New users may be added to the system using the following procedure.

1. Select the **New** item under the **User button** from the toolbar or from the menu bar to open the **User Information** window, shown below.

User Information

Basic info. | Access Rights | Detail Info.

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

* **User ID**

Name

First Name

MI

Last Name

Card

None

* **Card ID**

* **Card Number**

PIN Show PIN

Eye

Enrolled eye :

Unenroll left eye

Unenroll right eye

Use warning eye

Left Right

Photo

Delete photo

Gender

Female

Male

2. In the **User Information** window, the **Basic information** about the user should be entered in the window with **Basic Info** tab field selected. In this window:
 - a. Enter the User ID in the text box labeled with **User ID**. The User ID may be any combination of numbers, letters (CAPITAL and lower case) and special characters, up to 20 characters total.
 - b. Enter the User's **First Name**, **Middle Initial** and **Last name** (optional)
 - c. Enter the **Gender** of the user (optional).
 - d. Select the card type in the drop-down list and enter the **Card ID** and **Card Number** (Optional, but required to use verification mode and card ID output).

Note:

Card ID: Card ID is the effective data that is used in verification mode or for Card ID, Wiegand or RS422 output. When the wiegnad/RS422 output ports are activated, Card ID is outputted in the configured format after the user is identified.

- Card Number: Card Number is assigned by Card manufacturer. It is commonly written on the surface of card.

Definition:

If the system is used with a card reader and/or access panel, select the card type in the card drop-down. When a card type is selected, the **Card ID** and **Card Number text boxes** will be activated. To complete the registration of card information, **Card ID** and **Card Number** must be filled. If not, the warning window will be displayed.



- ◆ **Card ID:** The minimum and maximum value of **Card ID** is 0 to 40 digits decimal respectively.
 - ◆ **Card Number:** The minimum and maximum value of **Card Number** is 0 to 40 digits decimal respectively.
- e. Enter **PIN** (Personal Identification Number) assigned to the user. (Optional, required only for PIN verification) The PIN has to be numeric and the valid range for PIN is 1000 to 99999999. By default PIN field is masked. To display unmasked PIN, select “Show PIN” check box.
- f. Select **Photo** (Optional)
- ◆ Allowed image formats: jpg, bmp and gif. The size of the photo cannot exceed the maximum allowable size (300*400 pixels).

If both eyes are enrolled, one of them can be assigned as a **warning eye**. If a user is forced to access the door by an unauthorized intruder, the user may use the **warning eye**. The remote unit opens the door as an authorized user but notifies **IrisServer** (or **IrisMonitor**) of the emergency. This is NOT applicable with ROU4000 camera system.

If you want to delete the left (or right) IrisCode of the user, select the

Unenroll left (or right) eye in the check box.

If you want to delete the registered photo of user, select the **Delete Photo** check box.

3. After entering the information, the window with sample information is shown below.

User Information

Basic info. | Access Rights | Detail Info.

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

* **User ID** 123456

Name

First Name Ravi

MI B

Last Name Kumar

Card

Smart Card

* **Card ID** 1

* **Card Number** 1

PIN ***** Show PIN

Eye

Enrolled eye : Nothing

Unenroll left eye

Unenroll right eye

Use warning eye

Left Right

Photo

Select Photo...

Delete photo

Gender

Female

Male

OK Cancel

4. The **access rights** of the user may be set by clicking the **Access Rights tab** in the User **Information** window.
5. The following window is displayed.

User Information

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

Assign access rights to the user.

Visitor

Remote Groups

All
Group1
Medical
NFC

Add

Time Groups

All
TG1

Add

Access Rights

Remote Groups	Time Groups	Delete
Medical	TG1	

A term of validity (mm/dd/yyyy)

Start Date : 05/01/2011 Delete

Expire Date : 05/25/2011 Delete

Detail

Remote group/Time group - Detailed information

Modify Cancel

6. In this window select the check box labeled **Visitor** if the **User** is a **Visitor** with temporary access rights.
7. If the user type is **General User**: (The **Visitor** check box is NOT selected)
 - a. Select the **Remote group** of this user.
 - b. Click on the **Add** button under the **Remote Group**.
 - c. Select the **Time Group** of the user.
 - d. Click on the **Add** Button under the **Time group**.
 - e. The Selected Remote Group and Time Groups may be viewed in the **Remote Group and Time Group** List in the **Access Rights** section.
 - f. **Users** may be removed from **Remote** and **Time Groups** by selecting the **Groups** in the **Access Rights** section and clicking on the **Delete** button.

- g. You may set the **Start Date** and **Expiration Date** for the user. If you do not select a **Start Date** and **Expiration Date** for the user, their **Access Rights** are always valid. **To set the Start Date:**
 - Press the **Calendar** button next to **Start Date**.
 - On the Calendar screen that opens, select the first date that the User's **Access Rights** will take effect.
 - Press the **Ok** button to enter the **Start Date**, or Press the **Cancel** button to cancel the date selection.
 - Repeat the process for the **Expire Date**

If a **Remote Group** or **Time Group** is selected, the **Detail** button may be pressed to display the **Remote Unit(s)** in the **Remote Group** or the valid times under the **Time Group**.

Remote Name	IP address	Channel ID	Use Type	Description
R137-1	150.140.62.131	1	Identification	
R137-2	150.140.62.132	2	Access In	
R137-3	150.140.62.133	3	Identification	
R137-4	150.140.62.134	4	Access In	

Sunday	Monday	Tues...	Wedn...	Thurs...	Friday	Satur...	Holiday
00:00...	00:00...	00:00...	00:00...	00:00...	00:00...	00:00...	00:00...

Multiple **Remote** and **Time Groups** may be assigned to a single user by repeating steps a - g. A maximum of 10 access rights may be assigned to a single user.

- 8. If the **User** is a **Visitor**:
 - a. Check the check box labeled **Visitor** and enter the visitor information.

User Information

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

 Assign access rights to the user.

Visitor

Remote Groups

ZC
RG1
 RG2
 RG3

Add

Access Rights

Remote Groups		Delete
RG1		

A term of validity
 (mm/dd/yyyy)

Start Date : 05/01/2011 Delete

Expire Date : 05/25/2011 Delete

Reservation time for visitor

03:00 ~ 16:00

Detail

Remote Name	IP address	Channel ID	Use Type
24_1	172.24.17.24	1	Identification
24_2	172.24.17.24	2	Identification

Modify Cancel

- b. Select the **Remote group** of the visitor,
- c. Click on the **Add** button under **Remote Group**, to add the **Visitor** to the **Remote Group**.
- d. The selected **Remote Group** will be listed in the **Remote Group** list under **Access Rights**.
- e. You may set the **Start Date** and **Expiration Date** for the user. If you do not select a **Start Date** and **Expiration Date** for the user, their **Access Rights** are always valid. To set the **Start Date**:
 - Press the **Calendar** button next to **Start Date**.
 - On the Calendar screen that opens, select the first date that the User's **Access Rights** will take effect.
 - Press the **Ok** button to enter the **Start Date**, or Press the **Cancel** button to cancel the date selection.
- f. Repeat the process for the **Expire Date**.

- g. The valid access times (start time and the end time) during the selected valid days for the visitor can be selected by choosing the starting and ending hours and minutes in **Reservation time for Visitor**. Only one Reservation time can be set.

The User's detailed information can be entered by selecting the **Detailed Info** tab on the **User Information** window, as shown below.

The screenshot shows a window titled "User Information" with three tabs: "Basic info.", "Access Rights", and "Detail Info.". The "Detail Info." tab is selected. The window contains a magnifying glass icon and the text "Detail information of the user". Below this, there are several input fields:

Department	<input type="text"/>	Position	<input type="text"/>
Phone(Home)	<input type="text"/>	Phone(Mobile)	<input type="text"/>
Phone(Office)	<input type="text"/>	E-mail	<input type="text"/>
Address	<input type="text"/>		
Resident Num	<input type="text"/>		
Memo 1	<input type="text"/>		
Memo 2	<input type="text"/>		
Memo 3	<input type="text"/>		
Memo 4	<input type="text"/>		
Memo 5	<input type="text"/>		

At the bottom right of the window, there are "OK" and "Cancel" buttons.

9. **Department** of the user, **Position** of the user, **Phone numbers** of the user (both **Home** and **Office**), **Mobile number**, **E-mail**, **Address**, **Resident Number** and some **description** of the user can be entered.

10. Once all the required information is entered, click on the **OK** button to add the user into the system. Clicking on the **Cancel** button will cancel the entire operation of adding the user.

The successful addition of the user causes the **Status** window to open, explained in section 2.2.4. Click on the **Close** button in the **Status** window to close it.

The following **error** window is displayed on the screen, if any necessary information is not entered, depending upon the field. For example if the **User ID** field is not entered, the following window will be displayed.

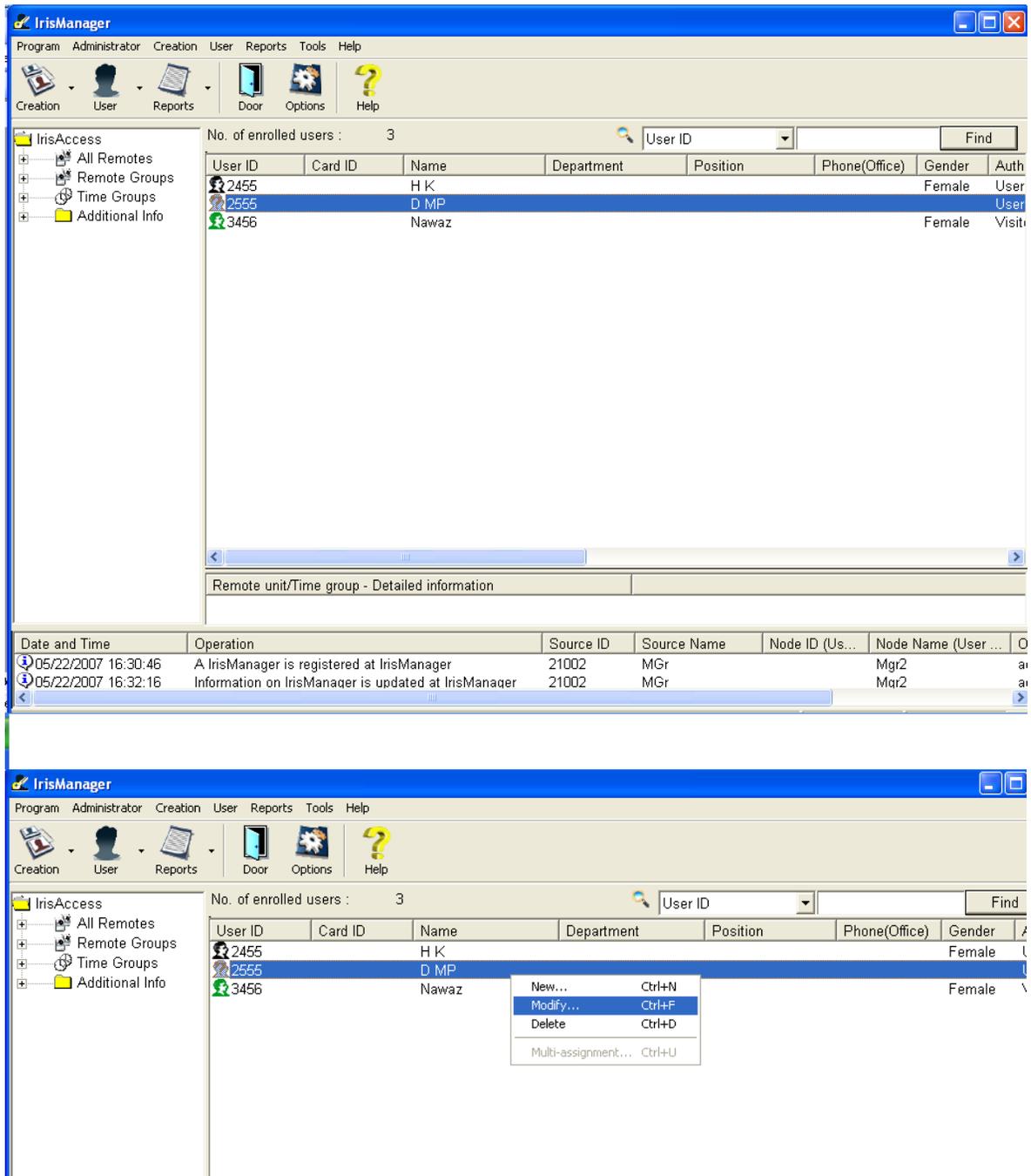


In this case click on the **OK** button and to return to the **User Information** window and enter the required information.

2.2.9.2 Modify User Information

Existing **User(s)** information may be modified using the following procedure.

1. Select the User whose information is to be modified from the list of users in the **IrisManager** window. For example, the selection of the user Brandy Park can be seen in the following window.



- To modify the information of the selected user, select **Modify** from the **User** Icon on the tool bar or from the menu bar to open the following **User Information** window. Double-clicking on the selected user will also open the window.

The image shows a 'User Information' dialog box with a blue title bar and a close button. It has three tabs: 'Summary' (selected), 'Basic info.', and 'Access Rights'. The 'Summary' tab contains a 'Summary of the user Information' section with a lock icon. Below this is a list of user attributes: User ID (2555), First Name (D), MI, Last Name (MP), Phone(Home), Phone(Mobile), Phone(Office), Department, Position, E-mail, and Address. A large empty rectangular box is positioned to the right of the attribute list. At the bottom right, there are 'Modify' and 'Cancel' buttons.

User ID :	2555
First Name :	D
MI :	
Last Name :	MP
Phone(Home) :	
Phone(Mobile) :	
Phone(Office) :	
Department :	
Position :	
E-mail :	
Address :	

3. Change Picture(PIN no longer visible)

4. The **Basic information** of the user may be modified by clicking on the **Basic Info** tab. The following **User Information** window is displayed with the existing Basic Information.

User Information

Basic info. | Access Rights | Detail Info.

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

* **User ID** 123456

Name

First Name Gob

MI B

Last Name T

Photo

Select Photo...

Delete photo

Gender

Female

Male

Card

Smart Card

* **Card ID** 1

* **Card Number** 1

PIN ***** Show PIN

Eye

Enrolled eye : Nothing

Unenroll left eye

Unenroll right eye

Use warning eye

Left Right

OK Cancel

5. **Modify** the desired fields in this window. The mandatory fields should not be left blank.

If both the eyes are enrolled, one of them can be assigned as **warning eye (Not valid for ROU4000 camera system)**. If a user is forced to access the door by an unauthorized intruder, the user can use the warning eye. Then the door is open as an authorized user but notifies IrisServer (or IrisMonitor) of the emergency.

If you want to delete the left (or right) IrisCode of the user, select the **Unenroll left (or right) eye** in the check box.

If you want to delete the registered photo of user, select the **Delete Photo** in the check box.

6. The **Access Rights** of the user may be modified by clicking on the **Access Rights** tab in the **User Information** window.
7. The following picture displays a **User Information** window with existing access rights.

User Information

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

Assign access rights to the user.

Visitor

Remote Groups

All Group1 Medical NFC

Add

Time Groups

All TG1

Add

Remote Groups	Time Groups		Delete
All	All		

A term of validity (mm/dd/yyyy)

Start Date : 05/16/2011 Delete

Expire Date : 05/31/2011 Delete

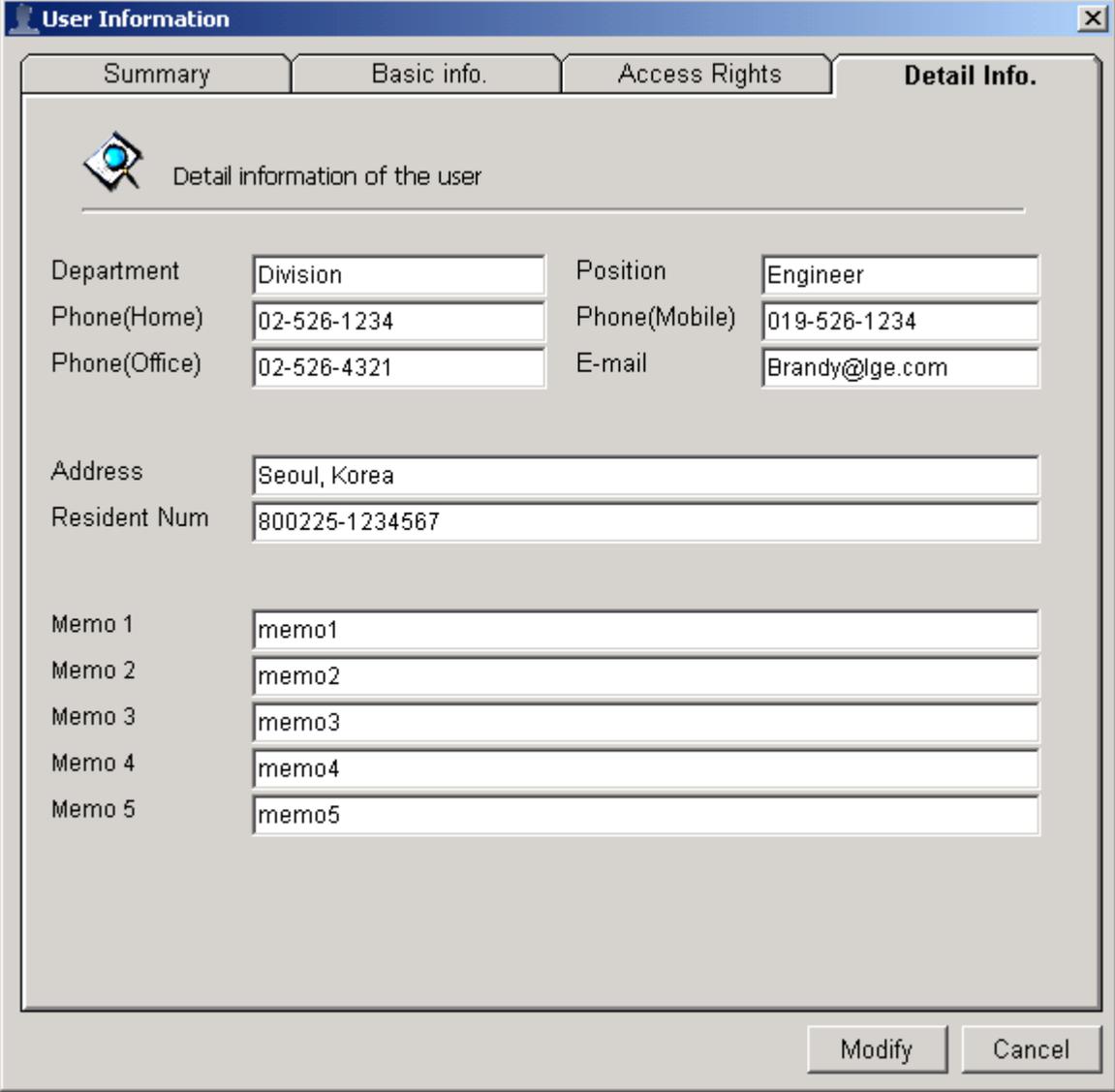
Detail

Sunday	Monday	Tuesday	Wednes...	Thursday	Friday	Saturday	Holiday	
00:00-...	00:00-2...	00:00-2...	00:00-2...	00:00-2...	00:00-2...	00:00-2...	00:00-2...	

Modify Cancel

8. The information related to the **Access Rights** can be modified by
 - a. Changing the **type** of the user.
 - b. **Adding / Removing** the **Remote/Time** groups.
 - c. Modifying the valid **date(s)/time(s)** of different **Remote-Time** groups. (Optional for non-visitors)

9. The **detailed information** of the user may be modified by selecting the **Detailed Info** tab in the **User Information** window.
10. The following picture displays the **User Information** window with existing **detailed information** of the user.



The screenshot shows a window titled "User Information" with four tabs: "Summary", "Basic info.", "Access Rights", and "Detail Info.". The "Detail Info." tab is selected. The window contains a magnifying glass icon and the text "Detail information of the user". Below this, there are several input fields for user details:

Department	Division	Position	Engineer
Phone(Home)	02-526-1234	Phone(Mobile)	019-526-1234
Phone(Office)	02-526-4321	E-mail	Brandy@lge.com
Address	Seoul, Korea		
Resident Num	800225-1234567		
Memo 1	memo1		
Memo 2	memo2		
Memo 3	memo3		
Memo 4	memo4		
Memo 5	memo5		

At the bottom right of the window, there are two buttons: "Modify" and "Cancel".

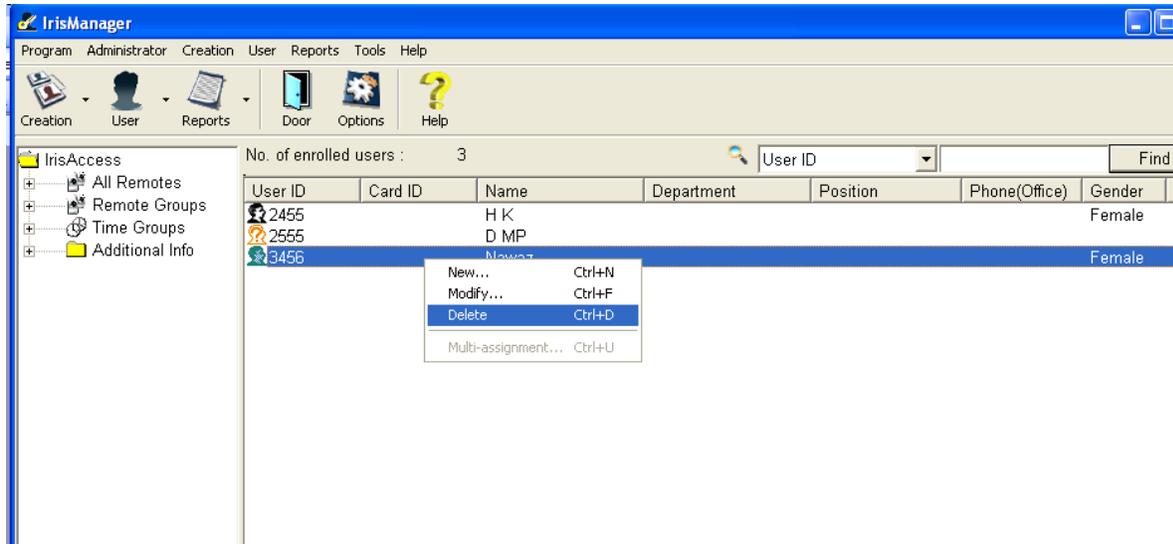
11. **Modify** the **detailed information** fields with the desired modifications.
12. Click on the **Modify** button to complete the Modification. Click on the **Cancel** button to cancel the modification.

The successful modification of the user causes the **Status** window to open, as explained in section 2.2.4. Click on the **Close** button in the **Status** window to close it.

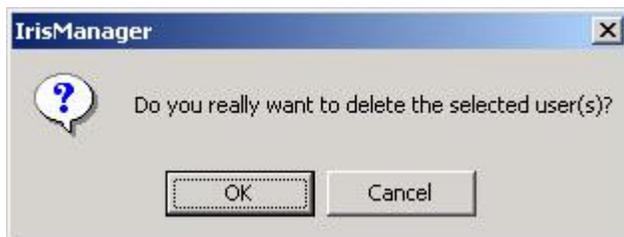
2.2.9.3 Delete User Information

Existing **User/Visitors** information may be deleted from the system using the following procedure.

1. Select the user that you want to delete from the **IrisManager** window. For example the selection of the user Brandy Park can be seen in the following window.



2. To delete the selected user, select the **Delete** within the **User** Item from the menu bar or toolbar.



3. Click on the **OK** button to delete the user. To avoid deleting the user, click on the **Cancel** button.

The successful deletion of the user causes the **Status** window to open, as explained in section 2.2.4. Click on the **Close** button in the **Status** window to close it.

2.2.9.4 Multi-Assignment for Users

Access rights may be assigned to the selected users by using this feature.

When you select more than one user, you can use this feature.

(Specifically, the **Multi-assignment** menu item will be enabled if you select more than one user.)

To select a series of users:

Left-Click on the first user in the series.

Hold down the **Shift** key on the keyboard.

Left-Click on the last user in the series.

Release the **Shift** key

This will select the first and last user selected, as well as all the users between the first and last selected.

To select a number of users:

Left-Click on the first user.

Hold down the **Control (Ctrl)** key on the keyboard

Left-Click on the other users you want to select.

When all the users desired have been selected, release the **Control** key.

This will select all the users left-clicked on.

1. On selecting the **Multi-assignment** item under the **User** icon from the toolbar or from the menu bar after selecting more than one user, the following **Multi Assign** window is displayed.

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
0414	RAMA KRISH...
0425	BEJU SINGH
0433	KRISHNAIAH K
0443	K HANUMANT...
0462	M GNANESH...
0496	VENKAT SWA...
0597	B GYANESH...
0710	KAMALAVATH...

Visitor

Remote Groups

- All
- Group1
- Medical
- NFC
- EM Office

Add

Time Groups

- All
- TG1

Add

Access Rights		Remote Groups	Time Groups	Delete

A term of validity (mm/dd/yyyy)

Start Date : Delete

Expire Date : Delete

OK Cancel

2. Or selecting more than one user and right-clicking on one of the users will show the menu below.

New...	Ctrl+N
Modify...	Ctrl+F
Delete	Ctrl+D
Multi-assignment...	Ctrl+U

3. Selecting **Multi-assignment** will display the box displayed below.

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.

Visitor

Selected Users

User ID	Name
0414	RAMA KRISH...
0425	BEJU SINGH
0433	KRISHNAIAH K
0443	K HANUMANT...
0462	M GNANESH...
0496	VENKAT SWA...
0597	B GYANESH...
0710	KAMALAVATH...

Remote Groups

- All
- Group1
- Medical
- NFC
- EM Office

Add

Time Groups

- All
- TG1

Add

Access Rights

Remote Groups	Time Groups	
		Delete

A term of validity (mm/dd/yyyy)

Start Date : Delete

Expire Date : Delete

OK Cancel

4. In this window select the type of the user (general user/visitor) using the check box labeled **Visitor**.

5. If the selected users are not visitors:

- Select the **Remote group** for these selected users.
- Click on the **Add** button under the **Remote Group**. This will add the users to that Remote Group.
- Select the **Time Group** of the users.
- Click on the **Add** Button under **Time group**. This will add these users into the selected time group.
- The Selected Remote Group and Time Groups may be viewed in the **Remote Group and Time Group List** under the **Access Rights**.
- The Time Group and the Remote Group may be deleted by clicking on the **Delete** button, after selecting the Remote/Time Group to be removed.
- Select the **Start Date** for access and the **Expiration Date** for validation term of the users (optional). Click **Calendar** to set the Start Date and the Expiration Date, respectively. Click **Delete** to clear the existing Start Date and Expiration Date, respectively.

Multiple Remote and Time Groups may be assigned for the selected users by repeating the steps (a) to (g). Maximum 10 access rights can be assigned to users.

6. If the User Type is **Visitor**, (When the **Visitor** check box is selected)
 - a. Check the check box labeled **Visitor**.
 - b. Select the **Remote group** for the Visitors
 - c. Click on the **Add** button under **Remote Group**, to add the **Visitors** into that **Remote Group**.
 - d. The selected **Remote Group** may be viewed in the **Remote Group** list under **Access Rights**.
 - e. Select the **Start Date** and the **Expiration (End Date) Date** for the **Visitors** to access the system. Click **Calendar** to set the Start Date and the Expiration Date, respectively. Click **Delete** to clear the existing Start Date and Expiration Date, respectively.
 - f. The valid access times (start time and the end time) for the selected valid days can be selected by choosing the starting and ending hours and minutes in **Reservation time for Visitor**. Only one Reservation time can be set.
7. Click on the **OK** button to update the access rights.

The successful update causes the **Status** window to open, explained in section 2.2.4. Click on the **Close** button in the **Status** window to close it.

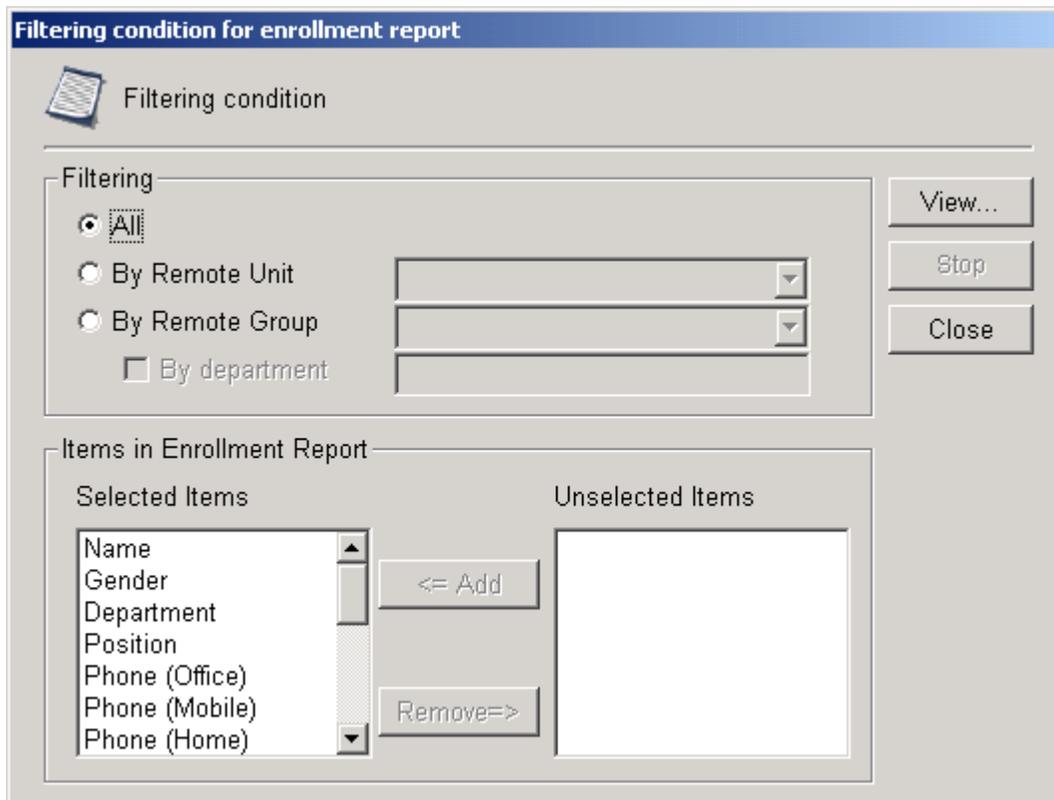
2.2.10 Reports

2.2.10.1 Enroll Report

Information about the list of enrolled users may be obtained using this feature. This feature can be used as follows:

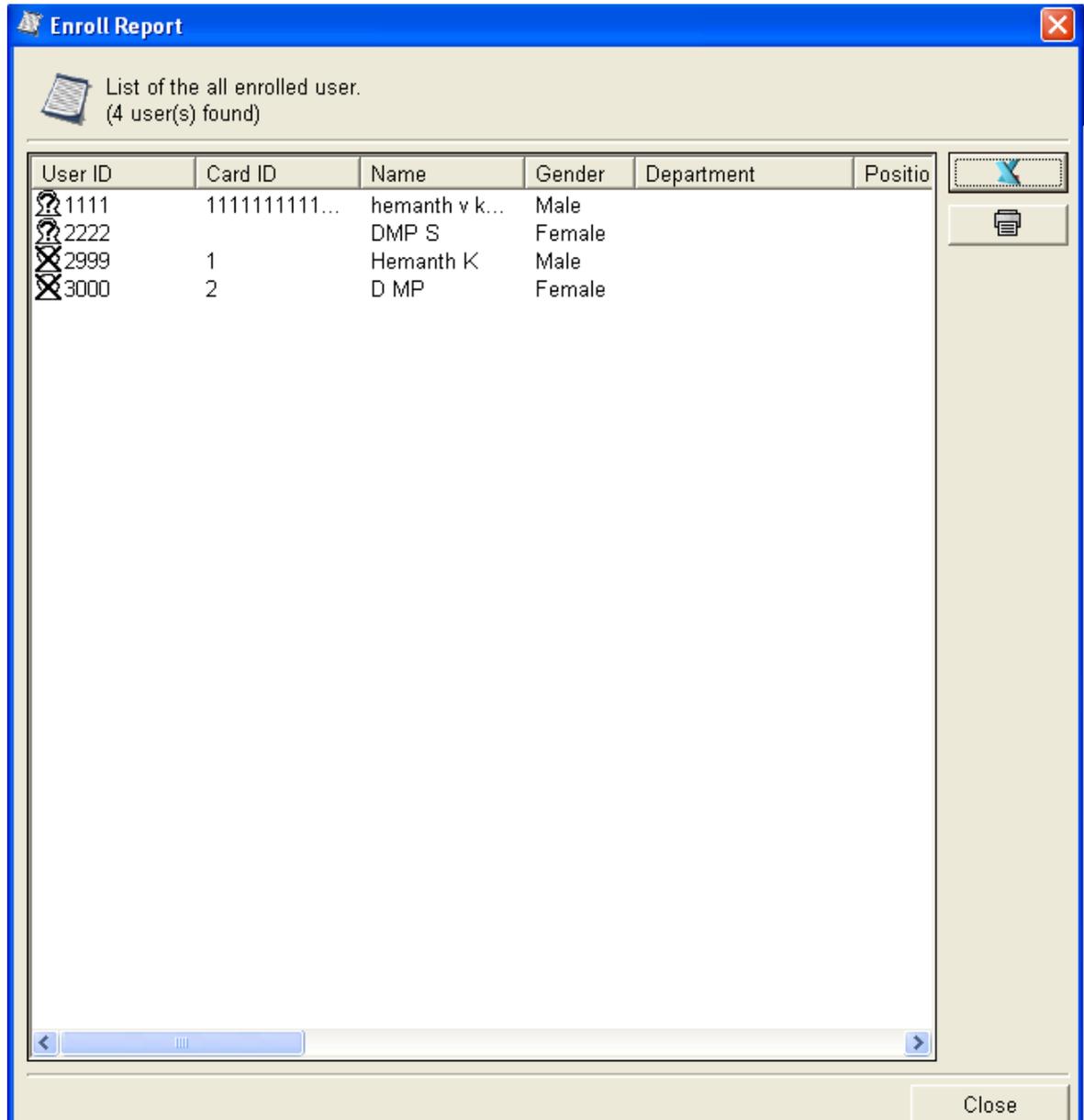
1. Select the **Reports** from the toolbar or menu bar.
2. Select the **Enroll report** Item from **Reports**.

The following **Filtering condition for enrollment report** window will be displayed on the screen, after the selection of the **Enroll report** item.



3. The user information for all the users can be obtained by selecting **All** in the Filtering part of the window.
4. If the information about the users in a specific **Remote Unit** is required, then this may be obtained by selecting the **By Remote Unit** and selecting the appropriate **Remote Unit** in the drop-down box in the Filtering part.
5. If the information about the users in a specific **Remote Group** is required then this may be obtained by selecting the **By Remote Group** and selecting the appropriate **Remote Group** in the drop-down box in the Filtering part
6. Further filtering of the users can be done by selecting **By Department** after selecting any of the items explained in steps 4 to 5
7. The report cannot be filtered by any other items except for Remote unit, Remote group and Department.
8. The information about the selected users included in the report may be selected by selecting the necessary fields from the **Unselected Items** and then clicking the **Add** button.
9. Selected fields may be removed by selecting the field from the **Selected Items** list and clicking on the **Remove** button.

- The information about the selected users, selected information can be viewed by clicking on the **View** button after selecting the required items. This information will open as a new window with the title **Enroll report** as shown below:
- Click on the **Stop** button to stop the report creation. When you click the **Stop** button, information already transferred from the server database will be displayed in the **Enroll Report** window.



- This information can be saved into an **Excel** sheet (Microsoft Excel must be installed) or printing can be done using the buttons **Excel** and **printer** indicated by arrows above. The more user information included in the report, the more time required for processing.
- Clicking on the **Close** button will close the **Enroll Report** screen and return to the **Filtering condition for enrolment report** screen.

2.2.10.2 Access Reports

A report displaying the access records through the doors can be obtained using this feature. This feature can be used as follows:

1. Select the **Reports** from the toolbar or menu bar.
2. Select the **Access Report** Item from the **Reports** menu.

The following **Filtering condition for access report** window will be opened on the screen, after the selecting the **Access report** item.

Filtering condition for access report

Filtering condition

All
 Filtering

Date and Time range (mm/dd/yyyy)
 5 /16/2011 00:00 ~ 5 /25/2011 24:00

Basic filtering
 Additional filtering

By Remote Unit
 401-I

By Remote Group
 All

By IrisEnroll
 Iris Enroll

User ID
 19

First Name

Last Name

Process Result

Department

Items in Access Report

Selected Items

User ID
 Card ID
 User Name
 Department

Unselected Items

<= Add

Remove =>

Filtering in the previously backed-up log file

Select the folder in which the log file to be filtered is located.

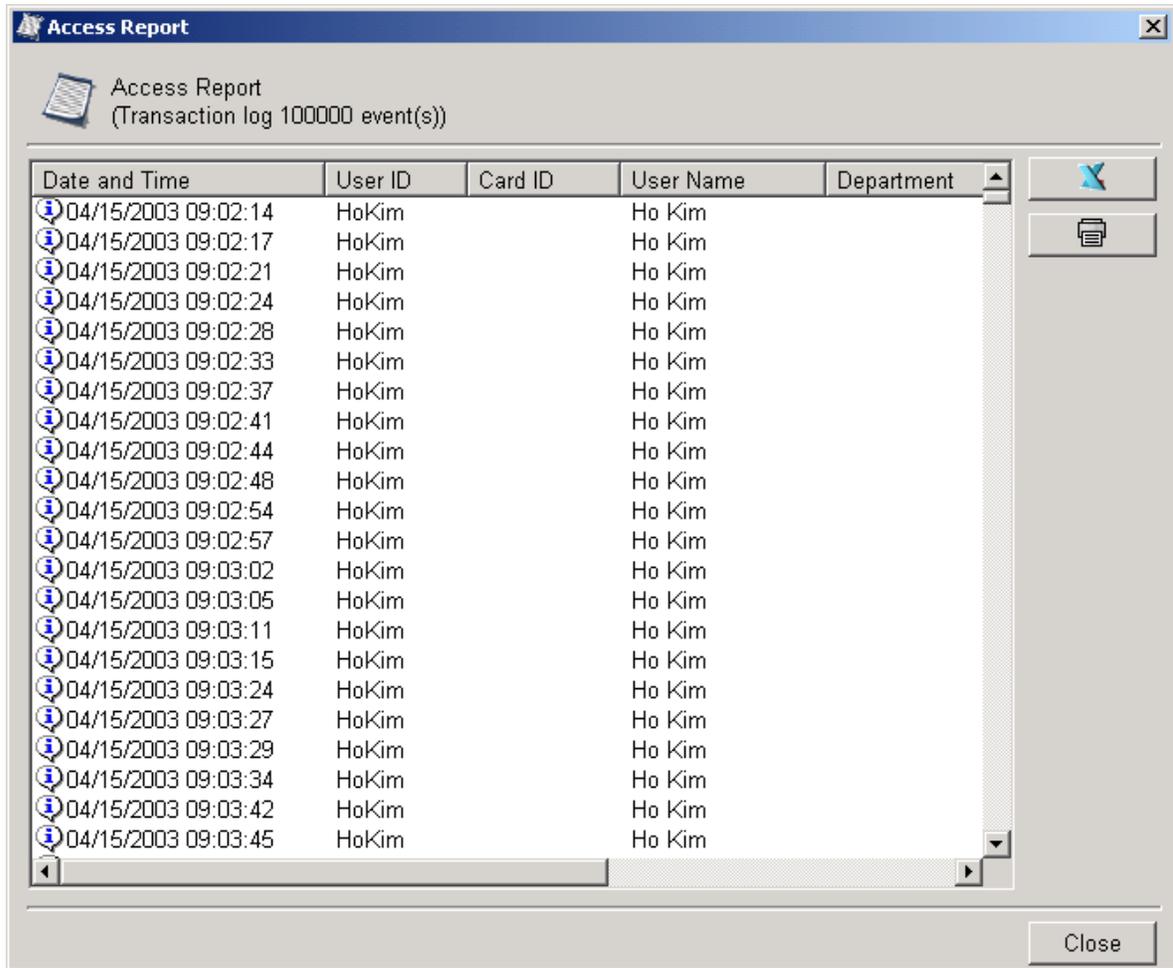
D:\tmp\

Browse...

3. Select **All** or **Filtering**. Select the **All** item to view all logs.
4. Select **Filtering** to view the filtered logs based on
 - a. **Date and Time range**
 - b. Filtering by **Remote Unit**, **Remote Group** and **IrisEnroll** can be done by selecting the respective items after selecting **Basic filtering**.
 * When a user tries to identify or verify with IrisEnroll, corresponding logs are created as followings.
 Identified

Not Identified (Iris NOT enrolled)	Warning
Not Identified (Fake eye)	Warning
Verified	
Not Verified (Iris NOT enrolled)	Warning
Not Verified (Fake eye)	Warning

- c. Additional filtering based on **User ID, Card ID, Last Name, First Name, Department, Remote Unit and Process Result** can be done by selecting the required items, after selecting the **Additional filtering** option.
5. Select the items to be viewed in the **Access Report**. This can be done by selecting the items from the **Unselected Items** and clicking on the **Add** button. Selected items can be removed by selecting the items from the **Selected items** and clicking on the button **Remove**.
 6. If you want to view the logs stored in a **backed-up log file**, select the “**Filtering in the previously backed-up log file**” check box. And then click on the **Browse** button and select the folder in which the log files to be filtered are located. Refer to the section 2.6.2.4 LOG BACKUP. **The backup log file’s name created after log back up should be not changed**. If this name is changed, information cannot be filtered from the backup log files.
 7. Click the **View** button to view the results in the **Access Report** window as shown below.
 8. Click on the **Stop** button to stop the report generation. When you click the **Stop** button, logs already transferred from the server database will be displayed in the **Access Report** window.
 9. This information can be saved into an **Excel** sheet (Microsoft Excel must be installed) or printed with the buttons indicated by arrows, respectively.
-



10. Clicking on the **Close** button will close the **Access Report** screen and return to the **Filtering Condition for Access Report** screen.

2.2.10.3 Time & Attendance Reporting / Filtering

Additional Filtering of access logs using Function Key value is supported in IrisManager. See image that follows:

Filtering condition for access report

Filtering condition

All
 Filtering

Date and Time range (mm/dd/yyyy)
 8 /30/2011 00 : 00 ~ 8 /30/2011 24 : 00

Basic filtering

By Remote Unit (OPT3)
 By Remote Group (All)
 By IrisEnroll (IrisEnroll)

Additional filtering

User ID
 First Name
 Last Name

Process Result
 Department
 Function Key (1)

Items in Access Report

Selected Items	Unselected Items
User ID	
Card ID	
User Name	
Department	

Filtering in the previously backed-up log file
 Select the folder in which the log file to be filtered is located.
 Browse...

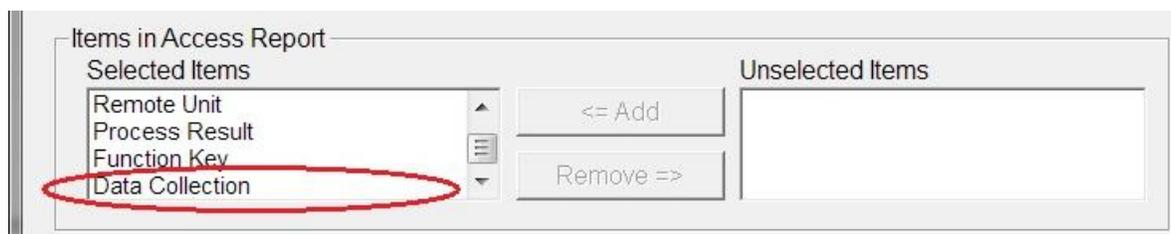
An *Access Report* is generated with Function Key information as shown in picture below. If the time and attendance feature is disabled, the function key value will be **blank**. Otherwise, the entered function key value is displayed in the access report. If the user fails to press a valid function key within the timeout period, the report displays the function key value as **0**.

Date and Time	User ID	Card ID	User Name	Function
08/30/2011 19:50:53				
08/30/2011 19:51:07	1954	1A80820A00	Vinodkumar Medidar	1
08/30/2011 19:51:17	1954	1A80820A00	Vinodkumar Medidar	2
08/30/2011 19:51:26	1954	1A80820A00	Vinodkumar Medidar	4
08/30/2011 19:51:35	1954	1A80820A00	Vinodkumar Medidar	5
08/30/2011 19:51:44	1954	1A80820A00	Vinodkumar Medidar	6
08/30/2011 19:52:03	1954	1A80820A00	Vinodkumar Medidar	0
08/30/2011 19:56:09	1954	1A80820A00	Vinodkumar Medidar	0
08/30/2011 19:56:20	1954	1A80820A00	Vinodkumar Medidar	1
08/30/2011 19:56:31	1954	1A80820A00	Vinodkumar Medidar	2
08/30/2011 19:56:40	1954	1A80820A00	Vinodkumar Medidar	4
08/30/2011 19:56:46				
08/30/2011 19:56:56	1954	1A80820A00	Vinodkumar Medidar	5
08/30/2011 19:57:04	1954	1A80820A00	Vinodkumar Medidar	6
08/30/2011 19:57:26	1954	1A80820A00	Vinodkumar Medidar	0

2.2.10.4 Data Collection Report

A report displaying the access records through the doors can be obtained using this feature. This feature can be used as follows:

1. Select the **Reports** from the toolbar or menu bar.
2. Select the **Access Report** Item from the **Reports** menu.
3. The following **Filtering condition for access report** window will be opened on the screen, after the selecting the **Access report** item called **Data Collection** as shown in the following image.



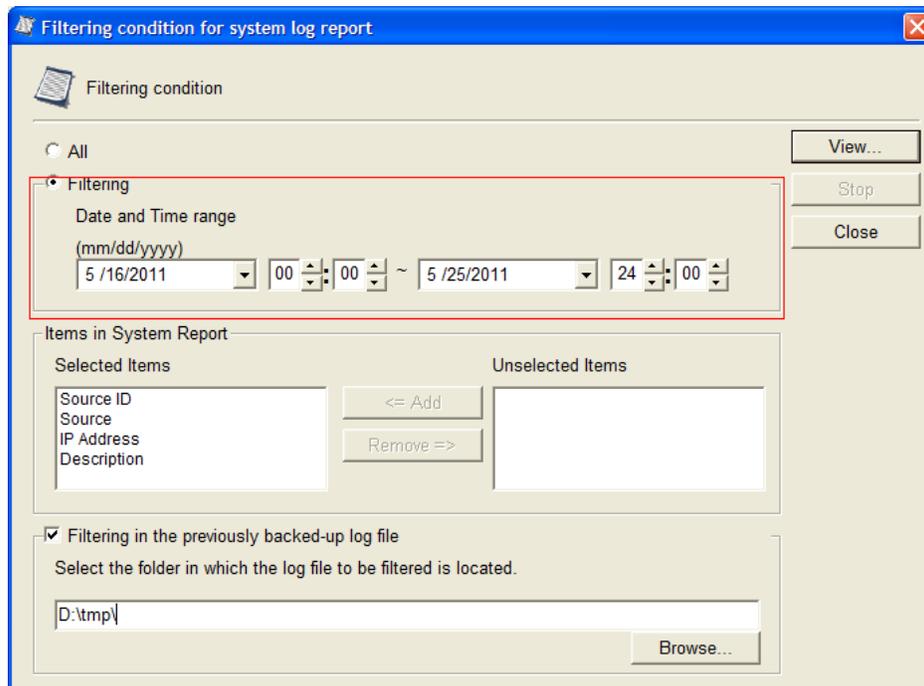
4. View the access report indicating the Data Collection (and any other selected filtering conditions) as shown in the following image.
 - a. When an access report is generated from Iris Manager, it shall contain the Data Collection field. If the value of DecisionTimeInterval field in TTransactionLog table is within the **valid range i.e. 1 to 99999999**, then it is **displayed in the Data Collection** field of access report according to table. If value of DecisionTimeInterval field is **100000000** i.e. timeout then Data Collection field shall **display 0**; otherwise if user **authentication failed** or user has presses “Enter key” **without any data collection** or data collection is **disabled** then in Iris manager data collection field shall be **left blank**. Data Collection field should also be available when access report is exported to Microsoft excel format or printed.
 - b. The following picture shows the above mentioned scenarios in access report.

Date and Time	User ID	Card ID	User Name	Function Key	Data Collection	Department	Remote Unit	Process Result
11/28/2012 19:11:23	2996	2996	shashidhar kanuka...		0		103	Accepted (Normal)
11/28/2012 19:12:00	1954	80829FC0	VinodKumar M		0		103	Accepted (Normal)
11/28/2012 19:12:25	2996	2996	shashidhar kanuka...		0		103	Accepted (Normal)
11/28/2012 19:12:46	2996	2996	shashidhar kanuka...		124		103	Accepted (Normal)
11/28/2012 19:13:00							103	Denied (Iris not enrolled)
11/28/2012 19:13:16	2996	2996	shashidhar kanuka...		0		103	Accepted (Normal)

2.2.10.5 System Reports

The information from the system log can be obtained using this feature.

1. Select **Reports** from the toolbar or menu bar.
2. Select the **System Report** Item from **Reports**.
3. The following **Filtering condition for system log report** window will open on the screen, after the selection of the **System Report** item.



4. Select **All** or **Filtering**. Select the **All** item to view all logs. Select **Filtering** to view the filtered logs based on **Date and Time range**
5. If you select **Filtering**, select the date and time range in the **Filtering** frame. To select the date range, click on the **Calendar...** button. Select the desired date, and click on the **Ok** button. Set the time by using the up/down arrow buttons next to the hour and minute boxes.
6. Select the items to be viewed in the system log window. This can be done by selecting the items from the **Unselected Items** list and clicking on the **Add** button. Selected items can be removed by selecting the items from the **Selected items** list and clicking on the button **Remove**.
7. If you want to view the logs stored in a **backed-up log file**, select the “**Filtering in the previously backed-up log file**” check box. And then click on the **Browse** button and select the folder in which the log files to be filtered are located. Refer to section 2.6.2.4 LOG BACKUP. **The backup log file’s name created after log back up should be not changed.** If the name is changed, information cannot be filtered from the backup log files.
8. Click the **View** button to view the results in the **System Report** window as shown below.
9. Click on the **Stop** button to stop the report generation. When you click the **Stop** button, logs already transferred from the server database will be displayed in the **System Report** window.

Date and Time	Source ID	Source	IP Address	Descr
04/18/2002 05:36:01	21003	IrisMgr44	160.160.47.85	IrisMa
04/18/2002 05:37:47	21003	IrisMgr44	160.160.47.85	IrisMa
04/18/2002 05:49:11	21003	IrisMgr44	160.160.47.85	IrisMa
04/18/2002 05:49:46	21003	IrisMgr44	160.160.47.85	IrisMa
04/18/2002 05:50:13	21003	IrisMgr44	160.160.47.85	IrisMa
04/18/2002 05:55:48	21003	IrisMgr44	160.160.47.85	IrisMa
04/18/2002 06:03:35	2	R76-1	160.160.47.88	Remo
04/18/2002 06:03:51	3	R76-2	160.160.47.88	Remo
04/18/2002 06:04:02	21003	IrisMgr44	160.160.47.85	IrisMa
04/18/2002 06:04:06	4	R76-3	160.160.47.88	Remo
04/18/2002 06:04:07	21003	IrisMgr44	160.160.47.85	IrisMa
04/18/2002 06:04:07	5	R76-4	160.160.47.88	Remo
04/18/2002 06:04:42	21003	IrisMgr44	160.160.47.85	IrisMa
04/18/2002 06:06:42	3	R76-2	160.160.47.88	Remo
04/18/2002 06:06:54	3	R76-2	160.160.47.88	Remo

10. This information may be saved into an **Excel** spreadsheet (Microsoft Excel must be installed) or printed with the buttons indicated by the arrows, respectively.
11. Clicking on the **Close** button will close the **System Report** screen and return to the **Filtering Condition for System Log Report** screen.

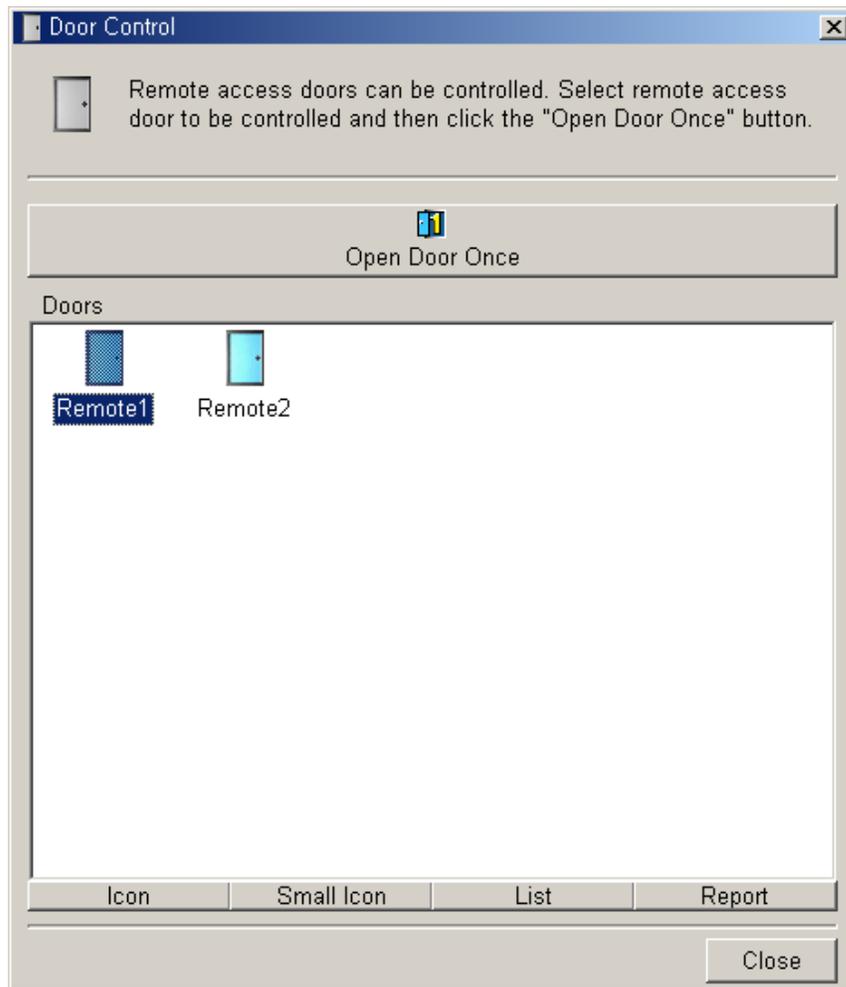
2.2.11 Door Control

Remote access door(s) may be controlled with the door control feature.

2.2.11.1 Opening Door(s) Once

You may open door(s) one time.

1. Select the **Door Control** item on the **Tools** menu on the menu bar or select the **Door** item on the toolbar to open the following window.



2. Select remote access door(s) to be controlled and then click the **Open door one time** button.
3. Click on **Close** button to close the window.

2.2.12 Tool Operation

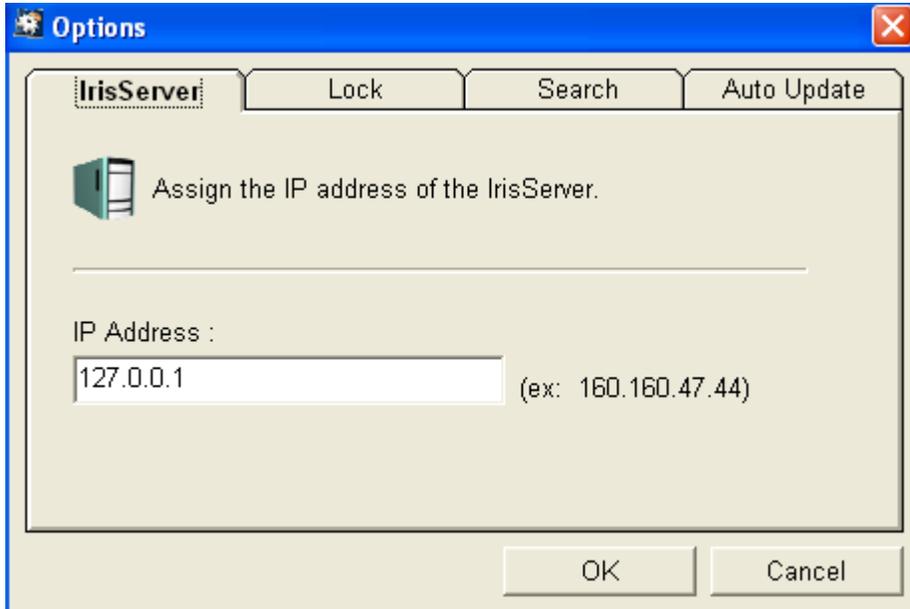
2.2.12.1 Options

The Options can be used to set the **IrisServer** IP Address and to lock the **IrisManager** program.

The Options screen may be opened by selecting the **Options icon** from the toolbar or by selecting the **Options** item from the **Tools** menu on the menu bar. This will open the following **Options** window. Select the **IrisServer** tab field to set the IP address of the IrisServer.

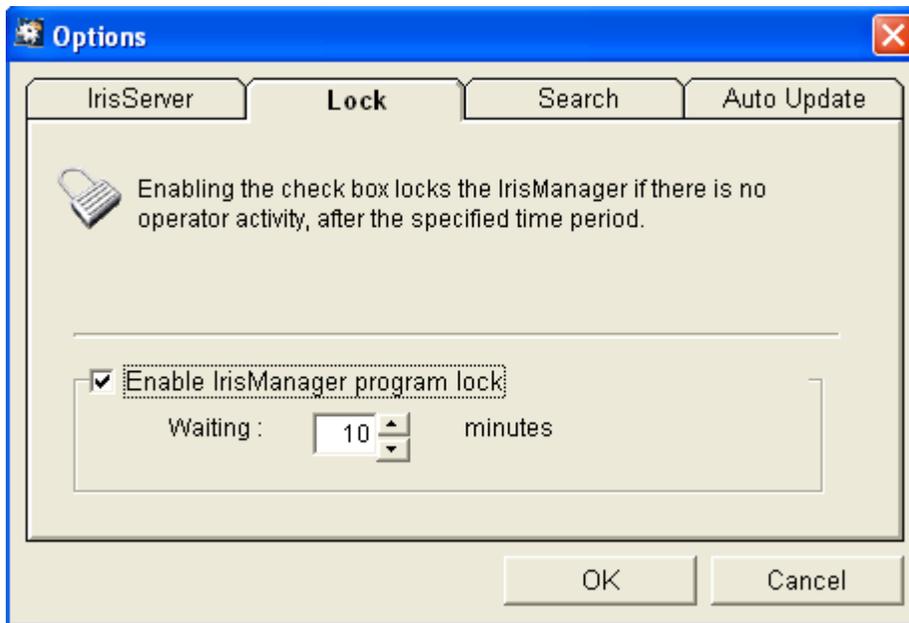
2.2.12.1.1 IrisServer IP Address

Set the **IP address** in the text box labeled with **IP Address**. If **IrisManager** is located on the same computer as **IrisServer**, we recommend setting the IP Address to the loopback address (127.0.0.1).



2.2.12.1.2 Program Lock

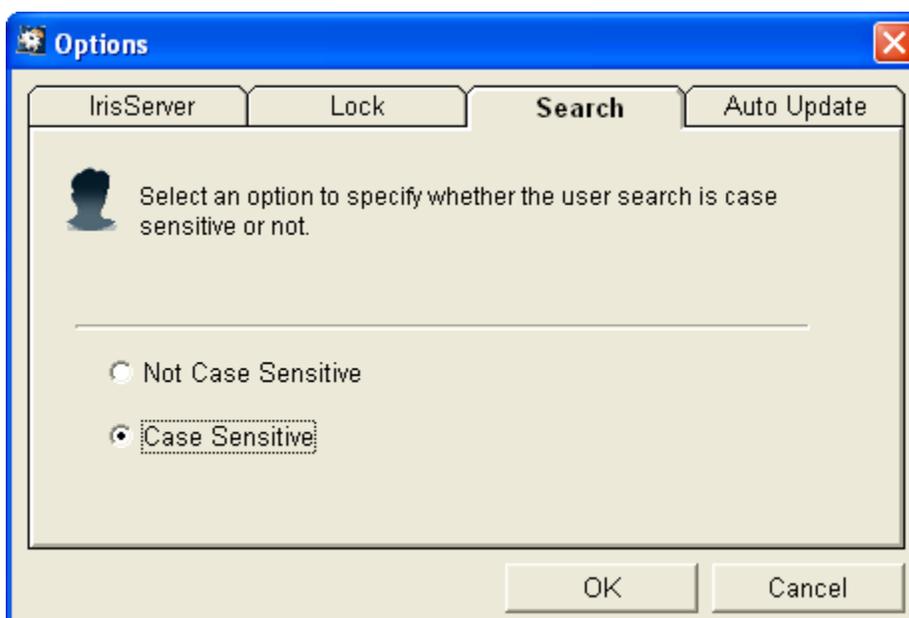
1. The **Program Lock** functionality is used to Lock the application if there is no action within the specified time. Once the program is locked, the Operator must re-login to use the application.
2. The **Lock** may be enabled by selecting the **Lock** tab field.
3. Check the check box labeled **Enable IrisManager Program lock** function to enable the **lock**.



4. Specify time period in **Wait**.

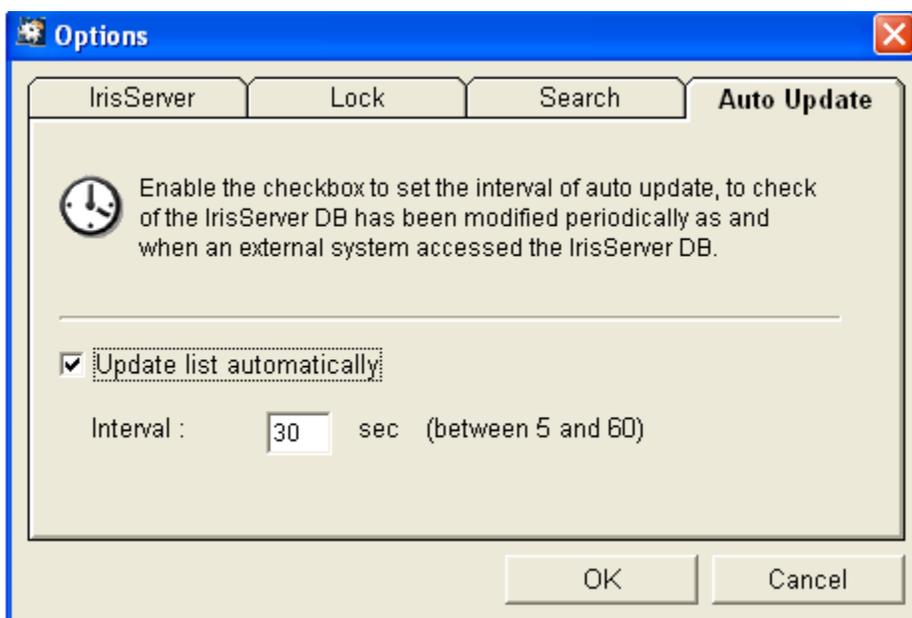
2.2.12.1.3 Search Option

1. The **Search Option** functionality is used to specify whether to match case when use the **Find** option.
2. If you select **Not Case Sensitive** in the search option as following figure, the search text is NOT case-sensitive (For example, 'a' will match with 'A'). But if you select **Case Sensitive** in the search option, the search text is case-sensitive (For example, 'a' will not match 'A').



2.2.12.2 Auto Update

1. The **Auto Update** function is used to set the how frequently **IrisManager checks the database has been updated**. This option is only required if applications outside the IrisAccess system have access to the IrisAccess database (For example, a custom enrollment application)
2. To enable this, check the “Update list automatically” check box and set the time interval. The interval time may be from 5 to 60 seconds.
3. Every interval, **IrisManager** checks the database for updates.



3. iCAM7000 Update

3.1 iCAM7000 Update

iCAM700 Update is an application utility that allows for new installation and upgradation of IrisRecog7000 software of an iCAM7000 for all operational: option modes (1, 2, and 3).

Note: Earlier versions of EAC iCAM firmware and EAC software utilized the Option3Admin application new installation and upgradation of IrisRecog7000.

This program is designed for use with iCAM7000 series camera units only.

- This is an independent application which can be run on any Windows XP or Windows 7 machine.
- It will support new installation or upgrade for 32 iCAMs that can be added to the list at one time.
- For new installation or Update process, the iCAM7000 IP address is required.
- For upgrade process the iCAM must be at a firmware version of 7.06.x or above, otherwise a New Installation will need to be performed.

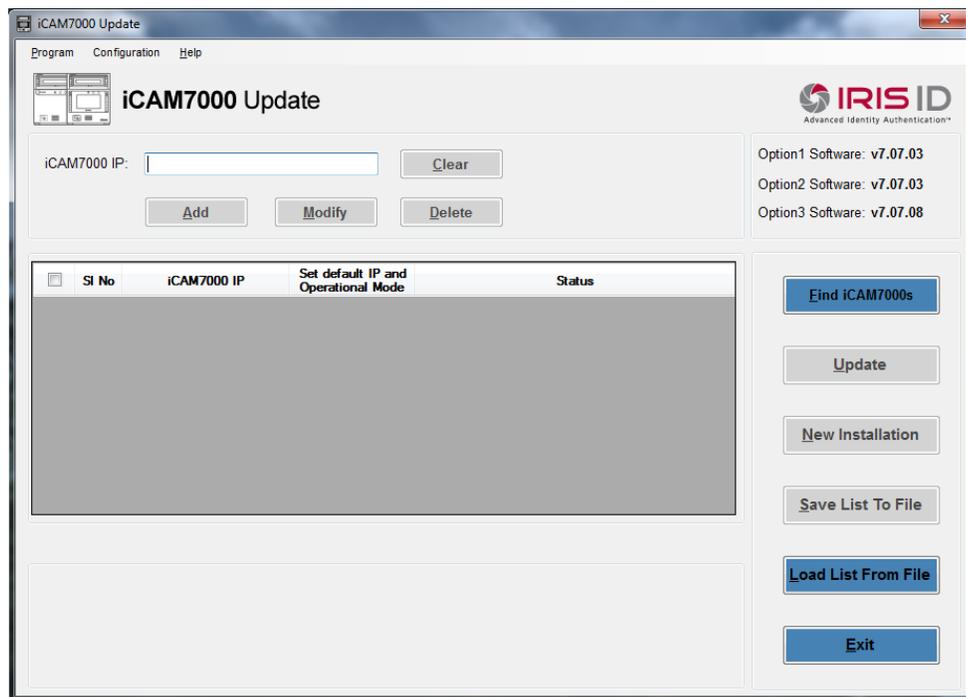
3.1.1 Minimum System Requirements

In addition to the system requirements for IrisAccess EAC (refer IrisAccess Software Installation Manual); the following pre-requisites are required to setup IrisAccess EAC with Option 3.

- Windows XP or Windows7 Operating system
- Microsoft .Net Framework 3.5 (not required on Windows 7)

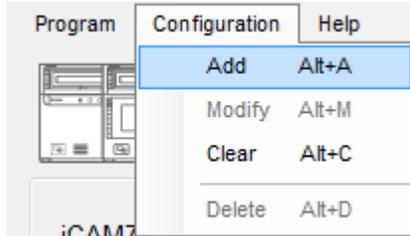
3.2 Standard usage for Installation / Updating iCAM

- To start the iCAM7000 Update, click **iCAM7000Update.exe**. OR Click on iCAM7000 Update shortcut in start menu or desktop.
- The application window will appear as follows.



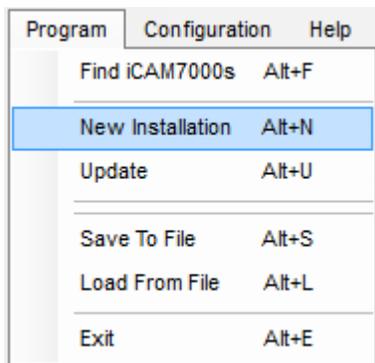
C. Entering valid iCAM7000 IP

D. Click the **Add button or select **Add** option from **Configuration** menu. The Add option is used to add the **iCAM7000 IP** to the list.**

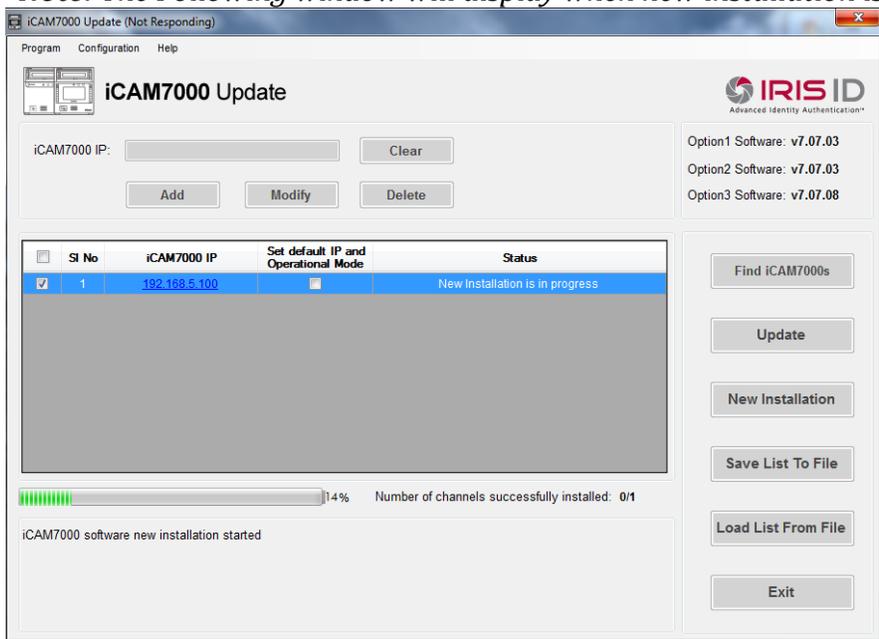


****Note:** The **Find iCAM7000s** button function can be used instead of the manual Add function if desired. It will search the network for available iCAM7000 units and display them in the list. To perform this process Click on > Find iCAM7000 button or select Find iCAM7000s option from Program menu. (Network settings, windows firewall, available ports, routers, and anti-virus applications can block the applications ability to find/detect iCAM7000s on the network.)*

E. Click on New Installation button or select New Installation option from Program menu.



****Note:** The Following window will display when new installation is in progress.*



F. After successful installation, iCAM7000 will reboot automatically.

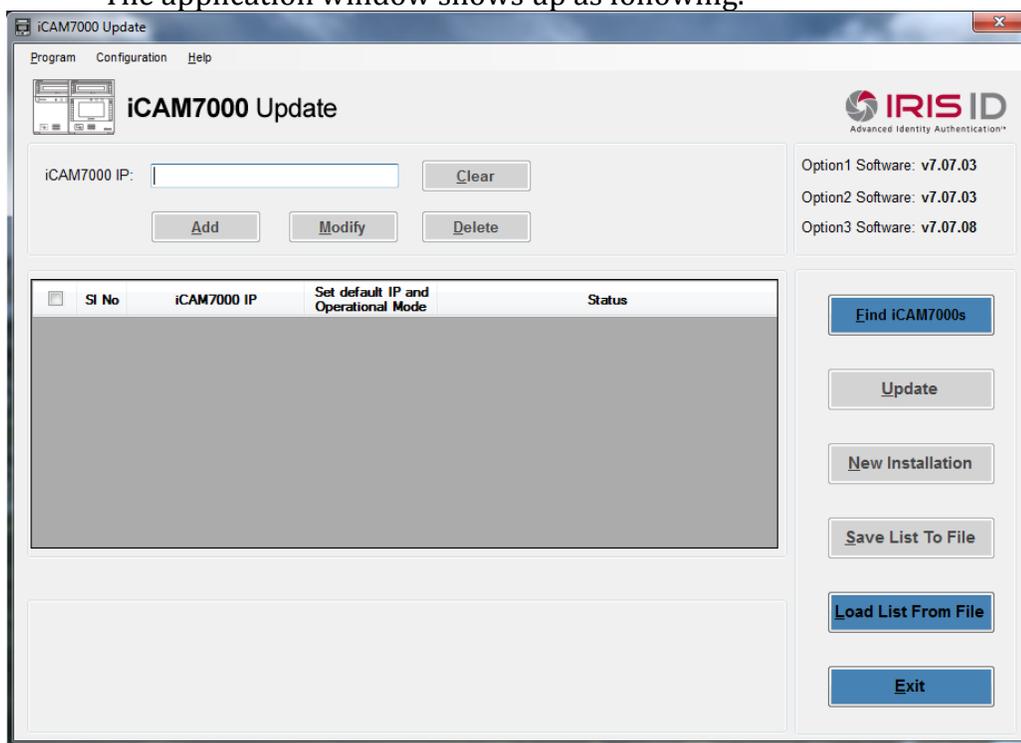
3.3 Full Description Use of IrisAccess™ iCAM7000 Update

To start the iCAM7000 Update, click **iCAM7000Update.exe**.

OR

Click on iCAM7000 Update shortcut in start menu or desktop.

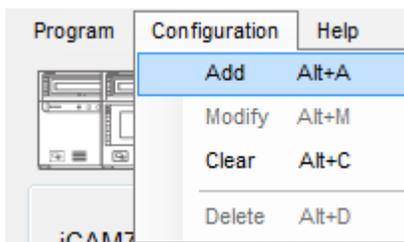
The application window shows up as following.



3.3.1 Add

Add option is used to add **iCAM7000 IP**, **IrisServer IP** and **Security ID** to the list.

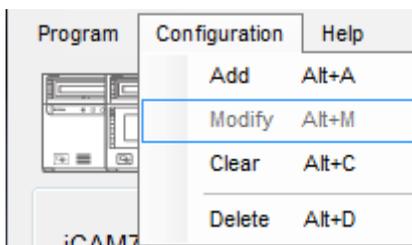
After entering valid **iCAM7000 IP**, click on **Add** button or select **Add** option from **Configuration** menu.



3.3.2 *Modify*

Modify option is used to modify the **iCAM7000 IP** from the list.

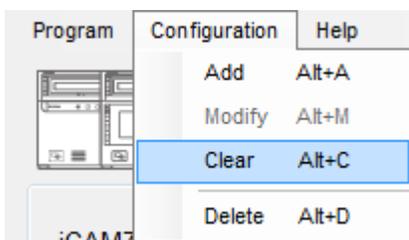
Click on the **Modify** button or select the **Modify** option from **Configuration** menu.



3.3.3 *Clear*

Clear option is used to clear the entered information from the text.

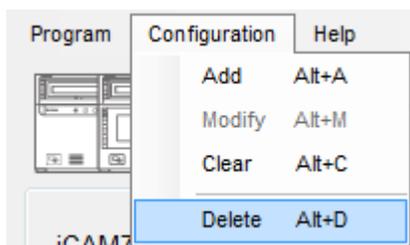
Click on **Clear** button or select **Clear** option from **Configuration** menu.



3.3.4 *Delete*

Delete option is used to delete all the entries from the list.

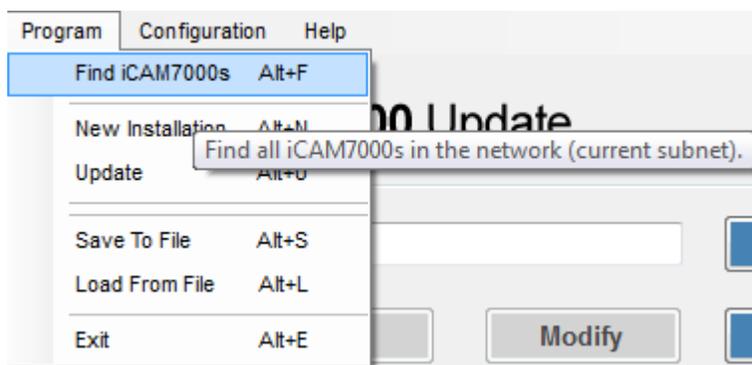
Click on **Delete** button or select **Delete** option from Configuration menu.



3.3.5 Find iCAM7000s

The Find iCAM7000s option will search the network for available iCAM7000 units and display them in the list.

Click on **Find iCAM7000s** button or select **Find iCAM7000s** option from the **Program** menu.



A “Finding iCAM7000s” scroll bar will display when the process is started. In the event that the Find iCAM7000 function does not work successfully, use the **Add** function to enter the IP address data manually.

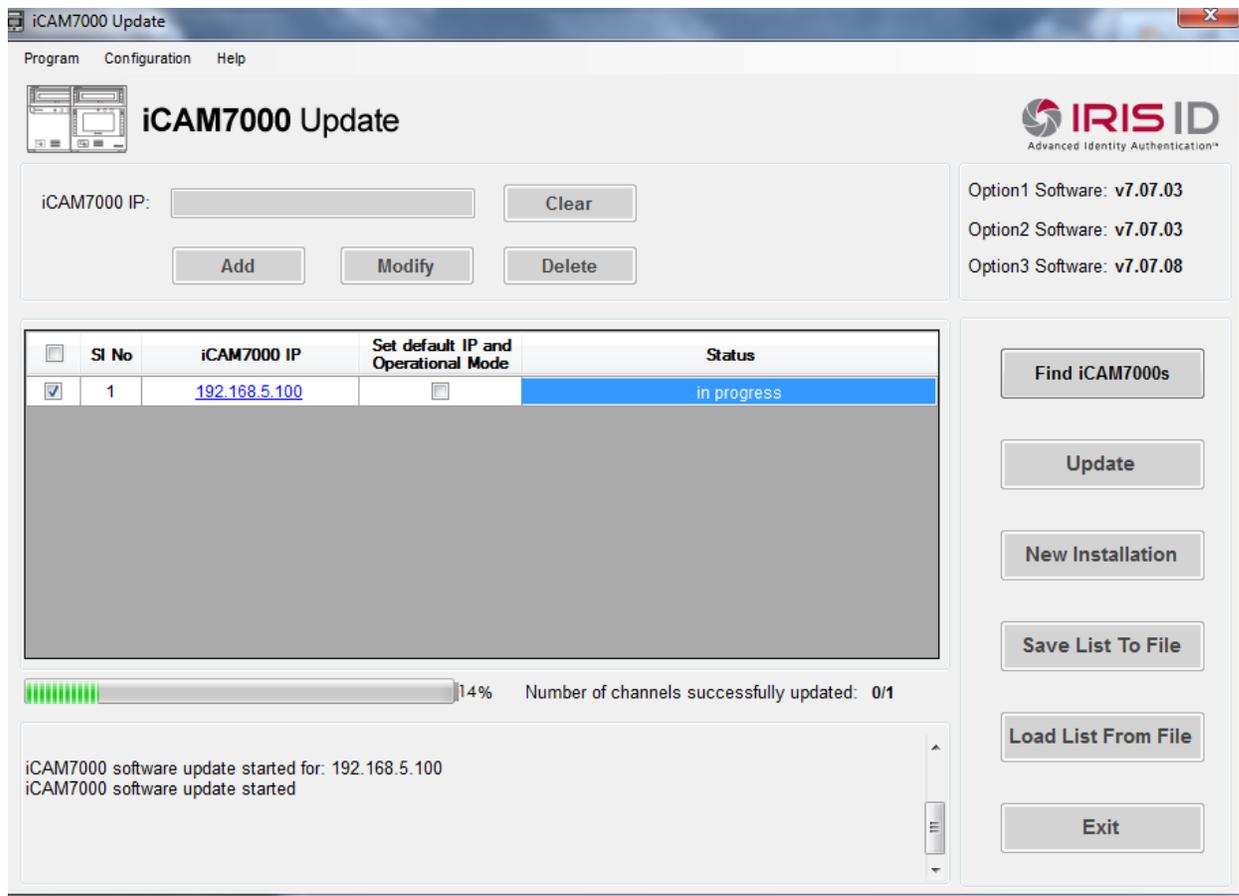
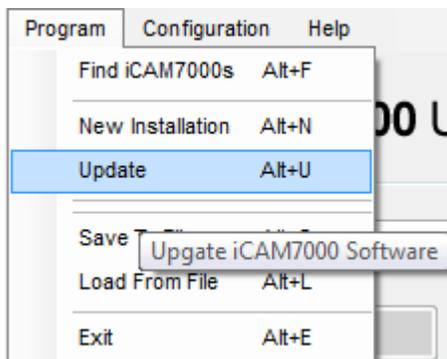
Note: The utility will search for iCAM7000 units on the same subnet only. Additionally, network settings, windows firewall, available ports, routers, and anti-virus applications can block the applications ability to find/detect iCAM7000s on the network.

3.3.6 Update

The Update function of iCAM7000 Update will update the IrisRecog7000 software in iCAM7000. (An update can be performed when the iCAM software version is at version 7.06.x or higher – if the version of iCAM7000 software is lower than 7.06.x performing a “New Installation” will be required.)

***Note:** The “Set Default IP and Operational Mode check box will default the iCAM7000 IP address back to factory default of 192.168.5.100 and place the Operational mode to operational mode: option 3.

Click on **Update** button or select **Update** option from **Program** menu.



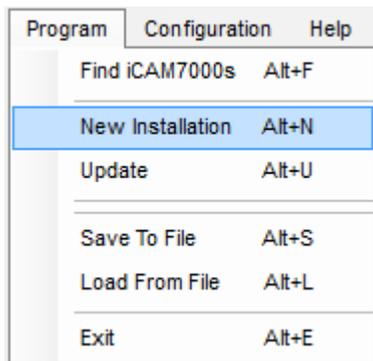
After successful upgrade, iCAM7000 will reboot.

3.3.7 New Installation

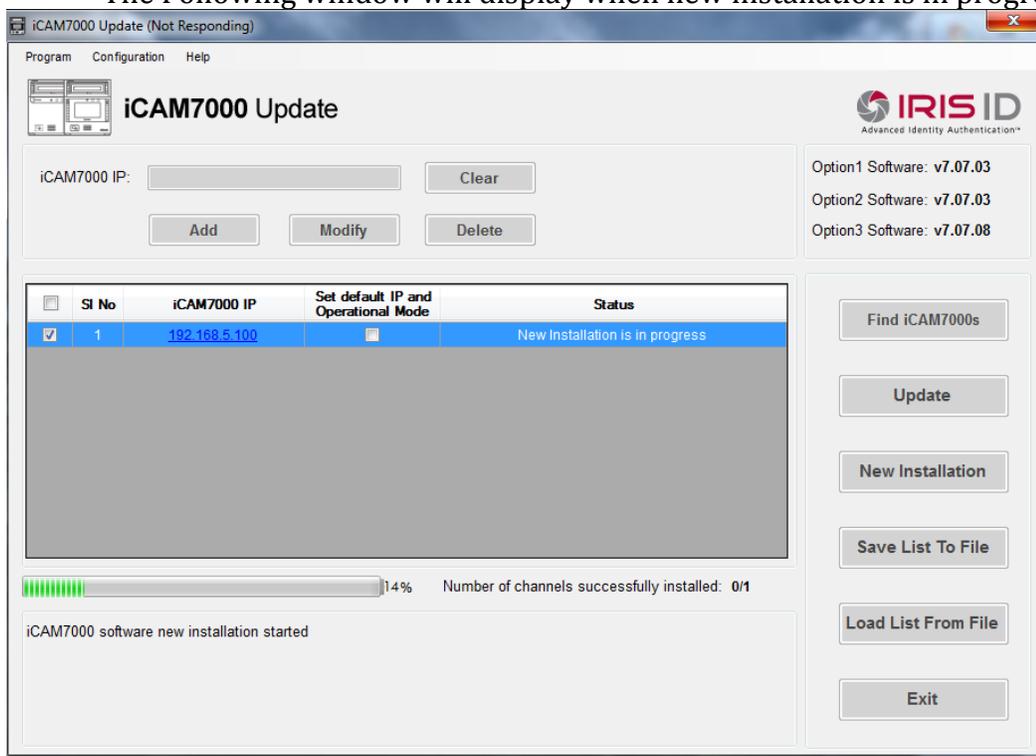
New installation of CAM7000 Update will install IrisRecog7000 software in iCAM7000 for all 3 iCAM7000 operational modes (Option 1, 2, and 3).

***Note:** The "Set Default IP and Operational Mode check box will default the iCAM7000 IP address back to factory default of 192.168.5.100 and place the Operational mode to operational mode: option 3.

Click on **New Installation** button or select **New Installation** option from **Program** menu.



The Following window will display when new installation is in progress

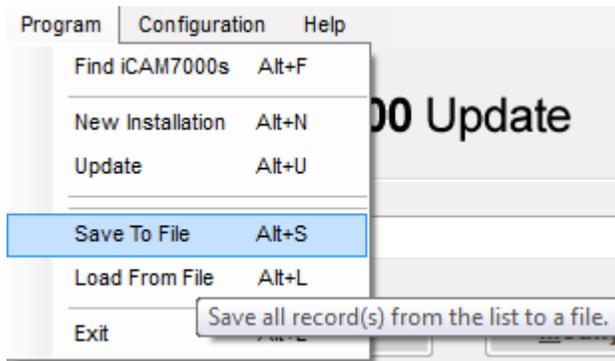


After successful installation, iCAM7000 will reboot automatically.

3.3.8 Save List to File

Save List To File option is used to save the entered list information to file with .csv format.

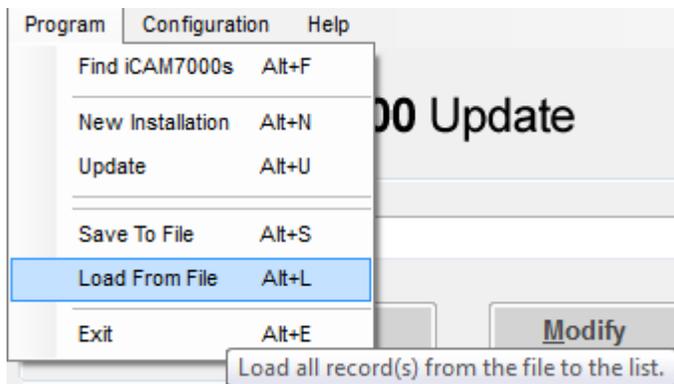
Click on **Save List To File** button or select **Save To File** option from **Program** menu.



3.3.9 Load List From File

Load List From File option is used to load the saved records from the file to the list that is in .csv format.

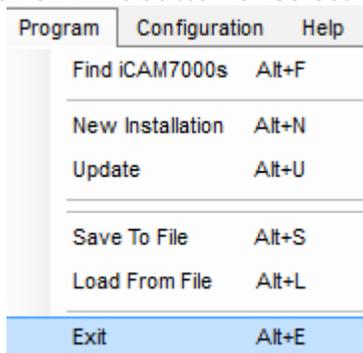
Click on **Load List From File** button or select **Load From File** option from **Program** menu.



3.3.10 Exit

Exit option is close the application and exit the program utility.

Click on **Exit** button or select **Exit** from **Program** menu.



4. IrisAccess™ Option3Admin

4.1 IrisAccess™ Option3Admin

Option3Admin is an application utility that allows for Update of IrisServer IP and security ID management of an iCAM7000 when used in operational mode: Option 3 only. This application will allow these settings to be saved to a file, or loaded from a file to apply or update IrisServer IP and Security ID settings in an iCAM7000.

Earlier versions of the Option3Admin application were used for new installation and upgradation of IrisRecog7000 software (3.03.07 through 3.06.04), however these functions are now performed using the iCAM7000Update program utility.

This Option3Admin program is designed for use with iCAM7000 series camera units only (when used with option 3).

- This is an independent application which can be run on any Windows XP or Windows 7 machine.
- It supports up to 32 iCAM units (referred to as channels in this program) that can be added to the list at one time for new installation and/or upgradation.
- For upgrade process only iCAM7000 IP address is required. IrisServer IP address and Security ID are optional.

4.1.1 *Minimum System Requirements*

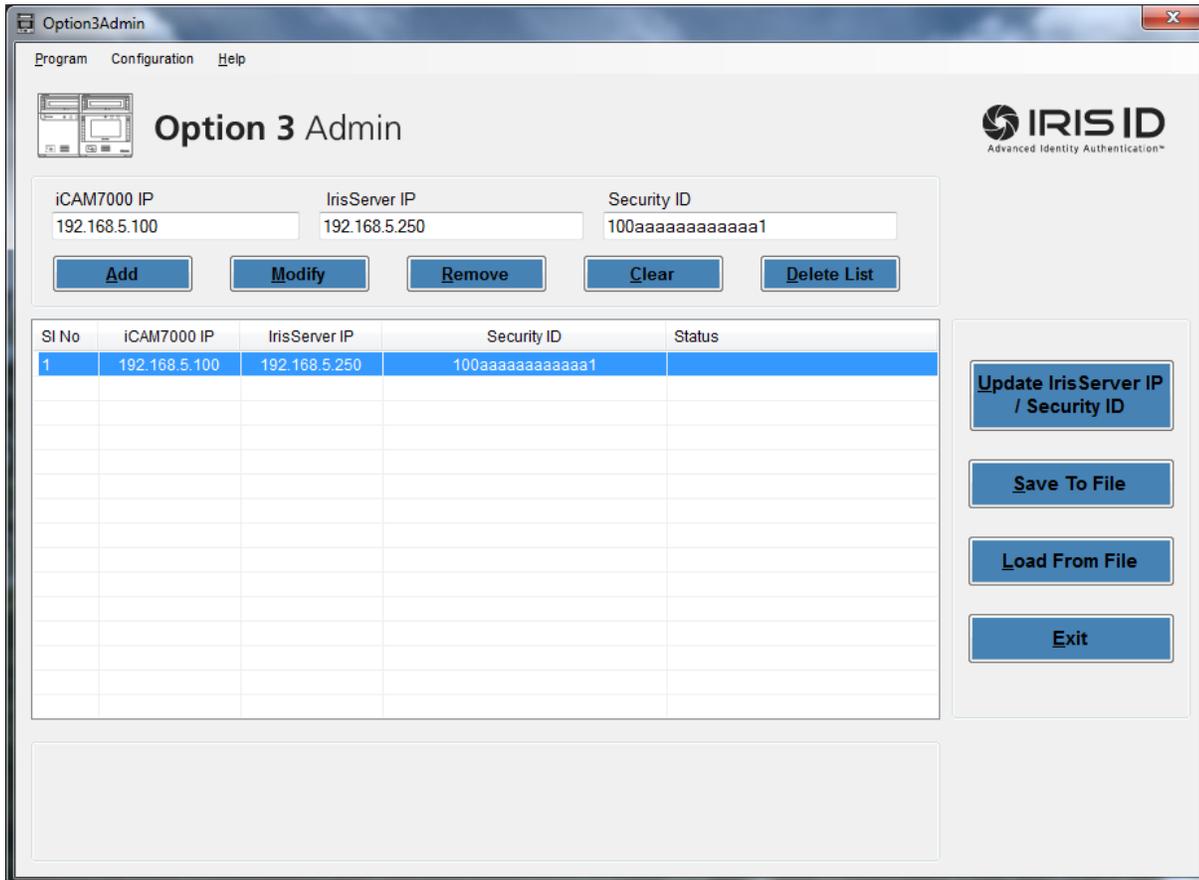
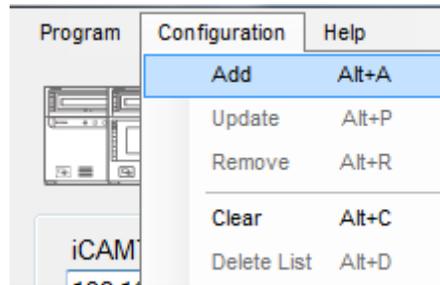
In addition to the system requirements for IrisAccess EAC (refer IrisAccess Software Installation Manual); the following pre-requisites are required to setup IrisAccess EAC with Option 3.

- Windows XP or Windows7 Operating system
- Microsoft .Net Framework 3.5 (not required on Windows 7)

4.1.2 *Version Compatibility*

EAC build v3.07x. Software mandates the following version compatibility check:

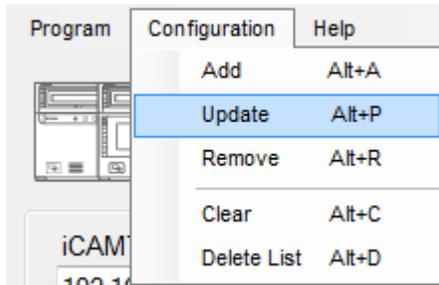
- ICU4000 installed with IrisRecog4000 v3.07x. Software can connect to IrisServer v3.07x..
- ICU3000 installed with IrisRecog3000 v3.06x. Software can connect to IrisServer v3.07x..
- iCAM7000/7100 installed with IrisRecog7000 v3.07x. or above software will connect to IrisServer v3.07x.
- IrisEnroll4000 v3.07x can connect to iCAM4000/4100, and iCAM7000/7100 with v3.07x software.



4.2.2 Modify

Modify option is used to modify the existing iCAM7000 information. This option is enabled when you select the item from the list.

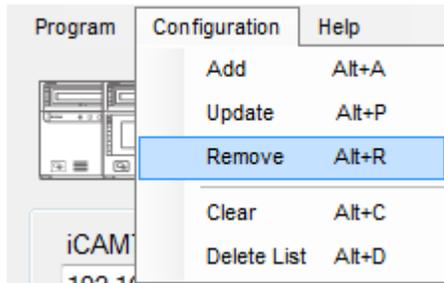
After modifying valid **iCAM7000 IP**, **IrisServer IP** and **Security ID**, click on Modify button or select Update option from **Configuration** menu.



4.2.3 Remove

Remove option is used to remove the selected iCAM7000 entry from the list. This option is enabled when you select the item from the list.

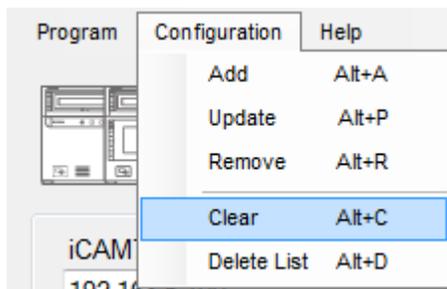
Click on Remove button or select Remove option from **Configuration** menu.



4.2.4 Clear

Clear option is used to clear the entered information from the text.

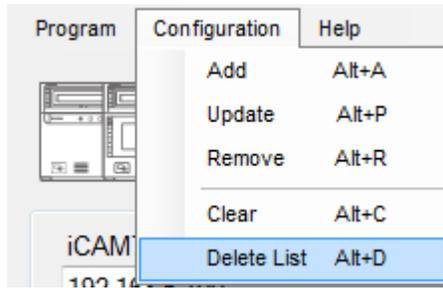
Click on **Clear** button or select **Clear** option from **Configuration** menu.



4.2.5 Delete List

Delete List option is used to delete all the entries from the list.

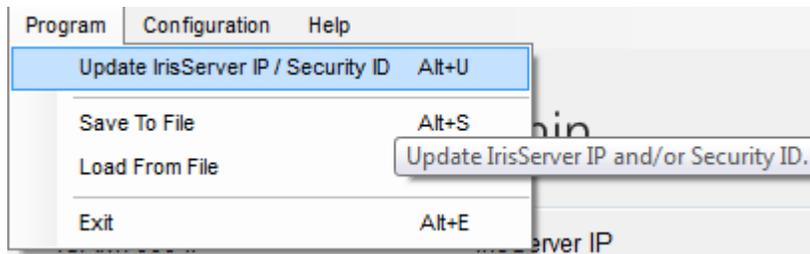
Click on **Delete List** button or select **Delete List** option from Configuration menu.



4.2.6 Update IrisServer IP / Security ID

Update IrisServer IP / Security ID update the information of Security ID and lirsServer IP configured for the iCAM7000s that are listed in the utility.

Click on **Update IrisServer IP / Security ID** button or select **Update IrisServer IP / Security ID** option from **Program** menu.



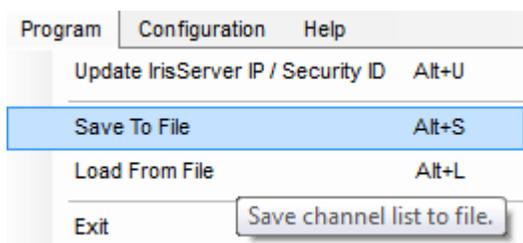
A status indicator will display the progress and result of this procedure.

After successful update, the iCAM7000 may be automatically reboot.

4.2.7 Save to File

Save To File option is used to save the entered list information to file with .csv format.

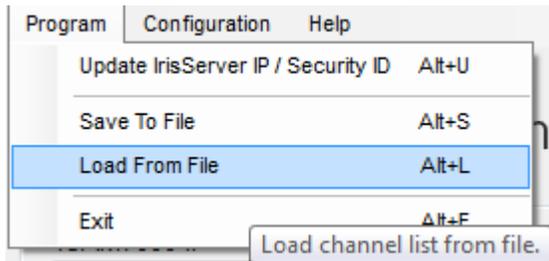
Click on **Save To File** button or select **Save To File** option from **Program** menu.



4.2.8 Load from File

Load From File option is used to load the iCAM7000 information from the file which is of .csv format.

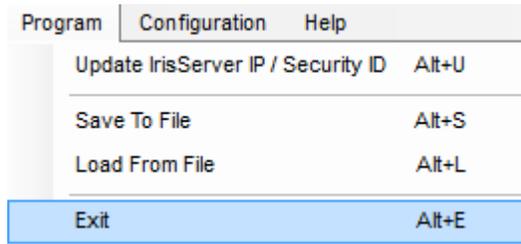
Click on Load From File button or select Load From File option from Program menu.



4.2.9 Exit

Exit option is close the application and exit the program utility.

Click on **Exit** button or select **Exit** from **Program** menu.



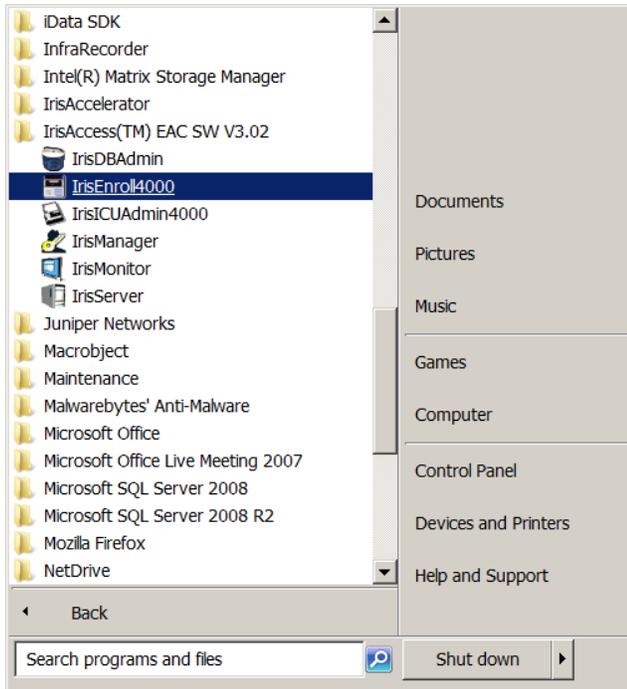
5. IrisAccess™ Enroll4000

5.1 IrisAccess™ IrisEnroll4000

5.1.1 How to Run IrisEnroll4000

To start the **IrisEnroll4000**, click on the **IrisEnroll4000** menu item. The location of the program is shown in the figure below.

Note: *IrisEnroll4000* is designed for use with either an iCAM7000 series camera unit (includes all 7000 and 7100 series models), and/or for use with the iCAM4000 series camera units (includes all 4000 and 4100 series models). When using *IrisEnroll4000* with an iCAM7000 Series camera unit, make sure that the iCAM7000 is set to operational mode: Option 1. The iCAM7000 can communicate with the *IrisEnroll4000* software only when in this Operational mode: Option 1.

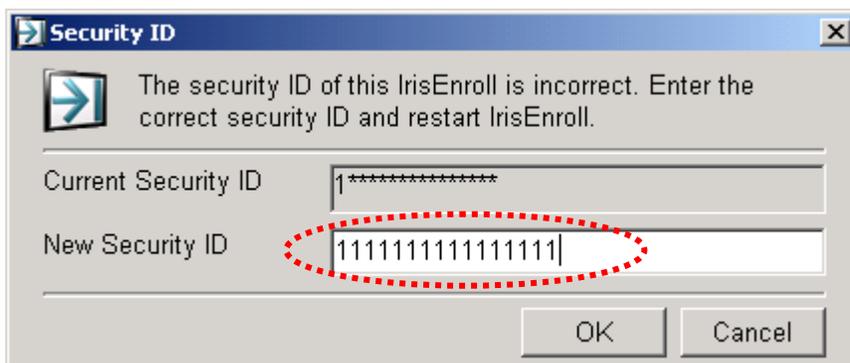


*Note:

IrisServer must be running before starting **IrisEnroll4000**.

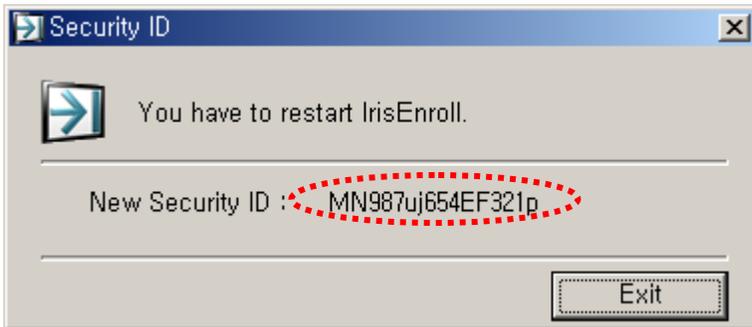
IrisEnroll4000 must first be registered in **IrisManager**.

If the security ID is not identical to the security ID typed in during IrisEnroll registration in IrisManager, the following **Security ID** window is displayed. This window is also displayed the first time IrisEnroll is started.



Enter the security ID of IrisEnroll. The security ID must be identical to the security ID typed in during IrisEnroll registration. Click the **OK** button.

The following Confirmation window is displayed.

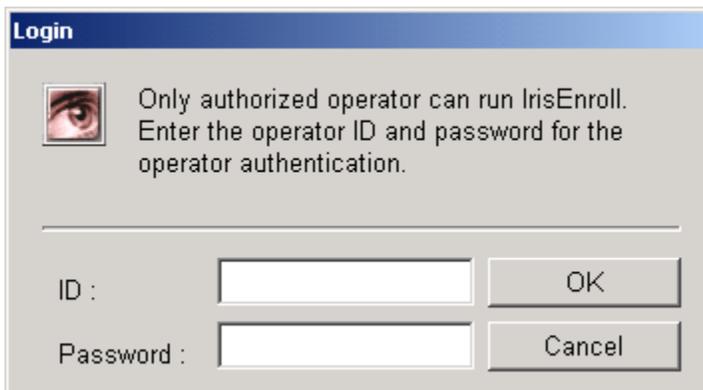


Check if the new security ID is correct and then click the **Exit** button.

Re-Start IrisEnroll.

5.1.2 How to Login to IrisEnroll4000

- Successful execution of the **IrisEnroll** will open the following **Login** window for entering the User ID and password required to execute the **IrisEnroll**.
 - ◆ The **IrisEnroll** may only be executed by **Administrators and Operators with IrisEnroll privileges**.



- Enter the **ID** and **Password** of the operator who has **IrisEnroll** rights and click on the **OK** button.
 - ◆ Default ID and password are “**administrator**” and “**iris3000**” respectively. They can only be changed by an administrator. Refer to the section 2.2.8.2 Modification of the Administrator/Operator

*Note:

If the login to the **IrisEnroll** is successful, then you may see the following **Notice** window,

if the password is not secured. (When you login with the default password “iris3000”)



Click on **No** to continue with the same password.

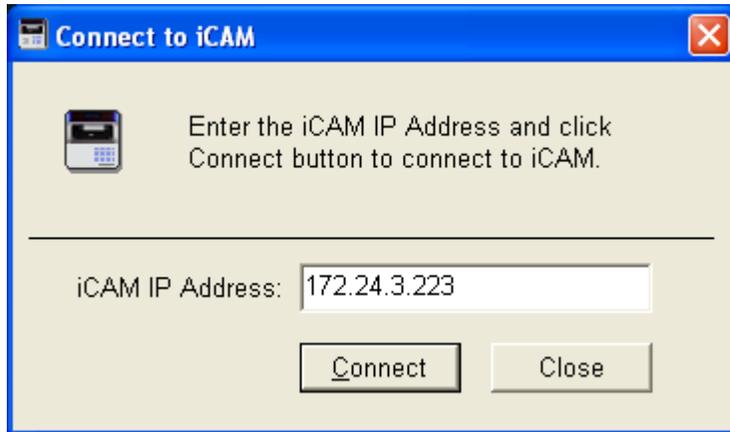
Click on **Yes** to open the following **Password** window to change the password.



Enter the current password in the **Current Password** field. Enter the **New Password** in the **New Password** field and the **Confirm Password** field, then before click on the **OK** button. This will change the password.

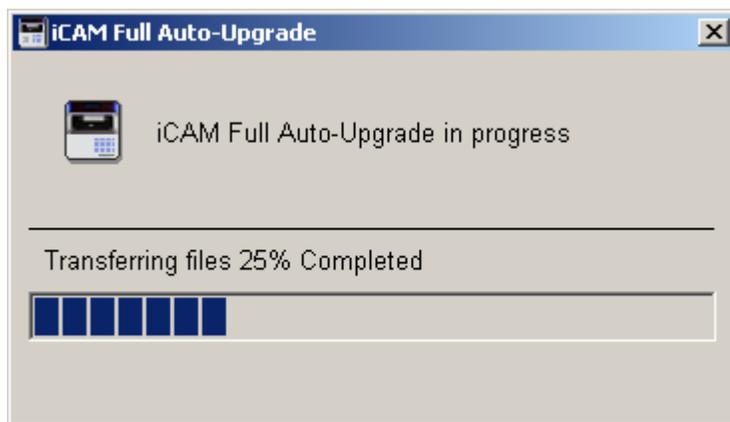
Then following **Connect iCAM** window will be displayed after changing the password successfully or aborting the password changing operation.

3. The same **Connect iCAM** window will be displayed without the **Notice** window, if the **ID** and **Password** are valid and the password is secured.



Enter the iCAM IP in **iCAM IP Address** and click **Connect** to connect iCAM. While connecting to iCAM, application will check the version of iCAMSoftware. If running iCAMSoftware version is less than the installed iCAMSoftware version, then application will automatically upgrade iCAMSoftware (IrisCapture & WebConfig) in iCAM. Application will also check the version of iCAM Files System. If running iCAM File System version is less than the installed iCAM File System version, then the application will also upgrade File System in iCAM. User will be notified about the status of iCAM Full Upgrade process with the following windows.

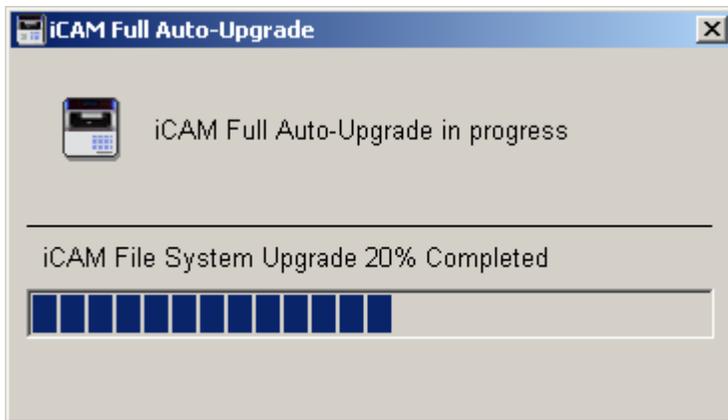
Files that may be required for iCAM Full Auto-Upgrade process are first transferred to iCAM. During files transfer, the following screen is displayed with the percentage of completion.



After transferring upgrade files, application will start upgrading iCAM Software (IrisCapture & WebConfig) only if the version of iCAM Software running in iCAM is less than the version of iCAMSoftware installed. If not, application will go for iCAM File System upgrade, if required. When iCAM Software is upgraded, following screen is displayed to notify the status of iCAM Software upgrade process.



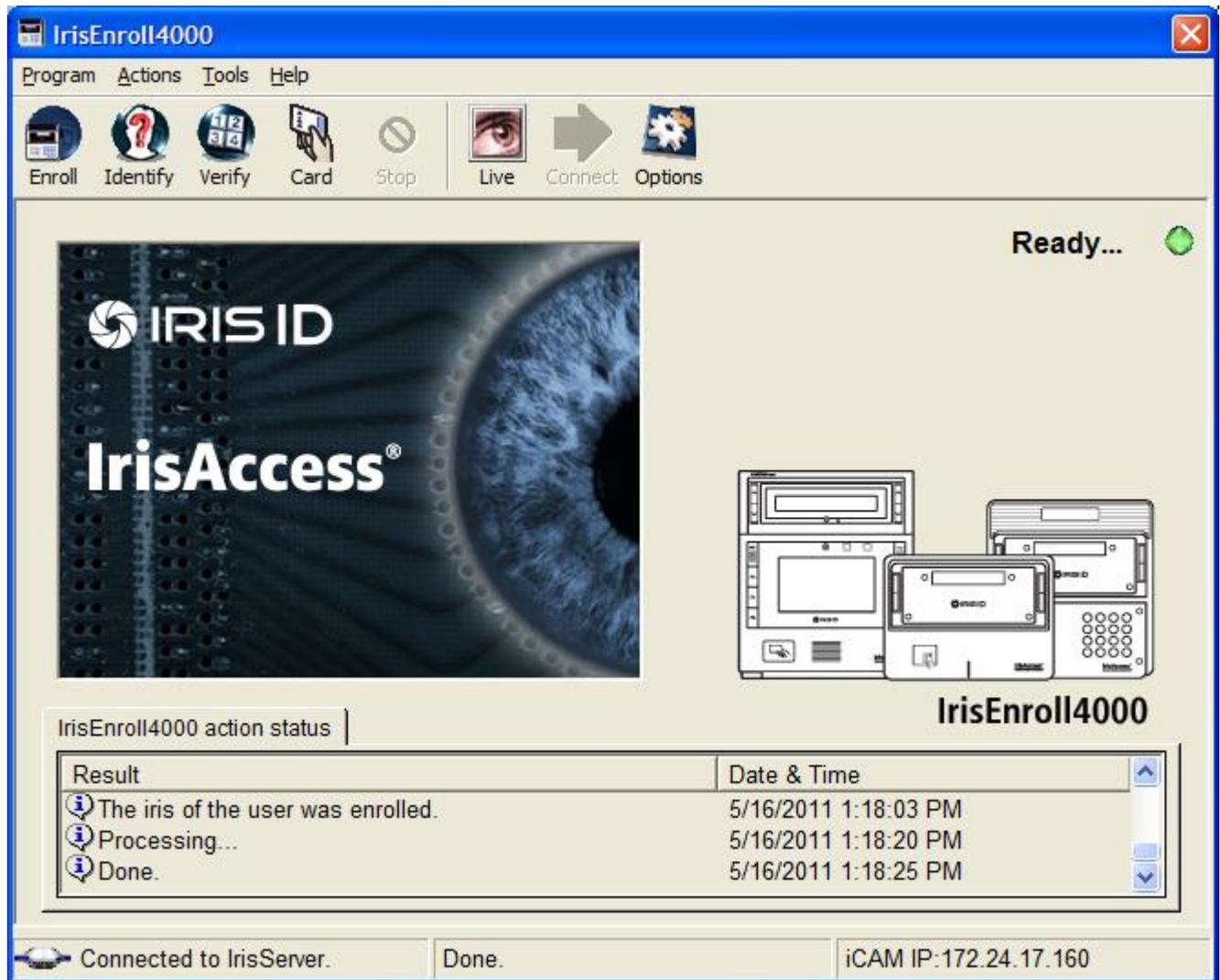
While upgrading iCAM File System, application will display the following screen to notify the user about the status of iCAM File System upgrade process.



After successful completion of iCAM Full Auto-Upgrade, iCAM will be rebooted and IrisEnroll4000 will re-connect to iCAM.

After IrisEnroll4000 is connected to iCAM, the following IrisEnroll window will be displayed.

If iCAM Full Auto-Upgrade is not required (i.e running IrisCapture version is greater than or equal to installed IrisCapture version), IrisEnroll4000 will be connected to iCAM and following IrisEnroll window will be displayed.



5.1.3 Enroll

Enrollment is the process of **adding new IrisCodes** into the system. The records are used during the **identification and verification** process to validate the user for access (entering or existing through the door).

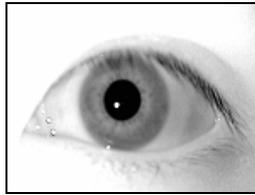
Eye selected in “Options->Eye Selection->Enrollment” will be enrolled.

The maximum number of users that can be registered is determined by each EAC S/W version.

*Cautions:

1) To decrease the “False Reject Rate” (Rejection of an Iris that should be accepted) and generate higher-quality IrisCodes, the user should follow the below recommendation.

- ◆ The user should open his/her eye as widely as possible. For example,

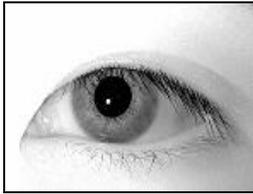


Correct



Incorrect

- ◆ The user should NOT rotate, pan and tilt his face. For example,



Correct



Incorrect



Incorrect



Incorrect

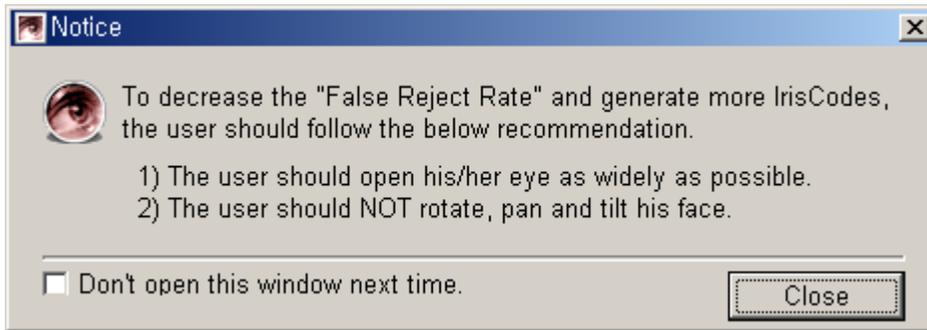
- ◆ Eyeglasses must be removed before enrollment, but may be worn during verification and identification.
- ◆ Contact Lenses with patterns that cover any part of the Iris may not be worn.

Limitation of ambient light in working environment

- ◆ When Fake Eye Detection is not used: 1,000 lx Fluorescent light and 100 lx Incandescent or sunlight.
- ◆ When Fake Eye Detection is used: 500 lx Fluorescent light and 50 lx Incandescent or sunlight.
- ◆ If the ambient light exceeds these limitations, the False Reject Rate will be increased.

The **enrollment** of the user can be performed using the following procedure.

1. Select the **Enroll** Item from the **Actions menu** in the menu bar or select the **Enroll** icon from the tool bar.
2. If you didn't select the "**Don't open this window next time**" check box on the following **Notice** window in previous enrollment, the **Notice** window is displayed. Read the message on the **Notice** window for good enrollment and click on the **Close** button. If you don't want this window to open next time, select the "**Don't open this window next time**" check box and then click on the **Close** button.



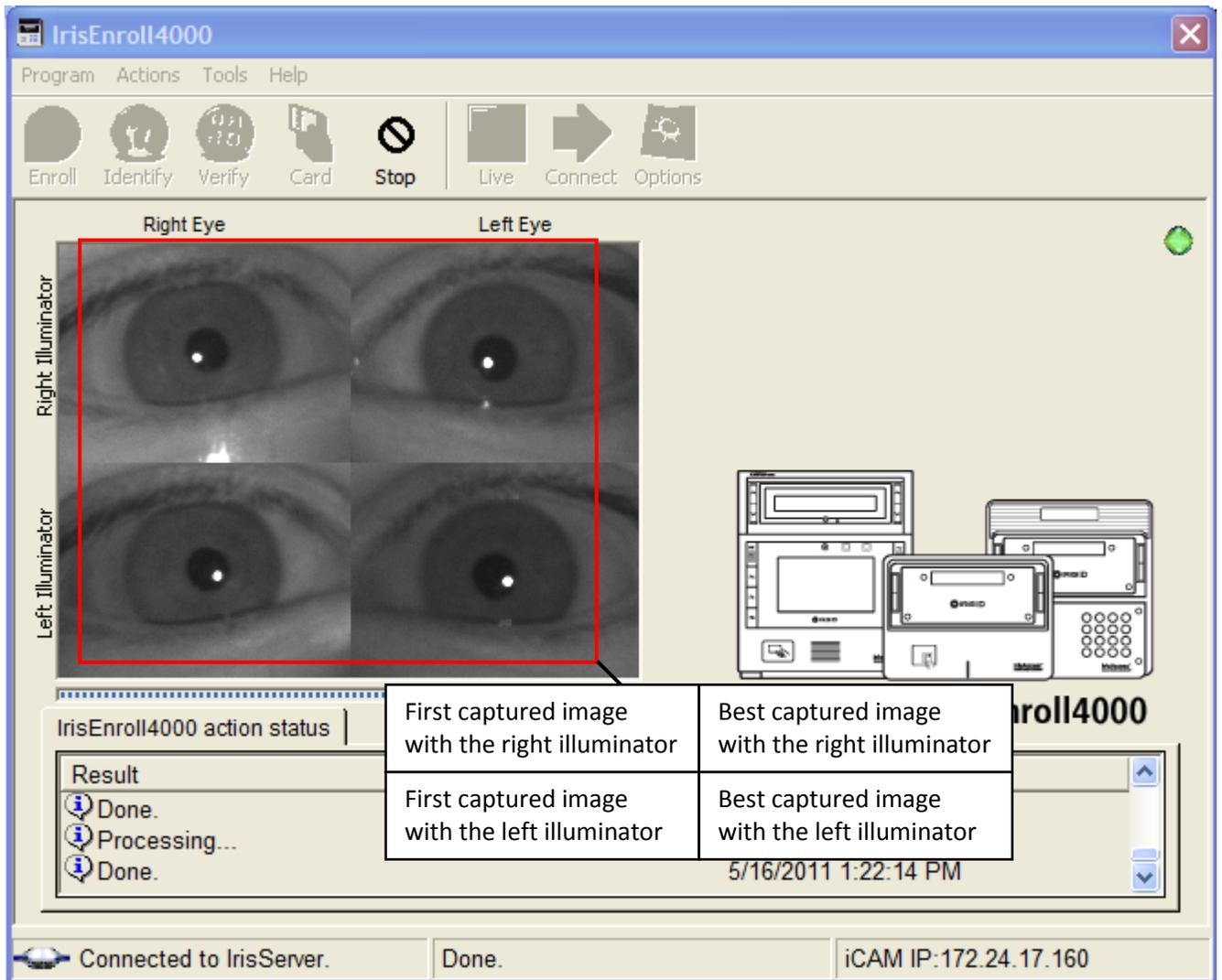
3. With the eye wide open, have the user center their eye in the rectangle on the mirror of the EOU, until the voice message of "We finish taking pictures of your eyes" is heard. Any display, such as 'Please move back' should be followed.
4. If the image is not captured properly for enrollment, the following window opens on the screen.



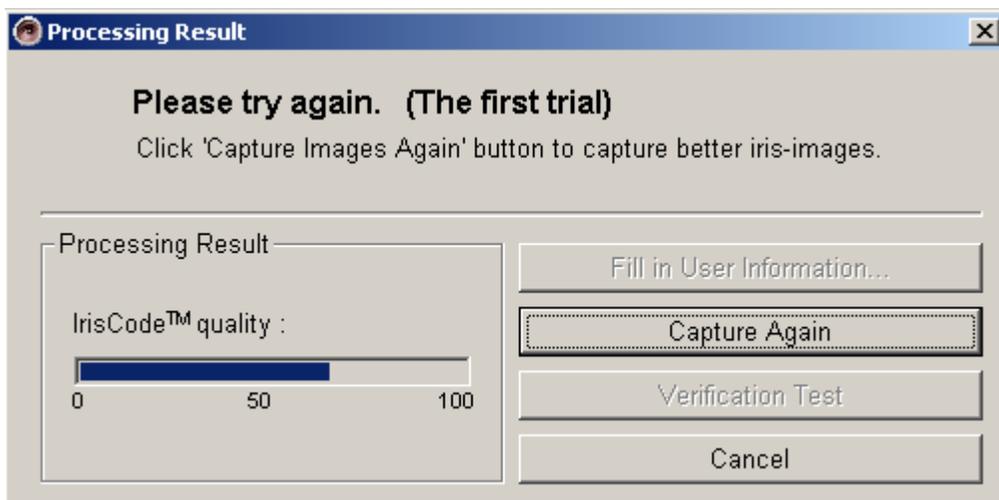
5. If your eye has already been enrolled in Server DB, the following window opens on the screen. In other words, if any iris already exists in the Server database, the iris may not be enrolled again.



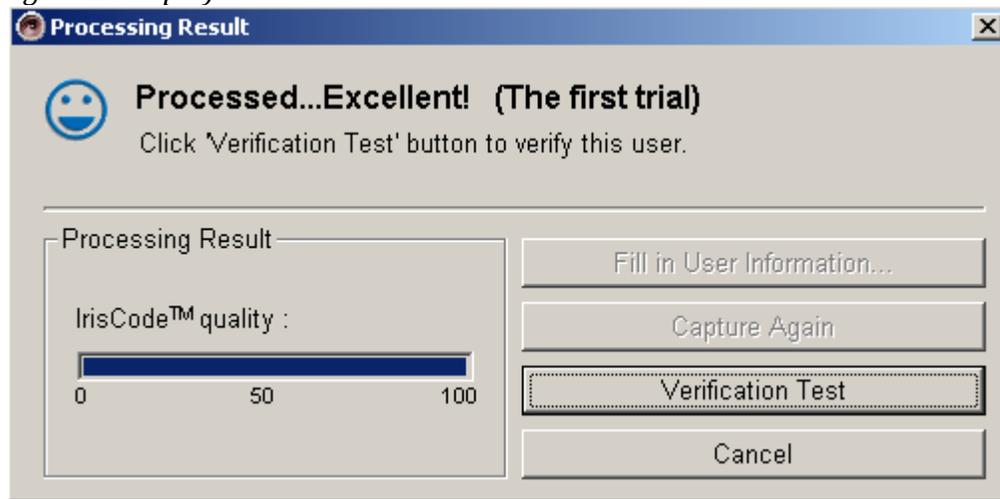
6. After getting the Images, four captured images are displayed on the Main window and the quality of the IrisCode created is displayed in the **Processing Result** window.



The system will ask to try again if the results of image processing are not of sufficient quality.

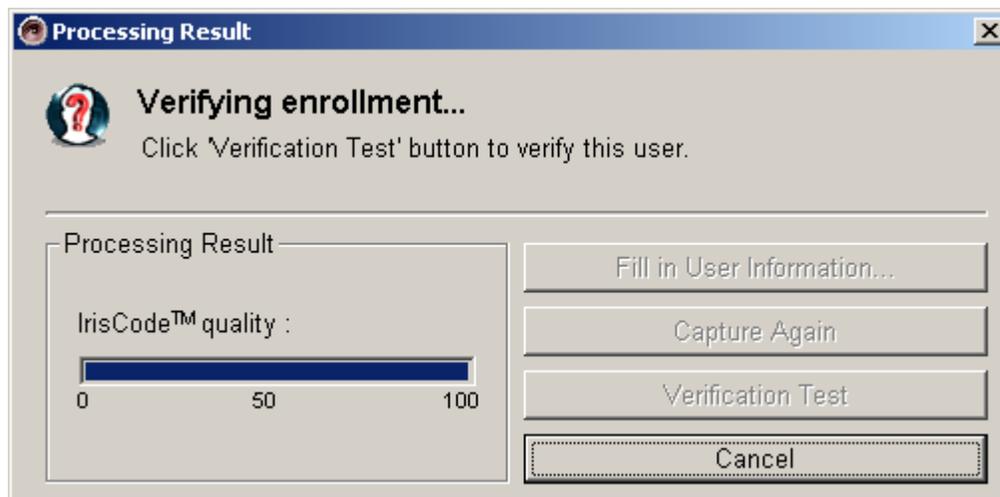


- Click on the **Capture Again** button in the above box and the system will attempt to enroll the person again. The box below will be displayed if the image was properly captured. (**The system will ask to try again if the image was not captured properly on the second try. It can be tried a maximum of three times. If you do not succeed on the third attempt, begin again at step 1)*



- You must perform a verification test by clicking on the **Verification Test** button. IrisEnroll will prompt the user to present his/her iris again to the camera while displaying the window below.

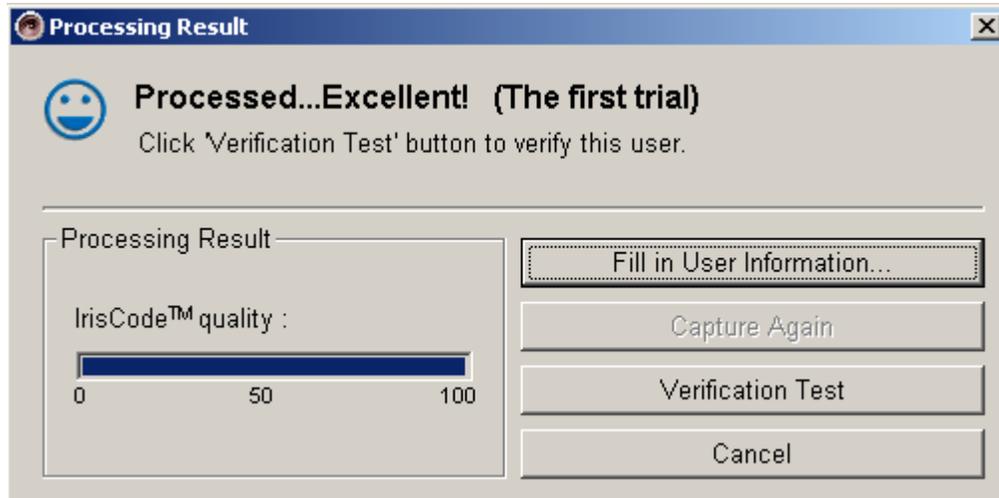
◆ After you click **Verification Test**, look into the center of the mirror of the iCAM.



- Once the verification is complete the window below is displayed.



10. To verify again, you may click the **Test again** button, or click the **OK** button, which will display the window shown below.



11. The User information can be entered on the **User Information** window, which may be opened by clicking on the button labeled **Fill in User Information**.

User Information

Type user ID and then click 'Get user information' button, then the rest of options will be enabled. If the user information already exists in the server DB, the information will be displayed.

* User ID

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

Name

First Name

MI

Last Name

Photo

Delete photo

Card

Use as Prox Card

Wiegand Data Length (No of Bits)

* Card ID

* Card Number

PIN

Show PIN

* Eye

Right Use warning eye

Left Left Right

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

If the user with the entered User ID does not exist in the Server database, the message box titled “User Information is not found. Do you want to register the new user ID?” is shown and the rest of the text boxes will be enabled.

User Information

All fields of user information except for the 'Use warning eye' are not enabled. The operator cannot either enter new information or modify the information, but it is possible for the operator to see the existing information.

* User ID

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

Name

First Name

MI

Last Name

Photo

Delete photo

Card

Use as Prox Card

Wiegand Data Length (No of Bits)

* Card ID

* Card Number

PIN

Show PIN

* Eye

Right Use warning eye

Left Left Right

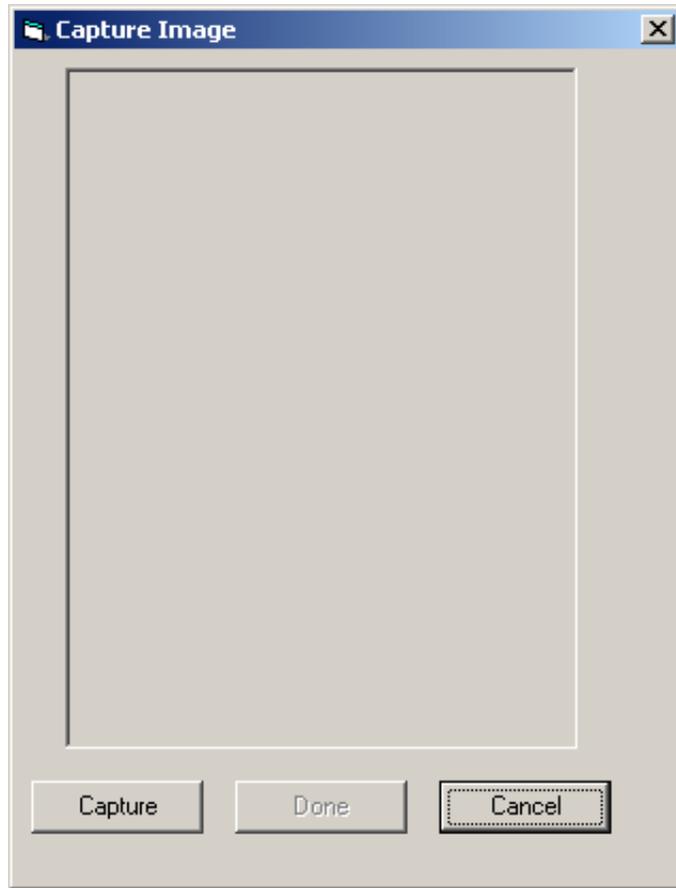
Click the 'Next' button to continue.

When a user that does not already exist in the Server database is enrolled (Refer item 11.A), the window above is shown.

13. Enter the following information in their respective text boxes.

- a. Enter the **First Name, MI and Last Name of the user.** (Optional)

- b. If the system is used with a card reader and/or access panel, select the card type in the card drop-down. When a card type is selected, the **Card ID** and **Card Number text boxes** will be activated. To complete the registration of card information, **Card ID** and **Card Number** must be filled. If not, the warning window will be displayed.
- ◆ **Card ID: Card ID is the effective data that is used in verification mode or for Card ID, Wiegand or RS422 output. When the wiegand/RS422 output ports are activated, Card ID is outputted in the configured format after the user is identified.**
- ◆ **Card Number: Card Number is assigned by the Card Manufacturer. It is commonly printed on the card.**
- If both the eyes are enrolled, one eye may be assigned as a **warning eye**. If a user is forced to access the door by an unauthorized intruder the user may use the warning eye. The remote unit opens the door as an authorized user, but notifies IrisServer (or IrisMonitor) of the emergency.
- c. Select the **Gender** (Female/Male) from the radio buttons. (Optional)
- d. Enter PIN no.
- e. **Select Photo** (Optional). If you want to delete the registered photo of user, select the **Delete Photo** in the check box. Or you can choose Capture Image, following window will be displayed:



Press Capture button to start Live Image and this will also enable done button.
Press done button to capture image and the image will be displayed in the User
Information Window, like:

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

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

Name

First Name

MI

Last Name

Photo



Delete photo

Card

* Card ID Use as Prox Card

* Card Number

PIN

Show PIN

* Eye

Left Right

Use warning eye

Left Right

Gender

Female

Male

Click the 'Next' button to continue.

(If using Wiegand or RS422, the user ID should be a positive integer and the configuration of the ICU should be completed properly. Please refer to section 2.4.2 and 2.4.3 in the document **IrisAccess™ 4000 Software Installation Manual** (Document No. DV002S501)).

User Information

Enter the Department, Position, Home Phone number, Mobile Phone number, Office Phone number, E-mail, Address, Resident Number and descriptions (Memo1-5) of the user.

* User ID:

 Detail information of the user

Department	<input type="text" value="Division"/>	Position	<input type="text" value="Engineer"/>
Phone(Home)	<input type="text" value="02-526-1234"/>	Phone(Mobile)	<input type="text" value="019-526-1234"/>
Phone(office)	<input type="text" value="02-526-1234"/>	E-mail	<input type="text" value="Brandy@lgris.com"/>
Address	<input type="text" value="Seoul, Korea"/>		
Resident Num	<input type="text" value="800225-1234567"/>		
Memo 1	<input type="text" value="Memo1"/>		
Memo 2	<input type="text" value="Memo2"/>		
Memo 3	<input type="text" value="Memo3"/>		
Memo 4	<input type="text" value="Memo4"/>		
Memo 5	<input type="text" value="Memo5"/>		

14. Enter the **Department, Position, Home Phone number, Office Phone number, Mobile Phone number, E-mail, Address, Resident Number** and **descriptions (Memo1-5)** of the user. (All Optional)
15. Click on the **Next >** button to set the User's Access Rights.

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:

Access Rights

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

Time Group:

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

< Back Next > Cancel

16. In this window select the check box labeled **Visitor** if the **User** is a **Visitor** with temporary access rights.

17. If the user type is **General User**: (The **Visitor** check box is NOT selected)
- Select the **Remote group** of this user.
 - Click on the **Add** button under the **Remote Group**.

- c. Select the **Time Group** of the user.
- d. Click on the **Add** Button under the **Time group**.
- e. The Selected Remote Group and Time Groups may be viewed in the **Remote Group and Time Group** List in the **Access Rights** section.
- f. **Users** may be removed from **Remote** and **Time Groups** by selecting the **Groups** in the **Access Rights** section and clicking on the **Delete** button.
- g. You may set the **Start Date** and **Expiration Date** for the user. If you do not select a **Start Date** and **Expiration Date** for the user, their **Access Rights** are always valid.

To set the Start Date:

- Press the **Calendar** button next to **Start Date**.
- On the Calendar screen that opens, select the first date that the User's **Access Rights** will take effect.
- Press the **Ok** button to enter the **Start Date**, or Press the **Cancel** button to cancel the date selection.
- Repeat the process for the **Expire Date**

If a **Remote Group** or **Time Group** is selected, the **Detail** button may be pressed to display the **Remote Unit(s)** in the **Remote Group** or the valid times under the **Time Group**.

Remote Name	IP address	Channel ID	Use Type	Description
R137-1	150.140.62.131	1	Identification	
R137-2	150.140.62.132	2	Access In	
R137-3	150.140.62.133	3	Identification	
R137-4	150.140.62.134	4	Access In	

Sunday	Monday	Tues...	Wedn...	Thurs...	Friday	Satur...	Holiday
00:00:00	00:00:00	00:00:00	00:00:00	00:00:00	00:00:00	00:00:00	00:00:00

Multiple **Remote** and **Time Groups** may be assigned to a single user by repeating steps a - g. A maximum of 10 access rights may be assigned to a single user.

18. If the **User** is a **Visitor**:

- a. Check the check box labeled **Visitor** and enter the visitor information
- b. Select the **Remote group** of the visitor,
- c. Click on the **Add** button under **Remote Group**, to add the **Visitor** to the **Remote Group**.
- d. The selected **Remote Group** will be listed in the **Remote Group** list under **Access Rights**.
- e. You may set the **Start Date** and **Expiration Date** for the user. If you do not select a **Start Date** and **Expiration Date** for the user, their **Access Rights** are always valid. To set the **Start Date**:
 1. Press the **Calendar** button next to **Start Date**.

2. On the Calendar screen that opens, select the first date that the User's **Access Rights** will take effect.
 3. Press the **Ok** button to enter the **Start Date**, or Press the **Cancel** button to cancel the date selection.
- f. Repeat the process for the **Expire Date**.
 - g. The valid access times (start time and the end time) during the selected valid days for the visitor can be selected by choosing the starting and ending hours and minutes in **Reservation time for Visitor**. Only one Reservation time can be set.

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:

Access Rights

Remote Group			Delete
All			

A term of validity (mm/dd/yyyy)

Start Date:

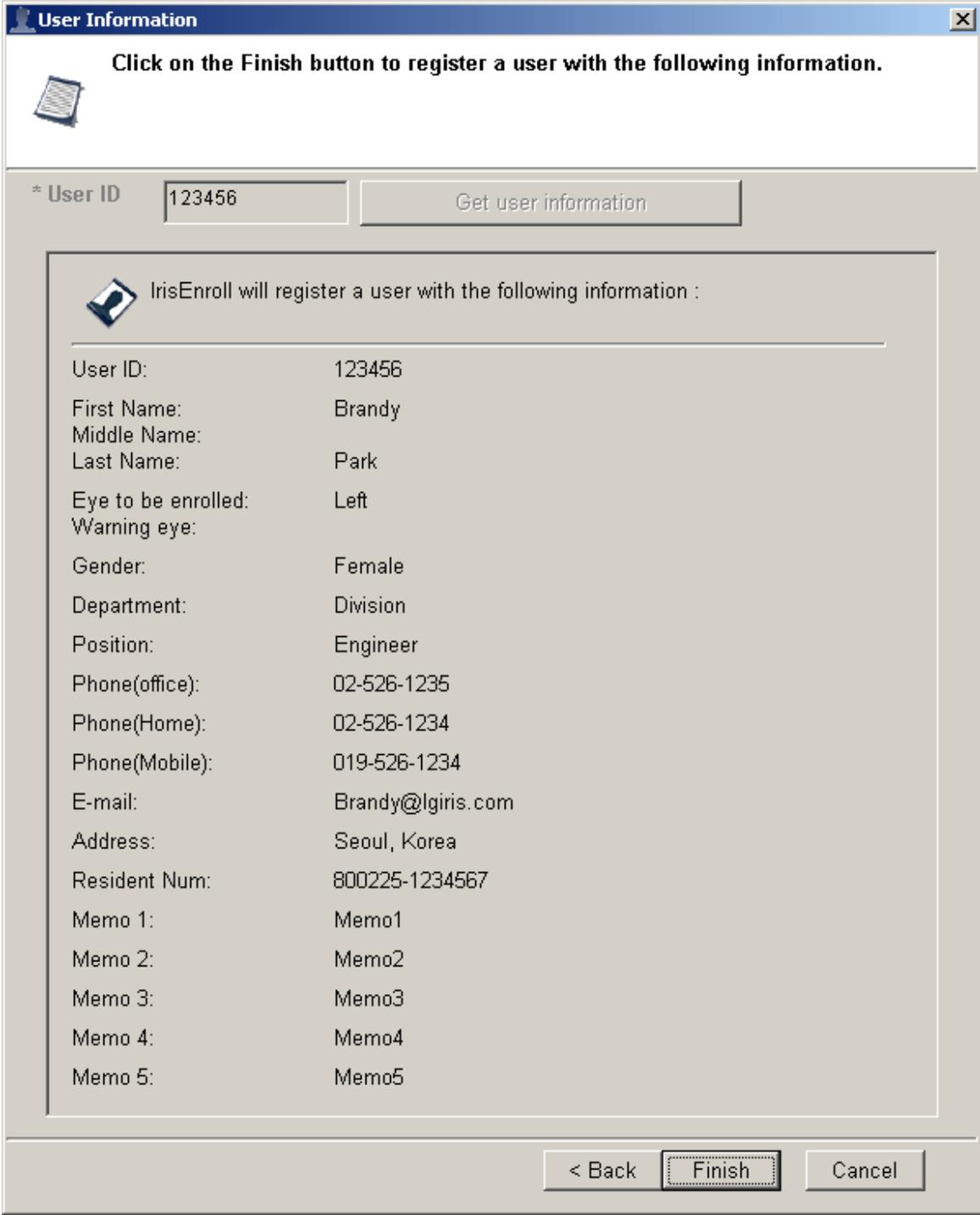
Expire Date:

Reservation time for visitor

: ~ :

Remote Name	IP address	Channel ID	Use Type
101-I	172.19.6.40	1	Access In
102-O	172.19.6.40	2	Access Out
103-I	172.19.6.41	1	Access In

19. Click the **Next** button.



The dialog box titled "User Information" contains a message: "Click on the Finish button to register a user with the following information." Below this is a text input field for "User ID" containing "123456" and a "Get user information" button. A summary box follows, titled "IrisEnroll will register a user with the following information :", listing various user attributes.

* User ID	123456	Get user information
-----------	--------	----------------------

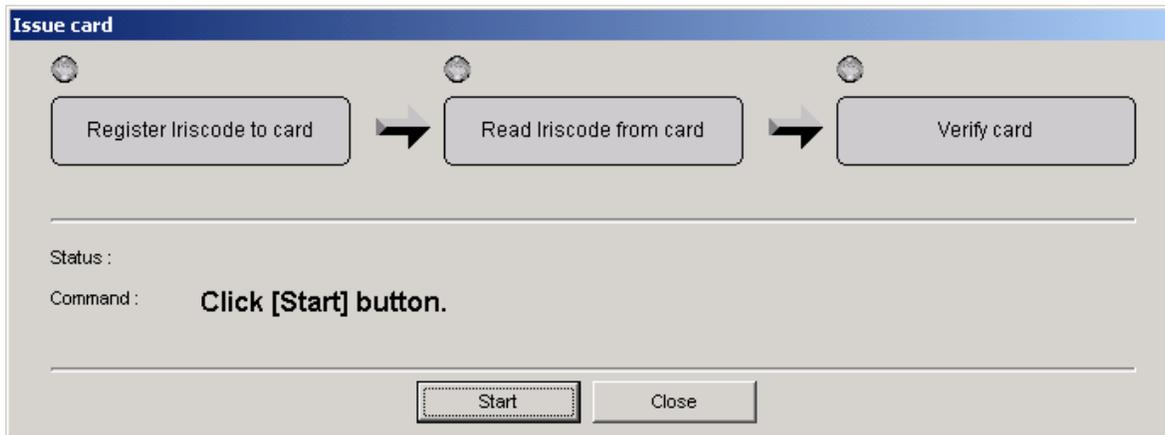
IrisEnroll will register a user with the following information :	
User ID:	123456
First Name:	Brandy
Middle Name:	
Last Name:	Park
Eye to be enrolled:	Left
Warning eye:	
Gender:	Female
Department:	Division
Position:	Engineer
Phone(office):	02-526-1235
Phone(Home):	02-526-1234
Phone(Mobile):	019-526-1234
E-mail:	Brandy@lgiris.com
Address:	Seoul, Korea
Resident Num:	800225-1234567
Memo 1:	Memo1
Memo 2:	Memo2
Memo 3:	Memo3
Memo 4:	Memo4
Memo 5:	Memo5

< Back Finish Cancel

20. This window shows a summary of the information of the enrolled user. Click on the **Finish** button.

21. If the user is selected to use a Smart Card, the next window opens. The card must be issued. The card may be issued by carrying out following steps:
- Encryption keys must have already been generated and registered in **IrisServer**.
 - **Use Smart Card** check box in the **Options** window of **IrisEnroll** must be checked.
 - Card combo box in the User Information window must have been set to Smart Card

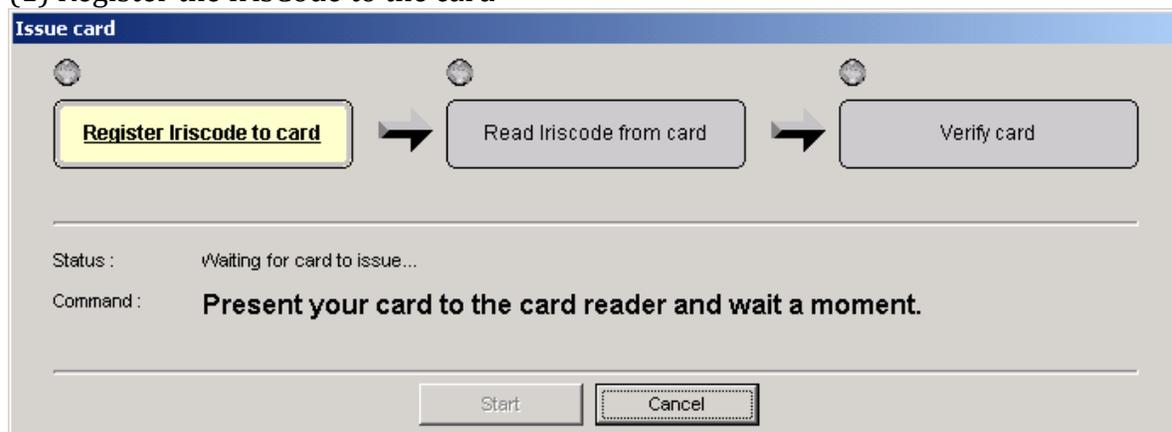
If user is enrolled with Left or Right eye then only respective Left or Right eye data will be written to Smart Card. If user is enrolled with both eyes then user can choose either Left, Right or Both eyes to be written on Smart Card from “Options>Which Eye>Issue Smart Card”.



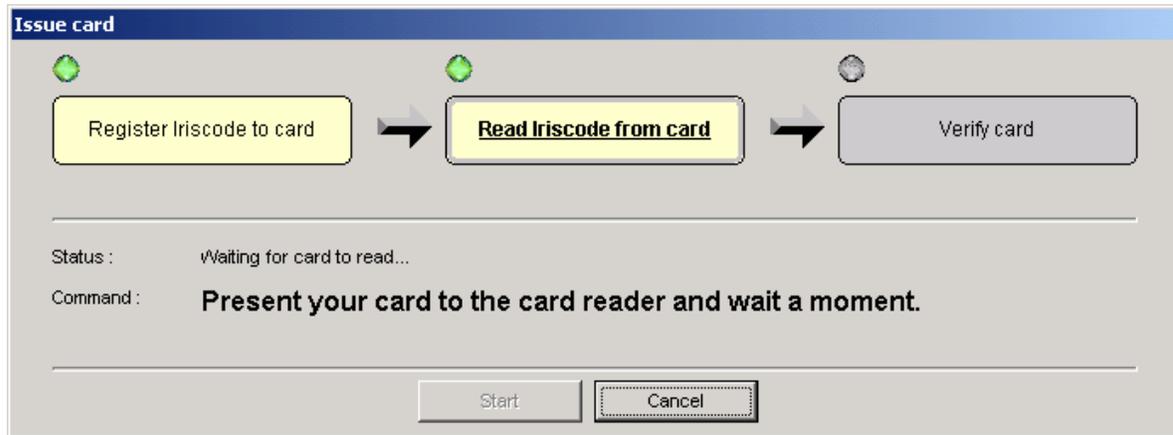
- a. If the operator clicks the “Start” button in the “Issue card” window, the 3 step Smart Card process begins:

***Note:** Before beginning the Smart Card issuing process, the Smart Card must already be within range of the Smart Card Reader / Writer. If not, an error will occur. If this happens, press the **Ok** button on the error window, place the Smart Card within range of the Smart Card Reader/Writer and press the **Start** button again.

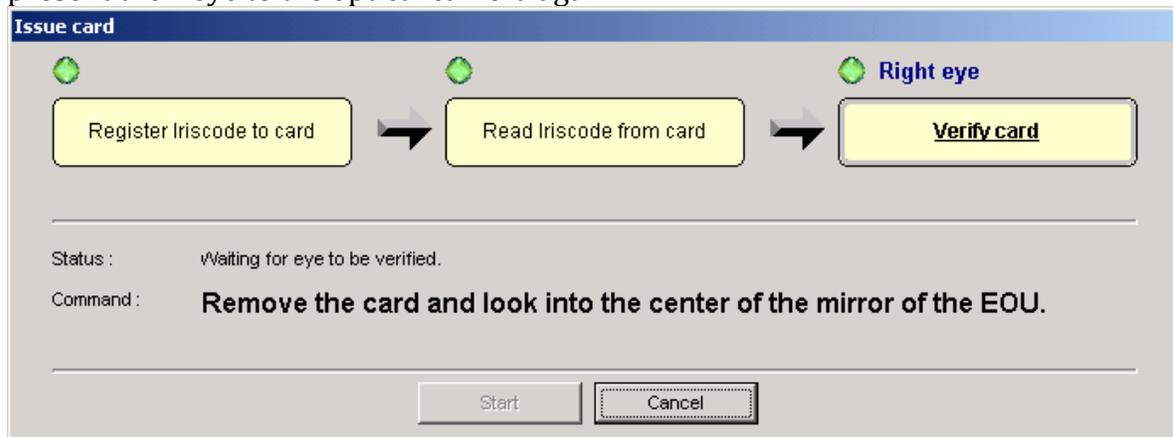
(1) Register the IrisCode to the card



(2) Read the IrisCode from card (for verification)



(3) Verify card by comparing the read IrisCode to a live Iris. The User will be asked to present their eye to the optical camera again.



If the process completes successfully, the following window is displayed.



5.1.4 Identify

The **Identify** feature is used to identify a user by comparing the IrisCode™ of the user to all existing IrisCodes™ in the system. (1: N matching)

Identification will happen with the eye selected in "Options>Which Eye>Identification/Verification"

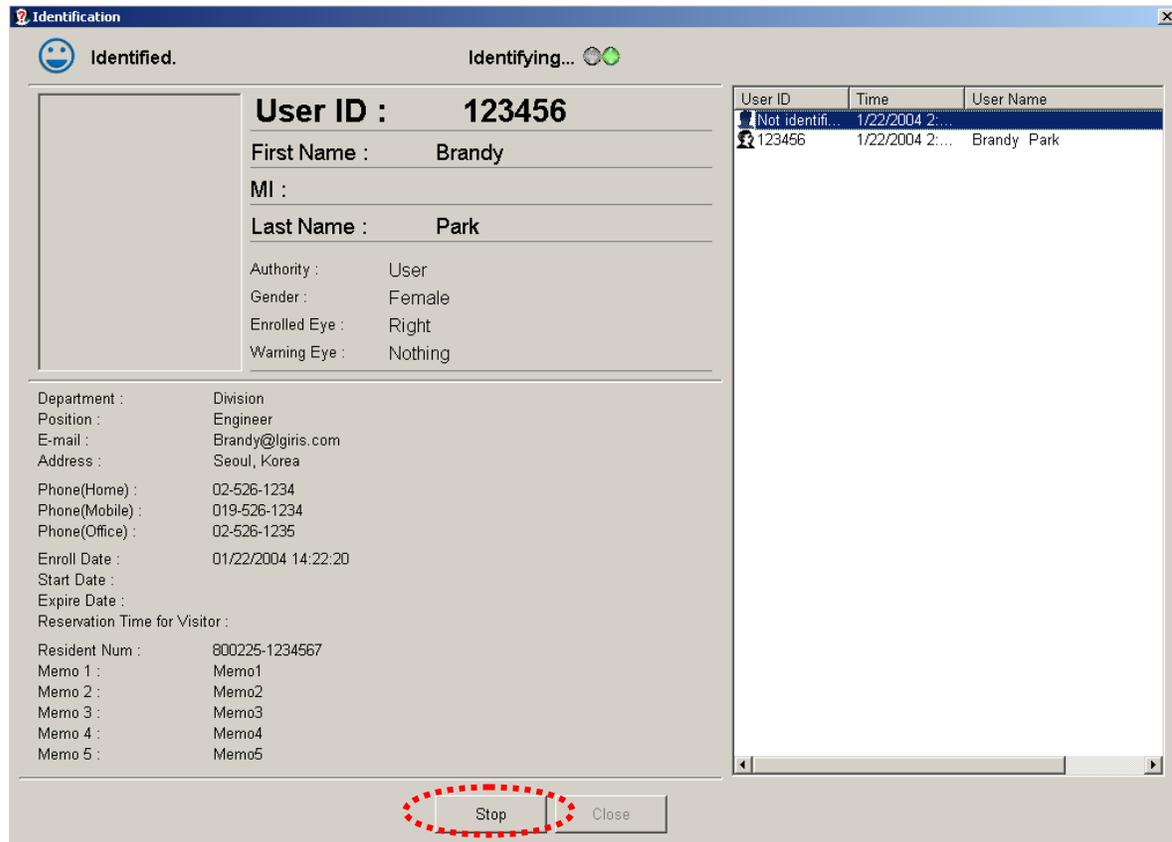
The Continuous Identification process can be done using the following steps.

1. Select the **Identify** Item from the **Actions menu** in the menu bar or select the **Identify** icon from the tool bar. The following identification window will be displayed.

User ID	Time	User Name
---------	------	-----------

2. Have the User look into the center of the mirror of the iCAM.

The IrisCode™ of the user will be generated from Iris images and compared with the existing IrisCode™ in the database. If the IrisCode™ matches with any of the enrolled IrisCodes™, then the user is identified as a valid user. The window after the identification of the sample user is shown below:



If the user's IrisCode™ does not match with an enrolled IrisCode™, then a **'Not Identified'** message will be displayed and all information items in the screen will be cleared.

- Identification mode runs continuously until the operator clicks the **Stop** button or the **Close** button.

Until the **Stop** button is clicked, the continuous identification process is active.

If you click on the **Close** button, the identification window will be closed.

- ◆ **Note: Information about the identified user to be displayed in the identification window can be selected by checking the check boxes in the option window. (Refer to section 2.3.7.5 Display)**

5.1.5 Verify

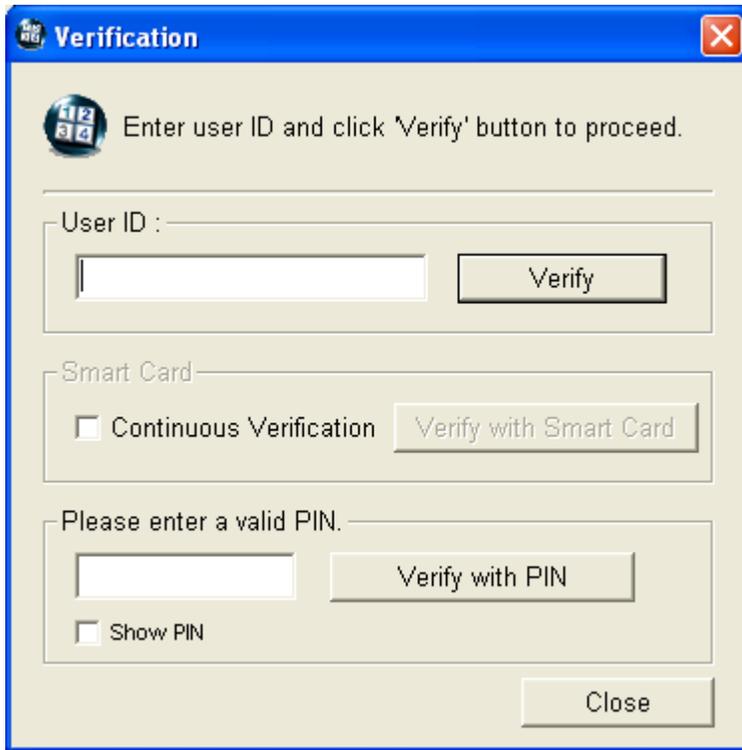
Verification is the process of verifying the user, by checking the IrisCode™ of the User with either:

- IrisCode™ of the User from the provided User ID in the database or
- IrisCode™ of the User from the provided IrisCode in the Smartcard or
- IrisCode™ of the User from the provided PIN in the database.

Verification will happen with the eye selected in “Options>Which Eye>Identification/Verification”

Select the **Verify** Item from the **Actions menu** in the menu bar or select **Verify** from the tool bar, to open the **Verification** window. **Verify with smartcard** button is enabled only when “Use smartcard” option is checked in the Smartcard window under **Options** menu. (Refer to the Smartcard Section in this manual).

To verify the User by User ID



Verification

Enter user ID and click 'Verify' button to proceed.

User ID :

Smart Card

Continuous Verification

Please enter a valid PIN.

Show PIN

1. Enter the User ID of the User in the **User ID** field in the **Verification** window
2. Clicking the **Verify** button begins the Iris Image capture process.
3. After you click the **Verify** button, look into the center of the mirror of the iCAM.
4. After the Iris image is captured, the result of the verification will be shown in the **Verification** window. A sample of the **Verification** window after a successful verification is shown below.



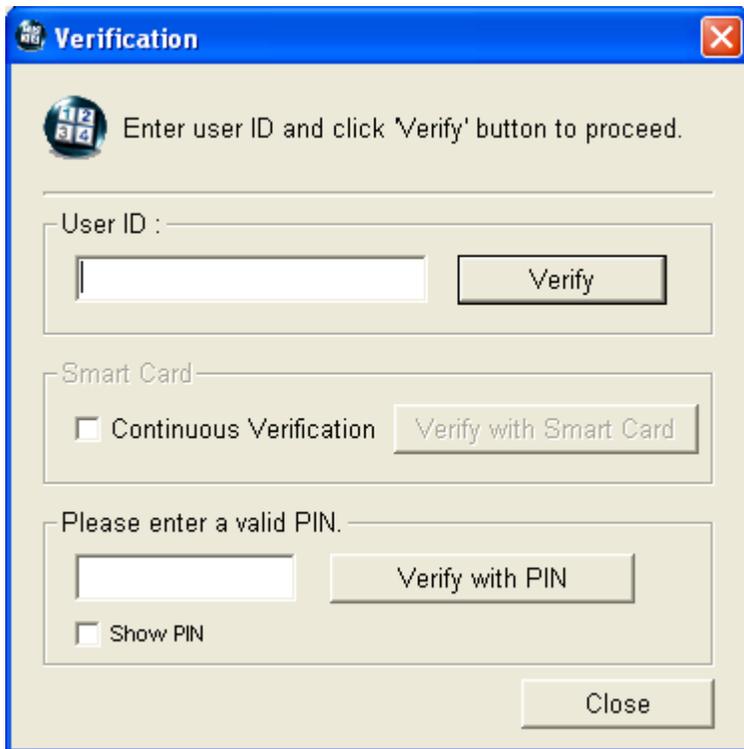
The image shows a 'Verification' window with a blue title bar and a close button. The window contains a 'Verified.' status with a smiley face icon. Below this, user information is displayed in a table-like format. The 'User ID' is 123456. The 'First Name' is Brandy, 'MI' is blank, and 'Last Name' is Park. Other fields include Authority (User), Gender (Female), Enrolled Eye (Right), and Warning Eye (Nothing). A second section lists contact and administrative information: Department (Division), Position (Engineer), E-mail (Brandy@lgiris.com), Address (Seoul, Korea), Phone numbers (Home: 02-526-1234, Mobile: 019-526-1234, Office: 02-526-1235), Enroll Date (01/22/2004 14:22:20), Start Date, Expire Date, Reservation Time for Visitor, Resident Num (800225-1234567), and five Memo fields (Memo1 to Memo5). At the bottom, there are 'Try again' and 'Close' buttons.

Verified.	
User ID :	123456
First Name :	Brandy
MI :	
Last Name :	Park
Authority :	User
Gender :	Female
Enrolled Eye :	Right
Warning Eye :	Nothing
Department :	Division
Position :	Engineer
E-mail :	Brandy@lgiris.com
Address :	Seoul, Korea
Phone(Home) :	02-526-1234
Phone(Mobile) :	019-526-1234
Phone(Office) :	02-526-1235
Enroll Date :	01/22/2004 14:22:20
Start Date :	
Expire Date :	
Reservation Time for Visitor :	
Resident Num :	800225-1234567
Memo 1 :	Memo1
Memo 2 :	Memo2
Memo 3 :	Memo3
Memo 4 :	Memo4
Memo 5 :	Memo5

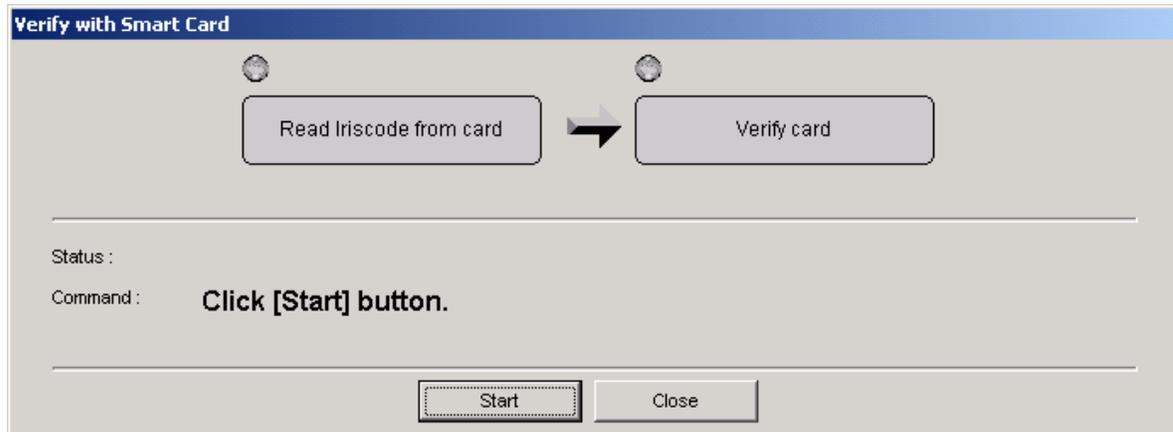
Try again Close

5. If not verified, click on the **Try again** button.
6. If you click the **Close** button, the verification window will be closed.

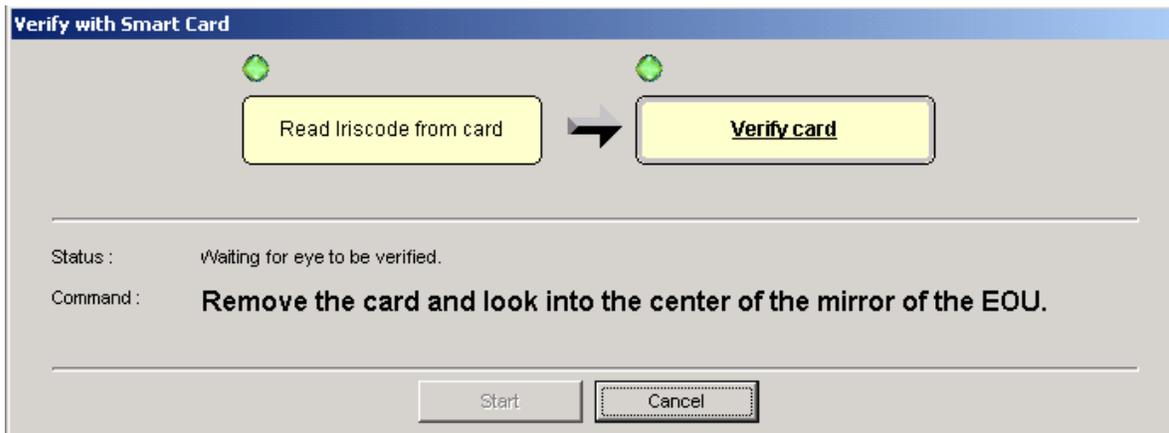
To verify a User with Smart Card



1. Click the **Verify with Smart Card button** in the **Verification** window and the **Verify with Smart Card** window will be displayed.



2. Click the **Start** button and the **Verify with Smart Card** window will begin reading the Smart Card. The Smart Card should be within range of the Smart Card Reader before pressing the **Start** button.



3. Present the Smart Card and wait until the EOU prompts the user to look into the mirror.
4. After the Iris image is captured, the result of the verification will be shown in the **Verification** window. A sample of the **Verification** window after a successful verification is shown below.



To verify a User with PIN

1. Press "Verify with PIN" field in the **Verification** window
2. User has to enter PIN from iCAM and press enter key (↵) on the keypad. Then iCAM will be in capture mode.
3. Look into the center of the mirror of the iCAM.
4. After the Iris image is captured, the result of the verification will be shown in the **Verification** window. A sample of the **Verification** window after a successful verification is shown below.



The image shows a software window titled "Verification" with a blue header bar. Inside the window, there is a smiley face icon and the text "Verified." Below this, a large empty rectangular box is on the left. To the right of this box, user information is displayed in a list format, with labels in bold. The information includes: User ID (123456), First Name (Brandy), MI (blank), Last Name (Park), Authority (User), Gender (Female), Enrolled Eye (Right), and Warning Eye (Nothing). Below this section, a list of personal and contact details is shown, including Department, Position, E-mail, Address, Phone numbers, and dates. At the bottom of the window, there are two buttons: "Try again" and "Close".

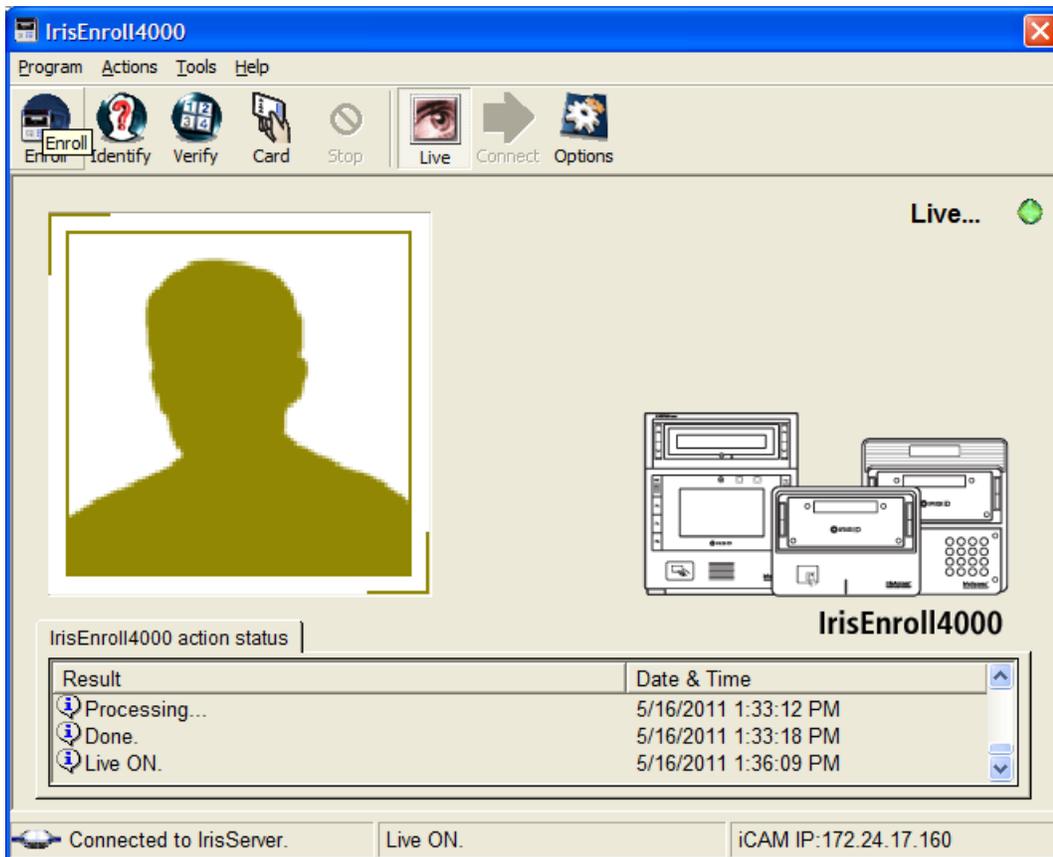
Verified.	
	User ID : 123456
	First Name : Brandy
	MI :
	Last Name : Park
	Authority : User
	Gender : Female
	Enrolled Eye : Right
	Warning Eye : Nothing
Department :	Division
Position :	Engineer
E-mail :	Brandy@lgiris.com
Address :	Seoul, Korea
Phone(Home) :	02-526-1234
Phone(Mobile) :	019-526-1234
Phone(Office) :	02-526-1235
Enroll Date :	01/22/2004 14:22:20
Start Date :	
Expire Date :	
Reservation Time for Visitor :	
Resident Num :	800225-1234567
Memo 1 :	Memo1
Memo 2 :	Memo2
Memo 3 :	Memo3
Memo 4 :	Memo4
Memo 5 :	Memo5

Try again Close

5. If not verified, click on the **Try again** button.
6. If you click the **Close** button, the verification window will be closed.

5.1.6 Live View

This functionality is used only to view the live video from iCAM.



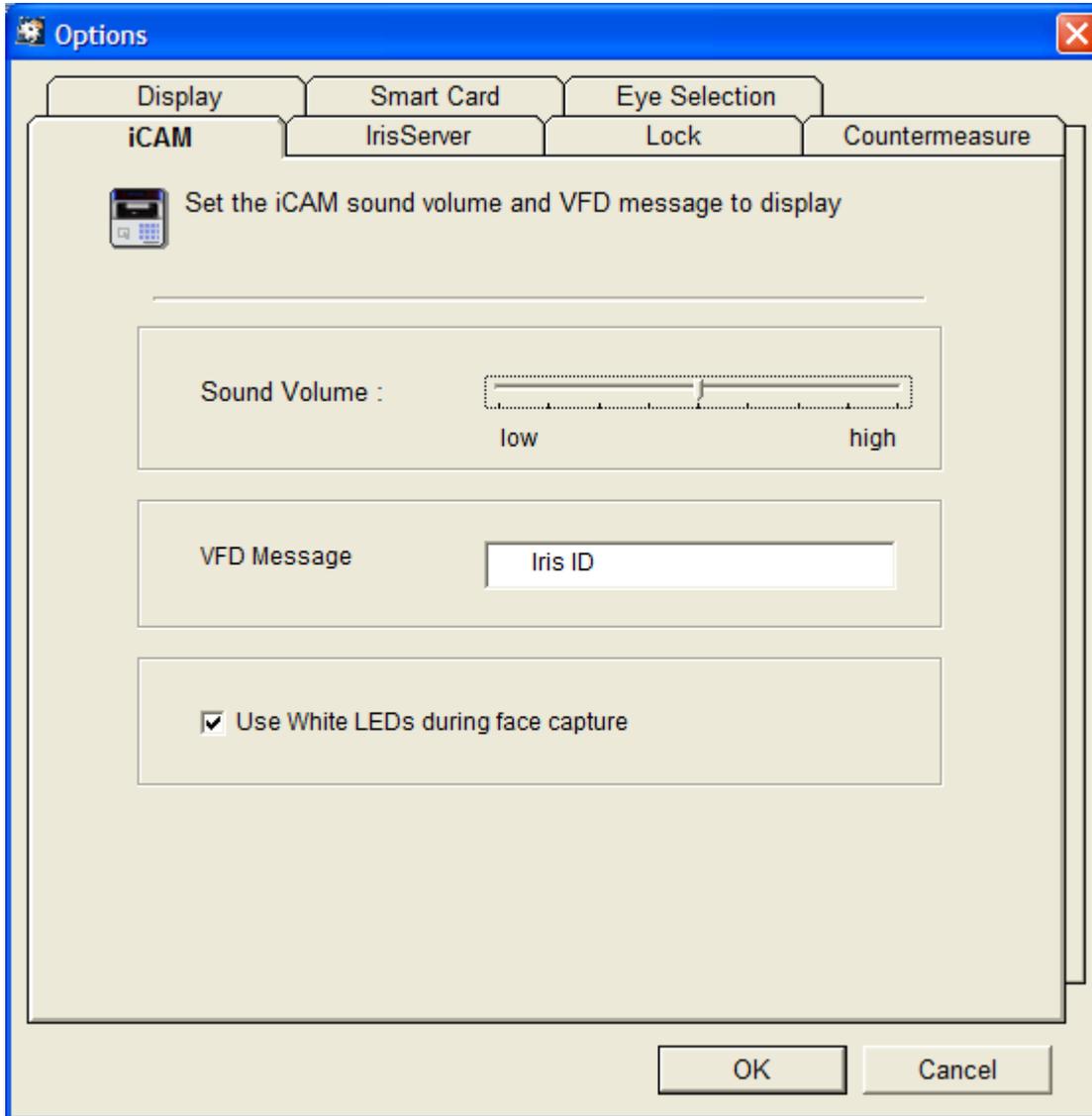
5.1.7 Option Settings

The **Options** Item is used to set various options such as:

1. To set the sound volume and VFD Message of ICAM.
2. To change the IrisServer's IP address.
3. To configure the program lock feature.
4. To enable/disable the fake eye detection.
5. To configure the items displayed in the continuous identification window.
6. To set which eye should be enrolled: left, right or both. When both eye's are enrolled, SmartCard which eye can also be configured left, right or both.
7. To set which eye for Identification and verification left, right, both or either.

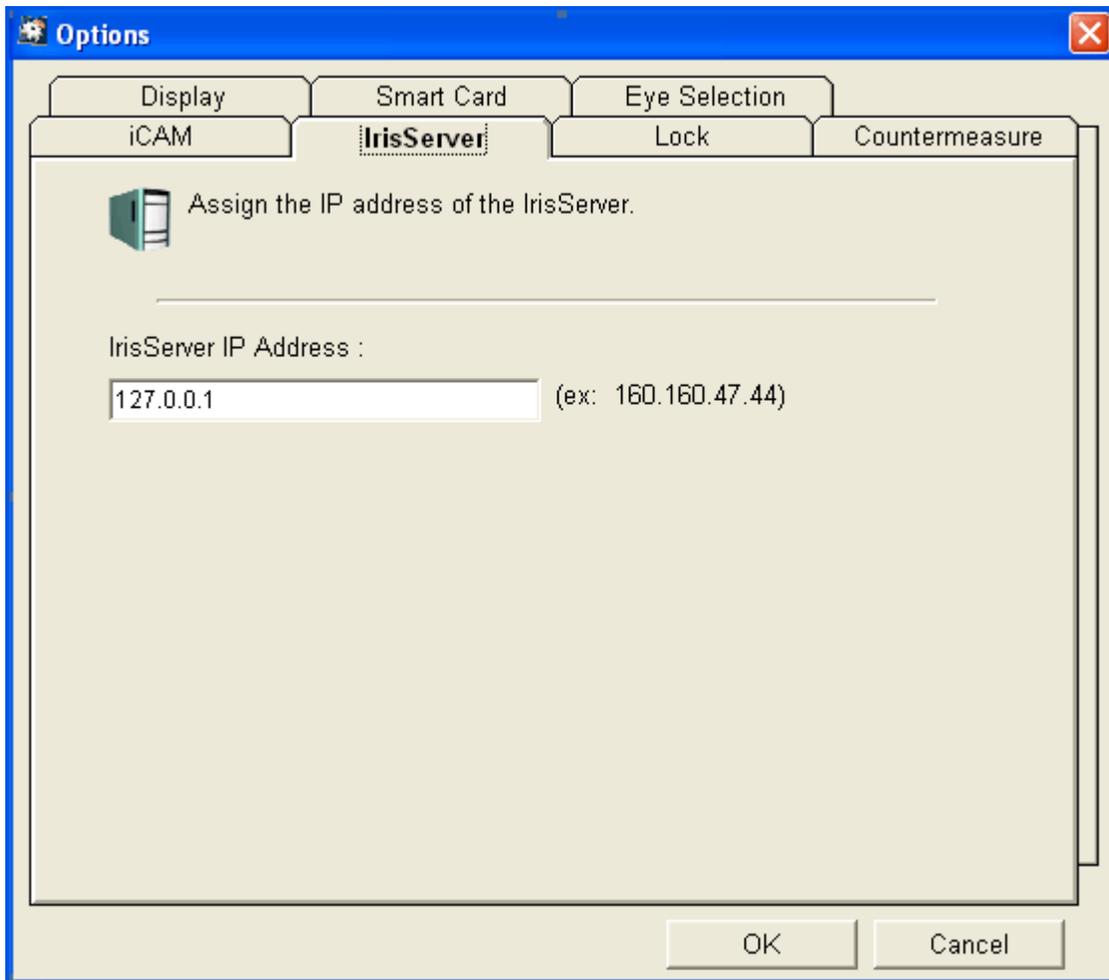
5.1.7.1 iCAM Setting

By selecting the iCAM tab on the Option dialog box you can set the Sound Volume of ICAM and VFD Message. By default VFD Message is Iris ID.



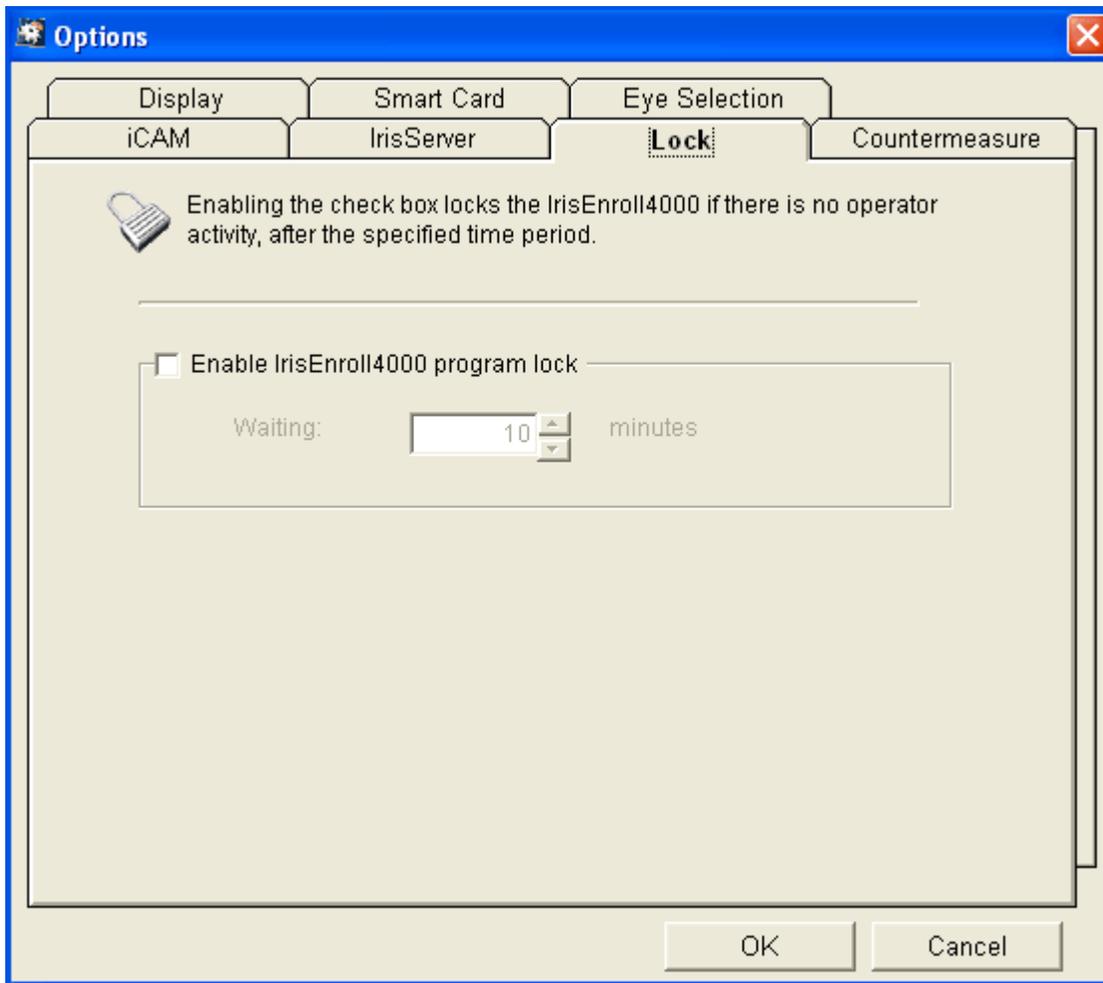
5.1.7.2 IrisServer IP Address

The IrisServer IP Address may be set by selecting the **IrisServer** tab field in the **Options** window and entering the IP Address of the IrisServer. If IrisEnroll is located on the same computer as IrisServer, we recommend setting the IP Address to the loop back address (127.0.0.1).



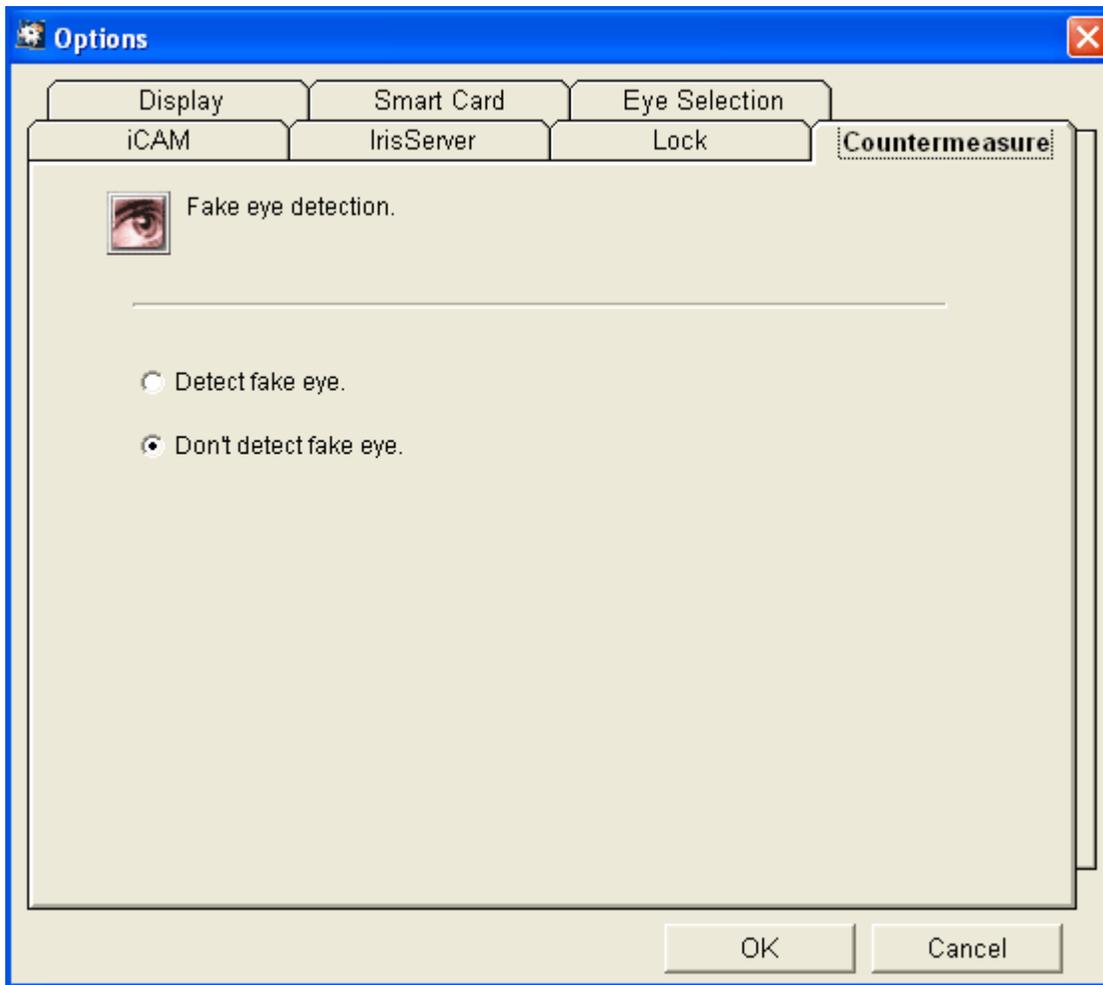
5.1.7.3 Program Lock

The **Program Lock** functionality is used to Lock the application if there is no action within the specified time. Once the program is locked, the Operator must re-login to use the application. The **Lock** may be enabled by selecting the **Lock** tab field. Check the check box labeled **Enable IrisEnroll Program lock** to enable the **lock**. To disable the program lock feature, uncheck the check box labeled **Enable IrisEnroll Program lock**.



5.1.7.4 Fake Eye Detection

Fake eye detection can be configured by selecting the fake eye tab of the option window, which will display the following window.



If you want the fake eye detection to be enabled, select the **Detect fake eye** radio button and click the **OK** button. Fake Eyes will be detected when a user tries to enroll, identify or verify.

Fake Eye detection does increase the time required for enrollment, identification or verification, but greatly enhances the security of the system.

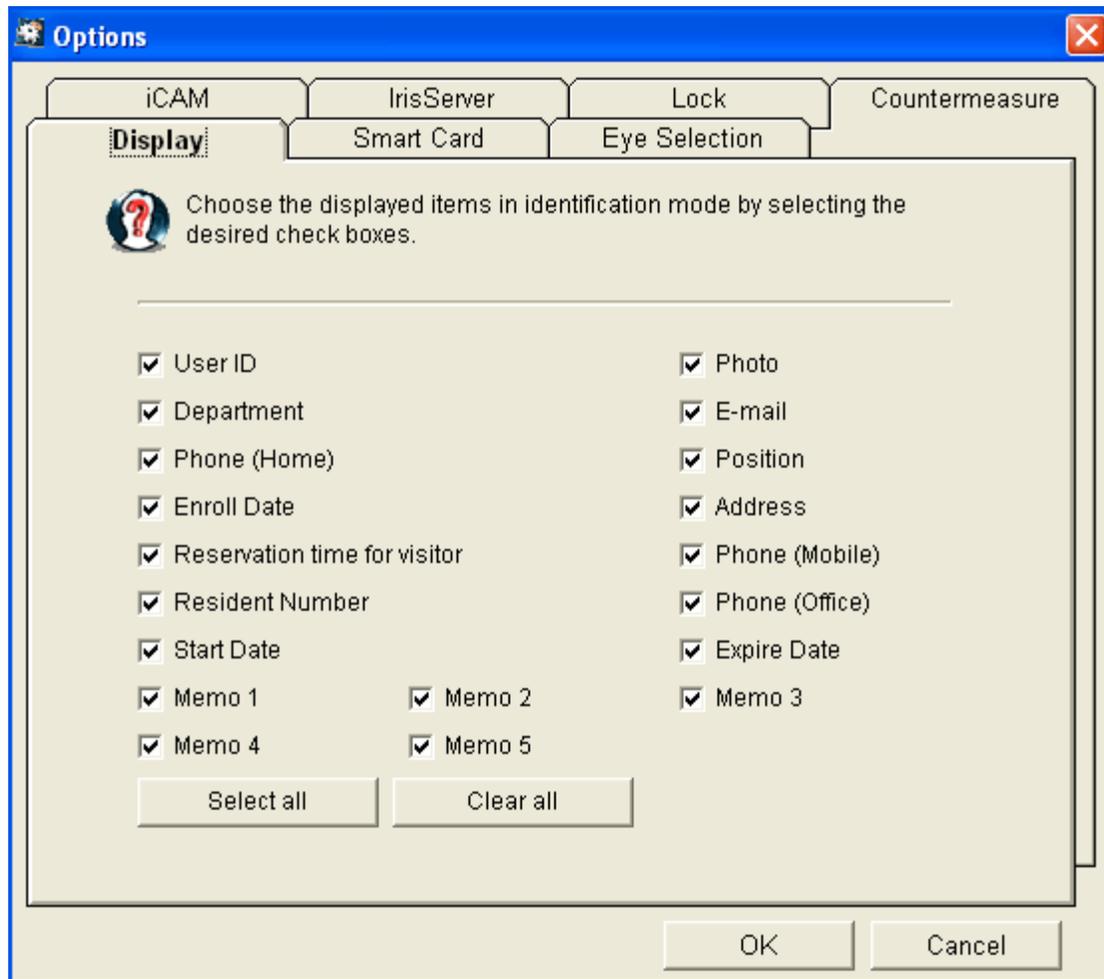
If you don't want the fake eye detection to be enabled, then select the **Don't detect fake eye** option and click the **OK** button. If so, fake eye will NOT be detected when a user tries to enroll, identify or verify.

- ◆ **Caution:** Limitation of ambient light in working environment
 - When Fake Eye Detection is not used: 1,000 lx Fluorescent light and 100 lx Incandescent or sunlight.
 - When Fake Eye Detection is used: 500 lx Fluorescent light and 50 lx Incandescent or sunlight.
 - If the ambient light exceeds the limitation, the False Reject Rate will be increased.

5.1.7.5 Display

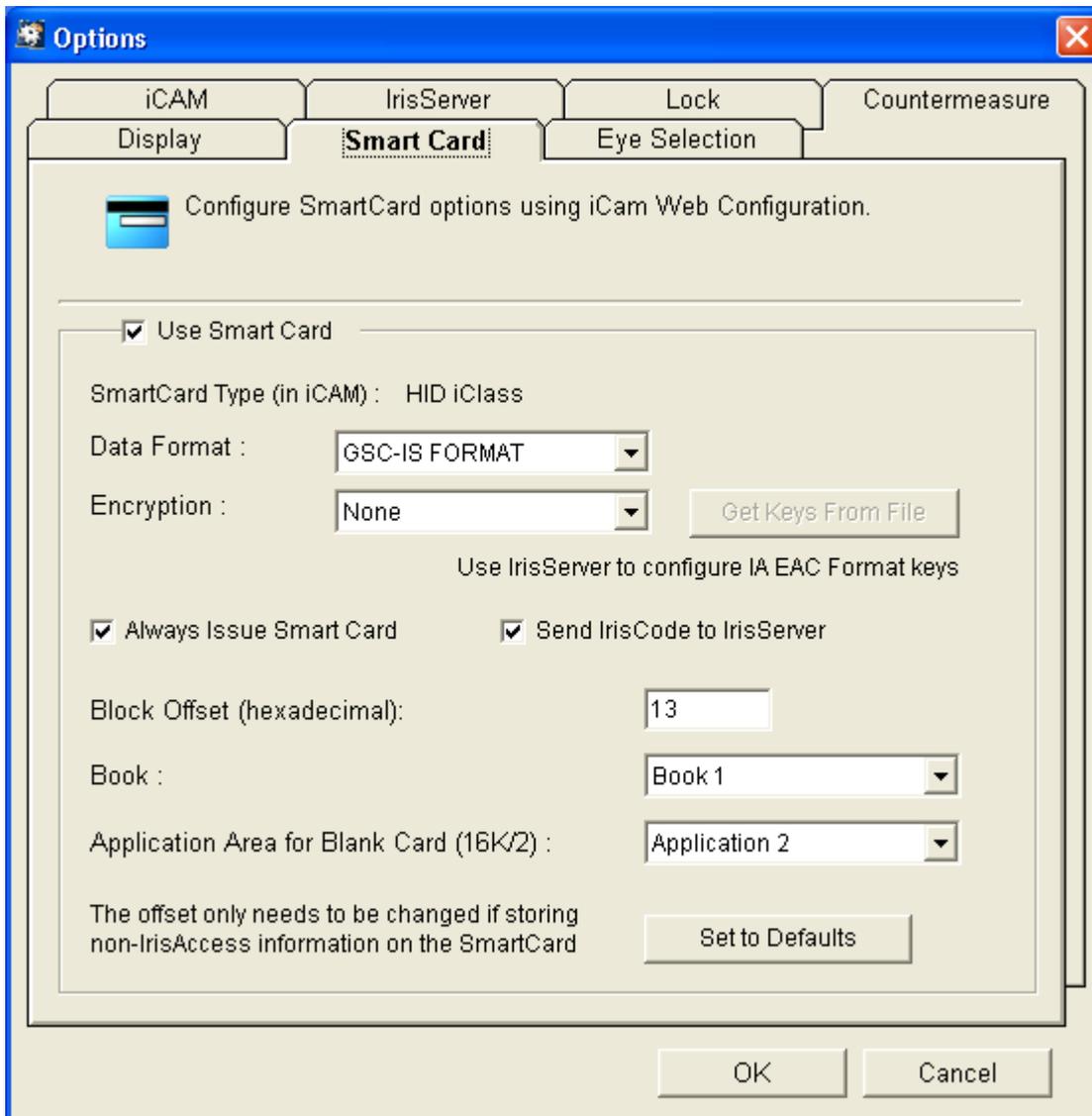
Items to be displayed during the continuous identification mode may be selected by checking check boxes below (Refer to the section 2.4.4. Identify in this manual).

All check boxes are checked by default when **IrisEnroll** program is first installed. If you click on the **Select all** button, all check boxes are checked. If you click on **Clear all** button, all check boxes are unchecked.



5.1.7.6 Smart Card

Using the Smart Card tab of the Options window you can configure Smart Card Data Format, Encryption key for GSC-IS Format, and Block Offset for HID iClass and Mifare smart cards. Selecting this tab displays the following window.



“SmartCard Type (in iCAM) :” – displays the currently configured smart card type in iCAM. It also displays appropriate error message if there is any error while accessing the smartcard reader on iCAM.

Tip: You can use iCAM Web Configuration to configure the smart card options in iCAM.

You may also configure the options “Always Issue Smart Card” and “Send IrisCode to IrisServer”.

By default, “Always Issue Smart Card” options are deselected.

The length of “Block Offset” is 1 byte (2 hexadecimal characters). Block Offset needs to be set only if storing non IrisAccess information. The valid values (range) for offset depends on the smartcard type.

Configure smartcard book selection by selecting an item (**‘Book 0’** or **‘Book 1’**) from **‘Book’**

combo box. **Book 1** configuration is applicable only for 32K smartcards. **Book 0** can be configured for 16K/2, 16K/16 and 32K cards.

Smartcard Application area can be configured by selecting an item (**Application 1** or **Application 2**) from the combo box with title **Application Area for Blank Card (16K/2)**. This configuration is applicable only for blank cards (16K/2).

When issuing Smart cards, data format and type of encryption to use may be set in this tab. "Data Format" displays the formats supported for Smart Cards namely, IA EAC Format and GSC-IS Format. When set to GSC-IS format, type of encryption can be set to AES, DES, DES3 or no encryption. In each of these, the encryption key file containing the corresponding encryption key has to be loaded clicking "Get Keys From File" button. Once set, the Smart Cards will be issued in the specified format with specified encryption.

"Get Keys From File" – Click this button to load the file containing the encryption key for the selected encryption type.

"Set to Defaults" – Click this button to set the default values for "Block Offset", Book Selection and Application Area Selection for Blank Card.

"Always Issue Smartcard" checkbox – When this is checked, IrisEnroll will issue a Smart Card for every user enrolled.

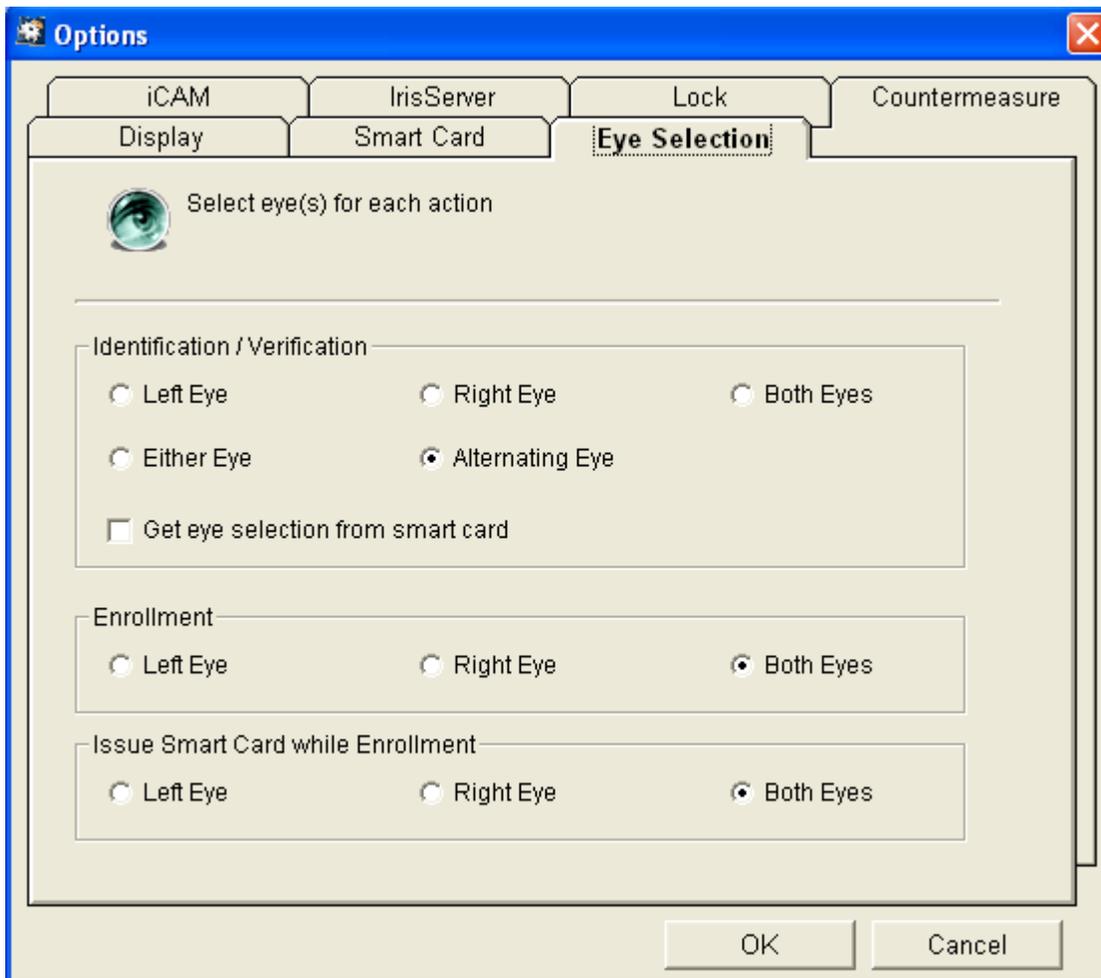
When this is unchecked, the operator can decide whether to issue a card and also the type of card to be issued during the enrollment process. In this case the "Card" combo box on the "User Information" window of the enrollment process provides 3 options to select from, "None", "Smartcard" and "Prox Card".

"Send IrisCode to IrisServer" checkbox – Selecting this checkbox configures IrisEnroll to send the IrisCode to the IrisServer after enrolling the user.

When "Send IrisCode to IrisServer" checkbox is deselected, the IrisCode is **not** sent to the IrisServer after enrolling. This option can be used to save the IrisCode on a Smart Card only instead of the IrisServer.

***Caution:** if the "Card" combo box of the "User Information" window has "None" or "Prox card" selected, the IrisCode will not be saved anywhere.

5.1.7.7 Eye Selection



In this tab user can set which eye should be considered while Identification and Verification, Left, Right, Both or Either.

User can also set which eye should be enrolled Left, Right or Both.

If smartcard is disabled "Issue Smart Card" group is also disabled else enabled.

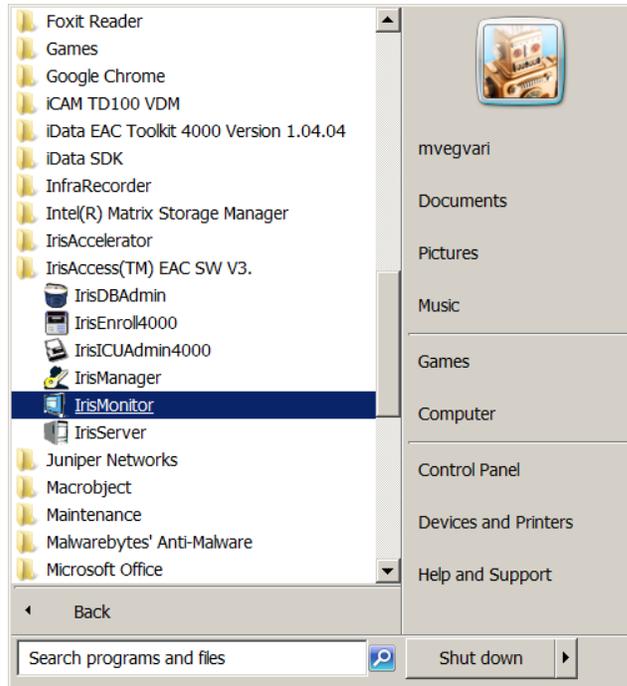
If user is enrolling both eyes he can select for which eye he wants Smart Card Left, Right or Both.

6. IrisAccess™ IrisMonitor

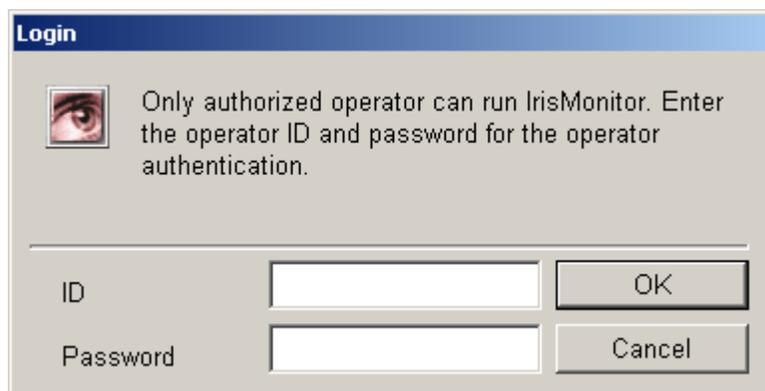
6.1 IrisAccess™ IrisMonitor

6.1.1 How to Run IrisMonitor

1. To start the **IrisMonitor**, click on the **IrisMonitor** menu item. The location of the program is shown in the figure below.



2. **Successful** execution of **IrisMonitor** will display the following **Login** window for entering the **ID** and **Password** information.



3. **IrisMonitor** can be executed by the **IrisMonitor Operators** and **Administrators** only.

6.1.2 How to Login to IrisMonitor

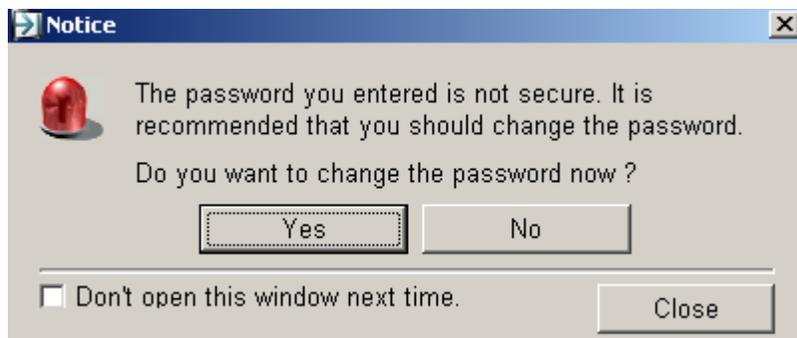
Running the IrisMonitor will open the Login window shown below.



1. Enter the **ID** and **Password** of an operator with monitoring rights or an **Administrator**. Click on the **OK** button.
 - ◆ The Default ID and password are “**administrator**” and “**iris3000**” respectively. They may be changed by an administrator.
(Refer to the section 2.2.8.2 Modification of the Administrator/Operator)

*Note:

If the login to the **IrisMonitor** is successful, then you may see the following **Notice** window on the screen, if the password is not secured. (When you login with the default password “iris3000”)



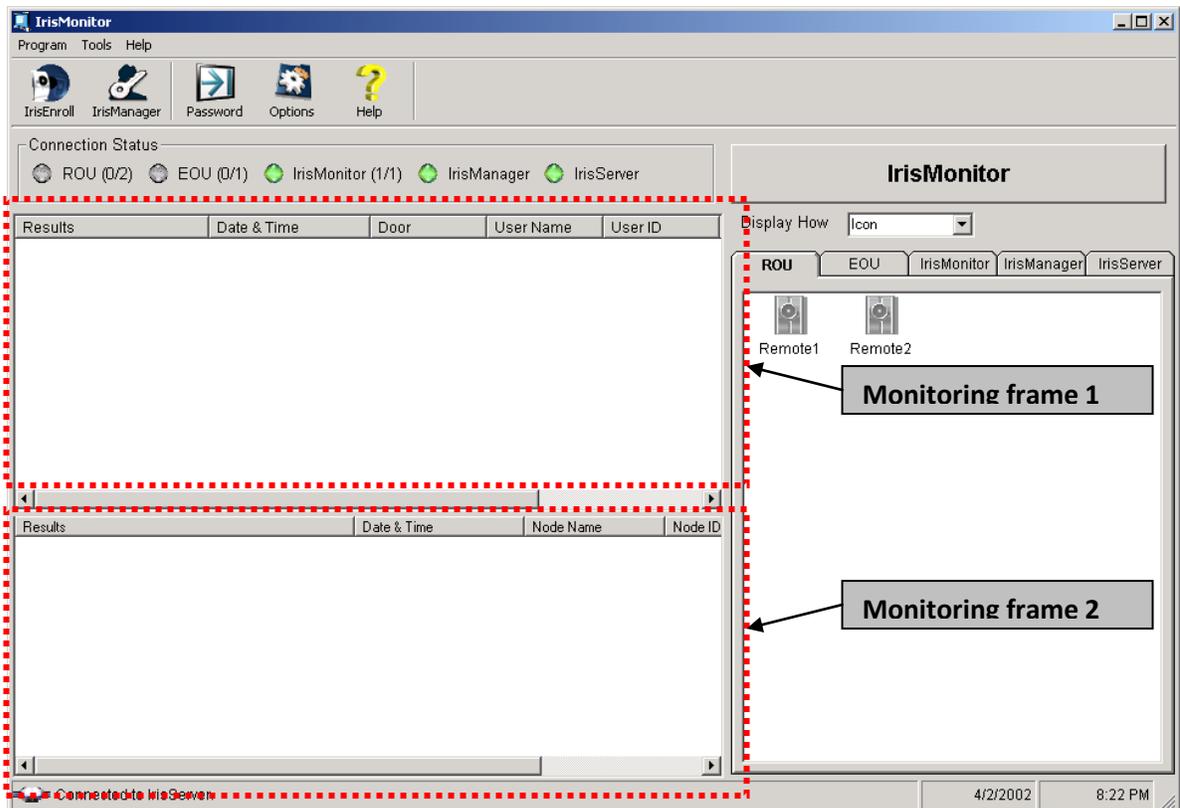
Click on **No** to continue with the same password.
Click on **Yes** to open the following **Password** window used to change the password.



Enter the correct value in the **Current Password** field, and enter the new password in the **New Password** and the **Confirm Password** fields before clicking on the **OK** button.

The **IrisMonitor** screen will be opened after changing the password successfully or aborting the password changing operation.

2. The same **IrisMonitor** window will be displayed without the **Notice** window, if the **ID** and **Password** are valid and the password is secured.



The following messages will be displayed in the top monitoring frame on user access.

Messages on access:

Denied (User ID found, Iris not tried)	Warning
Denied (User ID found, Iris not matched)	Warning
Denied (User ID not enrolled)	Warning
Accepted	
Accepted (Coming in and out during special time)	Warning
Accepted (Warning eye)	Warning
Accepted (Super User)	
Denied (Unauthorized -No access authority for door)	Warning
Denied (Unauthorized -No access authority for time)	Warning
Denied (Expired)	Warning
Denied (Unauthorized -Iris NOT enrolled or No access authority)	Warning
Denied (Fake Eye)	Warning
Denied (Door access trial overtime)	Warning
Identified	
Not Identified (Iris check failed)	Warning
Not Identified (Iris NOT enrolled)	Warning
Verified	
Not Verified (Iris check failed)	Warning
Not Verified (Iris NOT enrolled)	Warning
Denied (Card ID not found, Iris matched, Live eye check failed)	Warning
Denied (Card ID not found, Iris matched)	Warning
Denied (Card ID not found, Time Out)	Warning
Denied (Verification failed, but Iris matched, Live eye check failed)	Warning
Denied (Verification failed, but Iris matched)	Warning
Denied (Verified, Live eye check failed)	Warning
Denied (Verified, Unauthorized)	Warning
Denied (Verification Time Out)	Warning
Denied (Wiegand format error – Wrong facility code)	Warning
Denied (Wiegand format error – Parity error)	Warning
Denied (Wiegand format error – Wrong facility code and Parity error)	Warning

The following system status messages will be displayed in the lower monitoring frame.

Message on system status

IrisEnroll connected

IrisEnroll disconnected	
IrisManager connected	
IrisManager disconnected	
IrisMonitor connected	
IrisMonitor disconnected	
IrisServer ON	
IrisServer OFF	Warning
Remote unit connected	
Remote unit disconnected	Warning
Fail to execute IrisEnroll (Unauthorized)	
Fail to execute IrisManager (Unauthorized)	
Fail to execute IrisMonitor (Unauthorized)	
Video connection Error (ROU)	Error
Serial connection Error (ROU)	Error
Video connection Error (EOU)	Error
Serial connection Error (EOU)	Error
Door open overtime	Warning
Server DB is inconsistent with remote DB	Warning
Door opened by force	Warning
Disk is full	Warning
Alarm on	Warning
Alarm off	
ROU Tamper ON (ROU opened)	Warning
ROU Tamper OFF (ROU closed)	
ICU Tamper ON (ICU opened)	Warning
ICU Tamper OFF (ICU closed)	
Egress ON	
Egress OFF	
RS422 format Error	Error
Wiegand format Error	Error
DB open Error	Error
Frame grabber Open Error	Error
Video connection Normal	

Do back up now!

Warning

Configuration file open error

IR-LED failure (700nm)

Error

IR-LED failure (800nm)

Error

Card Reader error

Error

Warning eye to GPO on

Warning eye to GPO off

Door open overtime to GPO on

Door open overtime to GPO off

Fire alarm to GPO on

Fire alarm to GPO off

ICU/DCU tamper to GPO on

ICU/DCU tamper to GPO off

ROU tamper to GPO on

ROU tamper to GPO off

Identify to GPO on

Identify to GPO off

Door lock but open to GPO on

Door lock but open to GPO off

ICU shutdown after GPO

ICU installation is completed

Card ID matched to GPO on

Card ID matched to GPO off

ICU Configuration File Error

Database Checksum Error

iCAM tamper to GPO on

iCAM tamper to GPO off

iCAM Full Auto-Upgrade started

iCAM Full Auto-Upgrade in progress

iCAM Full Auto-Upgrade completed

iCAM is being rebooted as its software is auto-upgraded

iCAM Software Auto-Upgrade failed

Connected to iCAM

Disconnected from iCAM

Failed to connect to iCAM

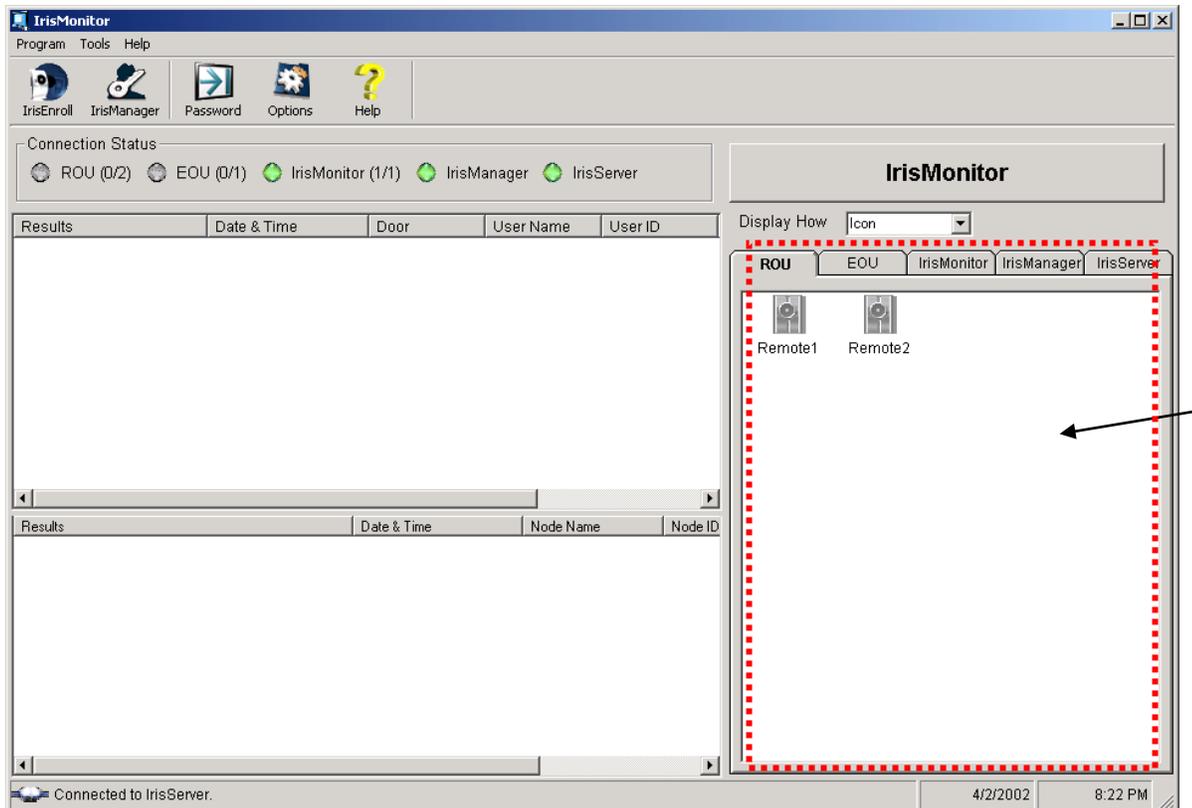
6.1.3 Other Program Launch

IrisMonitor may be used to start the other programs (**IrisEnroll and IrisManager**).

This can be done by selecting the desired program from the **Program** menu or from the toolbar.

6.1.4 System Status

The information about the Programs and the Control units can be obtained by selecting the desired Program / Optical unit tab in the IrisMonitor window. This section of IrisMonitor is indicated by an arrow in the picture below.



For example, the information about Monitor1 may be viewed by selecting the IrisMonitor tab and then double-clicking on Monitor1 from the resulting window. The information about the selected IrisMonitor (Monitor1) will be opened in a new window as shown below.



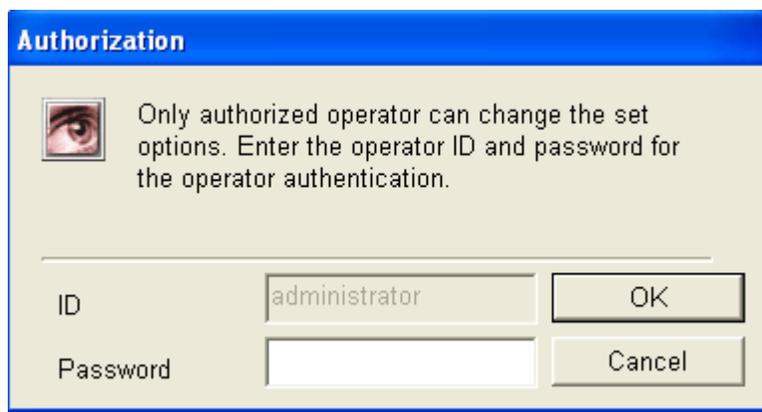
6.1.5 Option Settings

The **Options** Item is used to set the various options like

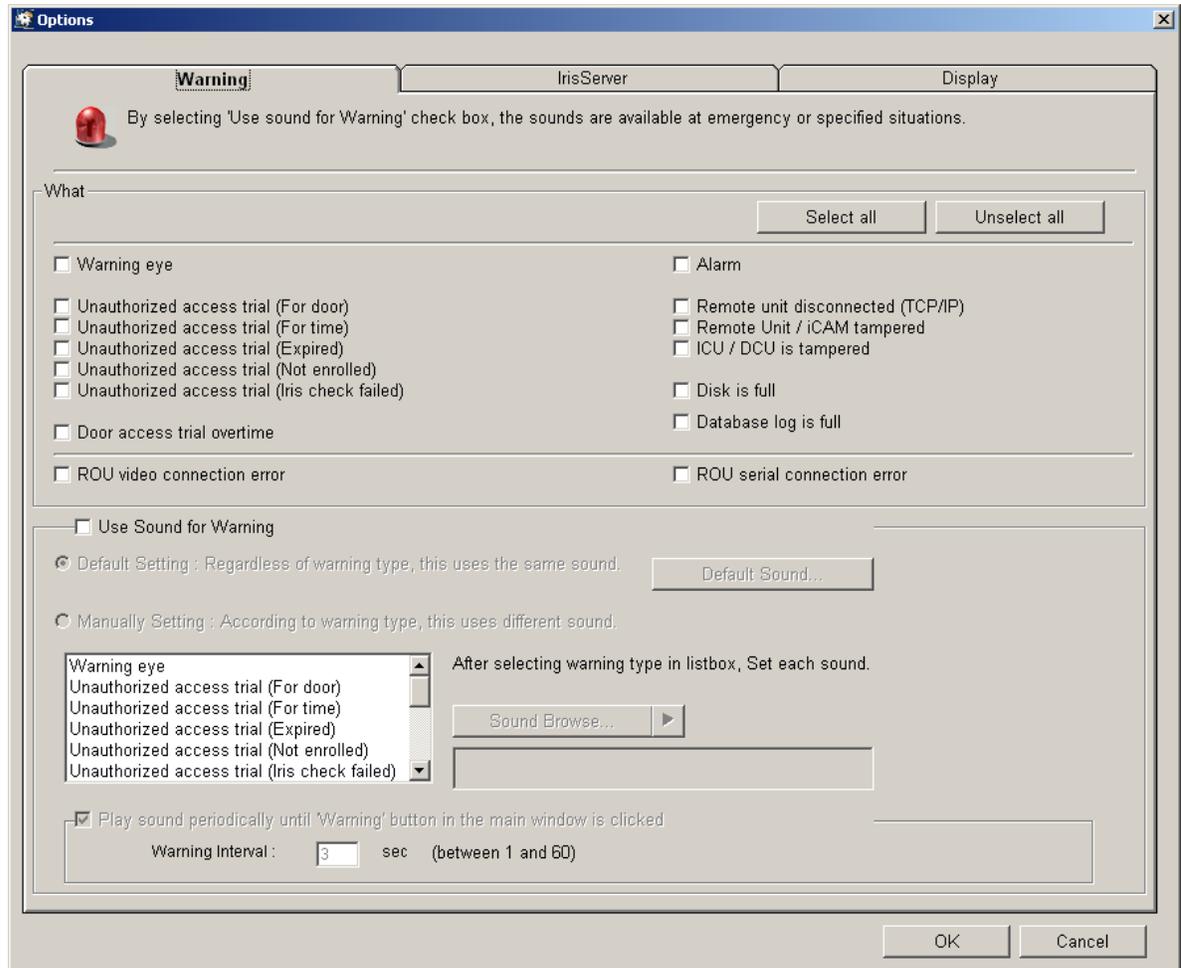
1. The IP address of IrisServer
2. The Display of the User ID in the transaction list.
3. By selecting the warnings from the list of warnings and setting the IrisMonitor sounds upon a specified situation.

To configure the **Options** in **IrisMonitor**,

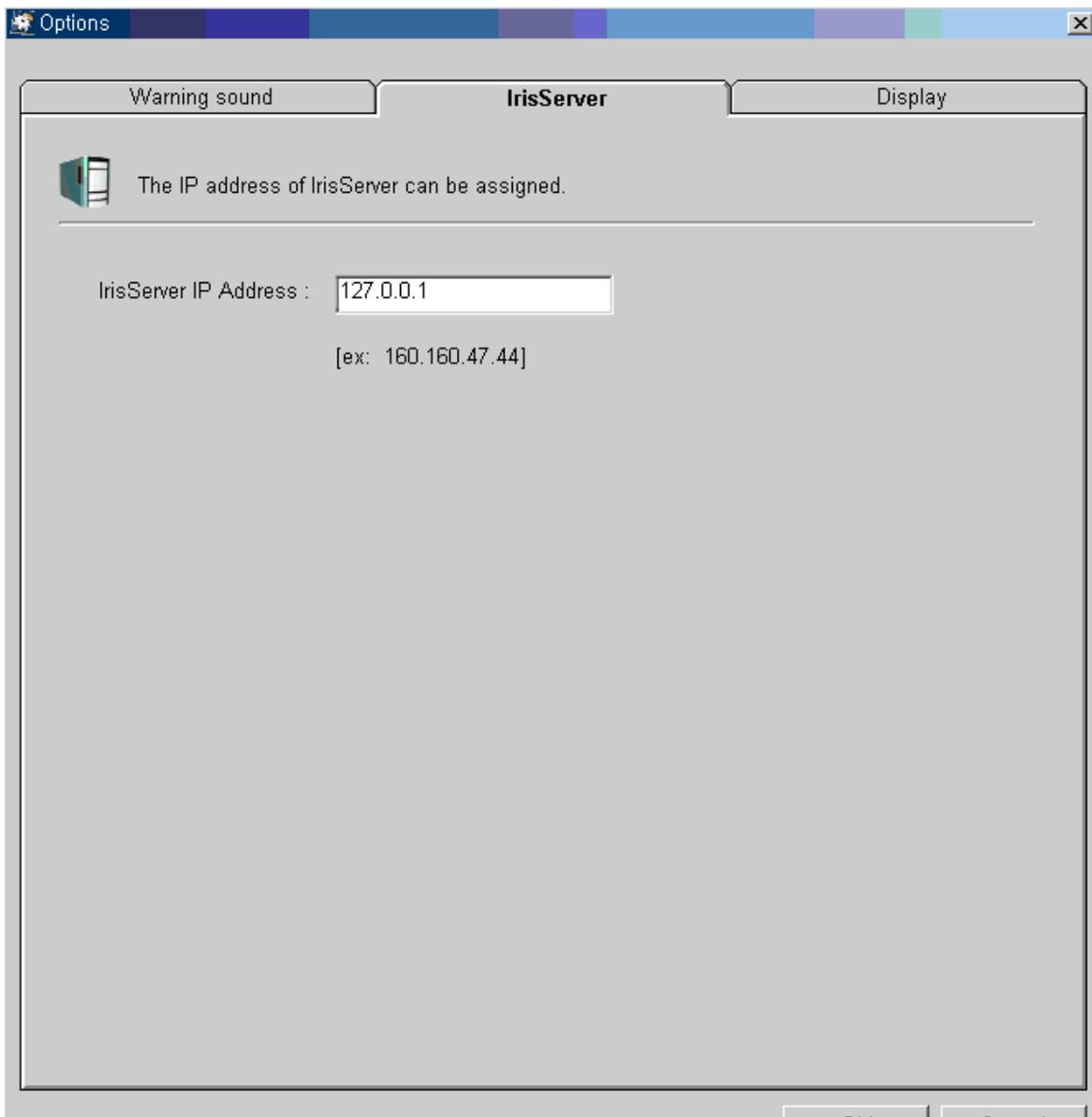
1. Only Authorized operators can change the Options.
2. Selecting options from the Tools menu will result in this popup window.



3. Enter Password and press **OK**. If the operator has the appropriate access rights, the Operator will be allowed to change the settings and the following window will be displayed.



6.1.5.1 Setting the IP Address of IrisServer



1. The **Options** window with the **IrisServer** tab field selected is shown above. This window may be used to specify the **IP address** of the IrisServer in the text box labeled with **IrisServer IP Address**. If **IrisMonitor** is located on the same computer as **IrisServer**, we recommend using the loopback address (127.0.0.1) as the IP Address.
2. Click on the **OK** button to register these changes.

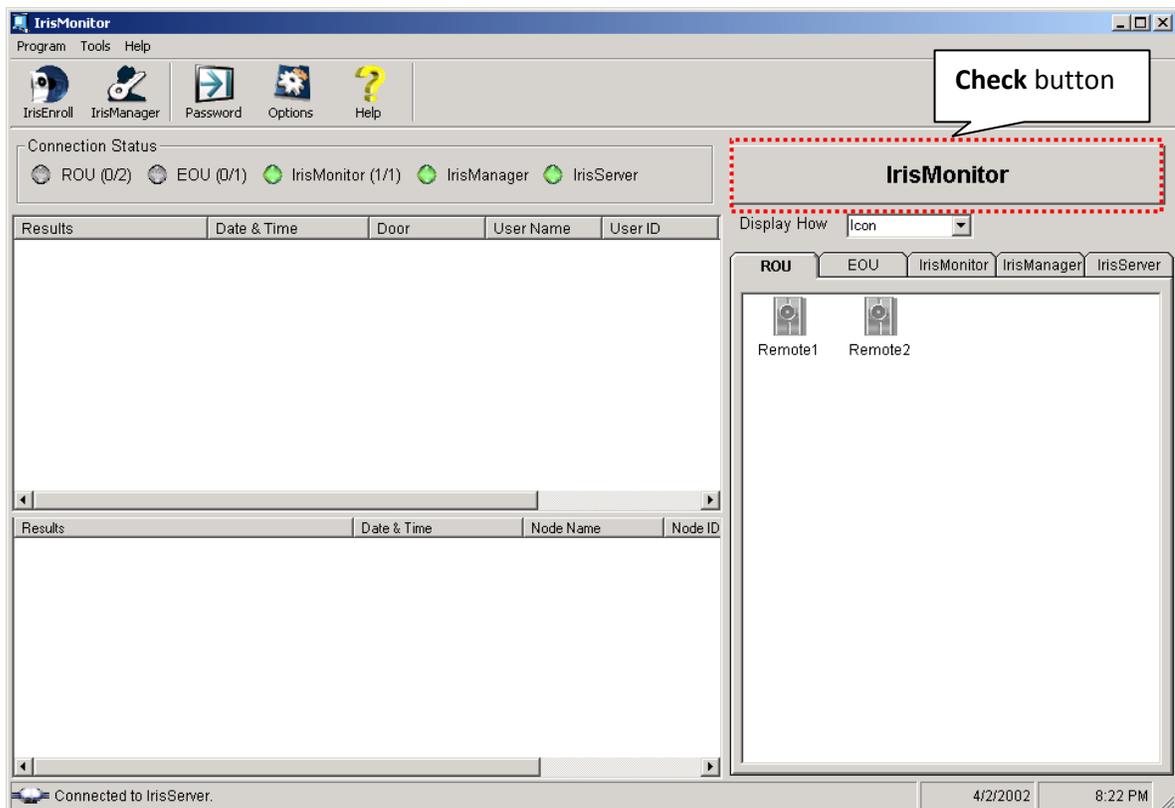
6.1.5.2 Selecting the Display of User ID



1. The **Options** window with the **Display** tab field selected is shown above. This window can be used to select whether the user ID will be displayed in the transaction list.
2. Click on the **OK** button to register these changes.

- b. Click the **Unselect all** button to deselect all the warnings in the **What** part of the window.
- c. Set warning sound. You may configure the Use Sound setting as follows:
 - d. **Default Setting:** The **same sound** is played regardless of warning type
 - e. **Manually Setting:** You can set a **different sound** for each warning type.
 - ◆ Click on **Default Sound** or **Sound Browse** button to select a sound file in .wav format. Several sounds are provided in the IrisAccess sound directory (default location: C:\Program Files\Iris ID\IrisAccess\Sound\).
 - ◆ By default, the sound has been set to "...IrisAccess\Sound\DefaultSound.wav." If you click on the ► button, can hear the selected sound.
 - f. Check the **Play sound periodically ...** checkbox to have the sound play continuously until the Operator clears the warning by pressing the **Check** button on the main **IrisMonitor** window. If this option is unchecked, the sound will only play once to signify a warning.
 - g. Click on the **OK** button after setting the desired configuration..

(* When this system alarm sounds for notification of a warning, click on the **check** button indicated in the following diagram. to stop the sound.)



6.1.6 Password

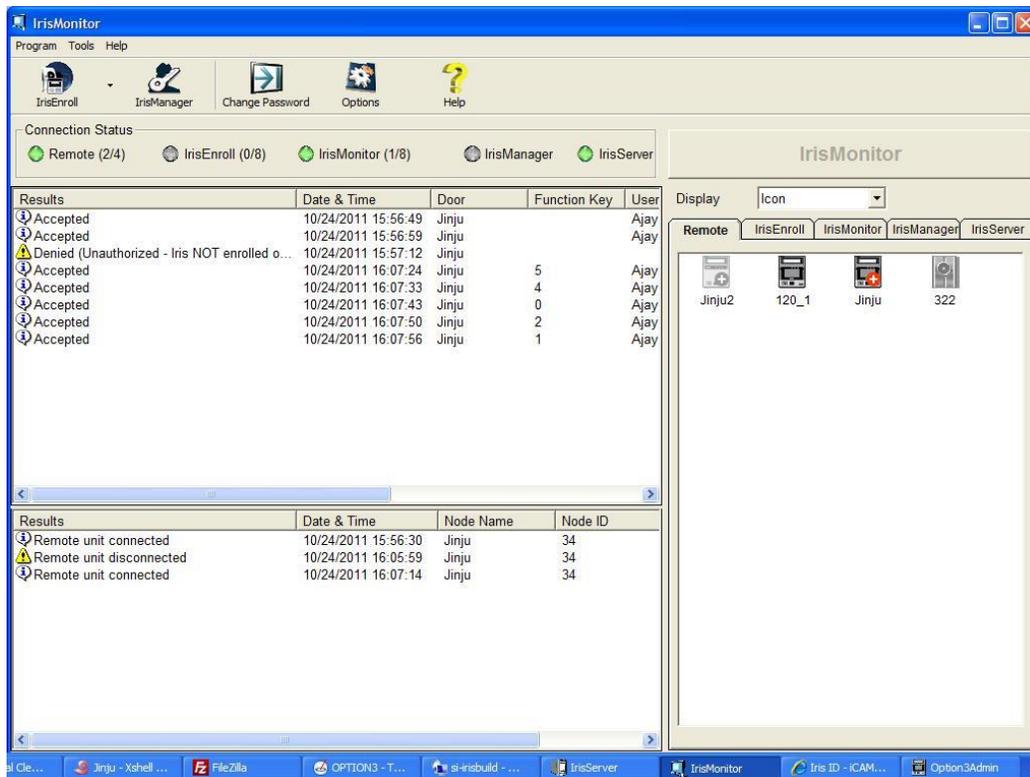
The current password of the **IrisMonitor** operator may be changed using this feature.

1. Select the **Change Password** Item from the **Tools** menu in the menu bar or select the **Password** icon from the tool bar, to open the following **Password** window.
2. Enter the **current password**.
3. Enter the **New password** and **Confirm Password** to confirm the new password.
4. Click on the **OK** button to complete the password change operation.



6.1.7 Time & Attendance Display information

Function key information is displayed on the IrisMonitor window along with transaction logs. If the time and attendance feature is disabled, then function key value is **blank**. Otherwise, the entered function key value is displayed in transaction log. If the user fails to press a valid function key within the timeout period, the log displays the function key value as **0**.



6.1.8 Data Collection Display information

Data Collection can be displayed when used with an iCAM71xx series camera unit. This Data Collection feature can be enabled in the iCAM from the iCAM7000 Series Web Configuration for each camera unit from the 7100 LCD & Pin Pad settings screen (for use with Operational mode: Option 3 Only with iCAM software version 3.08.03 and above). If this feature is enabled it is **displayed in the Data Collection** field of access report according to table. If no data is entered as a result of a timeout, the Data Collection field will **display 0**; otherwise if user **authentication failed** or user presses “Enter key” **without any Data Collection**, or Data Collection is **disabled**, then in Iris manager Data Collection field shall be **left blank**. View the following image for location of the Data Collection in IrisMonitor.

Results	Date & Time	Door	Function Key	Data Collection	User Name	User ID	Card ID
Denied (Unauthorized - Iris NOT enrolled or N...	02/27/2013 14:41:11	iCAM7100 O...					
Accepted	02/27/2013 14:41:27	iCAM7100 O...	1	22	M	V 5741	5741
Accepted	02/27/2013 14:43:44	iCAM7100 O...	4	1	M	V 5741	5741
Accepted	02/27/2013 14:48:02	iCAM7100 O...	0		M	V 5741	5741
Accepted	02/27/2013 14:56:34	iCAM7100 O...	0		M	V 5741	5741

6.1.9 Remote Unit Created for iCAM7100 – Option 3

Remote units created for Option3 is visible in IrisMonitor as shown below:

The screenshot shows the IrisMonitor application window. At the top, there is a menu bar with 'Program', 'Tools', and 'Help'. Below the menu bar are icons for 'IrisEnroll', 'IrisManager', 'Change Password', 'Options', and 'Help'. The main interface is divided into several sections:

- Connection Status:** Shows the status of various components: Remote (3/4), IrisEnroll (0/8), IrisMonitor (1/8), IrisManager, and IrisServer. All are indicated as active with green circular icons.
- Results Table:** A table with columns for Results, Date & Time, Door, Function Key, and User. It contains a list of access events, mostly 'Accepted' for user 'Ajay' at various doors (Jinju2, Jinju) and function keys. One event is marked as 'Denied (Unauthorized - Iris NOT enrolled o...)'.
- Display:** A dropdown menu set to 'Icon' and a grid of icons representing remote devices. The 'Remote' tab is selected, showing icons for 'Jinju2', '120_1', 'Jinju', and '322'. The 'Jinju2' and 'Jinju' icons are circled in red.

At the bottom, a taskbar shows several open applications, including 'Jinju - Xg...', 'filezilla', 'IrisMa...', 'Databases', 'OPTIONS...', 's-rsbuild...', 'Implemen...', 'IrisMonitor', and 'IrisServer'.

7. IrisAccess™ IrisDBAdmin

7.1.1 *IrisAccess™ IrisDBAdmin*

IrisDBAdmin is a database administration tool for **MS Access**, **MS SQL Server** and **Oracle** that makes it easier for a database administrator to **backup, import, create, drop, upgrade** and **manage** the IrisServer database.

The type of database used as the **IrisServer** database is set only during installation. The default database type is MS Access, and is sufficient for most installations.

When **MS Access** is used as the **IrisServer** database, the only functions used in IrisDBAdmin are **upgrade or import**.

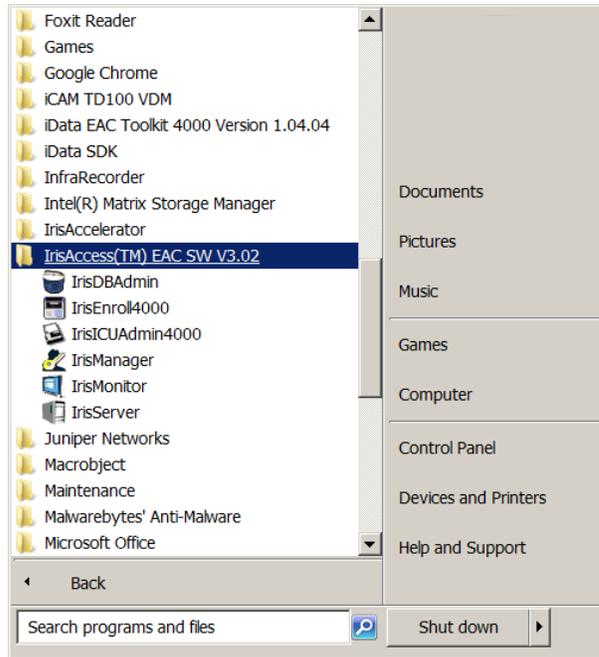
To use **MS Access** as the database type, **MS Access** does **NOT** need to be installed.

MS SQL Server and/or **Oracle** are supported in IrisAccess™ iData EAC software (when selected during installation).

In order to use **Oracle**, the **Oracle** DBMS should be installed on a database server PC and Oracle Objects for Oracle should be installed on Iris Server PC.

7.1.2 *How to Run IrisDBAdmin*

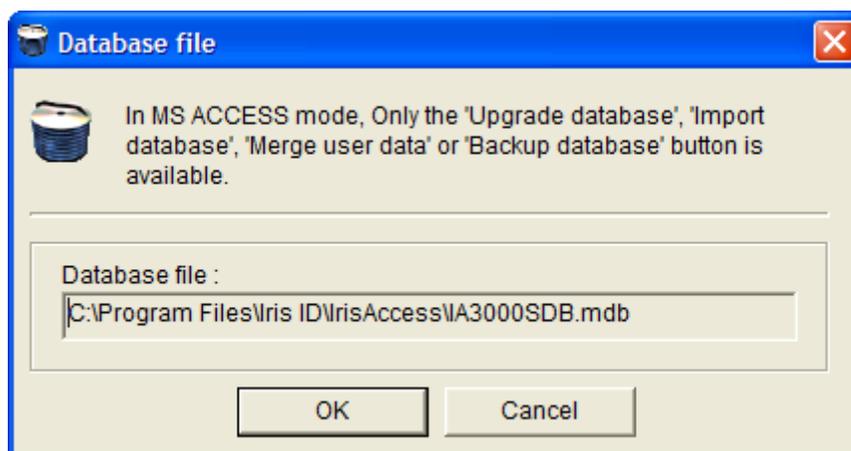
To start the **IrisDBAdmin** program, click on the **IrisDBAdmin** menu item. The location of the program is shown in the figure below.



7.1.3 IrisDBAdmin for MS ACCESS Database

When used with a **MS Access** database, **IrisDBAdmin** allows a user to **backup, import, upgrade** and **import** the **IrisServer** database.

1. When **IrisDBAdmin** is started, it will display the following window to select the path of the **IrisServer** database. (Default location is C:\Program Files\Iris ID\IrisAccess\)

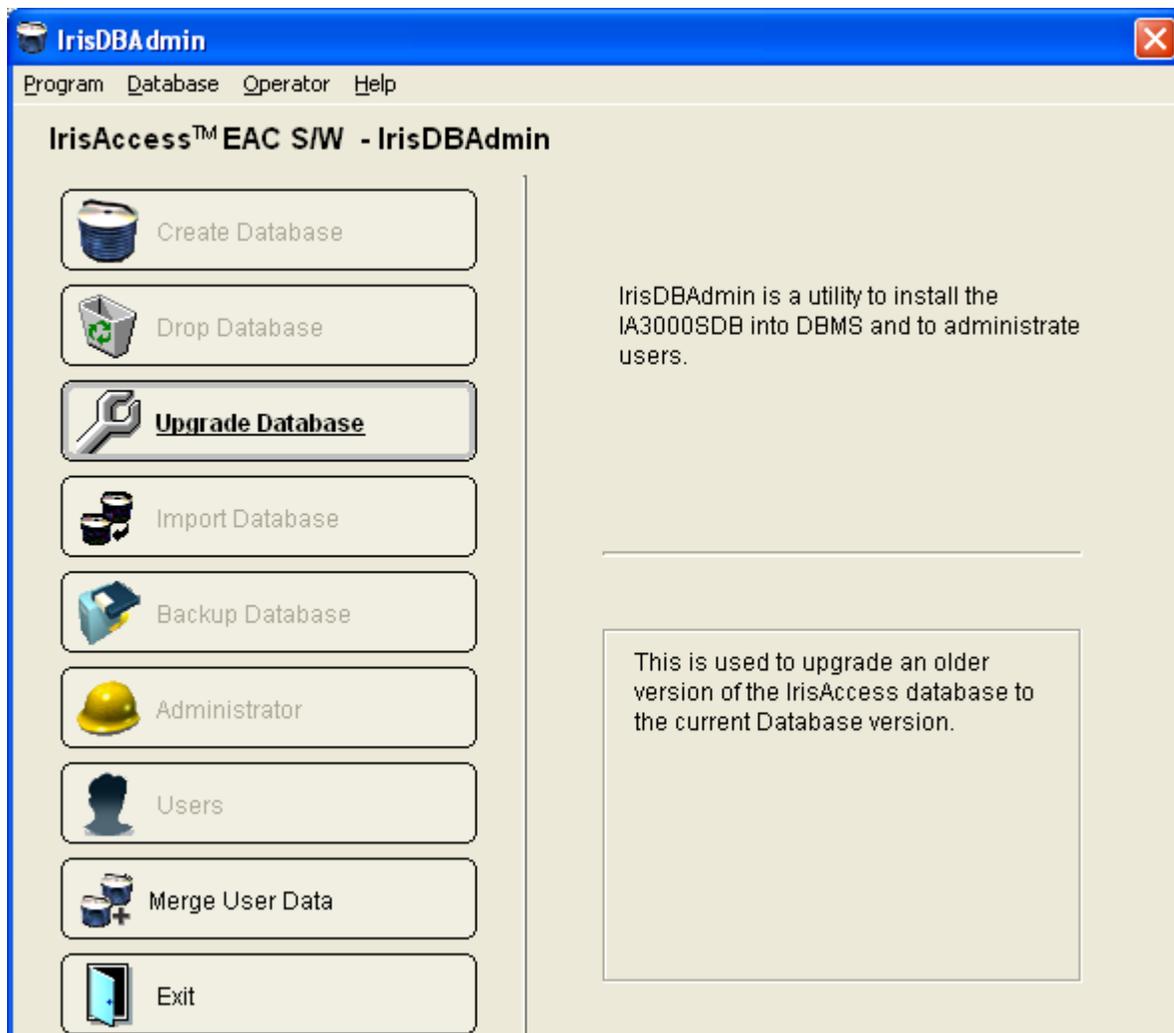


2. If the selected **IrisServer** database is from a previous version of the **IrisAccess** software, you will see the following message about upgrading **IrisServer** database.

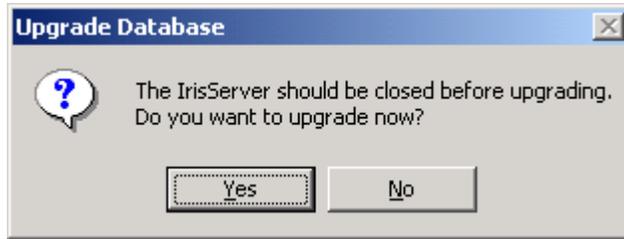


3. Click on the **OK** button. You must upgrade the **IrisServer** database before using it with **IrisServer**. We recommend backing up the database file before upgrading.

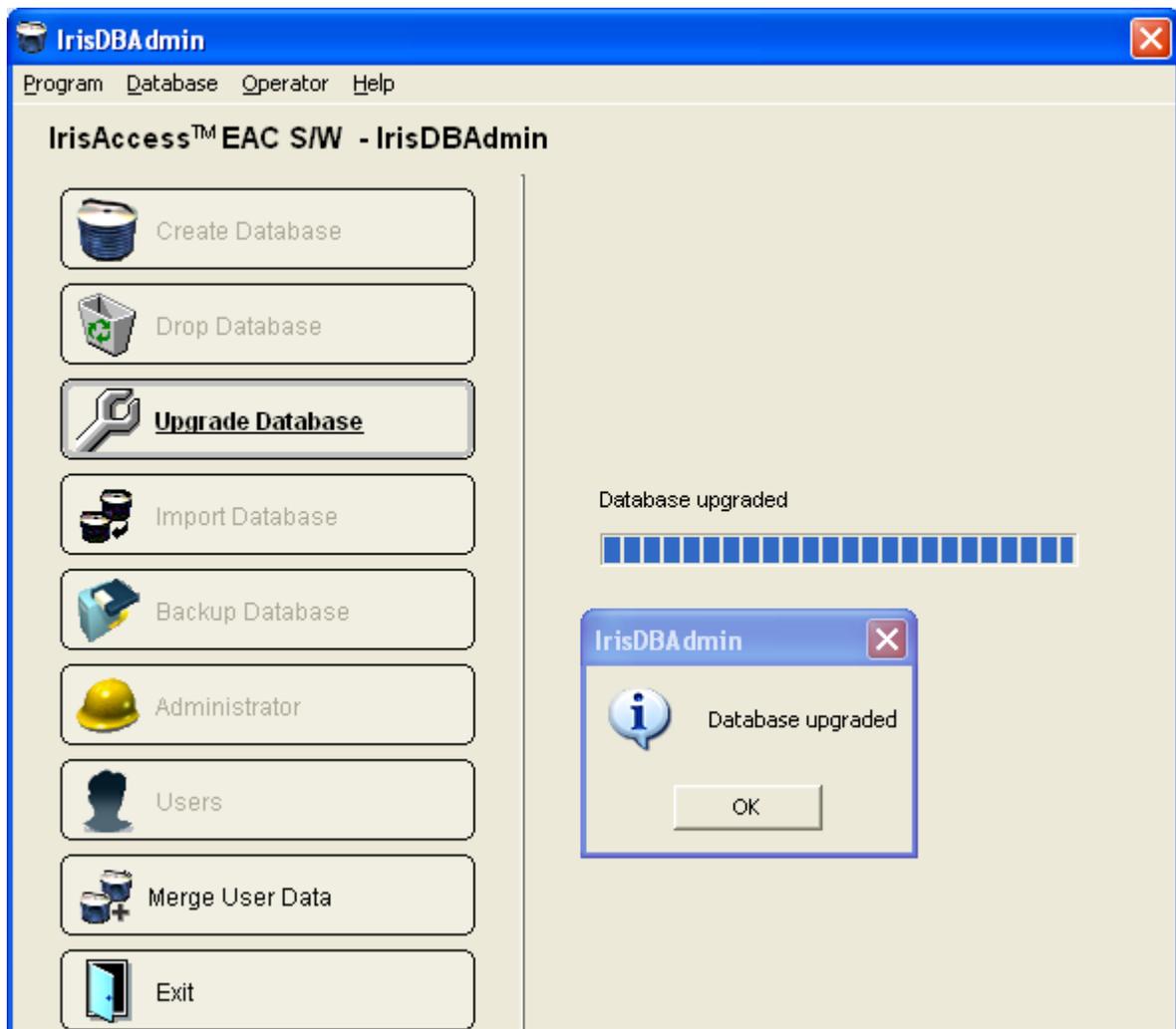
7.1.3.1 Upgrading Database



1. Click on the **Upgrade Database** button or select the **Upgrade Database** item from the **Database(D)** menu item in the menu bar and the next window will open to confirm the upgrade of the IrisServer DB.



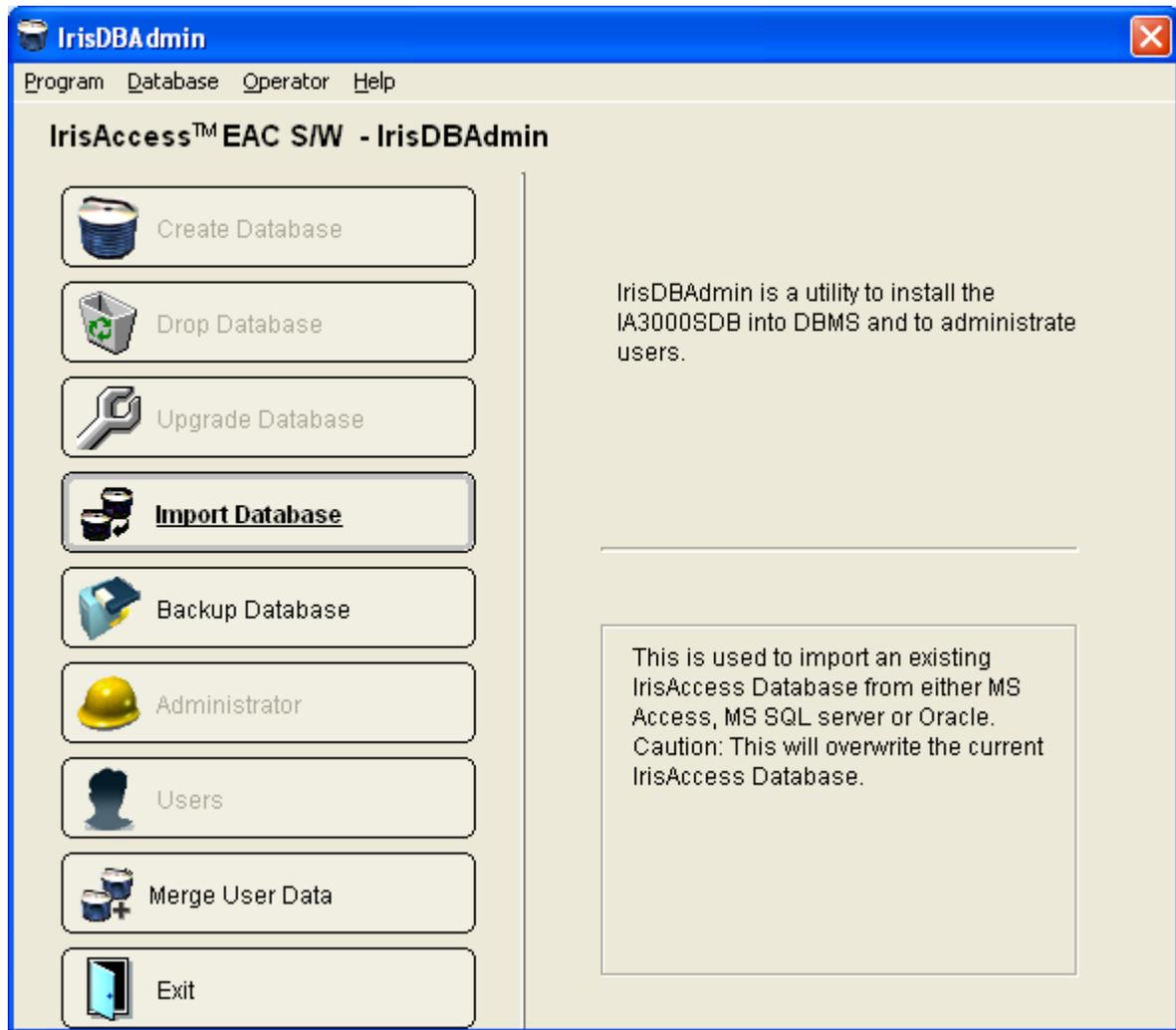
2. Click on the **Yes** button and **IrisDBAdmin** performs an upgrade of the IrisServer DB. When the upgrade completes, the following window will be displayed.



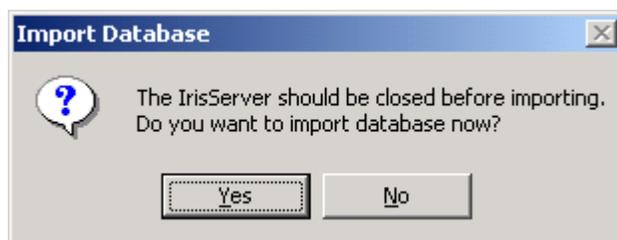
7.1.3.2 Importing Database

IrisDBAdmin allows users to **import** an existing IrisServer DB from MS Access, MS SQL

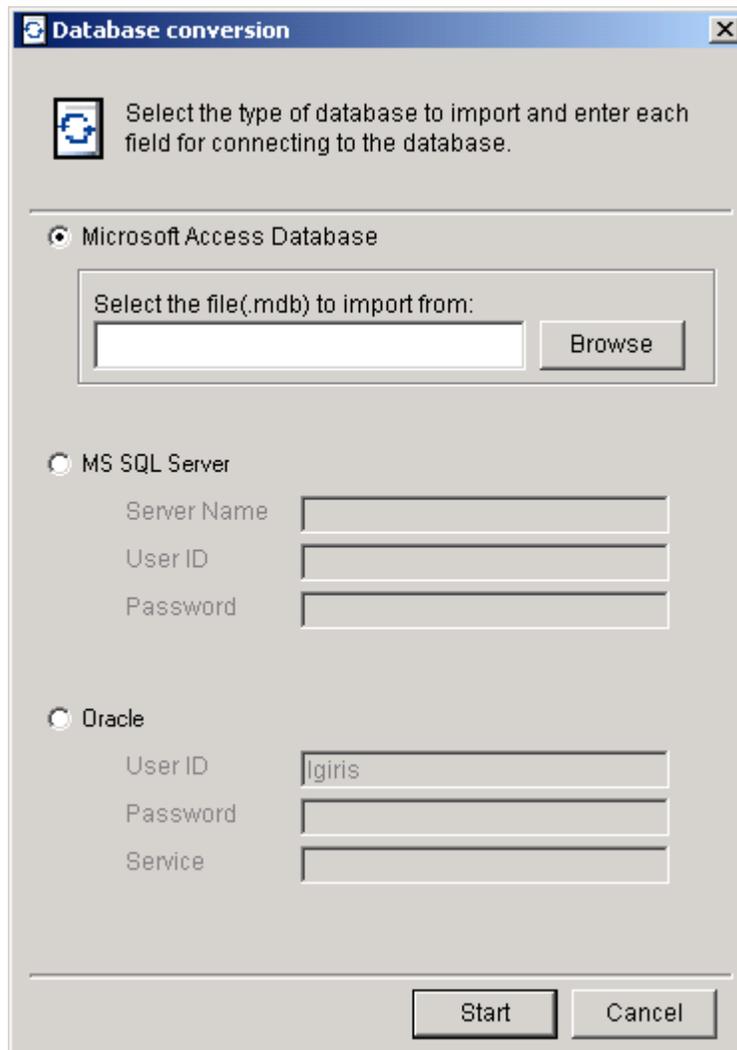
server or Oracle.



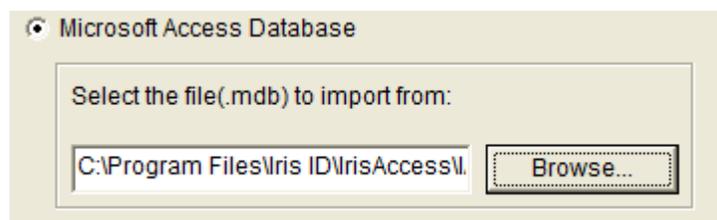
1. Click on the **Import Database** button or select the **Import Database** item in the **Database (D)** menu item in the menu bar and the next window will open to confirm the import of the IrisServer database.



2. Click on the **Yes** button and **IrisDBAdmin** begins importing the IrisServer database.



3. Select the type of database to import and enter the information to each field for connecting to the database.
 - A. If **importing the IrisServer database from Microsoft Access Database**, click on the **Browse** button and select the database file.



- B. If **importing the IrisServer database from MS SQL Server**, enter the **Server Name** (or **IP Address**), **ID** and **Password** for the MS SQL Server that you want to connect to. The following figure is the sample for connecting to the MS SQL Server named "irissserver".

MS SQL Server

Server Name : si-ajaywish\SQLEXPRESS

User ID : sa

Password : *****

- ◆ Server name is the name of the computer that MS SQL Server is installed on.
- ◆ Only **MS SQL Server** administrator(s) can import from **MS SQL Server** by using an ID and password that are registered in **MS SQL Server**
- ◆ User ID is case sensitive.

C. If **importing the IrisServer database from Oracle**, enter the **ID**, **Password** and **Service Name** for the **Oracle** server that you want to import from. The following figure is a sample for connecting the Oracle named “oracle_irisserver”.

Oracle

User ID : lgiris

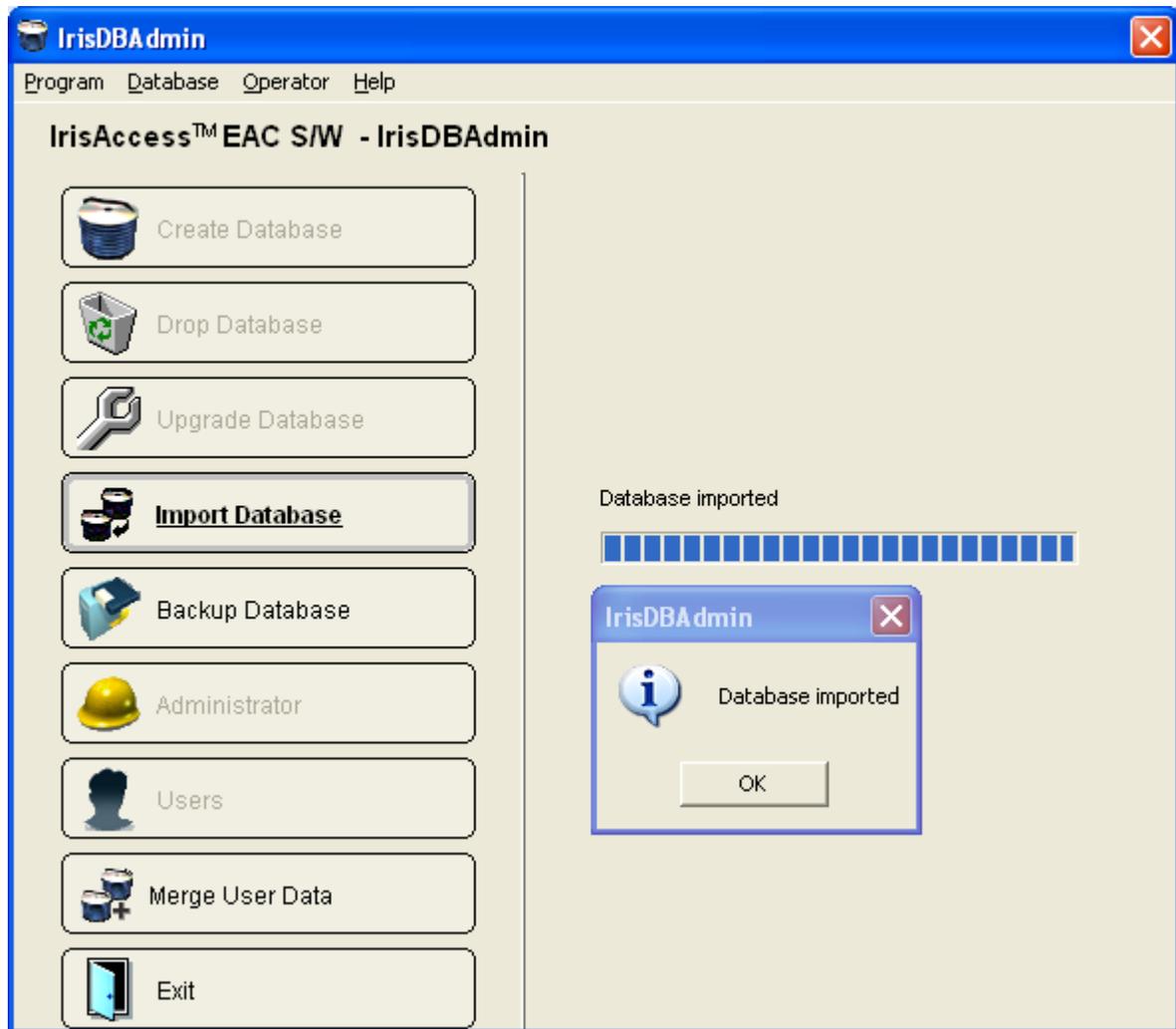
Password : *****

Service : orcalc_irisserver

- ◆ To use **IrisDBAdmin to import from Oracle**, **OO4O** Program (Client for Windows 98/NT/2000/XP) must be installed on the **IrisDBAdmin** computer.
- ◆ You can install OO4O for Windows 98/NT/2000/XP though EAC S/W CD package.
- ◆ The name of the install program is Oracle Universal Installer 2.2 and we recommend the administrator type of installation.
- ◆ After installation, set the Service Name for Oracle though the Enterprise Manager Console.

4. Click on the **Start** button.

5. If the **IrisServer** database is imported successfully, you will see the window below.



*Note:

If **IrisDBAdmin** fails to connect to database, the following messages will open on the screen.

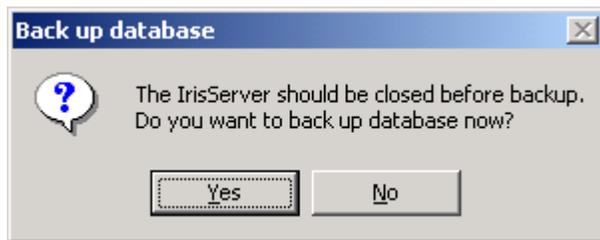


7.1.3.3 Database Backup

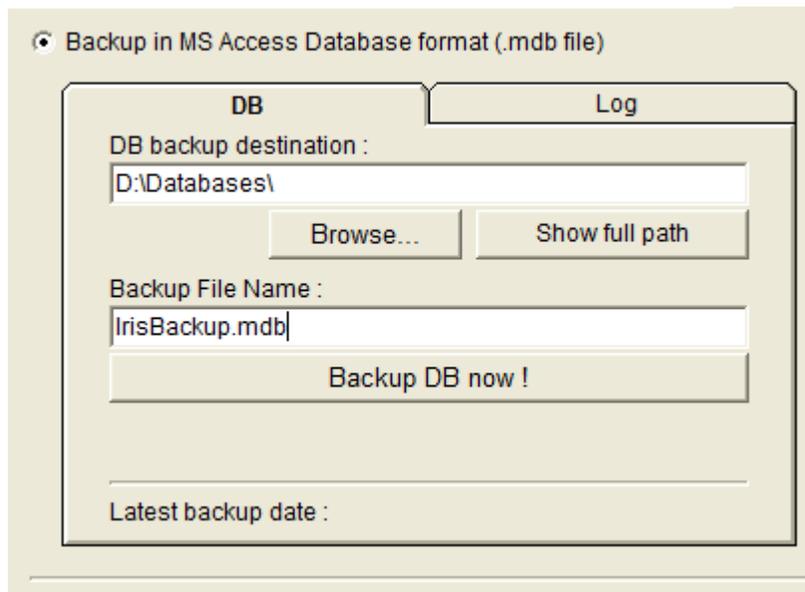
You can create a backup of your database file to prevent data loss caused by disk failures, power outages, virus infections and other potentially damaging events. The backup database created by this process will include the information of users, operators, remotes, holidays, time groups and remote groups.

Note: **IrisServer** must be closed before beginning the backup procedure.

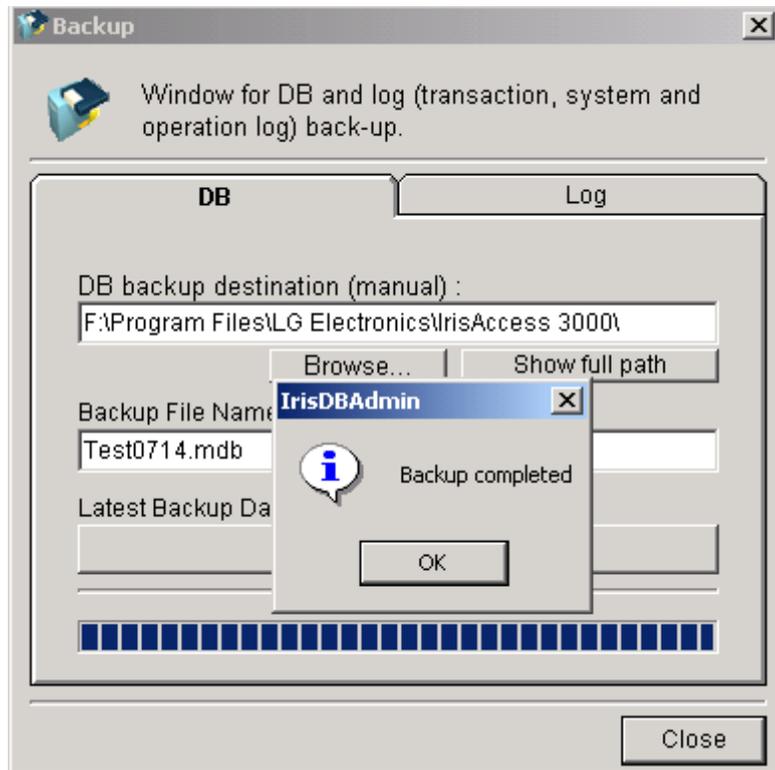
1. Select the **Back up Database** item on the **Database(D)** menu item in the menu bar or click on the **Back up Database** button to open the following window.



2. Click on the **Yes** button and the next window will open.



3. Click on the **Browse...** button and select the folder in which DB backup file will be located.
4. Enter the name of the backup file.
5. Click on the **Backup DB now!** Button. If the DB backup is successfully completed, the next window will display.

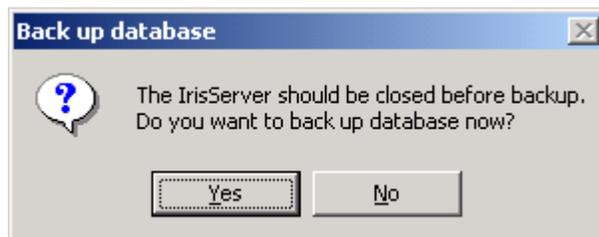


6. Click on the **Close** button to close the backup window.

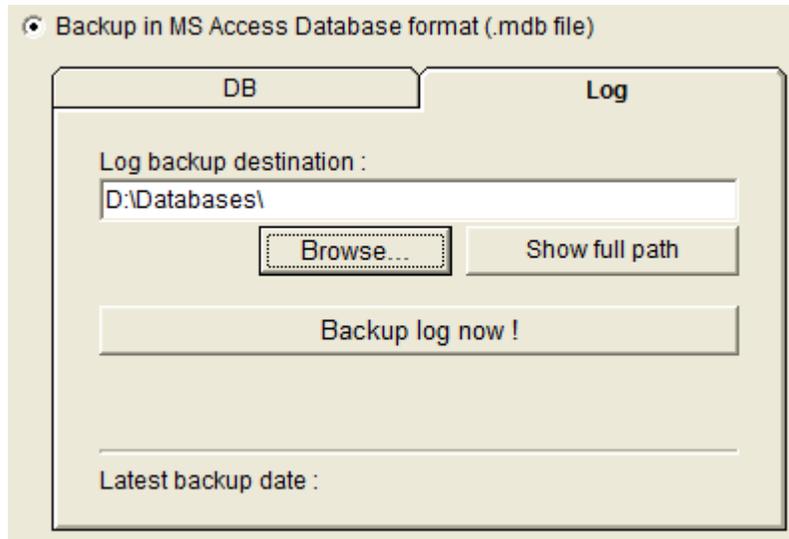
7.1.3.4 Log Backup

You may create a backup of your log files - transaction, system and operation log file. **The backup log file's name created after log back up must not be changed.** If the name is changed, **IrisServer** will be unable to filter the information from the backup log files into reports. **If you do a log backup, the logs will be removed from the database.**

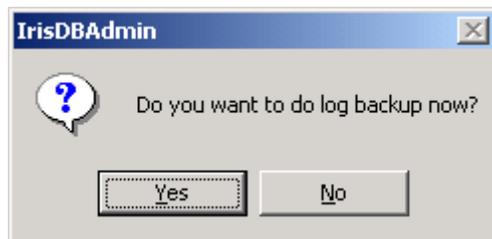
1. Select the **Backup Database** item in the **Database(D)** menu item in the menu bar or click on the **Backup Database** button to open the following window.



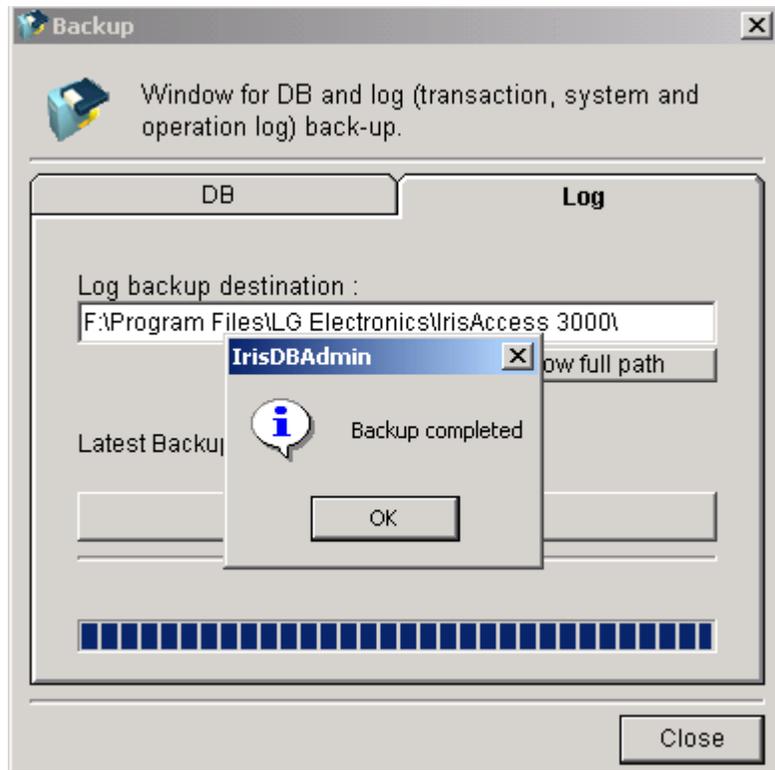
2. Click on the **Yes** button and the next window will open.
3. Select the **Log** tab to display the following window.



4. Click on the **Browse** button to select the folder in which log backup file will be located.
5. Click on the **Backup log now!** Button, to display the following window.



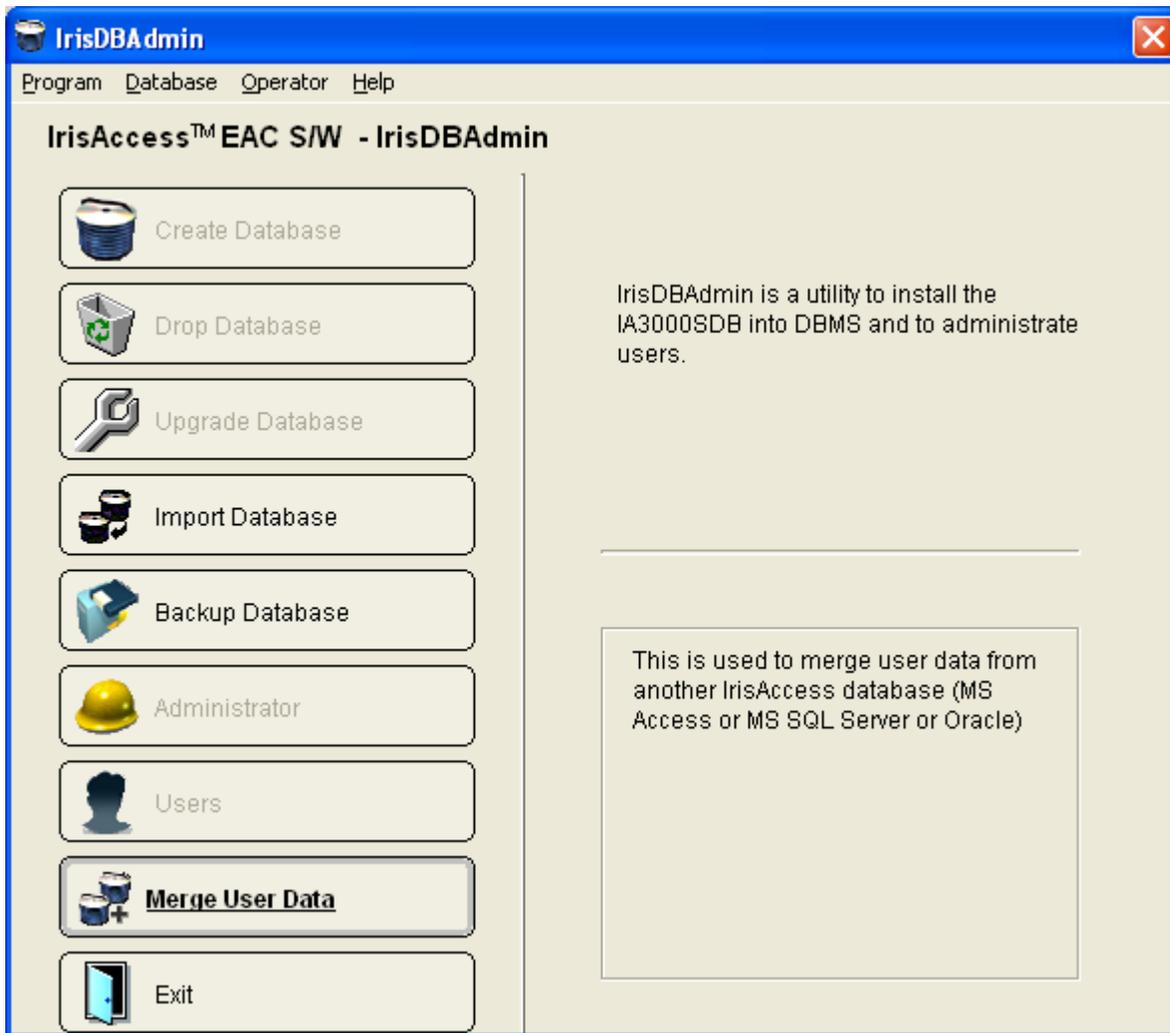
6. Click on the **Yes** button. If the Log backup is successfully completed, the next window will display.



7. Click on the **Close** button to close the backup.

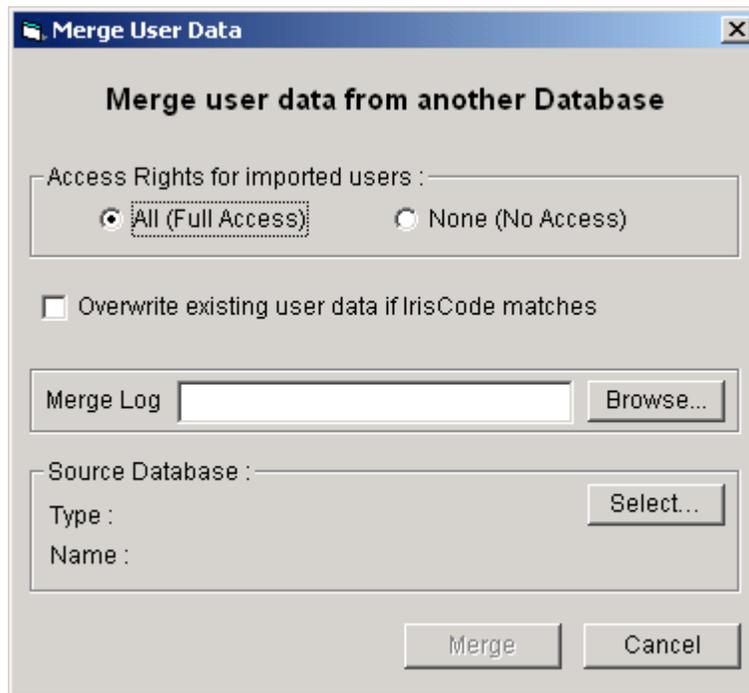
7.1.3.5 Merging User Data

User data can be merged from one database to another database. **Merge User data** is possible through **MS Access, Oracle and SQL server**.



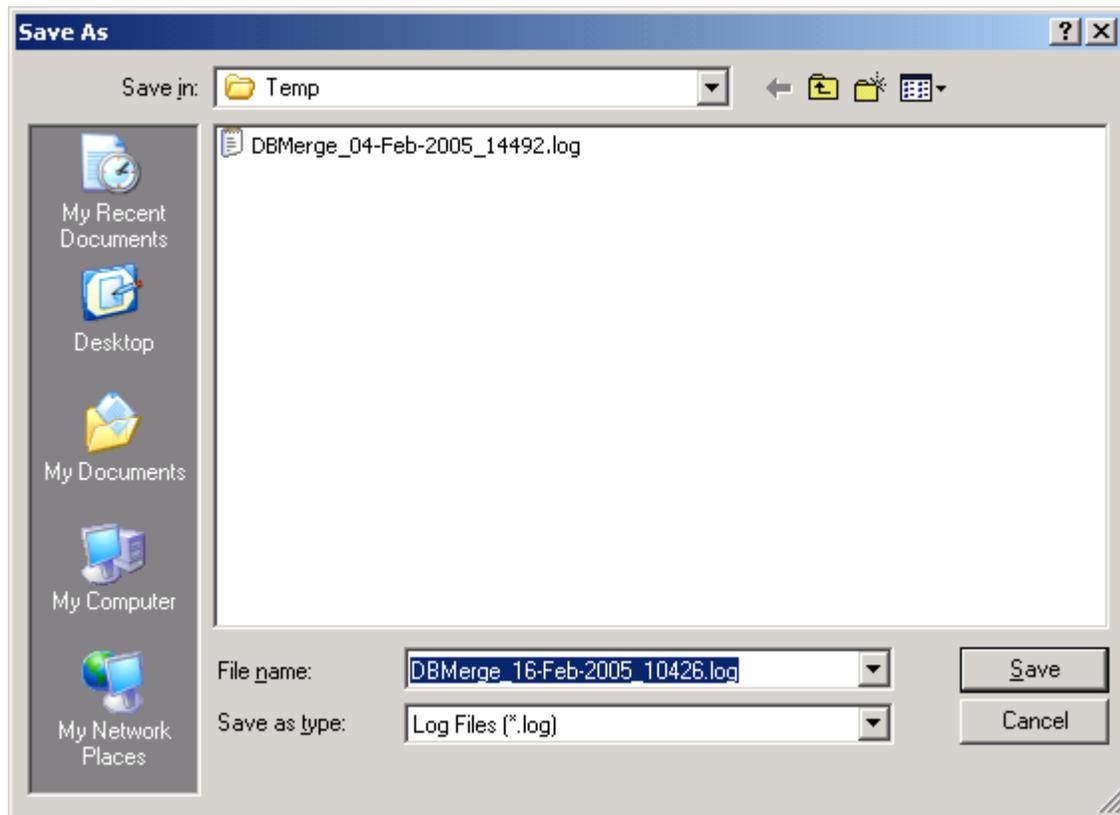
To merge the user data from one **database** to another **database** follow the procedure given below:

1. Click on the **Merge User Data** button or select the **Merge User Data** item from the **database (D)** menu item in the menu bar. The following window will open. You can choose merge the data options and give source database details.



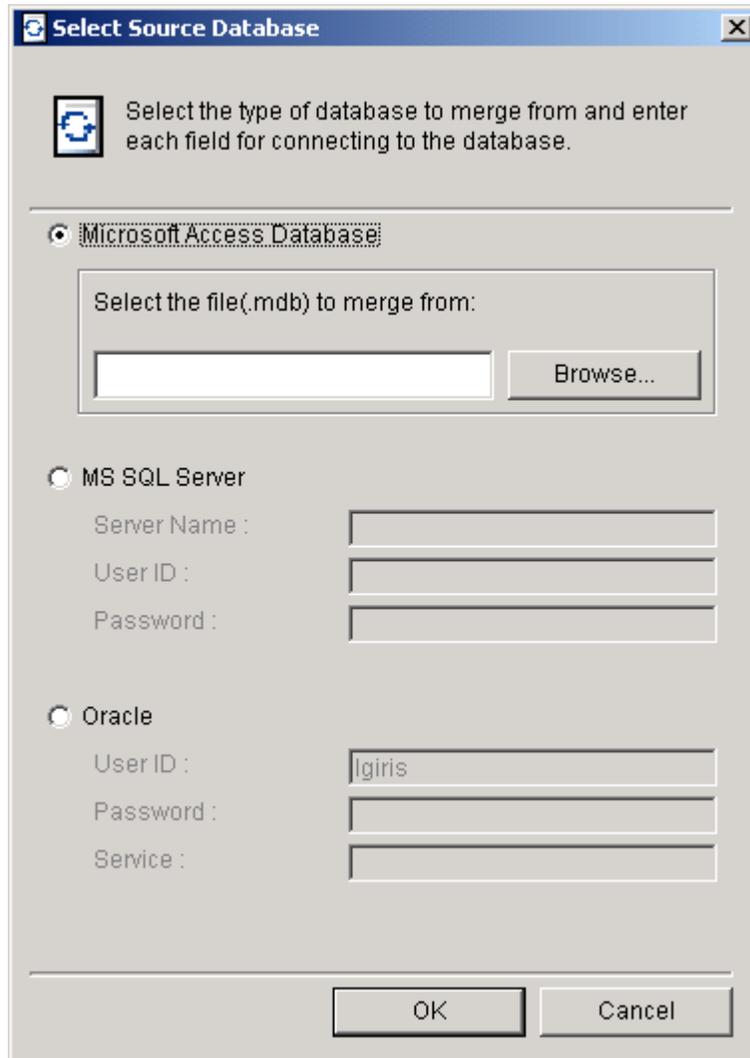
2. Merge User Data - Options:

- If All Access Rights has to be given to the user, select the **All (Full Access)** radio button,
 - If No Access Rights has to be given to the user, select the **None (No Access)** radio button,
 - If the data should be overwritten in case of IrisCode match, check the **Overwrite existing user data if IrisCode matches** check box.
3. Click on **Browse** button to select the Log file path. Errors or/and conflicts which occur during Merge operation will be written to the Log file.

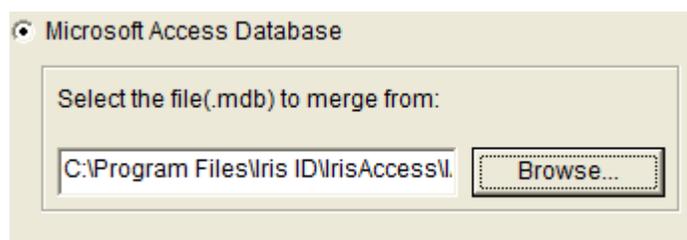


Select the log file path, and enter log file name.

4. Click on **Select...** button to select the source database, the following window will be opened.



5. Select the type of source database to merge from and enter the information to each field to connect to the database.
 - A. If **Merging the database from Microsoft Access database**, click on the **Browse** button and select the database file.



- B. If **Merging the database from MS SQL Server**, enter the **Server Name** (or **IP Address**), **ID** and **Password** for the MS SQL Server that you want to connect to.

MS SQL Server
 Server Name: irisserver
 User ID: sa
 Password: *****

- ◆ Server name is the name of the computer that MS SQL Server is installed on.
- ◆ Only **MS SQL Server** administrator(s) can import from **MS SQL Server** by using an ID and password that are registered in **MS SQL Server**
- ◆ User ID is case sensitive.

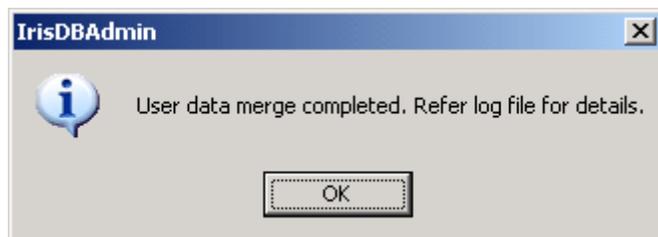
C. If **Merging the database from Oracle**, enter the **ID**, **Password** and **Service Name** for the **Oracle** server that you want to import from.

Oracle
 User ID: lgiris
 Password: *****
 Service: oracle_irisserver

- ◆ To use **to merge from Oracle**, **OO4O** Program (Client for Windows 98/NT/2000/XP) must be installed on the **IrisDBAdmin** computer.
- ◆ You can install OO4O for Windows 98/NT/2000/XP though EAC S/W CD package.
- ◆ The name of the install program is Oracle Universal Installer 2.2 and we recommend the administrator type of installation.
- ◆ After installation, set the Service Name for Oracle though the Enterprise Manager Console.

6. Click on **Merge** button.

7. If the **Merge is success**, the following message will be displayed.

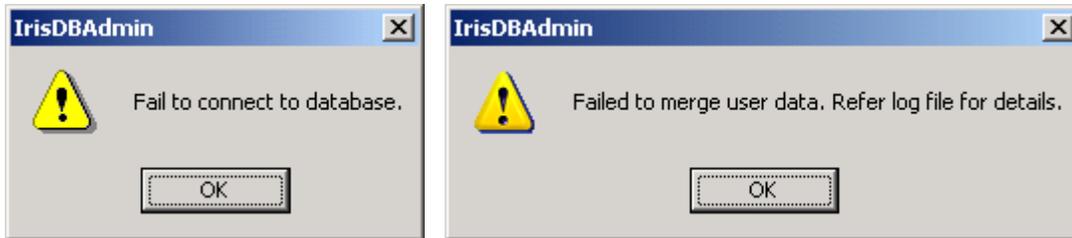


8. If the **Merge is not success**, the following message will be displayed.



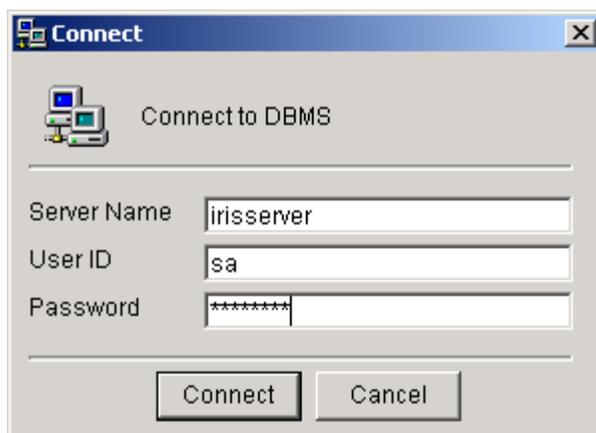
In case of failure, refer to log file for, more details.

- If failed to connect to Source database, the following messages will be displayed.



7.1.4 IrisDBAdmin for MS SQL Server

- When using **IrisDBAdmin** with **MS SQL Server**, **IrisDBAdmin** will display the following **Connect** window to enter the **MS SQL Server** connection information required to execute the **IrisDBAdmin**.
- Enter the name (or IP address), **ID** and **Password** of the **MS SQL Server** in each field. And then click **Connect** button to connect to the **MS SQL Server**.



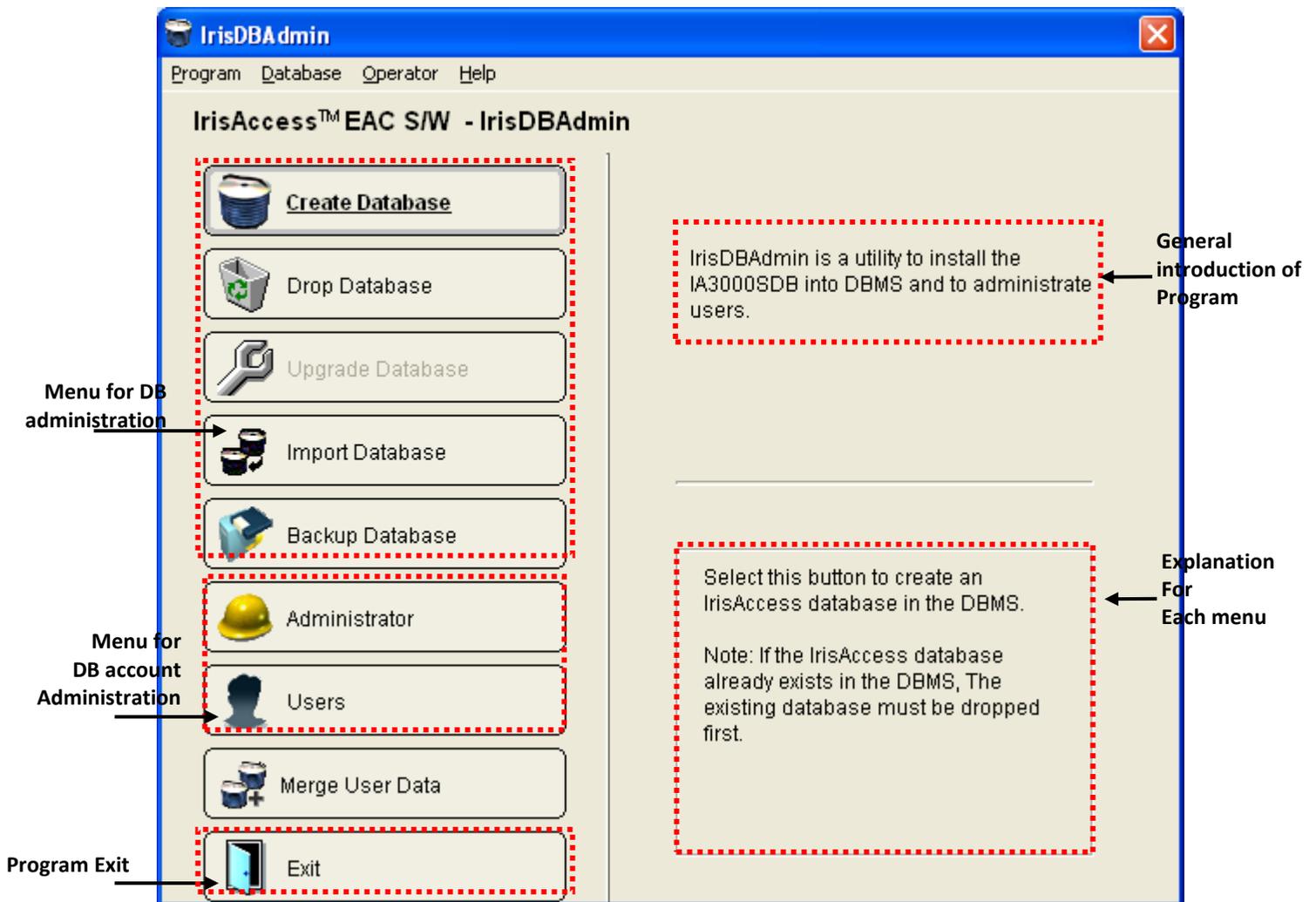
- If **IrisDBAdmin** cannot connect to the **MS SQL Server**, the following messages will open on the screen.



- ◆ Server name is the name of the computer that MS SQL Server is installed on.
- ◆ Only a **MS SQL Server** administrator can connect to **MS SQL Server** by using an ID and password that are registered in **MS SQL Server**. If the ID used is not an administrator, the following messages will display on the screen.



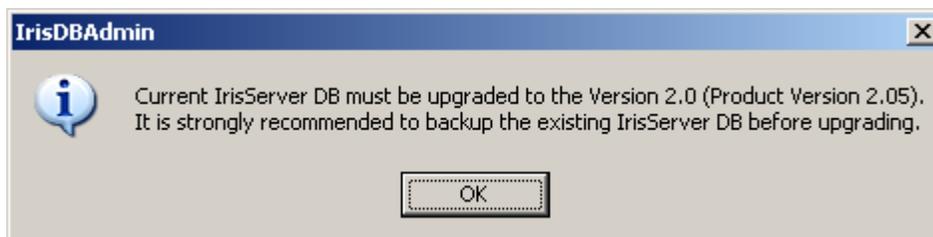
- ◆ User ID is case sensitive.
4. The following **IrisDBAdmin** main window will be shown after successful connection to the **MS SQL Server**.



Verify Diagram

*Note:

If the connection to **MS SQL Server** is successful but the **IrisServer** database present in the **MS SQL Server** is a previous version, the database must be upgraded using the procedure in section 2.5.2.1.

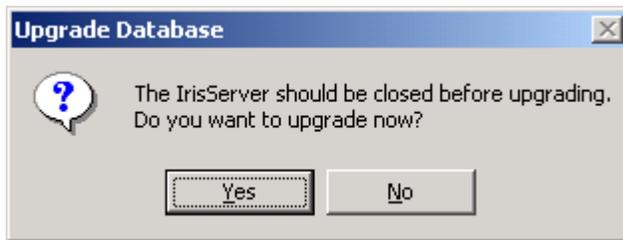


Click on the **OK** button and then upgrade the database. If the database requires upgrading, the next window will be displayed.

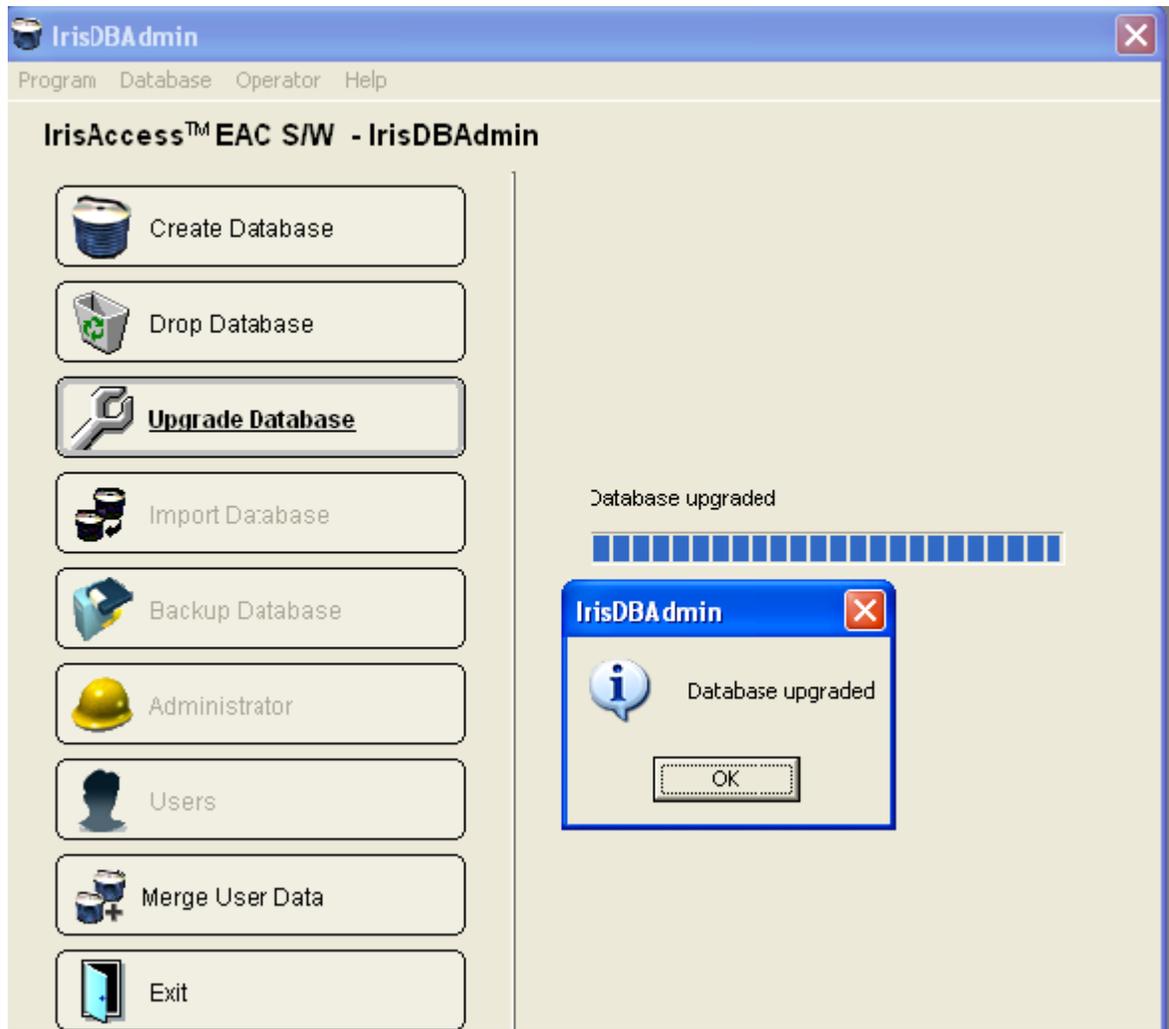
7.1.4.1 Upgrading Database

You can upgrade an IrisServer DB as follows.

1. Click on the **Upgrade Database** button or select the **Upgrade Database** item in the **Database(D)** menu item in the menu bar to display the next window.



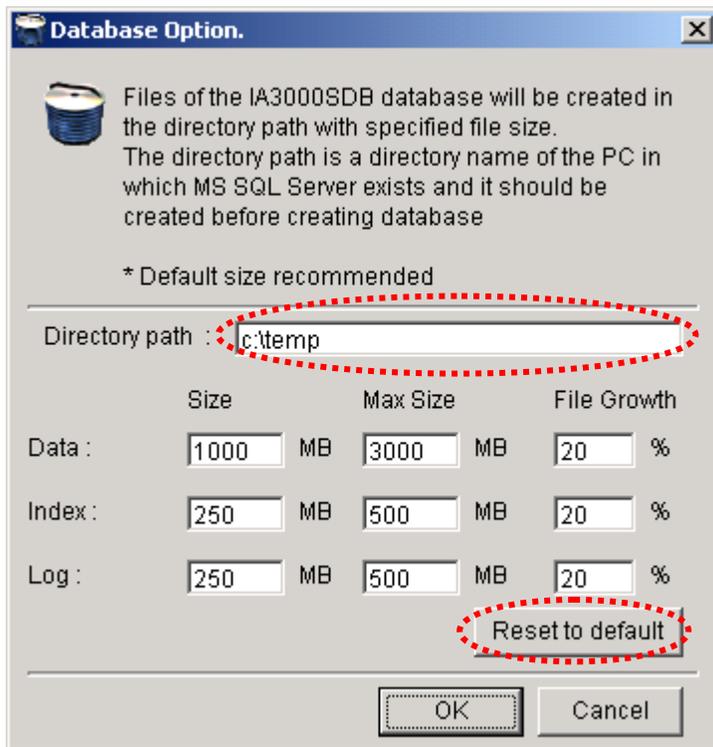
2. Click on the **Yes** button.
3. If **IrisDBAdmin** upgrades the **IrisServer** database successfully, the next window will display.



7.1.4.2 Creating Database

You can create an IrisServer DB as follows.

1. Click the **Create IA3000SDB** button or select the **Create Database** item in the **Database(D)** menu item on the menu bar to create a database.
2. If the IA3000SDB database does not exist on the **MS SQL Server**, the following **Database Option** window will open on the screen.



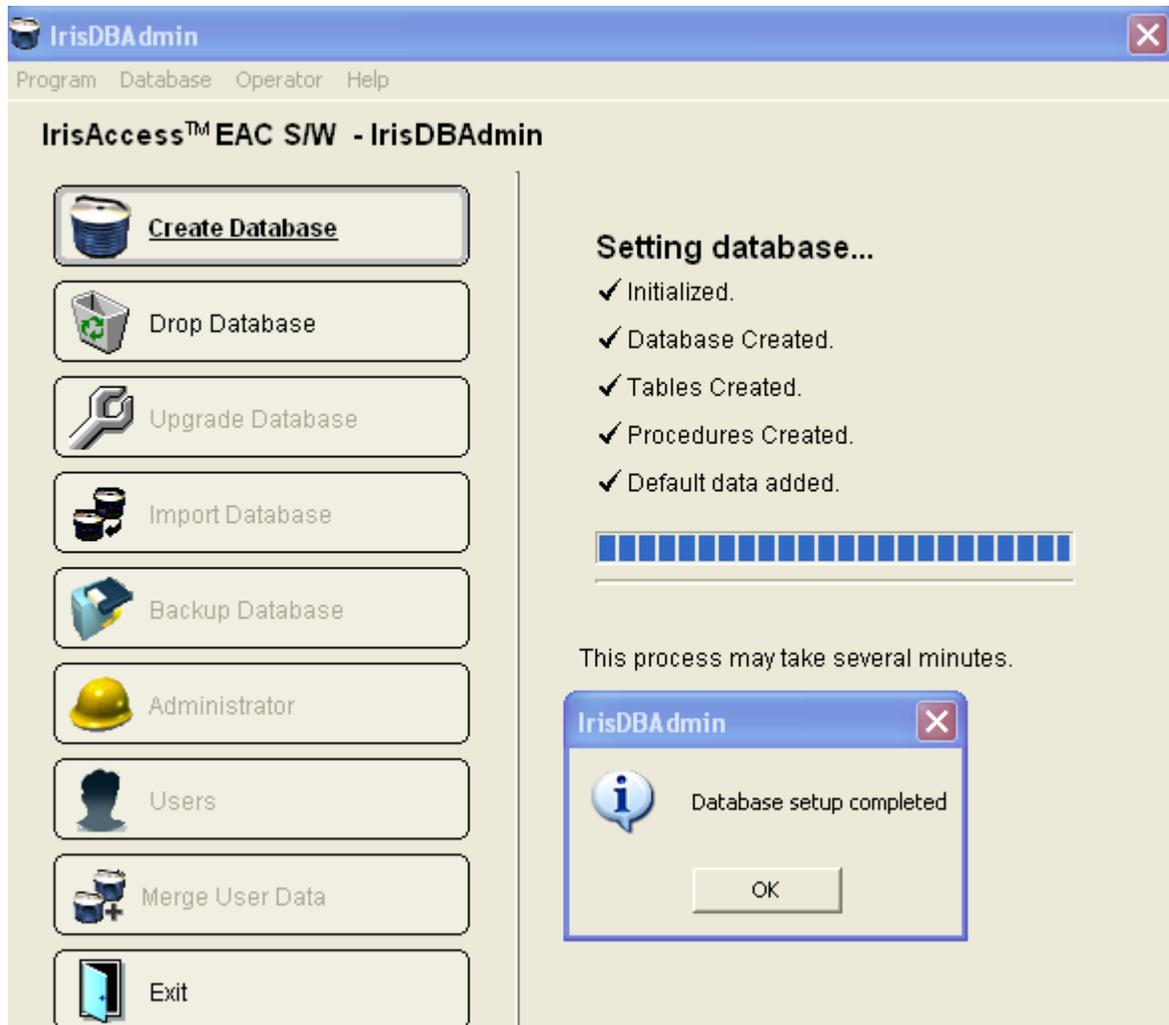
*Note:

If the IA3000SDB database already exists on the **MS SQL Server**, the following notification window will open on the screen. If you want to drop the current database from **MS SQL Server** and create a new database, click on the **OK** button.



3. Enter the directory path of the folder in which the database file will be located.
4. When you create an IrisServer database, you can set the following options for 3 files – primary file, index file, and log file of the **MS SQL Server** database.
 - ◆ **Size:** This option specifies the size of the file. You specify the size in megabytes. The minimum value is 1 MB. The default value is 1000 MB for the primary file. The default value is 250 MB for the index and log files.
 - ◆ **Max Size:** This option specifies the maximum size to which the file can grow. You specify the size in megabytes. The minimum value is 1 MB. The default value is 3000 MB for the primary file. The default value is 500 MB for the index and log files.

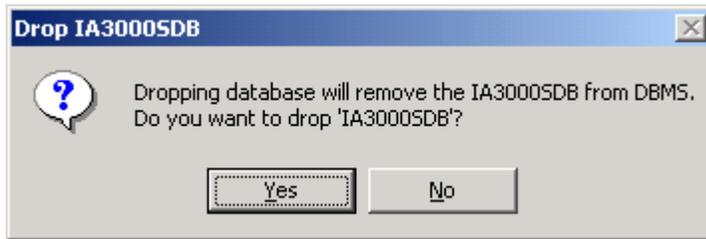
- ◆ **File Growth:** This option specifies the growth increment of the file. The **File Growth** setting for a file cannot exceed the **Max size** setting. A value of 0 indicates no growth. The value is specified as a percentage (%). The minimum value is 0% and the maximum value is 100%. The default value is 20 percent.
5. If you want to specify the default value for each of the options for all files - primary, index and log files of **MS SQL Server** database, click on the **Reset to default** button.
 6. After specifying the path and options for all 3 files, click on the **Ok** button. The following window will be displayed on the screen.



7.1.4.3 Dropping Database

You can drop a database when you no longer need it. Dropping a database deletes the database and the disk files used by the database.

1. Click on the **Drop Database** button in the **IrisDBAdmin** main window or select the **Drop Database** item in the **Database(D)** menu item in the menu bar to drop a database. A confirmation window will open on the screen as shown in the figure below.



2. Click on the **Yes** button on the confirmation window to drop a database. Accidental dropping of a database can be avoided by clicking on the **NO** button.
3. You cannot drop a database that is open for reading or writing by any user. If the database is open, and you click on the **Yes** button on the above confirmation window to drop a database, an error message box appears. For example, if the user ID is HCCHOI is using the database that you want to drop, the following window is displayed on the screen.

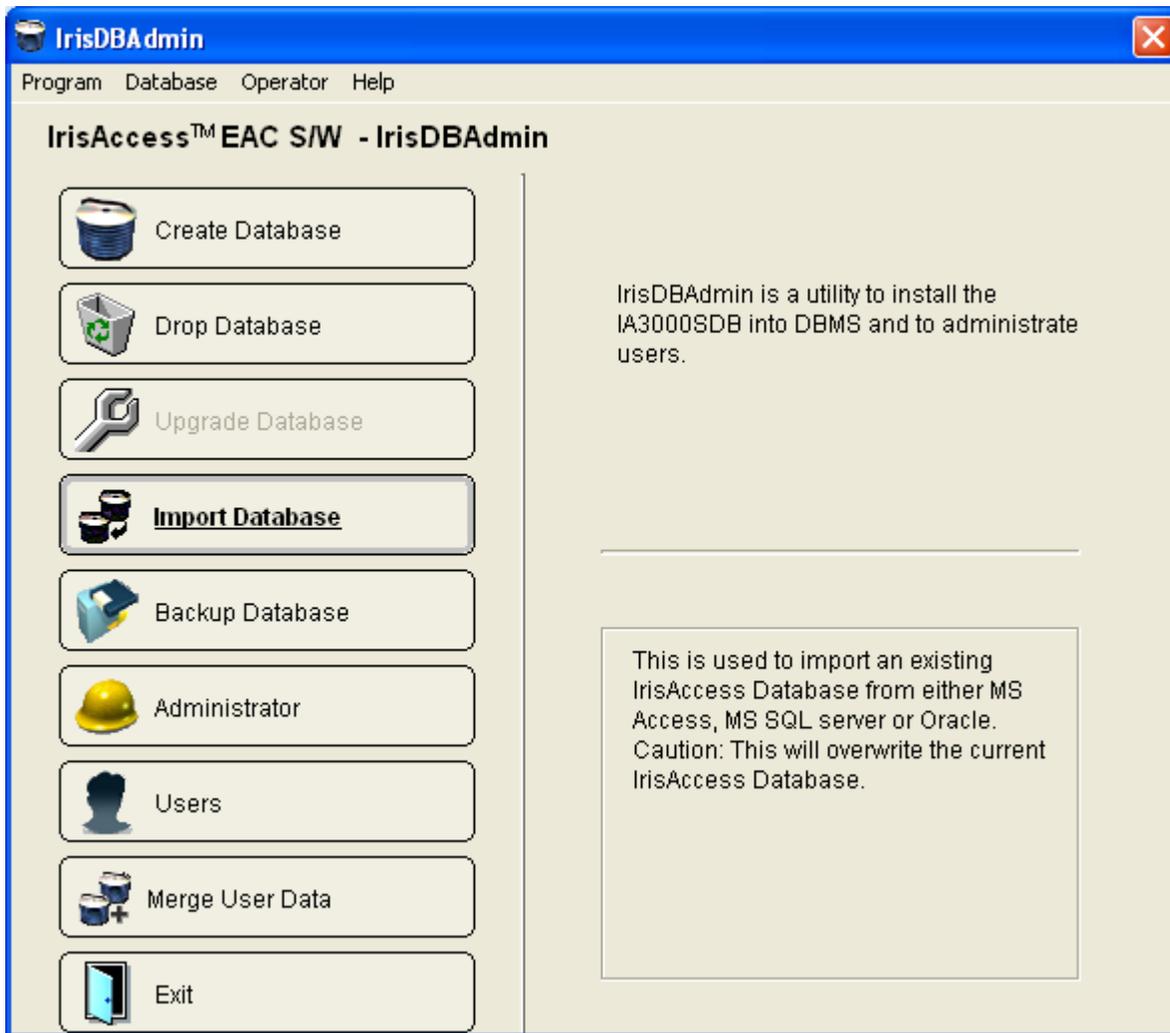


4. If the database is dropped successfully, the window shown below will display.

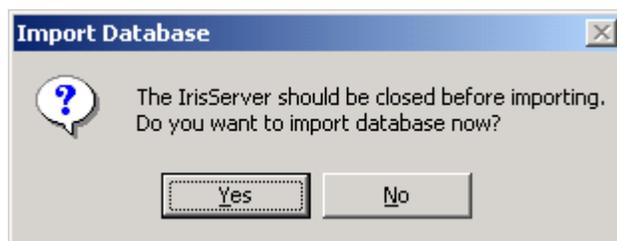


7.1.4.4 Importing Database

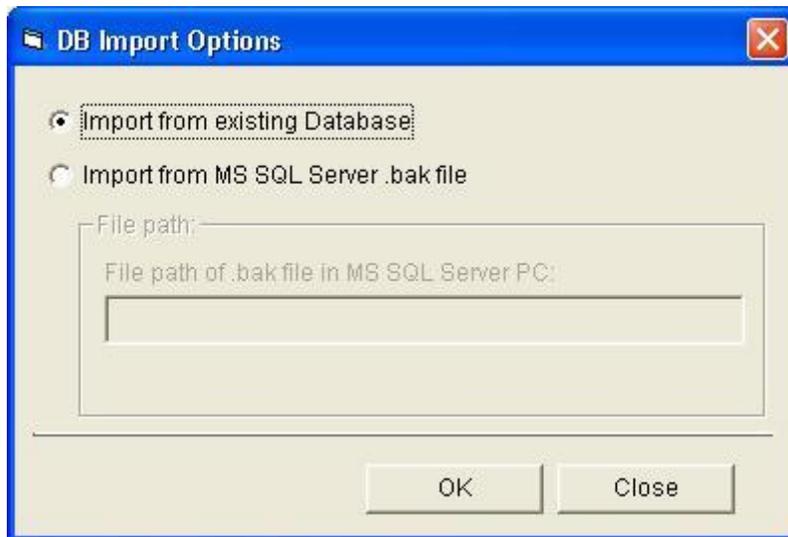
IrisDBAdmin allows users to import an existing IrisServer database from MS Access, MS SQL server or Oracle.



1. Click on the **Import Database** button or select the **Import Database** item in the **Database(D)** menu item in the menu bar and the next window will open to confirm the import of the **IrisServer** database.

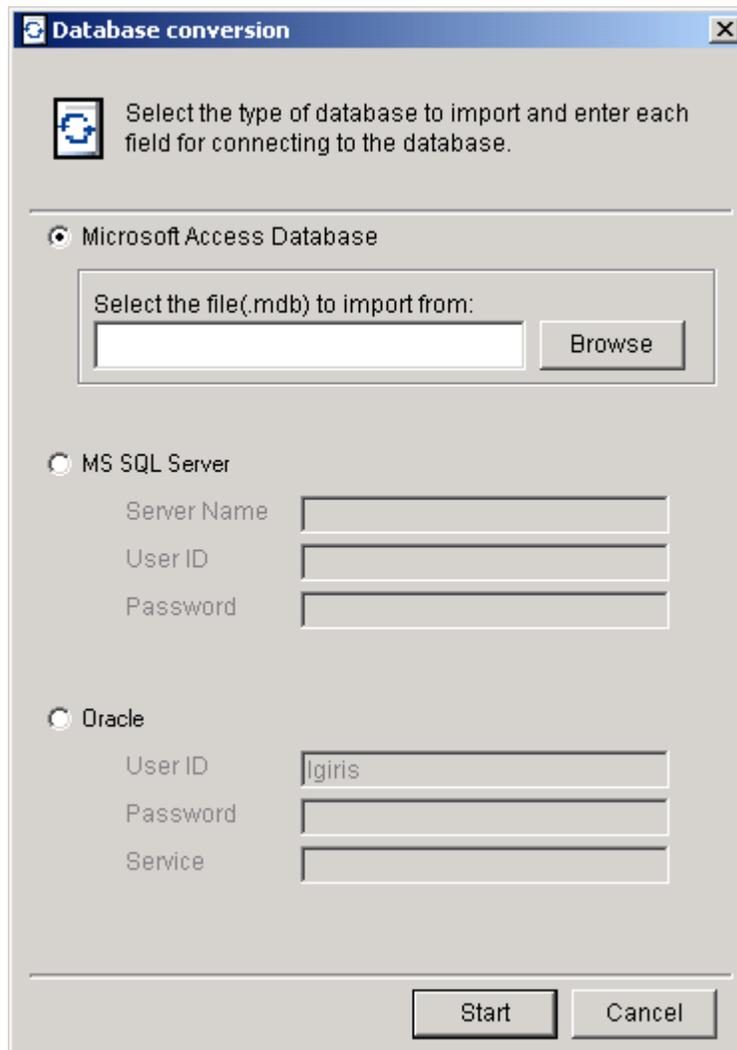


Click on the Yes button and next window will open

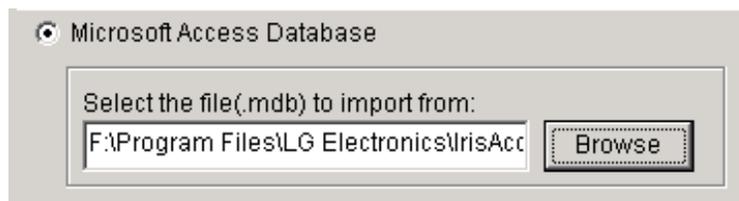


DB can be import by using existing Database or from MS SQL Server .bak file.

If the selected option is "Import from existing Database" and click OK next window will open.



2. Select the type of database to import and enter the information into each field to connect to the database.
 - a. If **importing the IrisServer database from a MS Access Database**, click on the **Browse** button and select the database file.



- b. If importing the IrisServer database from MS SQL Server, enter the Server Name (or IP Address), ID and Password for the MS SQL Server that you want to connect to. The following figure is a sample for connecting to the MS SQL Server named "irisserver".

MS SQL Server

Server Name: irisserver

User ID: sa

Password: *****

- ◆ Server name is the name of the computer that **MS SQL Server** is installed on.
 - ◆ Only **MS SQL Server** administrators can connect to **MS SQL Server** by using ID and password that are registered in **MS SQL Server**.
 - ◆ User ID is case sensitive.
- c. In case of importing the **IrisServer** database from **Oracle**, enter the **ID**, **Password** and **Service Name** for the **Oracle** server that you want to connect to. The following figure is a sample for connecting to the **Oracle** server named “oracle_irisserver”.

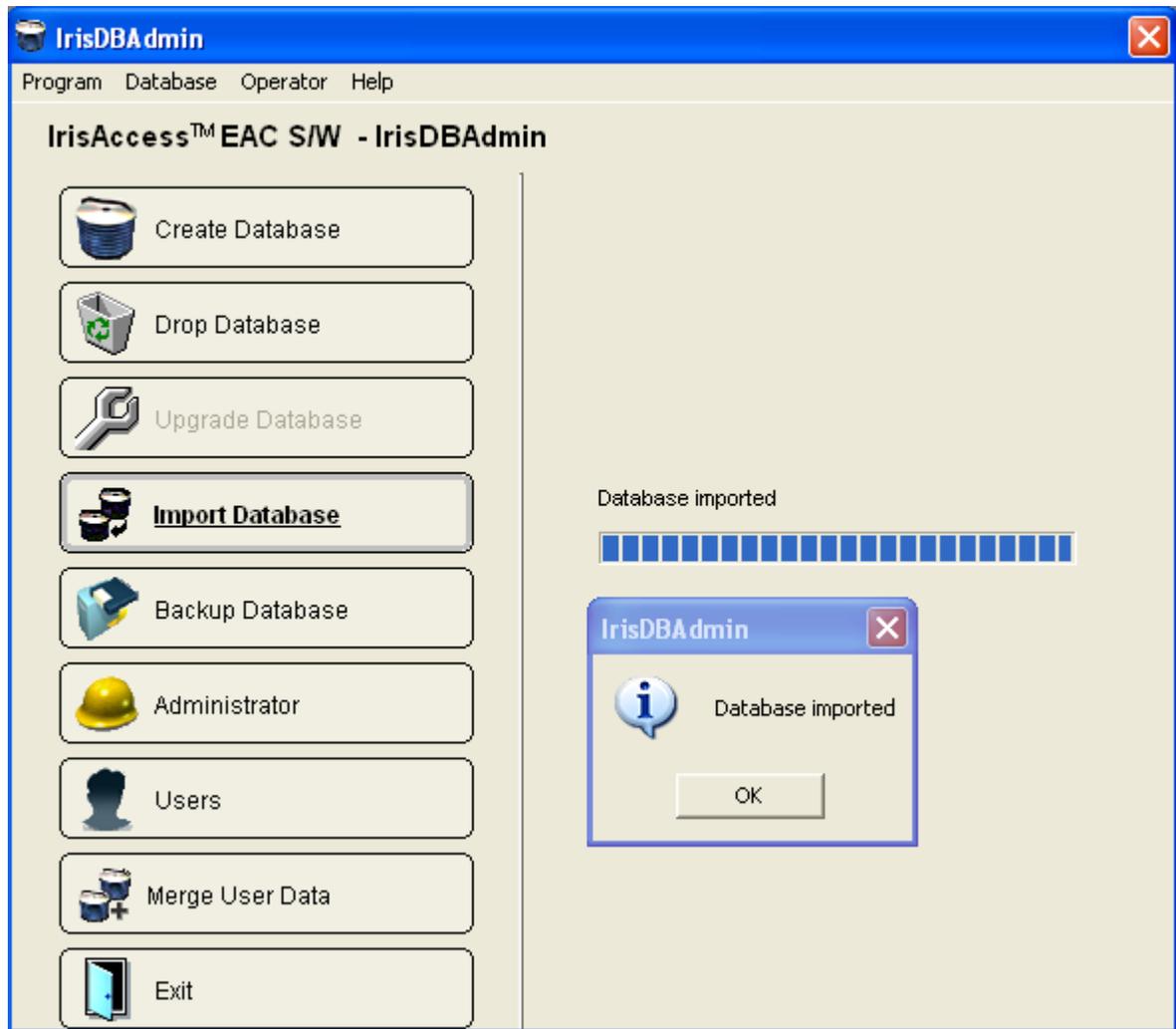
Oracle

User ID: lgiris

Password: *****

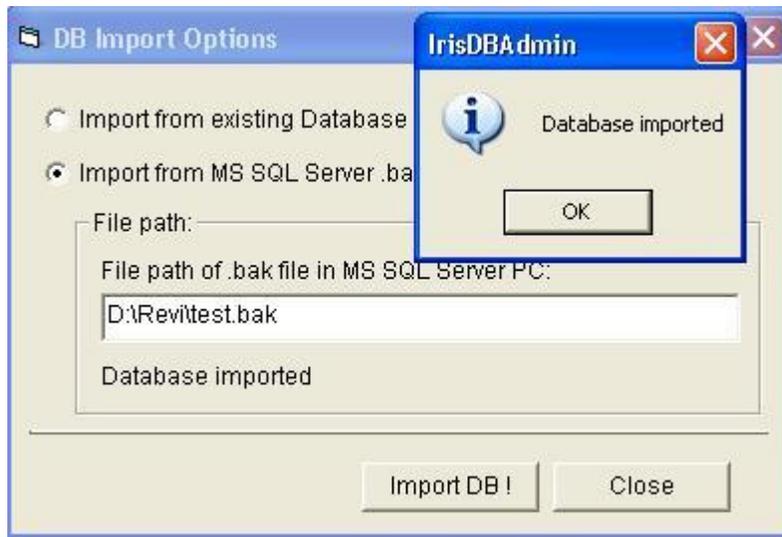
Service: oracle_irisserver

- ◆ In order to use **IrisDBAdmin for Oracle**, the **OO4O** (Client for Windows 98/NT/2000/XP) must be installed on the **IrisDBAdmin** computer first.
 - ◆ You can install OO4O for Windows 98/NT/2000/XP though EAC S/W CD package.
 - ◆ The name of the installation program is Oracle Universal Installer 2.2 and we recommend the administrator type installation.
 - ◆ After installation, set the Service Name for Oracle though the Enterprise Manager Console.
3. Click on the **Start** button
 4. If the **IrisServer** database was imported successfully, the next window will display.



If the selected option is "Import from MS SQL Server .bak file" and click "Import DB!" for import.

1. Enter the file path of .bak file in MS SQL Server PC.
2. Click "Import DB!" button for import.
3. If the IrisServer database is imported successfully, you will see the window below.



*Note:

 If IrisDBAdmin fails to connect to database, the following messages will display on the screen.



You can create a backup of your database file to prevent data loss caused by disk failures, power outages, virus infections and other potentially damaging events. The backup database created by this process will include the users, operators, remotes, holidays, time groups and remote groups. Refer to 2.6.2.3 Database Backup.

7.1.4.5 Database Backup

You can create a backup of your database file to prevent data loss caused by disk failures, power outages, virus infections and other potentially damaging events. The backup database created by this process will include the users, operators, remotes, holidays, time groups and remote groups.

IrisDBAdmin provides two formats for taking EAC DB backup. One is "Backup in MS Access database format (.mdb)" and second one is "Backup in MS SQL Server database format (.bak file)".

For backup in MS Access format (.mdb file) refer "Database backup" under "IrisDBAdmin for MS ACCESS Database" section.

For backup in MS SQL Server format (.bak file) refer the steps below.

1. Select the "Backup in MS SQL Server database format (.bak file)" option from below window.

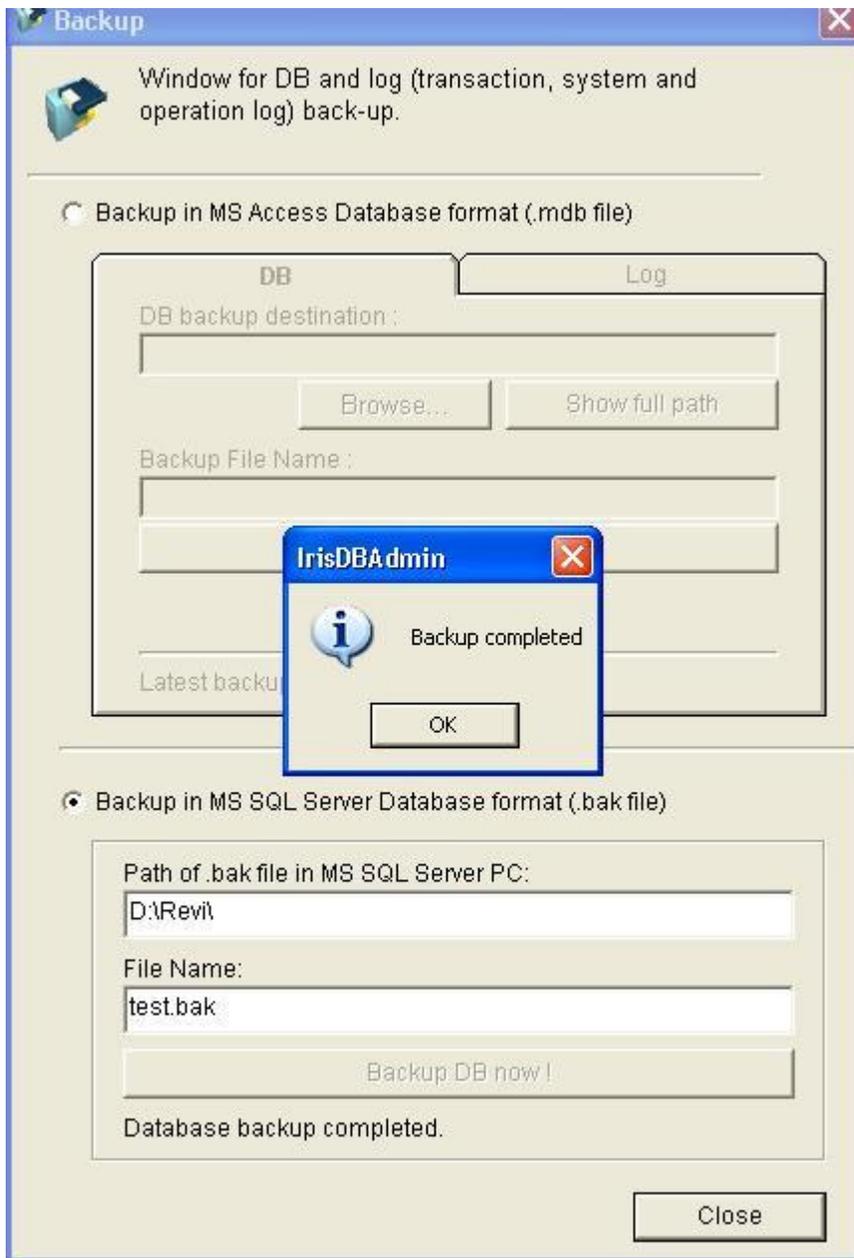
The screenshot shows a "Backup" dialog box with the following elements:

- Title bar: Backup
- Subtitle: Window for DB and log (transaction, system and operation log) back-up.
- Radio buttons:
 - Backup in MS Access Database format (.mdb file)
 - Backup in MS SQL Server Database format (.bak file)
- Section for MS Access Database format (disabled):
 - Tabs: DB (selected), Log
 - DB backup destination: [Text Field]
 - Buttons: Browse..., Show full path
 - Backup File Name: [Text Field]
 - Button: Backup DB now!
 - Latest backup-date: [Text Field]
- Section for MS SQL Server Database format (active):
 - Path of .bak file in MS SQL Server PC: [Text Field]
 - File Name: [Text Field]
 - Button: Backup DB now!
- Close button at the bottom right.

2. Enter the path of .bak file in MS SQL Server PC. For the successful DB Backup, the .bak file will be created in the MS SQL Server PC.

3. Enter the name of the backup file.

4. Click on the "Backup DB now!" button. If the DB backup is successfully completed, the following window will display.



Note: Transaction Log, System Log and Operator Log data is also copied to .bak file. So, you may consider taking backup of log data into .mdb file using log backup feature (Refer next section) before taking backup in .bak file.

7.1.4.6 Log Backup

You can create a backup of your log files - transaction, system and operation log file. **The backup log file's name created after log back up must not be changed.** If this name is changed, **IrisServer** cannot filter the information from the backup log files. **If you do a backup of the log, the logs will be deleted from the database.** Refer to 2.6.2.4 Log Backup.

7.1.4.7 Administrator

When **IrisAccess** applications access a **MS SQL Server** database by using **IrisServer**, a valid **MS SQL Server** account is required to access the database. A **MS SQL Server** administrator can change the ID and/or password of the account by using this feature. The default ID and password of the account is created when IA3000SDB is created.

1. Click the **Administrator** button on the **IrisDBAdmin** main window or select the **Administrator** item in the **Operator (O)** menu item in the menu bar to change the ID or password of an account that will be used to access the **MS-SQL Server** database. The following **Administrator** window will be open on the screen.



2. Modify the ID in the **New ID** field if you want to change the ID of the account. ID may consist of a maximum of 10 characters that are numbers and/or capital or lower case letters.
3. Enter the current password of the account in the **Current Password** field.
4. If you want to change the password of the account, click the **Change password** button. Enter the new password of the account in the **New Password** field and confirm the password in the **Confirm Password** field. Password may consist of a maximum of 10 characters that are numbers and/or capital or lower case letters.
5. Click the **OK** button to change the ID or password of the account.
6. Click **Cancel** button to cancel the change of the ID or password of the account.

7.1.4.8 User

When external applications access the **MS SQL Server** database, a user account is required to access the database. A **MS SQL Server** administrator can add or delete the user accounts by using this feature. Also he or she can change the password for user accounts and configure access rights for each database table for the users. Click the **User** button on the **IrisDBAdmin** main window or select the **User** item in the **Operator(O)** menu item in the menu bar to use this feature. The following **User** window will open on the screen.



■ Adding User Account

1. Click the **Add User** button on the **User** window to add a user account. The following **Add User** window will open on the screen.



2. Enter a User ID in the **User ID** field. ID may consist of a maximum of 10 characters that are numbers and/or capital or lower case letters.
3. Enter a password for the account in the **Password** field and confirm the password in the **Confirm Password** field. The password may consist of a maximum of 10 characters that are numbers and/or capital or lower case letters.
4. Click the **OK** button to add the user account with the entered ID and password.
5. The addition of a new user account can be cancelled by clicking the **Cancel** button.

■ *Setting Access Rights*

1. Click the User ID of the user whose access rights you want to configure, and then click the **Set Access Right** button on the **User** window. The following **Set Access Right** window will display on the screen.

Access rights must be set for each user to access each table of IA3000SDB.

User ID :

Table Name	SELECT	UPDATE	INSERT
TUser	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
TPicture	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
TOperator	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TTransactionLog	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
TSystemLog	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
TOperatorLog	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
TRemoteNode	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TEnrollNode	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TManagerNode	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TMonitorNode	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Check All Clear All

OK Cancel

2. Give access rights each for database table to the user by selecting the check boxes. For example, the access rights of a user are shown in the above window. The user may select, update and insert the data in TUSER, TPICTURE, TOPERATOR, TTRANSACTIONLOG, TSYSTEMLOG and TOPERATORLOG database table. The user

may only select the data in TREMOTENODE, TENROLLNODE, TMANAGERNODE and TMONITORNODE database table.

3. All access rights can be selected by clicking the **Check All** option button.
4. All selected access rights can be removed by clicking the **Clear All** option button.
5. Click **OK** button to set the access rights for the user after selecting the access rights.
6. The assigning of access rights to a user may be cancelled by clicking the **Cancel** button.

■ **Changing Password**

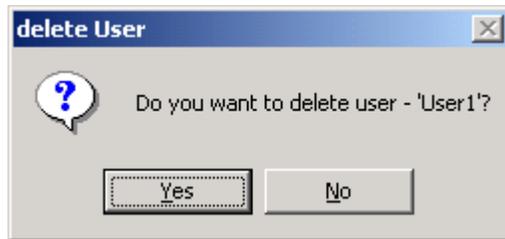
1. Click the User ID of the user whose password you want to change, and then click the **Change Password** button on the **User** window. The following **Password** window will display on the screen.



2. Enter the current password of the account in the **Current Password** field. The password is case sensitive.
3. Enter the new password of the account in the **new Password** field and confirm the password in the **Confirm Password** field. The password can consist of a maximum of 10 characters that are numbers and/or capital or lower case letters.
4. Click the **OK** button to change the password.
5. The password change can be cancelled by clicking the **Cancel** button.

■ **Deleting user account**

1. Click the User ID of the user whose account you want to delete, and then click the **Delete User** button on the **User** window. A confirmation window will open on the screen as shown in the figure below.



2. Click the **Yes** button on the confirmation window to delete the user account.
3. Accidental deletion of the user account may be avoided by clicking **NO** button.
4. If the deletion is completed, the result window below will display on the screen.



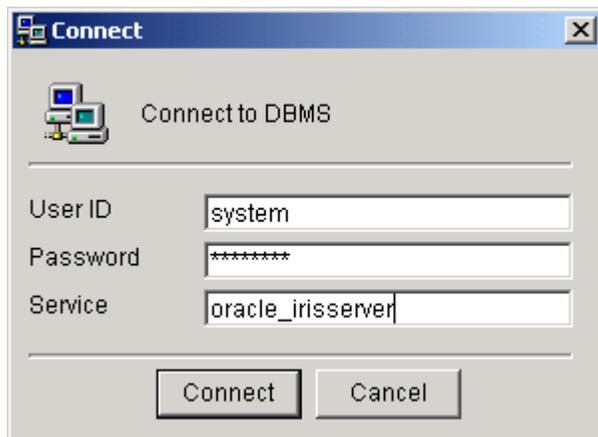
7.1.4.9 Merging User Data

Refer 2.6.2.5 Merge User Data

7.1.5 IrisDBAdmin for Oracle

1. When using **IrisDBAdmin** with an **Oracle** database, the following **Connect** window will open.

*** Note: In order to use Oracle as the database type, the OO4O (Oracle Objects For OLE) must be installed on the IrisServer PC.**



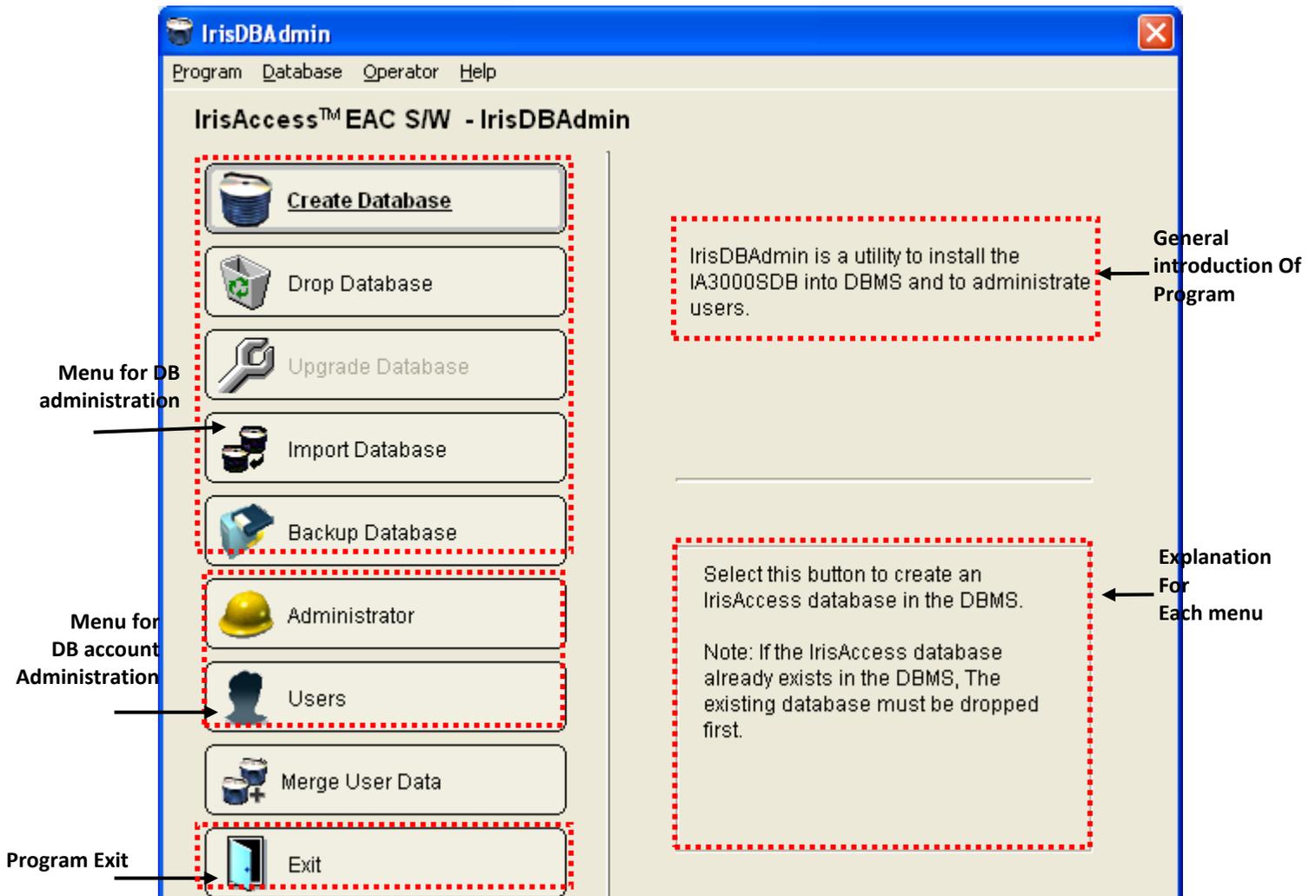
- ◆ Enter the **User ID** and **Password** of the **Oracle** Server in each field.
- ◆ Enter the **Service name** of an **Oracle** service that is used in **Oracle** Server.
- ◆ Click the **Connect** button to connect to the **Oracle**.

2. If **IrisDBAdmin** cannot connect to the **Oracle** server, the following messages will display on the screen.



- ◆ In order to use IrisDBAdmin for **Oracle**, OO4O (Client for Windows 98/NT/2000/XP) must be installed on the **IrisDBAdmin computer** first.
- ◆ You may install OO4O for Windows 98/NT/2000/XP though EAC S/W CD package.
- ◆ The name of the install program is Oracle Universal Installer 2.2 and we recommend using the administrator type installation.
- ◆ After installation, set the Service Name for **Oracle** though the Enterprise Manager Console.

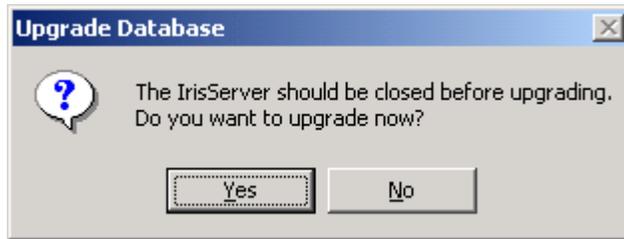
3. The following **IrisDBAdmin** main window will be shown after a successful connection.



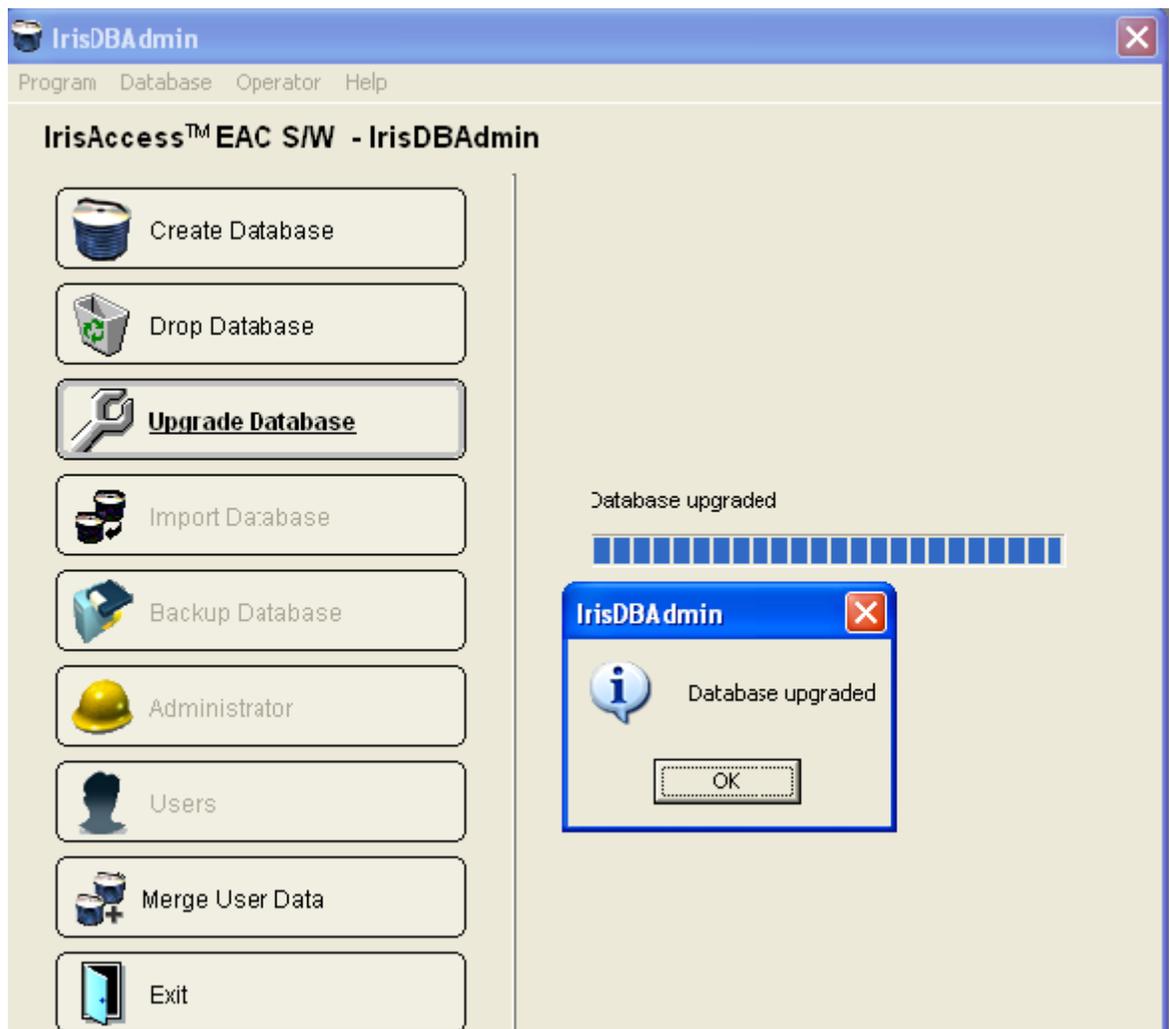
7.1.5.1 Upgrading Database

You may upgrade an **Iris Server** database as follows.

1. Click on the **Upgrade Database** button and you will see the confirmation window shown below.



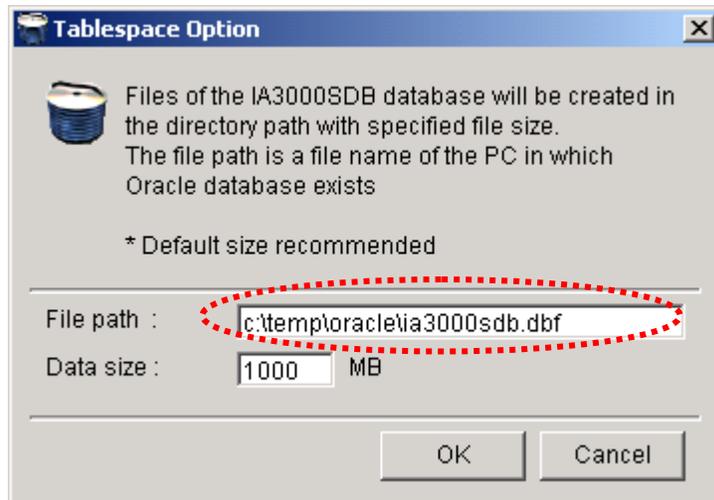
2. Click on the **Yes** button to continue **Upgrading** the database.
3. If **IrisDBAdmin** upgrades the **IrisServer** database successfully, you will see the window below.



7.1.5.2 Creating Database

You can create an IrisServer DB as follows.

1. Click the **Create IA3000SDB** button or select the **Create Database** item in the **Database(D)** menu item on the menu bar to create a database.
2. If **IA3000SDB** doesn't exist the **Oracle** server, the following **Tablespace Option** window will display on the screen.



*Note:

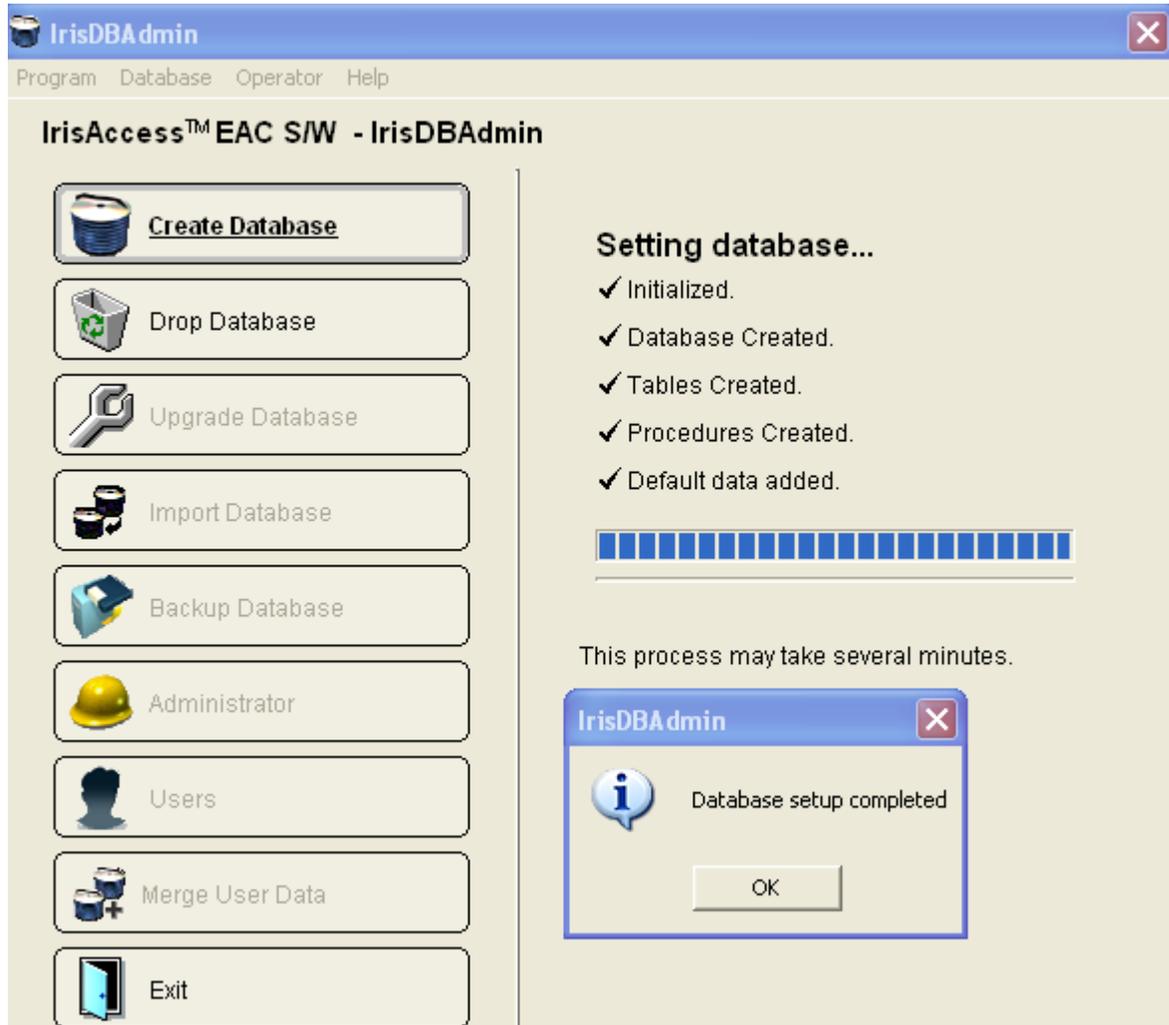
If **IA3000SDB** already exists in **Oracle** Server, the following message dialog box will open on the screen. If you want to drop the current database from **Oracle** Server and create a new database, click on the **OK** button.



Click **Drop Database** button on **the IrisDBAdmin for Oracle** main window.
(Please refer to section 2.6.4.3 Dropping Database in this Document)

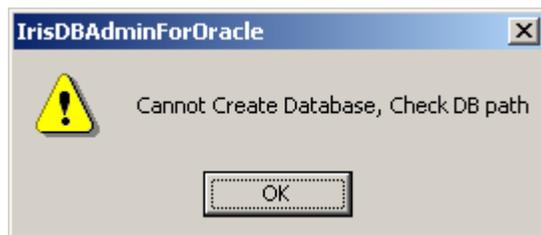
3. Enter the File path of the folder in which the database file will be located.
4. When you create an **IrisServer** database, you can set the Data size

- ◆ **Data Size:** This option specifies the size of the database file. You can specify the size in megabytes. The minimum value is 1 MB. The default value is 100 MB for the primary file.
5. After specifying the File path and the Data Size, click on the **OK** button. The following window will be displayed on the screen.



*Note:

If the file already exists in the File path or the file directory is invalid, the following window will display on the screen.

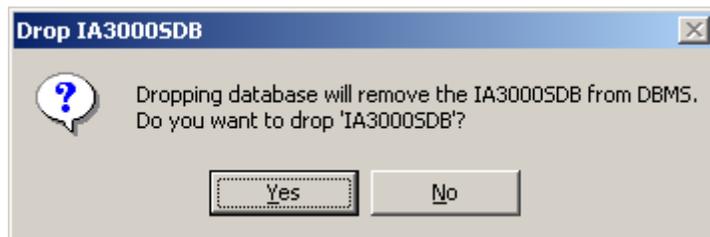


Click on the **OK** button, and re-enter the correct **File path** in the **Tablespace Option window**

7.1.5.3 Dropping Database

You can drop a database when you no longer need it. Dropping a database deletes the database and the disk files used by the database.

1. Click the **Drop Database** button on the **IrisDBAdmin** main window to drop the database. A confirmation window will display on the screen as shown in the figure below.



2. Click on the **Yes** button of the confirmation window to drop the database.
3. Accidental dropping of the database can be avoided by clicking on the **NO** button.

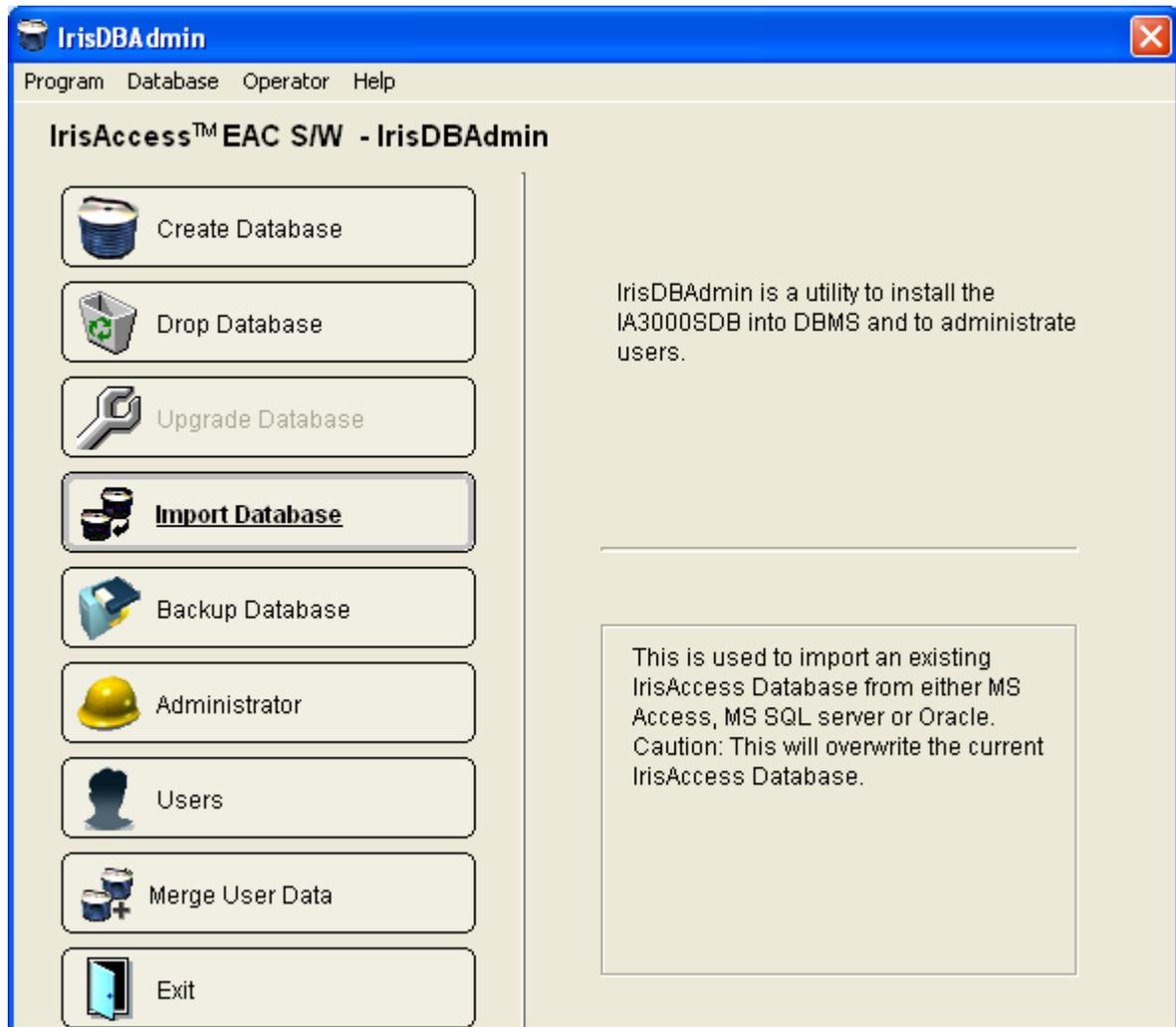
*Note:

You cannot drop a database that is open for reading or writing by the **IrisServer**. If the database is in use and you click the **OK** button on the above confirmation window, an error message box appears. For example, if the user **lgiris** is currently connected to the **IrisServer** using the database that you want to drop, the following window is displayed on the screen.

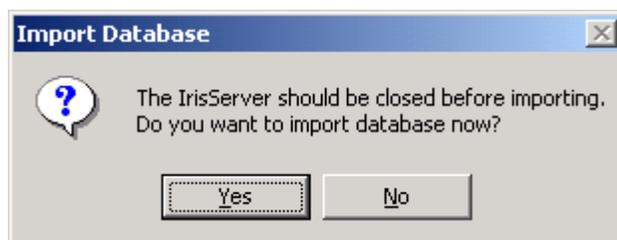


7.1.5.4 Importing Database

IrisDBAdmin allows a user to **import an existing IrisServer DB from MS Access, MS SQL server or Oracle.**



1. Click on the **Import Database** button or select the **Import Database** item in the **Database(D)** menu item in the menu bar and you will see the next window confirming the database import.



2. Click on the **Yes** button and **IrisDBAdmin** opens the window shown below.

3. Select the type of database to import from and enter the appropriate information into each field to connect to the database.
- A. If importing the **IrisServer database from a Microsoft Access Database**, click on the **Browse** button and select the database file.

- B. If **importing the IrisServer database from MS SQL Server**, enter the **Server Name** (or IP Address), **ID** and **Password** for the **MS SQL Server** that you want to import from. The following figure is a sample for connecting to the **MS SQL Server** named "irissserver".

MS SQL Server
 Server Name:
 User ID:
 Password:

- ◆ Server name is the name of the computer **MS SQL Server** is installed on.
- ◆ Only **MS SQL Server** administrator(s) can connect to **MS SQL Server** using IDs and passwords that are registered in **MS SQL Server**
- ◆ The User ID is case sensitive.

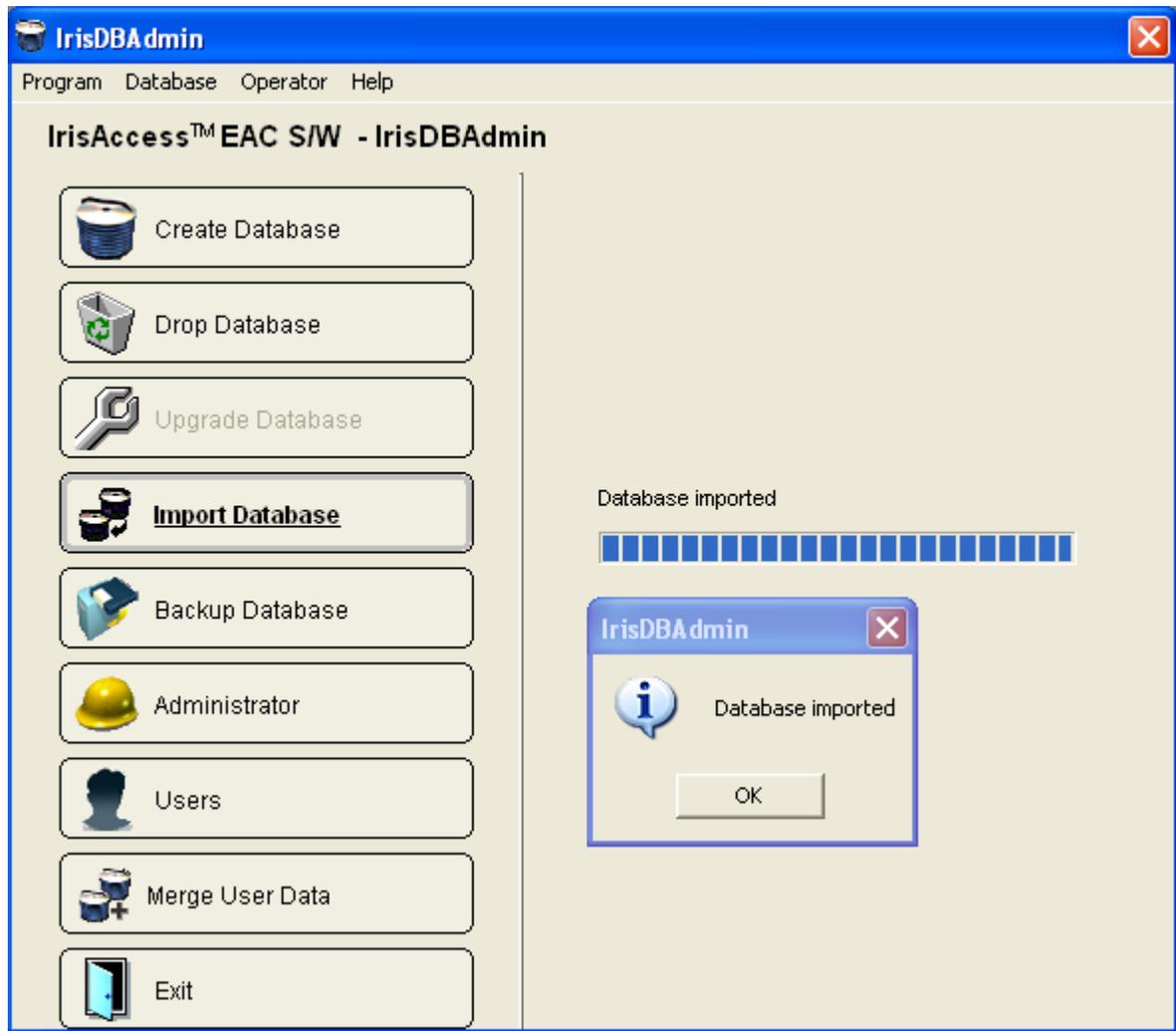
- C. If importing the IrisServer database from Oracle, enter the ID, Password and Service Name for the Oracle server that you want to import from. The following figure is a sample for connecting to the Oracle named "oracle_irissserver."

Oracle
 User ID:
 Password:
 Service:

- ◆ In order to use **IrisDBAdmin** with **Oracle**, the **OO4O** (Client for Windows 98/NT/2000/XP) must be installed on the same computer first.
- ◆ You can install OO4O for Windows 98/NT/2000/XP though EAC S/W CD package.
- ◆ The name of the install program is Oracle Universal Installer 2.2 and we recommend the administrator type installation.
- ◆ After installation, set the Service Name for Oracle though the Enterprise Manager Console.

4. Click on the **Start** button.

5. If the **IrisServer** database is imported successfully, you will see the next window.



*Note:

If IrisDBAdmin fails to connect to the database, the following messages will be displayed on the screen.



7.1.5.5 Database Backup

You may create a backup of your database file to prevent data loss caused by disk failures, power outages, virus infections and other potentially damaging events. The backup database created by this process will include users, operators, remotes, holidays, time groups and remote groups. Refer to section 2.6.2.3 Database Backup.

7.1.5.6 Log Backup

You may create a backup of your log files - transaction, system and operation log files. **The backup log file's name created after the log back up must not be changed.** If this name is changed, **IrisServer** cannot filter the information from the backup log files. **If you backup the logs, the logs will be deleted in the database.** Refer to section 2.6.2.4 Log Backup.

7.1.5.7 Administrator

When an **IrisAccess** application accesses the **Oracle** Server database through IrisServer, a valid account is required to access the database. An **Oracle** Server administrator can change the password of the account by using this feature. The Default ID of the account is created when IA3000SDB is created.

1. Click the **Administrator** button on the **IrisDBAdmin** main window or select the **Administrator** item in the **Operator (O)** menu in the menu bar to change the password of an account that is used to access the **Oracle** Server database. The following **Administrator** window will open on the screen.



2. If you want to change the password of the account, click the **Change password** button.
Enter the new password of the account in the **New Password** field and confirm the password in the **Confirm Password** field. Passwords may consist of a maximum 10 characters that are numbers and/or capital or lower case letters.
3. Click the **OK** button to change the password of the account.
4. Click the **Cancel** button to cancel the password change.

7.1.5.8 User

When an external application accesses an **Oracle** Server database, a user account is required to access the database. An **Oracle** Server administrator can add or delete the user accounts by using this feature. Also the administrator can change the password for user accounts and set the access rights for each database table. Click the **User** button on the **IrisDBAdmin** main window or select the **User** item in the **Operator (O)** menu in the menu bar to use this feature. The following **User** window will open on the screen.



■ Adding User Account

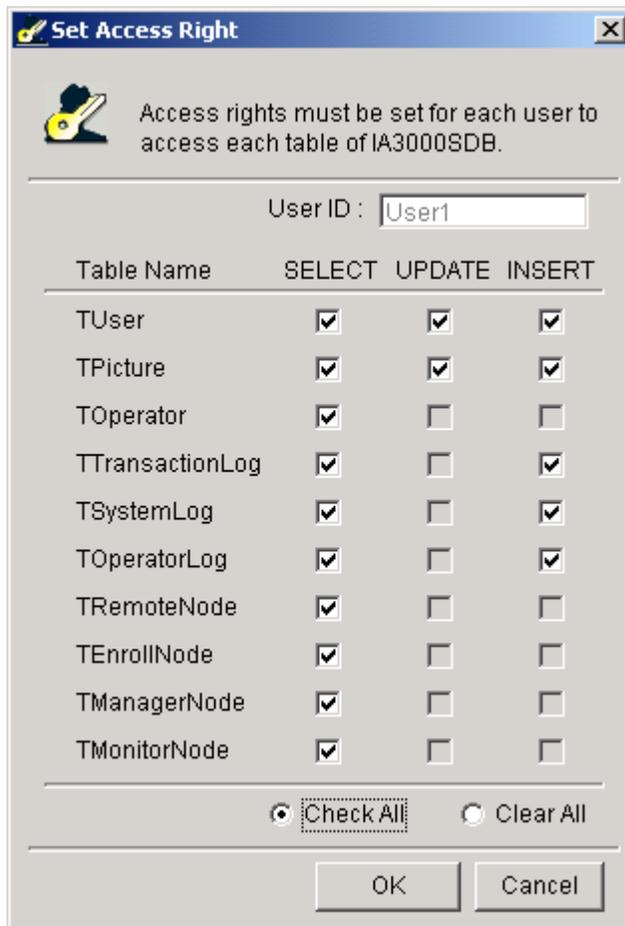
1. Click the **Add User** button on the **User** window to add a user account. The following **Add User** window will be displayed on the screen.



2. Enter a User ID in the **User ID** field. ID may consist of a maximum of 10 characters that are numbers and/or capital or lower case letters.
3. Enter a password for the account in the **Password** field and confirm the password in the **Confirm Password** field. The password may consist of a maximum of 10 characters that are numbers and/or capital or lower case letters.
4. Click the **OK** button to add the user account with the entered ID and password.
5. The addition of the new user account may be cancelled by clicking the **Cancel** button.

■ **Setting Access Rights**

1. Click the User ID of the user whose access rights you want to set, and then click the **Set Access Right** button on the **User** window. The following **Set Access Right** window will be displayed on the screen.



2. Set the access rights for each database table by selecting the check boxes.
3. All access rights may be selected by checking the **Check All** option button.
4. All selected access rights can be released by checking the **Clear All** option button.
5. Click the **OK** button to set the access rights of the user.
6. The configuration of access rights can be cancelled by clicking the **Cancel** button.

■ *Changing Password*

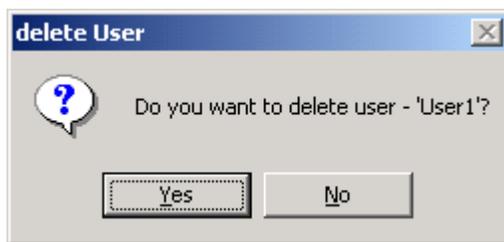
1. Select the User ID of the user whose password you want to change, and then click the **Change Password** button on the **User** window. The following **Password** window will open on the screen.



2. Enter the new password of the account in the **new Password** field and confirm the password in the **Confirm Password** field. The password may consist of a maximum of 10 characters that are numbers and/or capital or lower case letters.
3. Click the **OK** button to change the password.
4. The password change can be cancelled by clicking the **Cancel** button.

■ **Deleting User Account**

1. Select the User ID of the user whose account you want to delete, and then click the **Delete User** button on the **User** window. A confirmation window will be displayed on the screen as shown in the figure below.



2. Click the **Yes** button on the confirmation window to delete the user account.
3. Accidental deletion of the user account may be avoided by clicking the **NO** button.
4. If the deletion is completed successfully, the following window will open on the screen.



7.1.5.9 Merging Database

Refer 2.6.2.5 Merge Database.

8. IrisICUAdmin4000

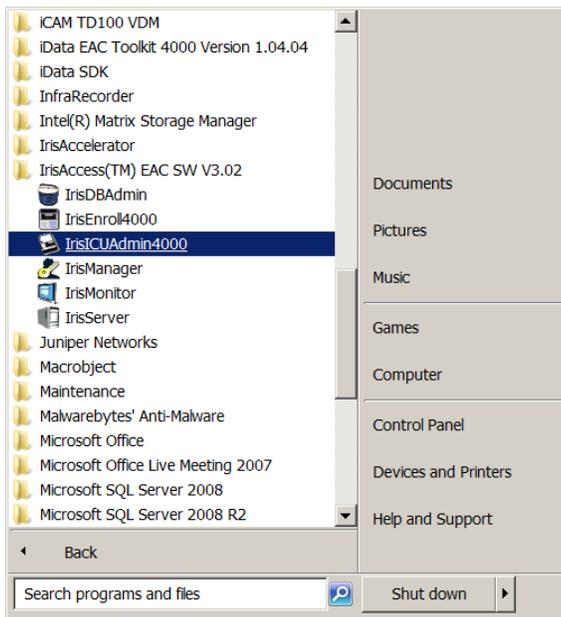
8.1 IrisICUAdmin4000

8.1.1 IrisICUAdmin40000 Program usage

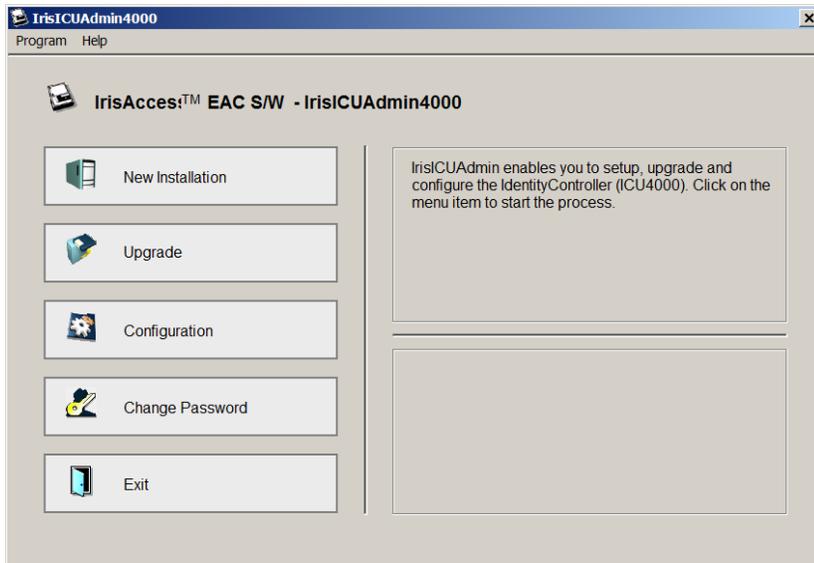
The ICUAdmin4000 application enables you to setup, modify, upgrade, and configure the IdentityController (ICU4000).

8.1.2 How to open IrisICUAdmin4000

To start the ICUAdmin4000, click on the IrisICUAdmin4000 menu item. The location of the program is shown in the figure below:



After starting, IrisICUAdmin4000 will open a new window, as illustrated in the following figure:

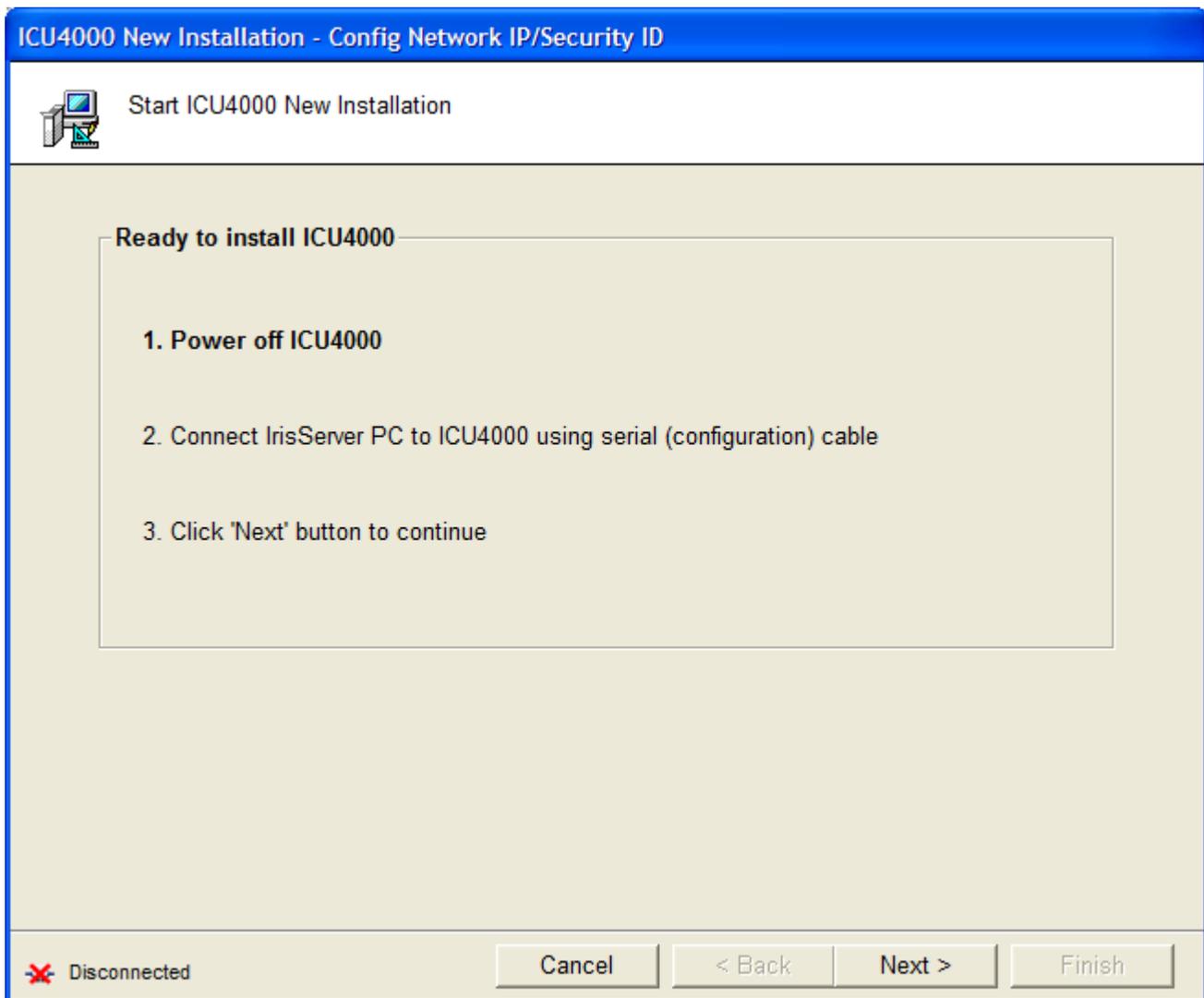


8.1.3 Description of Menu items in IrisICUAdmin4000

1. **New Installation** – Used for setup and initial configuration of an ICU4000 unit. The use of a provided “ICU Configuration Serial Cable” is needed for use with this option. This cable is required to perform a New Installation setup. (If the cable or use of Serial/Serial to USB is not available, the *ICU Admin Setup Utility program* may be used – available from the IrisID website at www.irisid.com).
2. **Upgrade** – Updates the ICU4000 controller unit(s) to the same version of EAC Software that is running/installed on the IrisServer. *Note: This is required after upgrading the iData EAC software version on the server PC.*
3. **Configuration** – Allows for modification of initially enabled channel settings within the ICU unit. Settings such as Remote unit IP, volume, Wiegand output settings, etc. are available (and configurable per channel per ICU).
4. **Change Password** – Allows for the password of the ICU unit to be changed. This is often used if the password has been forgotten or is unknown. *Note: The use of a provided “ICU Configuration Serial Cable” (provided with the ICU4000 unit) is required for use with this option. The password will be reset to the factory default if unknown.*
5. **Exit** – Closes out the application.

8.1.4 The ICUAdmin4000 New Installation Window

Select the “New Installation” button, the following window is displayed on the screen.



Click Next button to continue.

The following screen will appear.

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

Cancel < Back Next > Finish

Enter IrisServer IP Address, ICU IP Address, Gateway Address, Subnet Mask and click Next button. A warning message as shown below appears. Click OK and continue installation.

IrisICUAdmin 

 ICU4000 will allow the connection from only this Server (172.24.17.68) when Network IP/Security ID Configuration is finished.

It is not recommended to change IP address of this server PC.
If you want to change the IP address, you should setup 'ICU4000 New Installation', again!

OK

The following screen appears next.

ICU4000 New Installation - Config Network IP/Security ID

Configure iCAM Security ID

Security IDs

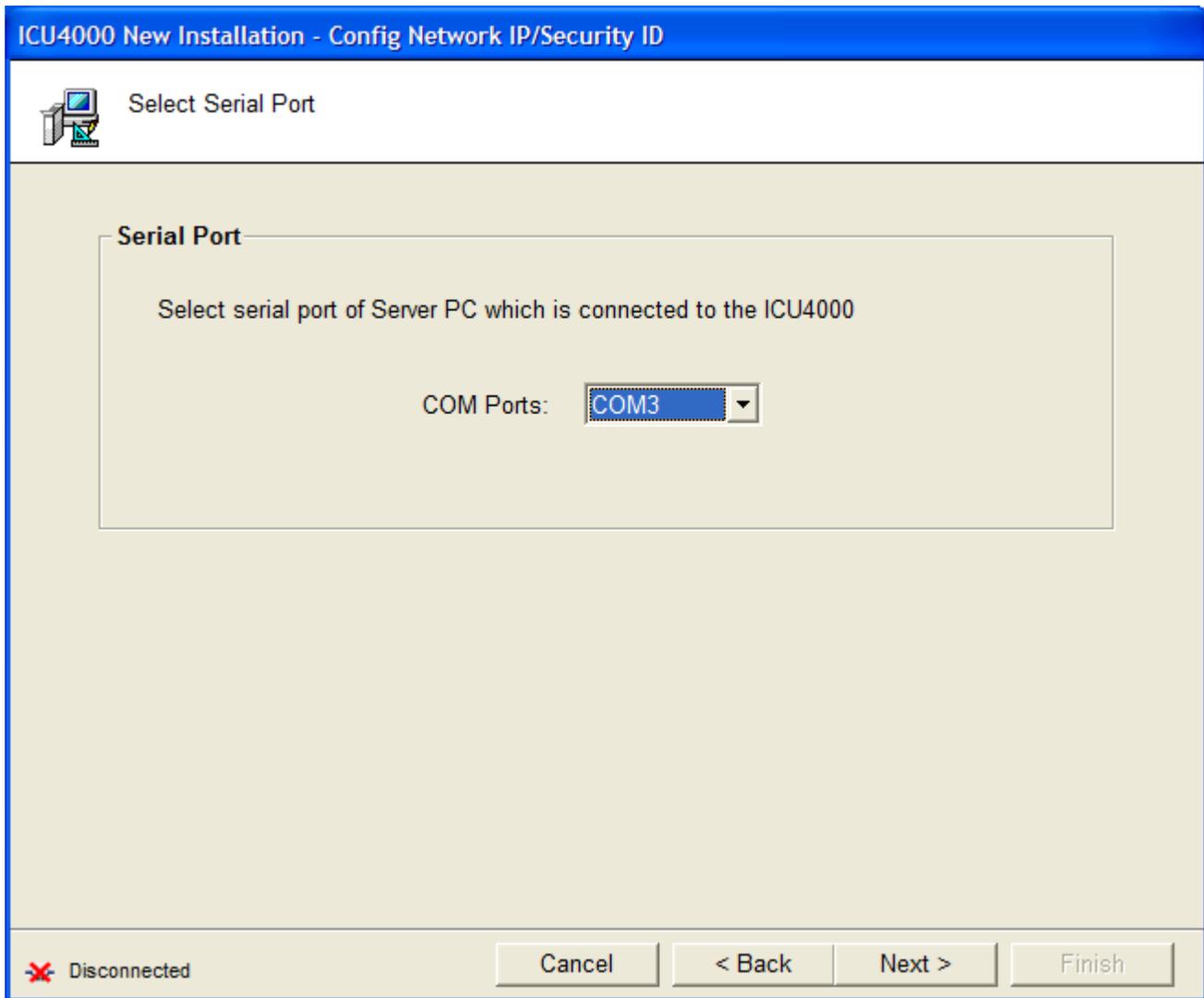
<u>Installed iCAM</u>	<u>Security ID</u>			
<input checked="" type="checkbox"/> iCAM 1	qqqq	qqqq	qqqq	qqqq
<input checked="" type="checkbox"/> iCAM 2	rrrr	rrrr	rrrr	rrrr
<input checked="" type="checkbox"/> iCAM 3	ssss	ssss	ssss	ssss
<input checked="" type="checkbox"/> iCAM 4	tttt	tttt	tttt	tttt

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

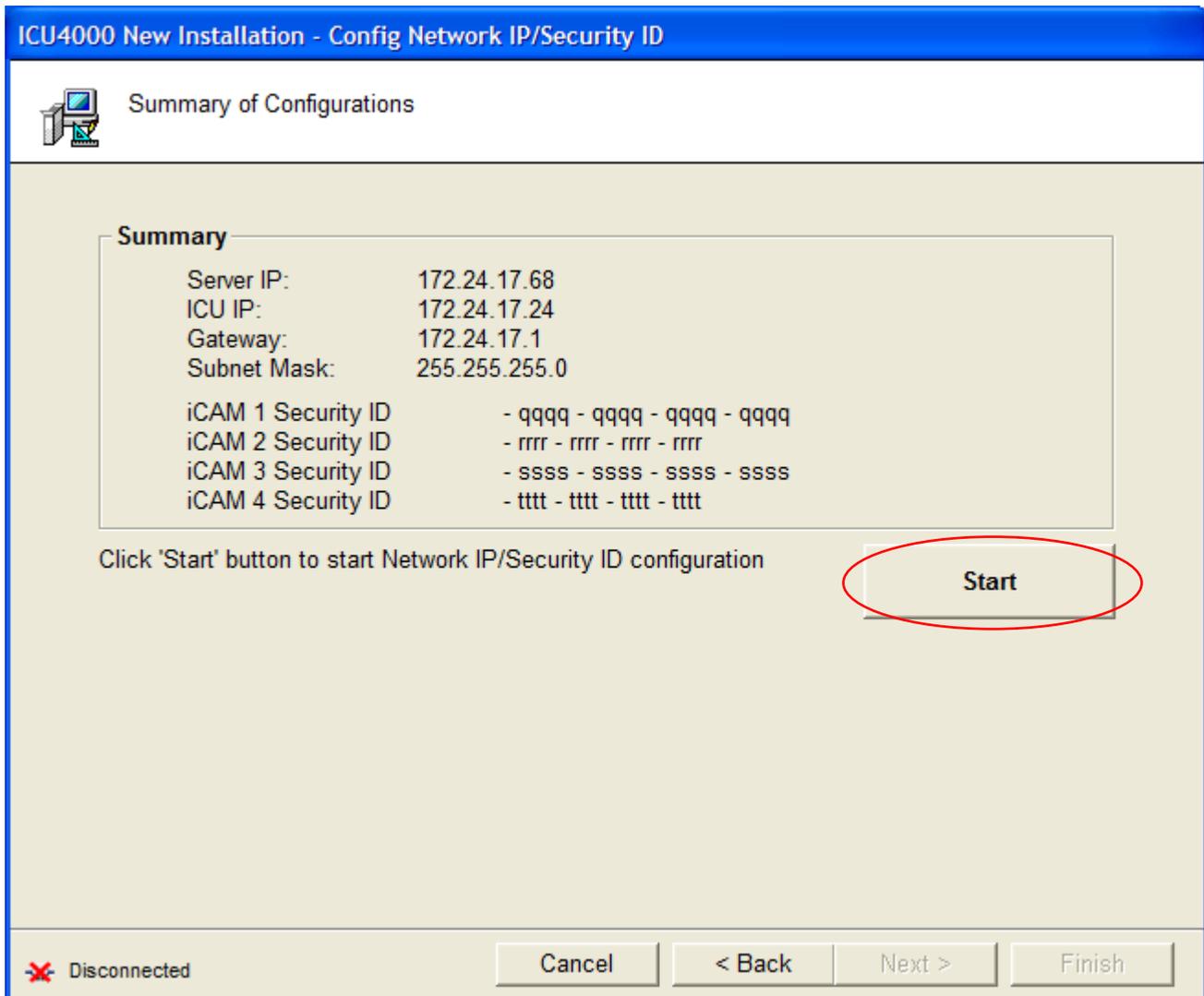
 Only select the iCAMs which are installed in this ICU. A unique security ID must be used for each iCAM connected in this system, this security ID can consist of numbers, upper and lower case letters and special characters. The security ID must be 16 characters long and is case sensitive. The security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

Disconnected

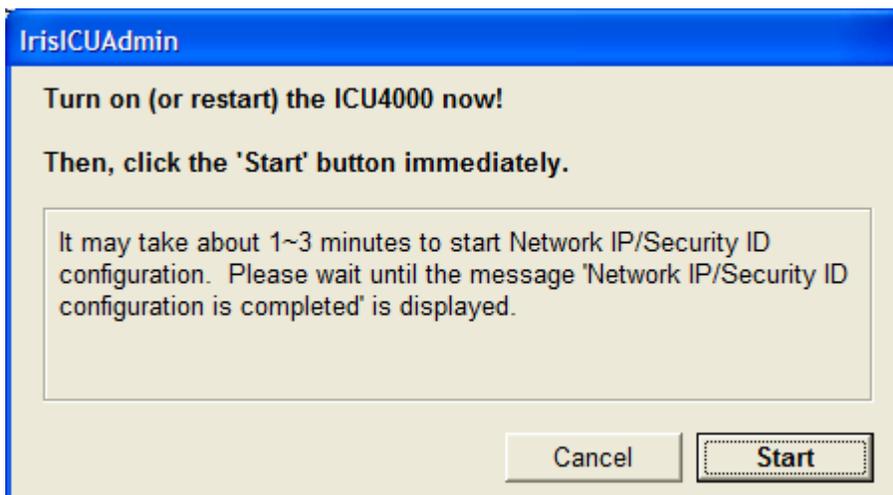
Enter Security IDs for iCAM1, iCAM2, iCAM3 and iCAM4. Click on next button. A screen to select serial port appears.

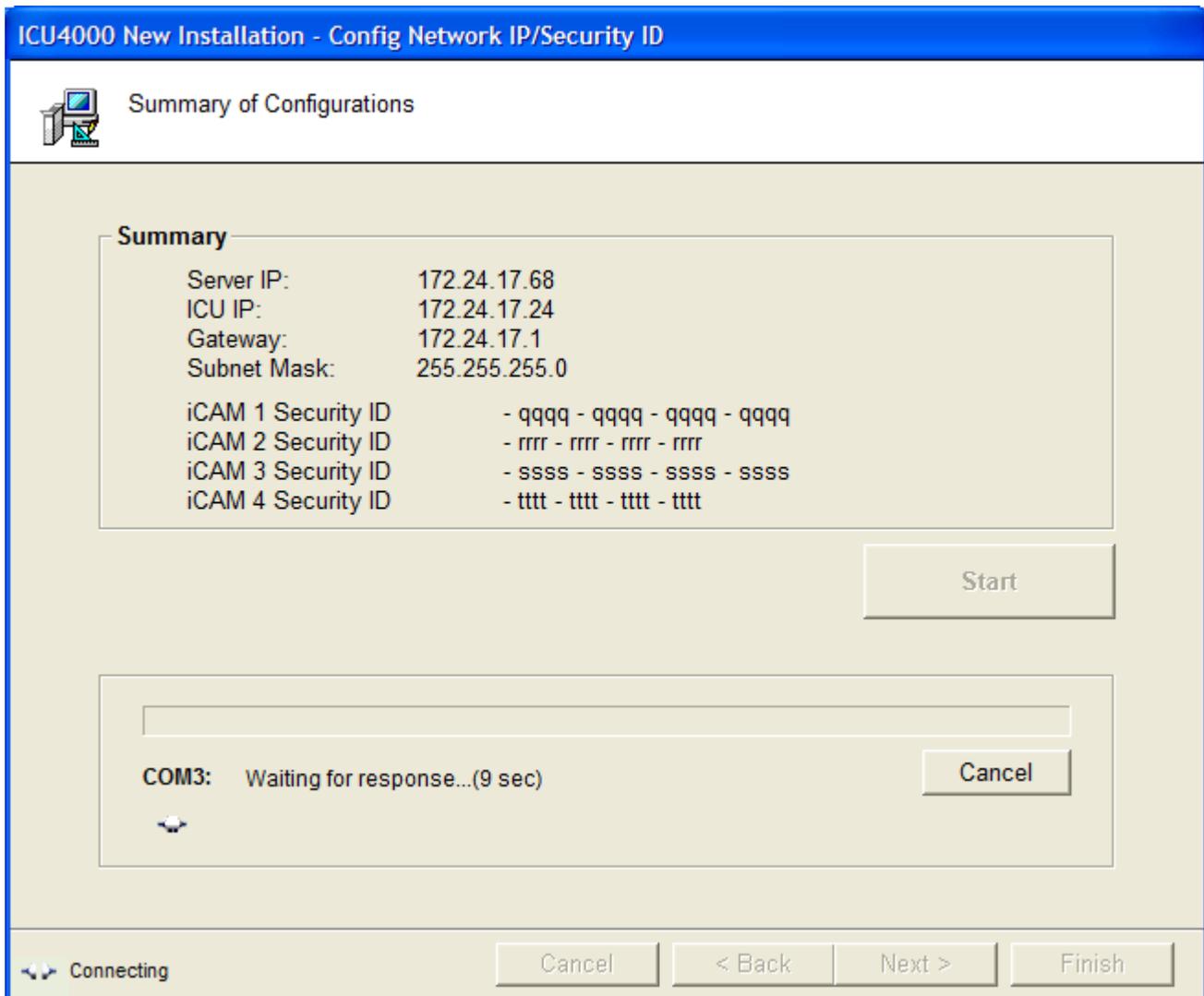


Select the serial port and click Next button. The settings summary screen appears as shown below.



Click on Start button to start new installation.





8.1.5 The ICUAdmin4000 Upgrade Window

Select the "Upgrade" button, the following window is displayed on the screen.

Upgrade ICU4000 EAC S/W

 Connect to the ICU (TCP/IP) for EAC S/W Installation

Enter IP address of the ICU4000

IP Address	<input type="text" value="172.24.17.24"/>
Password	<input type="password" value="*****"/>

Click 'Next' button to continue.

 Disconnected

IrisICUAdmin

 When the ICU4000 is connected, all process on the ICU4000 will be stopped.
Do you want to continue?

Upgrade ICU4000 EAC S/W

 Ready to Install the IrisAccess EAC S/W for ICU4000 Installation

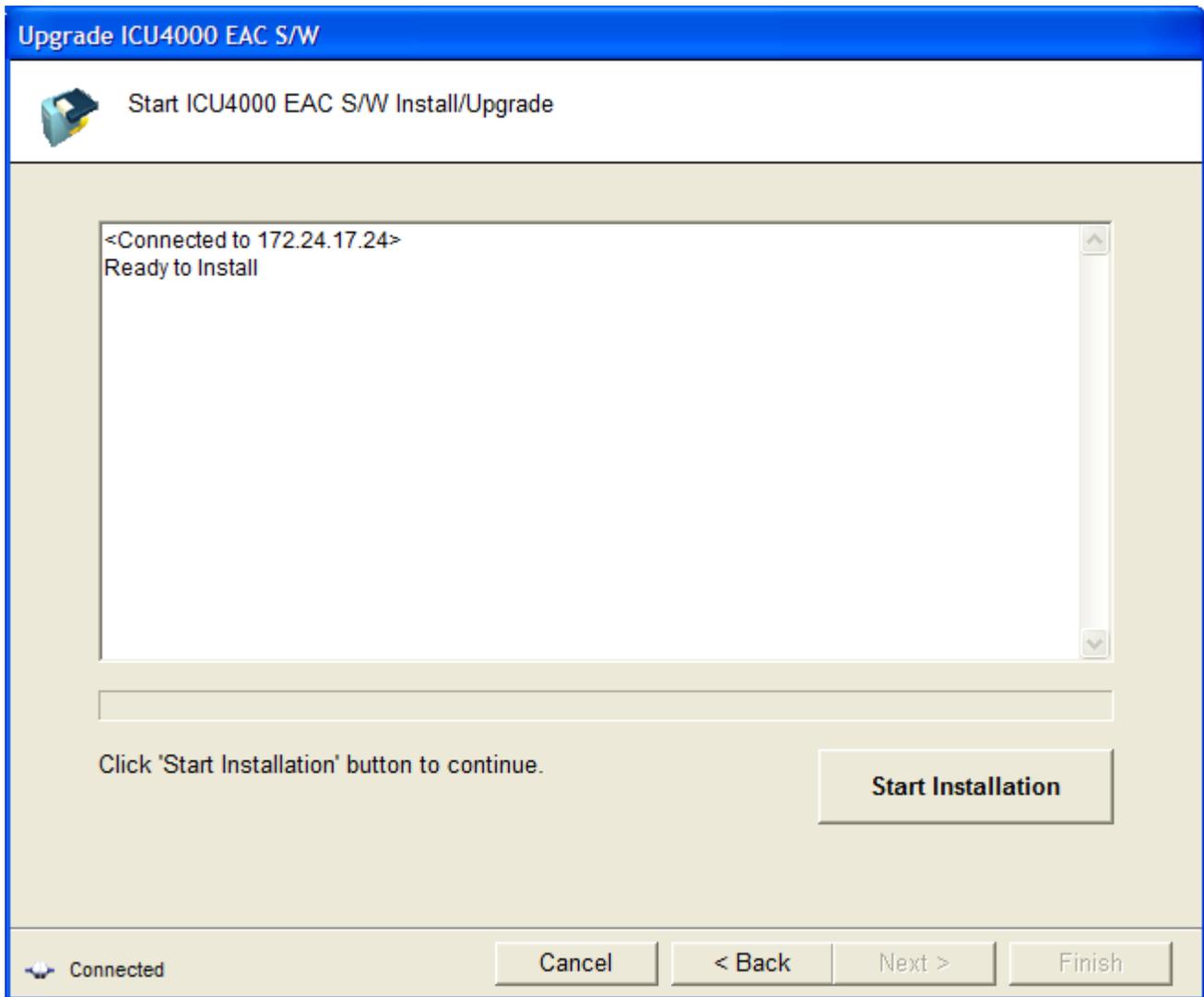
Information for ICU4000 Installation

S/W Version :
IrisAccess™ EAC S/W Version 3.02.10

Installation File :

Click 'Next' button to continue.

 Connected



Upgrade ICU4000 EAC S/W

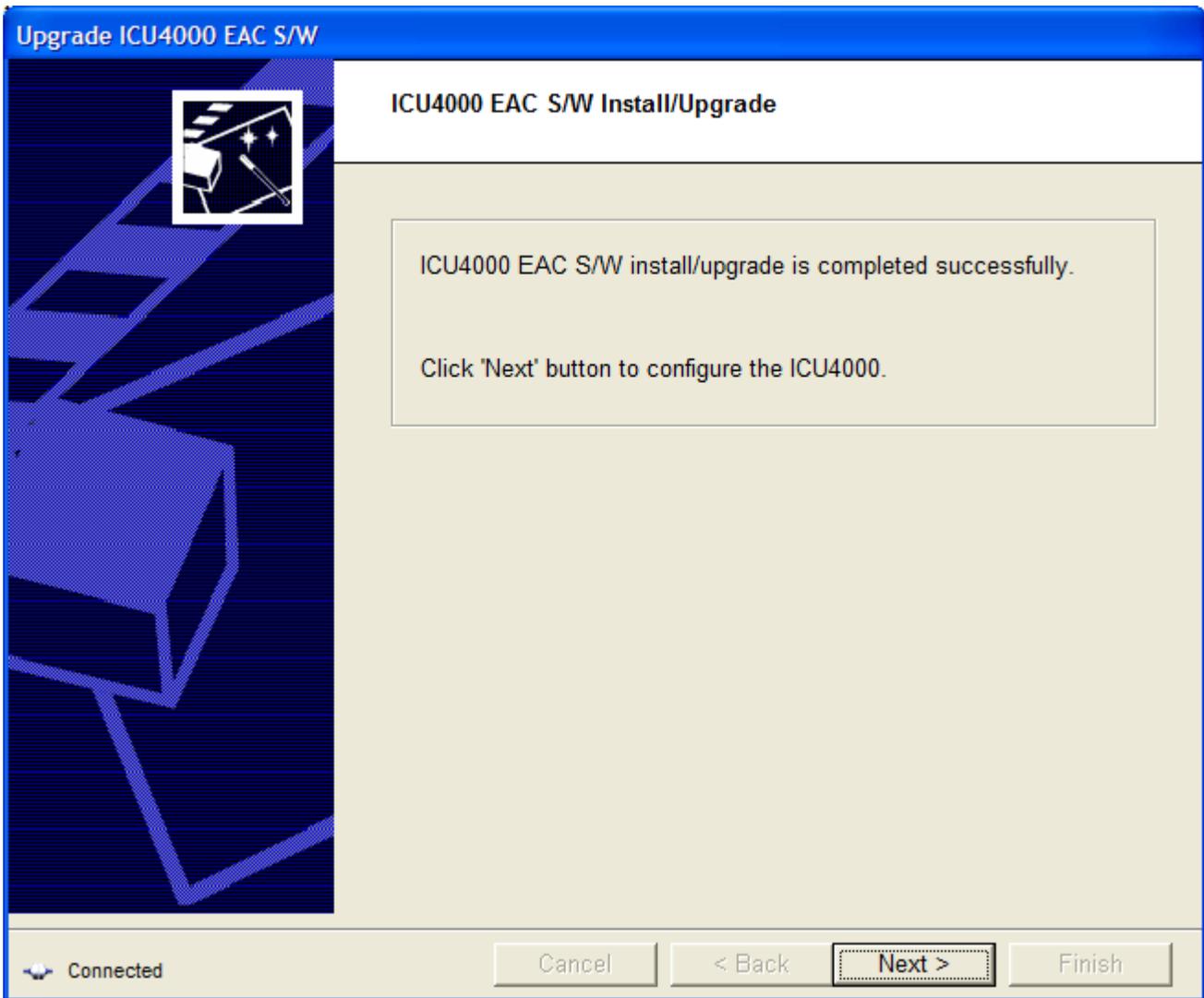
 Start ICU4000 EAC S/W Install/Upgrade

Backup ICU configurationsok
Clean up previous recognition application and driverok
Update kernelok
Update frame grabber driver V3.3 .ok
Copy recognition applicationok
Delete old DB files .ok
Install new DB filesok
Check installed DB files .ok
Copy necessary libraries .ok
Copy system init scripts .ok
Prepare network securityok
Set IDE hard disk I/O to 32bitok

Installation is completed !

Click 'Next' button to continue

 Connected



Upgrade ICU4000 EAC S/W - Configuration

 Get Configurations from the ICU4000

ICU IP address

Click 'Next' button to continue

 Disconnected

Cancel < Back Next > Finish

IrisICUAdmin 

 Get configurations from ICU4000 (172.24.17.24) is completed!
Click 'Ok' button to continue

Upgrade ICU4000 EAC S/W - Configuration

 **Configure the Settings for each Channel**

In order for each channel to function properly a configuration must first be performed. Click 'Configure...' to perform the configuration. Once the configuration is performed you may proceed to the Next step.

Configure...

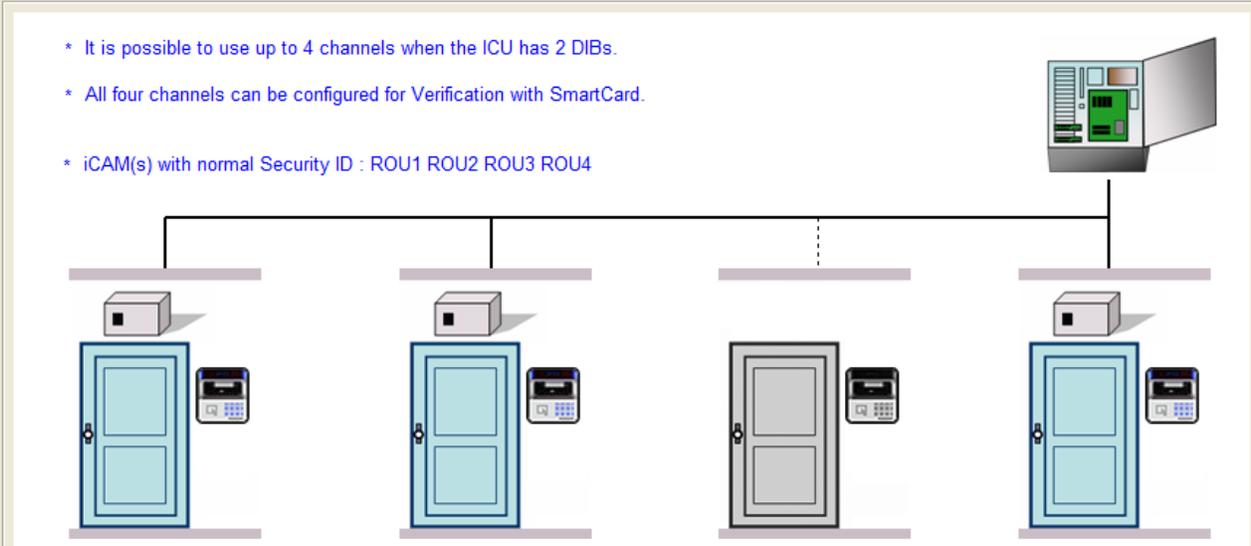
 Connected

Cancel < Back Next > Finish

Select Channels

Enable the check boxes labeled with each channel that you want it to be activated.

- * It is possible to use up to 4 channels when the ICU has 2 DIBs.
- * All four channels can be configured for Verification with SmartCard.
- * iCAM(s) with normal Security ID : ROU1 ROU2 ROU3 ROU4



<input checked="" type="checkbox"/> Channel 1	<input checked="" type="checkbox"/> Channel 2	<input type="checkbox"/> Channel 3	<input checked="" type="checkbox"/> Channel 4
<input checked="" type="checkbox"/> Use Access Panel 1	<input checked="" type="checkbox"/> Use Access Panel 2	<input type="checkbox"/> Use Access Panel 3	<input checked="" type="checkbox"/> Use Access Panel 4
iCAM	iCAM	iCAM	iCAM
Configure Channel 1	Configure Channel 2	Configure Channel 3	Configure Channel 4

When the lid of ICU is opened (ICU Tamper off), Don't stop the IrisRecog program in ICU.

OK Cancel

Loaded configuration from ICU IP 172.24.17.24

IrisICUAdmin

 Configuration in ICU will be updated with the new configuration.
Do you want to continue?

Yes No

IrisICUAdmin

 The channel(s) [Channel 1][Channel 2][Channel 4] is/are not configured directly now, and hence the default/previously configured settings will be used for these channels.
Do you want to continue?

Yes No

Upgrade ICU4000 EAC S/W - Configuration

 Configure the Settings for each Channel

In order for each channel to function properly a configuration must first be performed. Click 'Configure...' to perform the configuration. Once the configuration is performed you may proceed to the Next step.

 Connected

Upgrade ICU4000 EAC S/W - Configuration

 Send Configuration to the ICU4000

<Connected to 172.24.17.24>
Ready to send configurations

Progress Total

Ready to send configurations to the ICU4000. Click 'Send' button to continue.

Send

 Connected Cancel < Back Next > Finish

IrisICUAdmin 

 Configuration of ICU4000 is completed!

OK

Upgrade ICU4000 EAC S/W - Configuration

 Send Configuration to the ICU4000

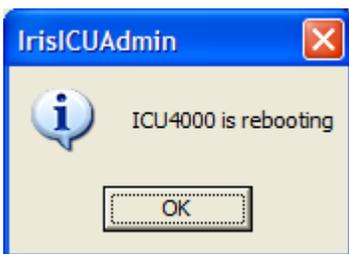
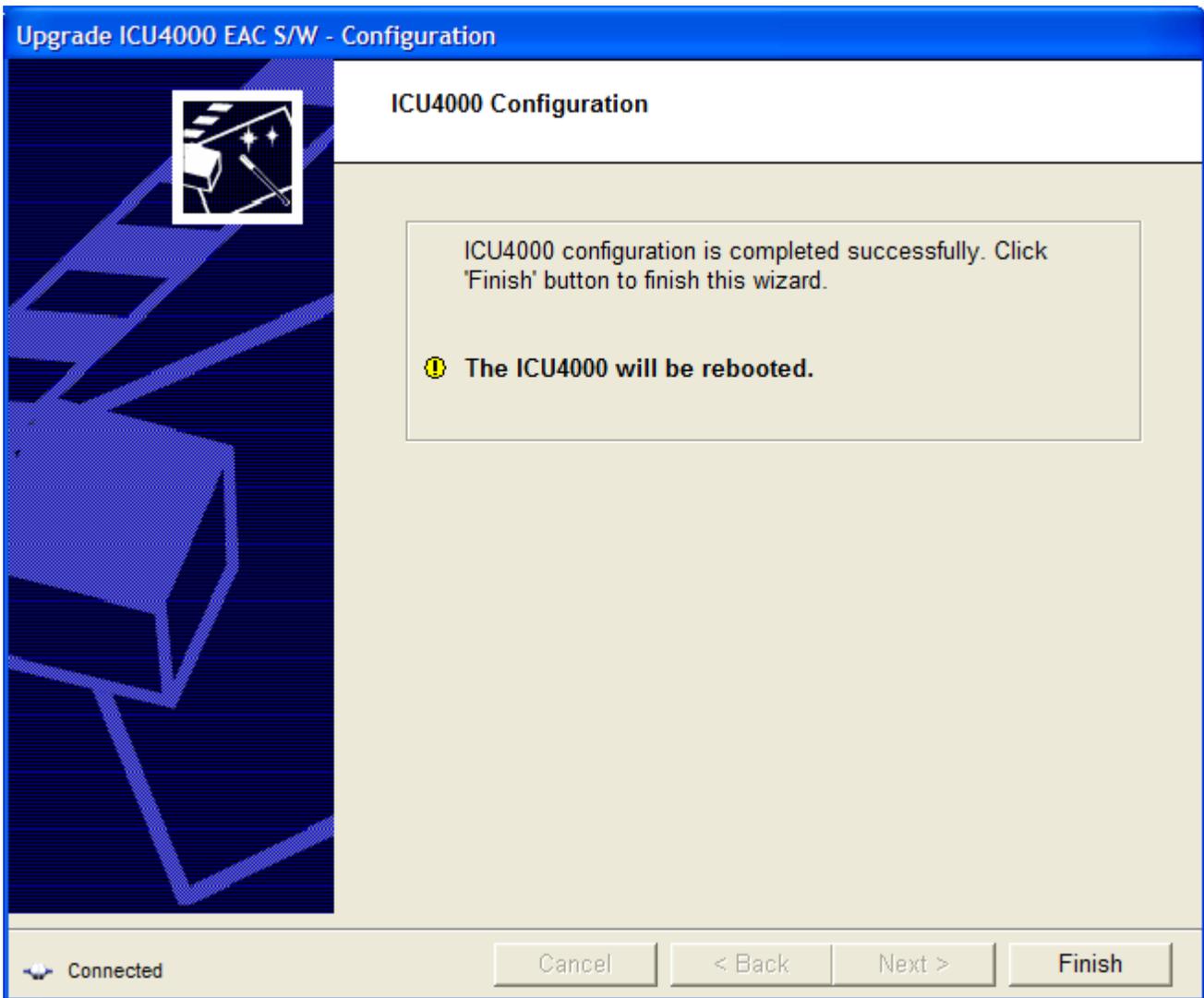
Setup configurations for Channel1...OK
Setup configurations for Channel2...OK
Setup configurations for Channel3...OK
Setup configurations for Channel4...OK
Setup SmartCardKey1.dat...OK
Setup SmartCardKey2.dat...OK
Setup SmartCardKey3.dat...OK
Setup SmartCardKey4.dat...OK
Setup Common.dat...OK
Setup hosts.allow...OK

Configuration setup of ICU4000 is completed!

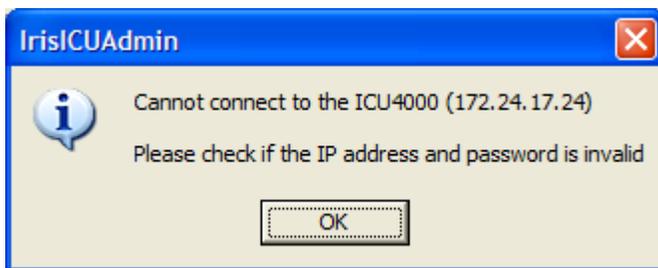
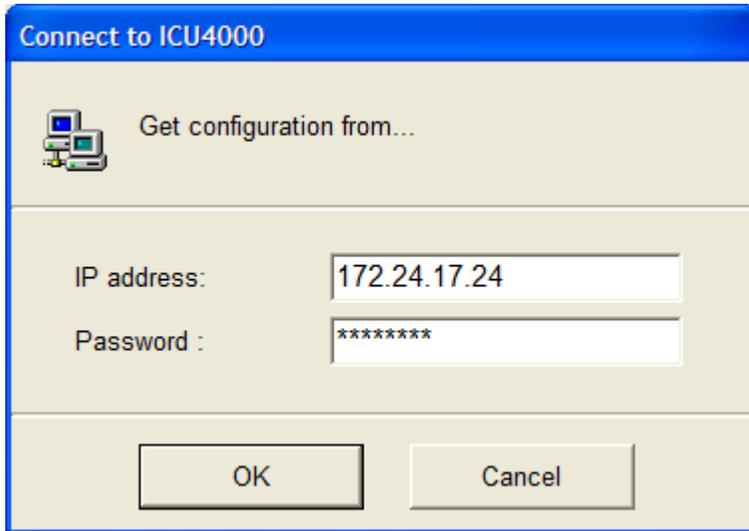
Done Total (100%)

Configuration setup of ICU4000 is completed!

 Connected



8.1.6 The ICUAdmin4000 Configuration Window



ICU Configuration

Before Settings After Settings

* It is possible to use up to 4 channels when the ICU has 2 DIBs.
 * All four channels can be configured for Verification with SmartCard.

<input checked="" type="checkbox"/> Channel 1	<input checked="" type="checkbox"/> Channel 2	<input checked="" type="checkbox"/> Channel 3	<input checked="" type="checkbox"/> Channel 4
<input checked="" type="checkbox"/> Use Access Panel 1 iCAM	<input checked="" type="checkbox"/> Use Access Panel 2 iCAM + Prox Card	<input checked="" type="checkbox"/> Use Access Panel 3 iCAM + Smart Card	<input checked="" type="checkbox"/> Use Access Panel 4 iCAM + PIN
Configure Channel 1	Configure Channel 2	Configure Channel 3	Configure Channel 4

When the lid of ICU is opened (ICU Tamper off), Don't stop the IrisRecog program in ICU.

Send Close

Loaded configuration from ICU IP 172.24.17.24

Channel Configuration ✕

Configure the iCAM, Access Panel, Access Door and GPO for the channel to be activated properly.

Channel 1 Configuration - iCAM Default Settings...

iCAM	Access Panel	Access Door	GPO
<p>iCAM IP Address: <input type="text" value="172.24.17.32"/></p> <p>Eye Selection: <input type="text" value="Right"/></p> <p>Default Message: <input type="text" value="Iris ID"/></p> <p>iCAM Tamper: <input type="checkbox"/> Detect iCAM tamper on connect to iCAM</p> <p>External Hardware Interface: <input type="text" value="DCU/WIB"/></p>			
<p>FakeEye Detection</p> <p> FakeEye Detection Level: <input type="text" value="Level 0"/></p>			
<p>iCAM Volume</p> <p> <input type="range" value="50"/> Mute Low High</p>			
<p>Activate iCAM</p> <p> Select the GPI port used to detect a manual iCAM activation. If 'Proximity Sensor' is selected the iCAM will active using the built in proximity sensor.</p> <p><input type="text" value="Proximity Sensor"/></p> <p>Select the type of activating signal for input port.</p> <p><input checked="" type="radio"/> Low <input type="radio"/> High GPI Settings...</p>			

Channel Configuration ✕

Configure the iCAM, Access Panel, Access Door and GPO for the channel to be activated properly.

Channel 1 Configuration - iCAM Default Settings...

iCAM **Access Panel** **Access Door** **GPO**

Access Rights

Select the system that checks user's access rights.

The IrisAccess System checks user's rights.

The Access Control System checks user's rights.

Wait For Access Panel Response Advanced...

Output Settings

Current Wiegand IN

No Wiegand IN

It is possible to output the input signal through Wiegand and RS422 port. You can select the one of them or both. But if you select to bypass the input, the RS422 output cannot be used.

Use Wiegand as output Wiegand Settings...

Additional Wiegand-out Time delay (sec): 3 Settings...

Lenel+Key Wiegand-out

Use RS422 as output RS422 Settings...

OK Cancel

GPI Settings

You can use 4 ports, 'Lock', 'Status', 'Alarm' and 'Egress' as GPI. The Lock, Egress and Alarm ports may be used to activate iCAM or get the result of recognition from Access Panel.

Current GPI Settings

	Lock	Status	Alarm	Egress	GPI1	GPI2
GPI	Accept	Reject				
Activate State	Low	Low	Low	Low	Low	Low

Activate iCAM

Select the GPI port used to activate the iCAM. If a GPI port is used to activate the iCAM, that port may

- None. iCAM will be activated using the internal proximity sensor.
- Use signal on Lock port to activate iCAM.
- Use signal on Alarm port to activate iCAM.
- Use signal on Egress port to activate iCAM.
- Use signal on GPI1 port to activate iCAM.
- Use signal on GPI2 port to activate iCAM.

Get the recognition results from Access Panel

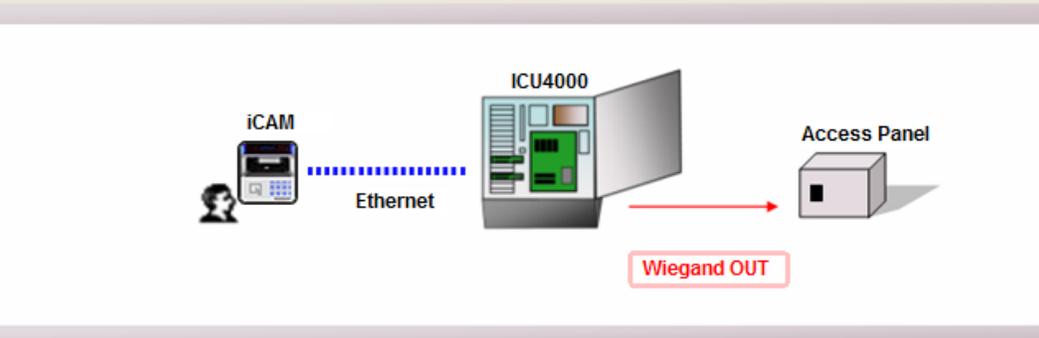
When an Access Control System checks user's access rights, select the ports that the IrisAccess System receives the results from Access Control System. Select the GPI port to detect the 'Accept' and 'Reject' signals from Access Panel.

<u>Lock port</u>	<u>Status port</u>	<u>Alarm port</u>	<u>Egress port</u>	<u>GPI1 port</u>	<u>GPI2 port</u>
<input checked="" type="radio"/> Accept	<input type="radio"/> Accept	<input type="radio"/> Accept	<input type="radio"/> Accept	<input type="radio"/> Accept	<input type="radio"/> Accept
<input type="radio"/> Reject	<input checked="" type="radio"/> Reject	<input type="radio"/> Reject	<input type="radio"/> Reject	<input type="radio"/> Reject	<input type="radio"/> Reject
<input type="radio"/> No Use	<input type="radio"/> No Use	<input checked="" type="radio"/> No Use	<input checked="" type="radio"/> No Use	<input checked="" type="radio"/> No Use	<input checked="" type="radio"/> No Use

OK Cancel

Wiegand Setting

Set the format, Active State, Pulse Duration, Bit Period, Total wiegand bits, Start Parity, Stop Parity and Facility code of Wiegand.



The diagram illustrates the Wiegand signal flow. On the left, an iCAM is connected to the ICU4000 unit via an Ethernet connection. The ICU4000 unit is then connected to an Access Panel via a Wiegand OUT signal line.

Wiegand OUT

Format	Typical format
Active State	Low
Pulse Duration (30~200)	40 μ s
Bit Period (1000~6000)	2000 μ s
Total Wiegand Bits (26~200)	26
Start Parity	Even
Stop Parity	Odd
Facility code and bits	0 8

Check Facility Code

Bypass the input signal through Wiegand IN into the output signal with no change.
 Output the signal with Facility Code and Card ID for only Accept. (Default)
 Change the input signal through Wiegand IN to the Defined output .

Event Report...

OK Cancel

Taskbar: http://ww... 2 IrisICU... Microsoft Vi... 3 Window... si-irisbuild ... IrisMonitor Z:\IA3000..

Event Reporting to Access Panel

When the following recognition results or System logs occurs, the ICU will send a changed Facility Code output through the Wiegand output of DIB. Set new facility code for each case.

Total Bits - 0-80 bits

0 0 0 0 0 0 0 0 1 1 0 0 1 0 0 0 0 0

15 8 0

The bit Value Starts = 8
Length of Value = 7, Value = 100

Recognition Results

Denied	Total Bits	Start Bit	Value Length	Value (Decimal)
Door access trial overtime	16	8	9	1
Live eye check failed	16	8	9	1
Unauthorized - No access authority	16	8	9	1
Warning Eye (Accepted)	16	8	9	1

System Logs

Video Connection Error	16	8	9	1
Serial Connection Error	16	8	9	1
IR-LED Failure	16	8	9	1

OK Cancel

RS422 Settings ✕

Set Baud rate, Number of data bits, Parity bit, Stop bits and dataset for RS422 communication.

The diagram illustrates the RS422 communication setup. On the left, an iCAM is connected to the ICU4000 unit via an Ethernet connection (indicated by a blue dotted line). The ICU4000 unit is connected to an Access Panel via an RS 422 connection (indicated by a red arrow and a red box labeled 'RS 422').

RS422

Bits / Second	<input type="text" value="9600"/>	▼	
Data Bits	<input type="text" value="8"/>	▼	
Parity	<input type="text" value="Even"/>	▼	
Stop Bits	<input type="text" value="1"/>	▼	
Start / End character	<input type="text" value="2 byte Start character, 2 byte End character"/>		
	<input type="text" value="7F"/> <input type="text" value="F7"/>	Data	<input type="text" value="0D"/> <input type="text" value="0A"/>
	Start		End
			(Hexa-Decimal)

Channel Configuration ✖

Configure the iCAM, Access Panel, Access Door and GPO for the channel to be activated properly.

Channel 1 Configuration - iCAM Default Settings...

iCAM	Access Panel	Access Door	GPO
Door Open Duration			
 Door Open Duration (0 ~ 65535 secs) : <input type="text" value="3"/> sec(s)			
Door Lock Device Status			
 Enable to check the Lock Device of a door. <input type="checkbox"/> Enable Activate State <input type="text" value="Low"/>			
Door Open Status			
 Enable to check whether a door stays open for the below 'Check Time'. <input type="checkbox"/> Enable Check Time (0 ~ 255 secs) : <input type="text" value="10"/> sec(s) Activate State <input type="text" value="Low"/>			
Alarm			
 Enable to get the fire alarm signal. When the fire alarm signal is detected, select how to operate the door. <input type="checkbox"/> Enable <input type="text" value="Close"/> Activate State <input type="text" value="Low"/>			
Egress Button			
 When an egress button near the entry area is pushed, the door is opened. <input type="checkbox"/> Enable Activate State <input type="text" value="Low"/>			

Channel Configuration

Configure the iCAM, Access Panel, Access Door and GPO for the channel to be activated properly.

Channel 1 Configuration - iCAM Default Settings...

iCAM	Access Panel	Access Door	GPO																																	
<p>In the specified state such as followings, a signal can be outputted through two general output ports. Decide the port to which to send the signal, and then select how long time to send the signal.</p> <p>When</p> <table border="1"> <thead> <tr> <th></th> <th>From Port</th> <th>During Time Out (0 ~ 65535 secs)</th> </tr> </thead> <tbody> <tr> <td>A user is accepted</td> <td>No</td> <td>0</td> </tr> <tr> <td>A user is denied</td> <td>No</td> <td>0</td> </tr> <tr> <td>Warning Eye is detected</td> <td>No</td> <td>0</td> </tr> <tr> <td>The result of matching a card ID is successful</td> <td>No</td> <td>0</td> </tr> <tr> <td>A door is opened more than the open duration time</td> <td>No</td> <td>0</td> </tr> <tr> <td>A door is opened without Identification or Verification</td> <td>No</td> <td>0</td> </tr> <tr> <td>An electromagnetic locking equipment is locked but a door is opened</td> <td>No</td> <td>0</td> </tr> <tr> <td>Fire Alarm signal is detected</td> <td>No</td> <td>0</td> </tr> <tr> <td>ICU / DCU Tamper signal is detected</td> <td>No</td> <td>0</td> </tr> <tr> <td>iCAM Tamper signal is detected</td> <td>No</td> <td>0</td> </tr> </tbody> </table>					From Port	During Time Out (0 ~ 65535 secs)	A user is accepted	No	0	A user is denied	No	0	Warning Eye is detected	No	0	The result of matching a card ID is successful	No	0	A door is opened more than the open duration time	No	0	A door is opened without Identification or Verification	No	0	An electromagnetic locking equipment is locked but a door is opened	No	0	Fire Alarm signal is detected	No	0	ICU / DCU Tamper signal is detected	No	0	iCAM Tamper signal is detected	No	0
	From Port	During Time Out (0 ~ 65535 secs)																																		
A user is accepted	No	0																																		
A user is denied	No	0																																		
Warning Eye is detected	No	0																																		
The result of matching a card ID is successful	No	0																																		
A door is opened more than the open duration time	No	0																																		
A door is opened without Identification or Verification	No	0																																		
An electromagnetic locking equipment is locked but a door is opened	No	0																																		
Fire Alarm signal is detected	No	0																																		
ICU / DCU Tamper signal is detected	No	0																																		
iCAM Tamper signal is detected	No	0																																		

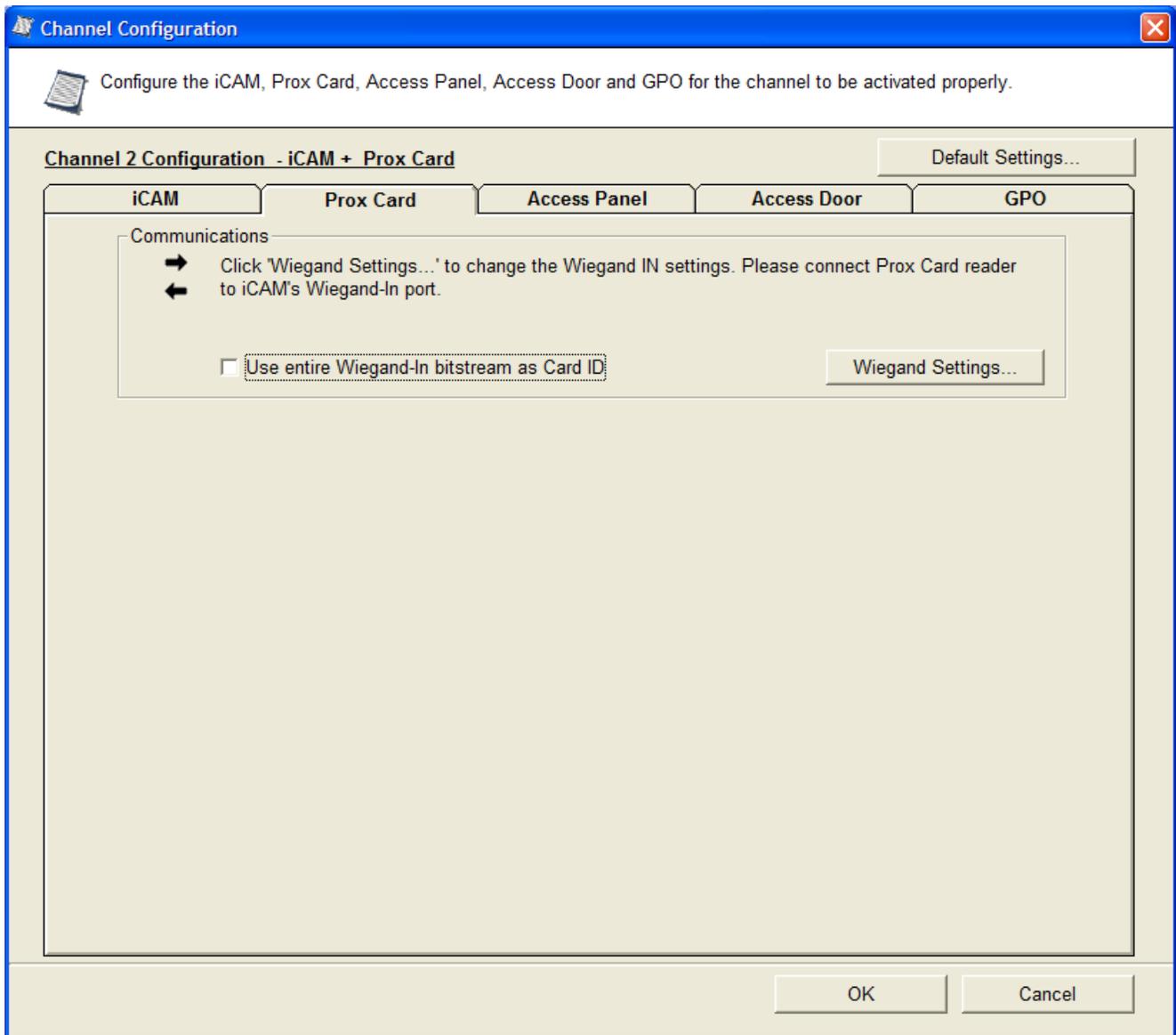
OK Cancel

Channel Configuration ✕

 Configure the iCAM, Prox Card, Access Panel, Access Door and GPO for the channel to be activated properly.

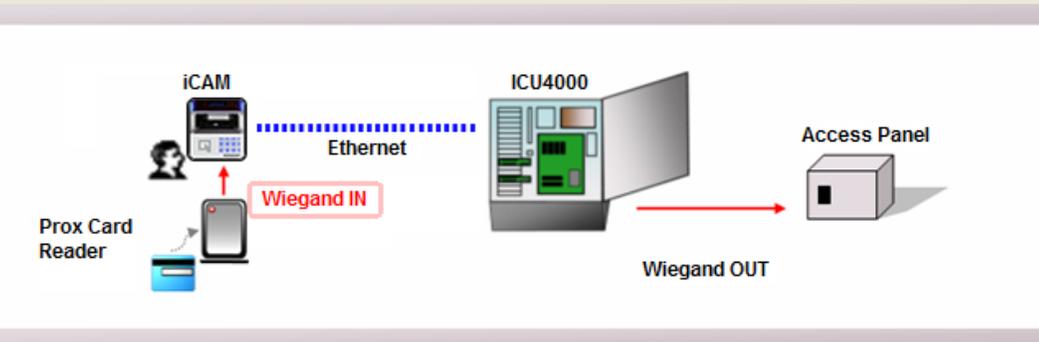
Channel 2 Configuration - iCAM + Prox Card Default Settings...

iCAM	Prox Card	Access Panel	Access Door	GPO
<p>iCAM IP Address: <input type="text" value="172.24.17.160"/></p> <p>Eye Selection: <input type="text" value="Both"/></p> <p>Default Message: <input type="text" value="Iris ID"/></p> <p>iCAM Tamper: <input type="checkbox"/> Detect iCAM tamper on connect to iCAM</p> <p>External Hardware Interface: <input type="text" value="DCU/WIB"/></p>				
<p>FakeEye Detection</p> <p> FakeEye Detection Level: <input type="text" value="Level 0"/></p>				
<p>iCAM Volume</p> <p> <input type="range" value="50"/> Mute Low High</p>				
<p>Verification Time Out</p> <p> This is the time period after the input of the card ID to the Wiegand input, until the system is no longer attempting to perform the iris recognition for this user.</p> <p>Time Out (0 ~ 65535 secs) : <input type="text" value="5"/> sec(s)</p>				



← Wiegand Setting

Set the format, Active State, Pulse Duration, Bit Period, Total wiegand bits, Start Parity, Stop Parity and Facility code of Wiegand.

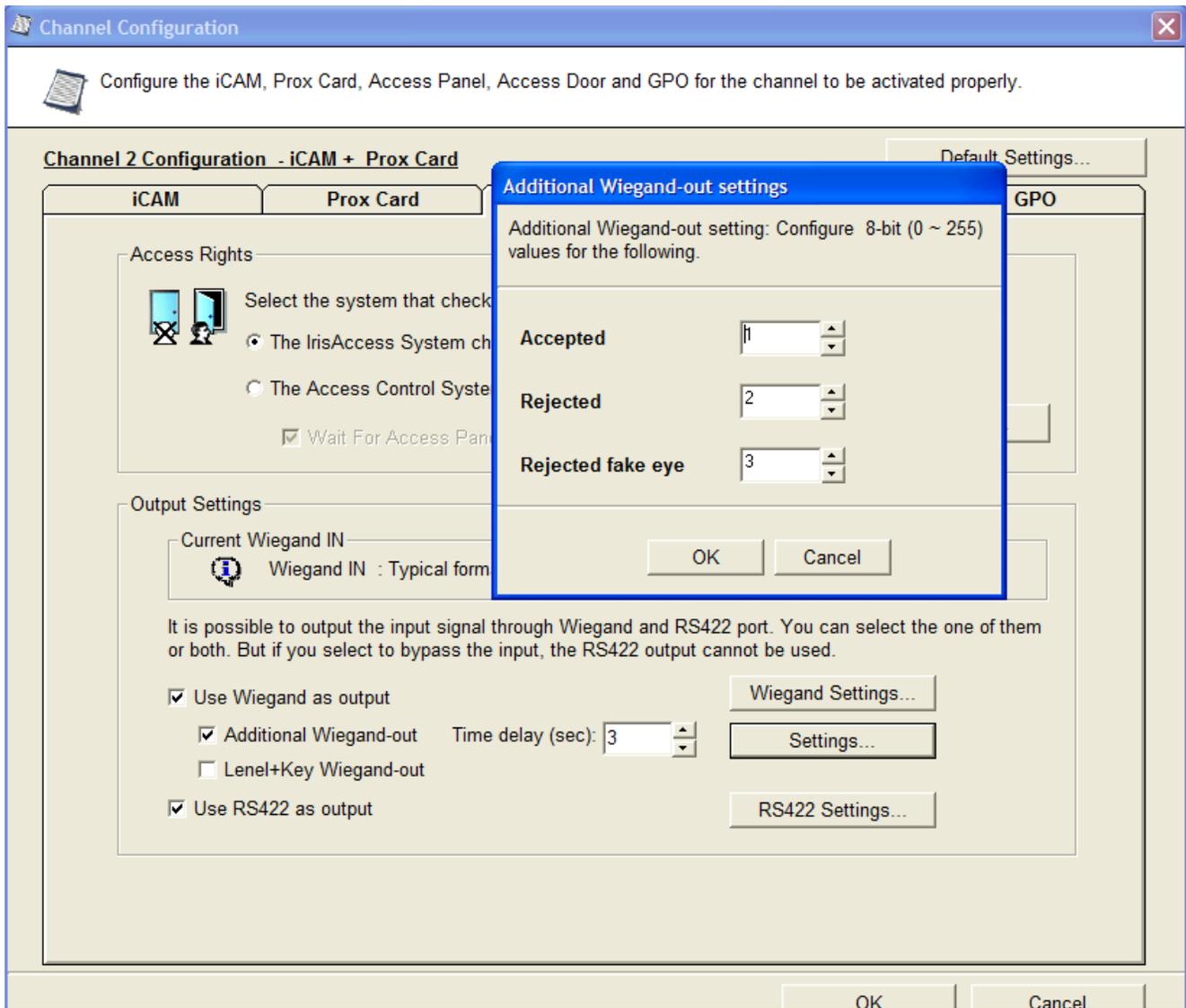


Wiegand IN

Format	Typical format
Start Parity	Even
Stop Parity	Odd
Facility code and bits	0 8

Check Facility Code

OK Cancel



Channel Configuration [Close]

Configure the iCAM, Smart Card, Access Panel, Access Door and GPO for the channel to be activated properly.

Channel 3 Configuration - iCAM + Smart Card [Default Settings...]

iCAM | **Smart Card** | **Access Panel** | **Access Door** | **GPO**

Smart Card

 The offset only needs to be changed if storing non-IrisAccess 4000 information on the SmartCard. Book : Block Offset (hexadecimal) :

Use as Prox Card [Set to Defaults]

Encryption Algorithm

 Select the Encryption Algorithm to encrypt the Smart Card

Data format in Smart Card : Encryption Algorithm :

Security Keys

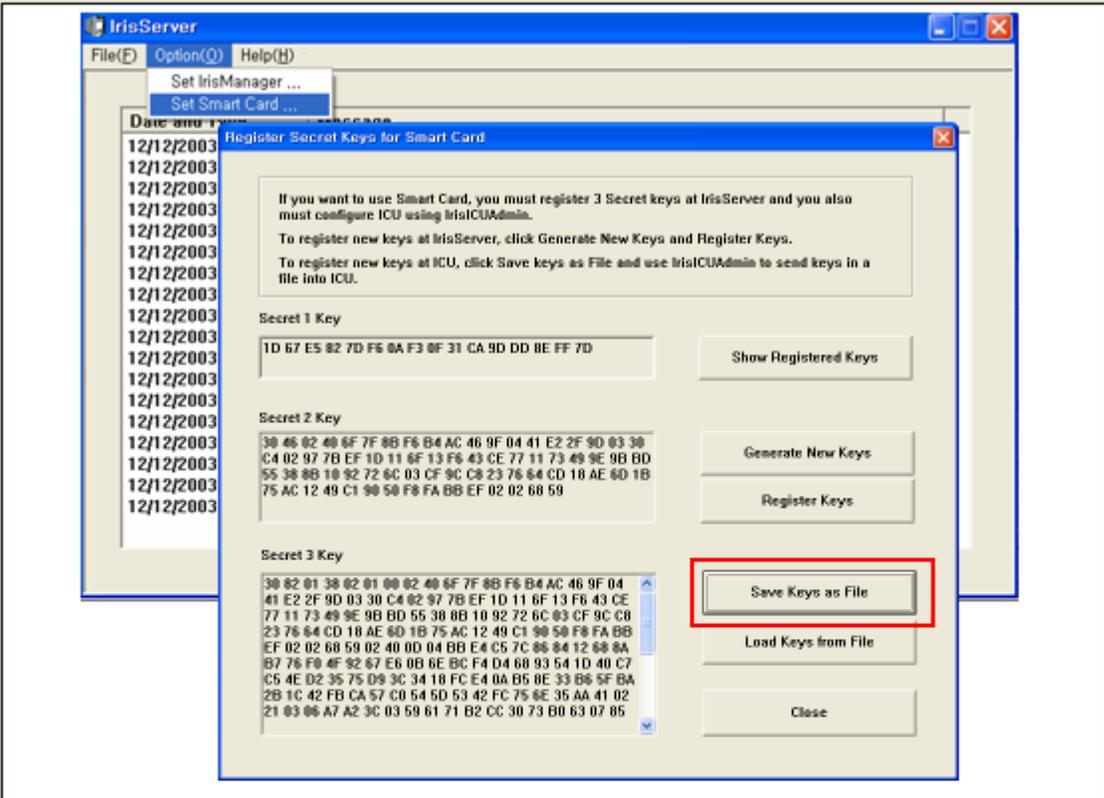
 Click 'Get Keys...' to get Smart Card keys file. A keys file can be generated in IrisServer. [Get Keys...]

Security Key 1 :

Security Key 2 :

[OK] [Cancel]

Load Smart Card Key



The screenshot shows the IrisServer application window with the 'Register Secret Keys for Smart Card' dialog box open. The dialog box contains the following text:

If you want to use Smart Card, you must register 3 Secret keys at IrisServer and you also must configure ICU using IrisICUAdmin.

To register new keys at IrisServer, click Generate New Keys and Register Keys.

To register new keys at ICU, click Save keys as File and use IrisICUAdmin to send keys in a file into ICU.

Secret 1 Key
1D 67 E5 82 7D F6 8A F3 0F 31 CA 9D DD 8E FF 7D

Secret 2 Key
30 46 02 40 6F 7F 8B F6 B4 AC 46 9F 04 41 E2 2F 9D 03 30
C4 02 97 7B EF 1D 11 6F 13 F6 43 CE 77 11 73 49 9E 9B BD
55 38 8B 10 92 72 6C 03 CF 9C C8 23 76 64 CD 18 AE 6D 1B
75 AC 12 49 C1 90 50 F8 FA BB EF 02 02 68 59

Secret 3 Key
30 82 01 38 02 01 00 02 40 6F 7F 8B F6 B4 AC 46 9F 04
41 E2 2F 9D 03 30 C4 02 97 7B EF 1D 11 6F 13 F6 43 CE
77 11 73 49 9E 9B BD 55 38 8B 10 92 72 6C 03 CF 9C C8
23 76 64 CD 18 AE 6D 1B 75 AC 12 49 C1 90 50 F8 FA BB
EF 02 02 68 59 02 40 0D 04 BB E4 C5 7C 86 84 12 68 8A
B7 76 F0 4F 92 67 E6 0B 6E BC F4 D4 68 93 54 1D 40 C7
C5 4E D2 35 75 D9 3C 34 18 FC E4 0A B5 8E 33 B6 5F BA
2B 1C 42 FB CA 57 C0 54 5D 53 42 FC 75 6E 35 AA 41 02
21 03 06 A7 A2 3C 03 59 61 71 B2 CC 30 73 B0 63 07 85

The 'Save Keys as File' button is highlighted with a red box.

1. IrisServer generates the 3 Keys for Smart Card and the ICU needs the 2 keys (for GSC-IS Format, 1 key) of them. If you didn't generate the keys yet, generate and save keys through the IrisServer above all.
2. Click 'Load' and select the file that you saved the keys through IrisServer.

Load

OK Cancel

ICU Configuration

Before Settings After Settings

- * It is possible to use up to 4 channels when the ICU has 2 DIBs.
- * All four channels can be configured for Verification with SmartCard.

<input checked="" type="checkbox"/> Channel 1	<input checked="" type="checkbox"/> Channel 2	<input checked="" type="checkbox"/> Channel 3	<input checked="" type="checkbox"/> Channel 4
<input checked="" type="checkbox"/> Use Access Panel 1	<input checked="" type="checkbox"/> Use Access Panel 2	<input checked="" type="checkbox"/> Use Access Panel 3	<input checked="" type="checkbox"/> Use Access Panel 4
iCAM	iCAM + Prox Card	iCAM + Smart Card	iCAM + PIN
Configure Channel 1	Configure Channel 2	Configure Channel 3	Configure Channel 4

When the lid of ICU is opened (ICU Tamper off), Don't stop the IrisRecog program in ICU.

Send Close

Loaded configuration from ICU IP 172.24.17.24

IrisICUAdmin

Configuration in ICU will be updated with the new configuration.
Do you want to continue?

Yes No

Connect to ICU4000

 Send configuration to...

IP address:

Password :

Restart ICU4000

Sending configuration is successful!

 You must restart the ICU4000 before the new settings will take effect.

Do you want to restart the ICU4000 now?

8.1.7 The ICUAdmin4000 Change Password Window

ICU4000 Change Password

 Connect to the ICU4000 to change password

Enter IP address of the ICU4000

IP Address	<input type="text" value="172.24.17.24"/>
Password	<input type="password" value="*****"/>

Please check below to reset the ICU password.
Note: ICU configuration cable connection is required.

Reset Password

Click 'Next' button to continue.

 Disconnected

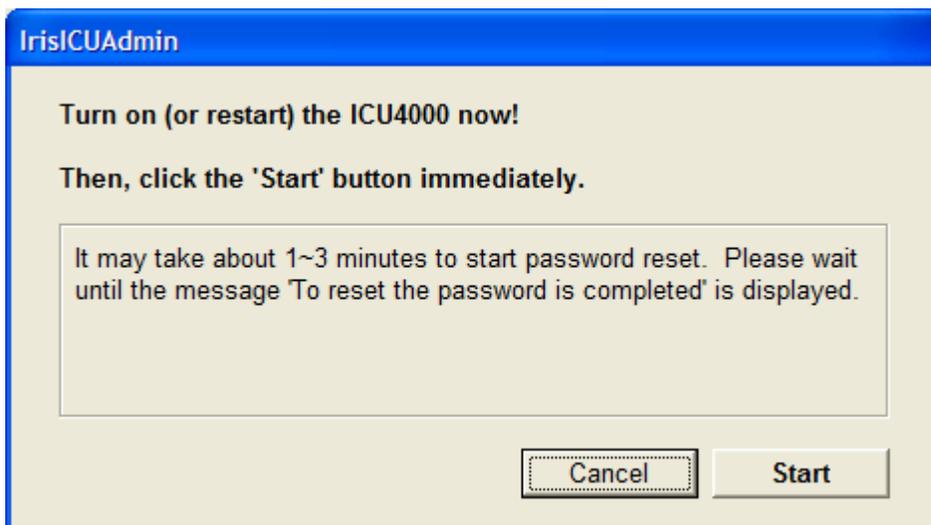
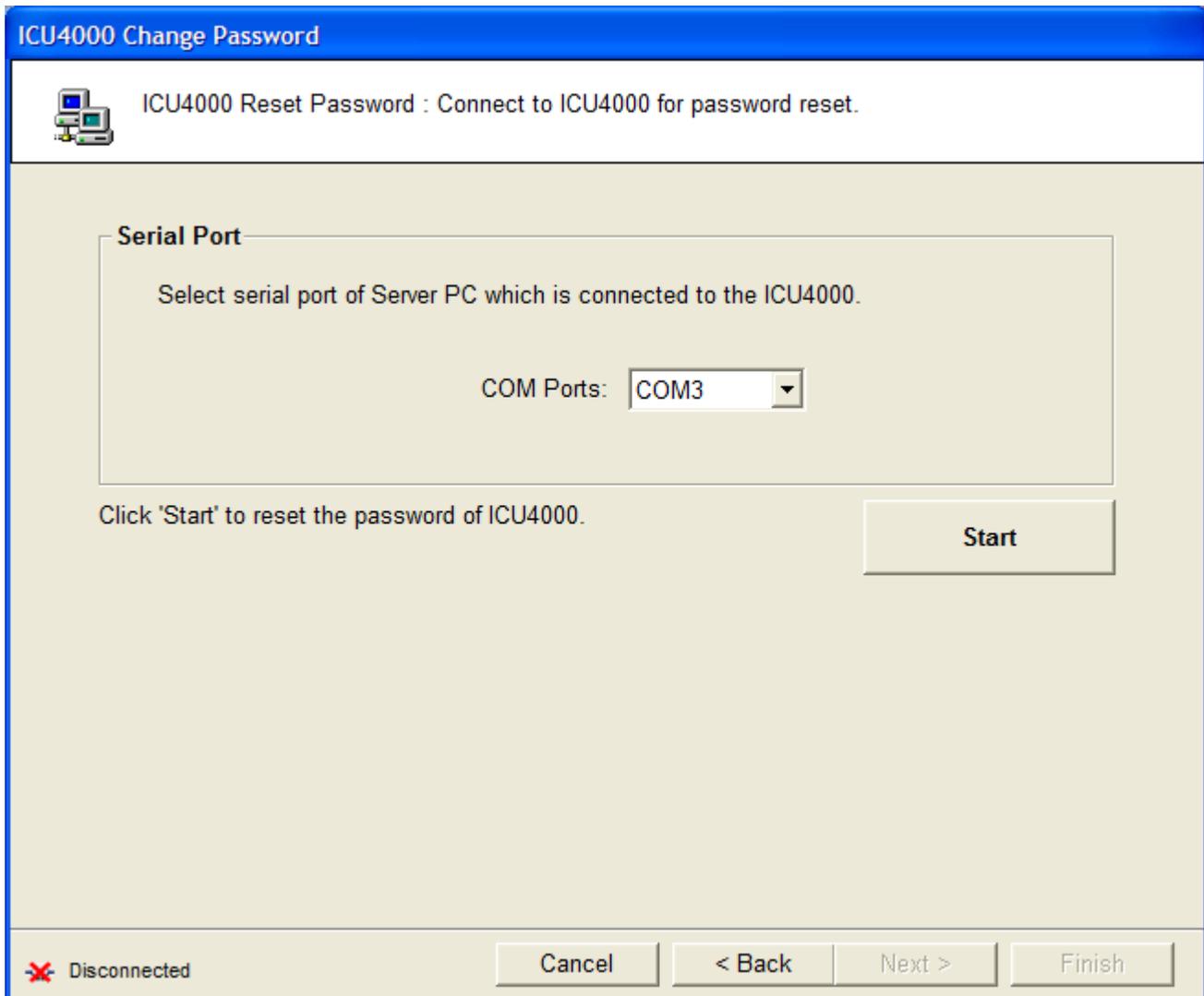
Cancel < Back Next > Finish

IrisICUAdmin

 **1. Power off ICU4000**

2. ICU configuration cable must be connected to reset the password.

OK



Change Password

ICU4000 Change Password

 Change Current Password to New Password

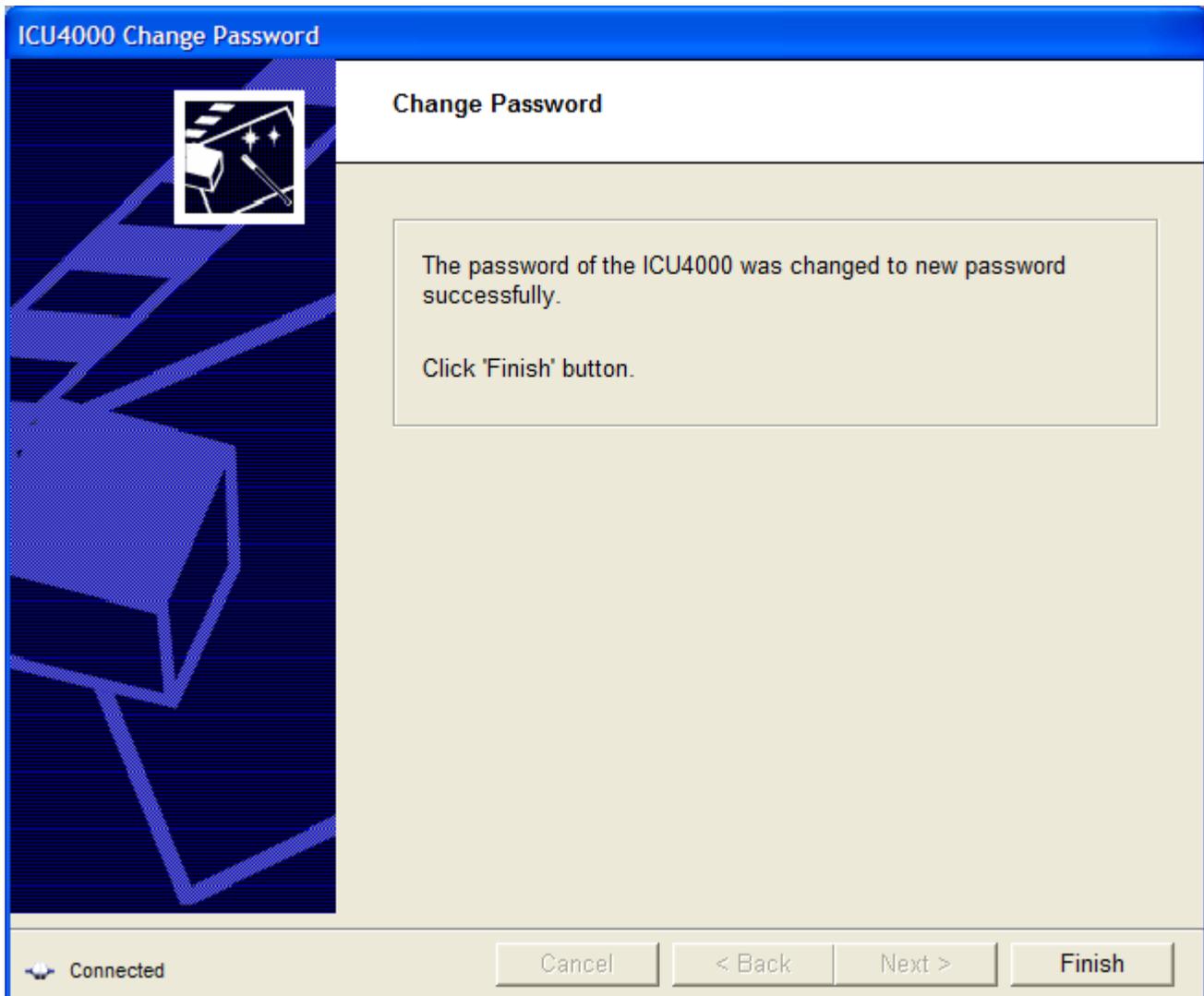
New password	<input type="password" value="*****"/>
Confirm new password	<input type="password" value="*****"/>

Click 'Next' button to continue.

Connected

IrisICUAdmin 

 The password has been changed



9. IrisICUAdmin7000

9.1 IrisICUAdmin7000 Information

9.1.1 About IrisICUAdmin7000

The ICU7000 makes use of an application called ICUAdmin7000 that is provided with the iData EAC software 7.07.08 and above versions. This application may also be downloaded directly from the irisid.com website (when available).

This application should be used before attempting to install and integrate the ICU7000 into a

deployed running environment.

ICU7000Update is an application utility that allows for management of an ICU7000.
ICU7000Admin is used for new installation and upgradation of the ICU7000 controller unit.

9.1.2 *IrisICUAdmin7000 Purpose and Technical Details*

The IrisICUAdmin7000 will update the version of software available on the ICU7000 to the compatible matched version of iData EAC.

After the IP address of the ICU unit(s) has been set, the ICU can be updated using the ICUAdmin7000 software individually or in groups. Updates and New installation options are available.

This program is designed for use with ICU7000 controller units that contain a single channel to control an iCAM7000 camera unit only (when used with option 1).

- This is an independent application which can be run on any Windows XP or Windows 7 machine.
- It will support new installation or upgrade for 32 channels placed in the software list at one time.
- For New Installation process, the ICU7000 IP address, IrisServer IP address and Security ID is required. The iCAM7000 IP address that is to be assigned for use with the ICU can also be entered but is not required for New Installations.

9.1.3 *Minimum System Requirements*

In addition to the system requirements for IrisAccess EAC (refer IrisAccess Software Installation Manual); the following pre-requisites are required to setup IrisAccess EAC.

- Windows XP or Windows7 Operating system
- Microsoft .Net Framework 3.5 (not required on Windows 7)

9.1.4 *Version Compatibility*

EAC build v3.07x. Software mandates the following version compatibility check:

- ICU7000 installed with IrisRecog7000 v3.07x. Software can connect to IrisServer v3.07x..
- iCAM7000/7100 installed with IrisRecog7000 v3.07x. or above software will connect to IrisServer v3.07x.
- IrisEnroll4000 v3.07x can connect to iCAM4000/4100 and icam7000/7100 with v3.07x software.

9.2 How to Use IrisAccess™ ICUAdmin7000

To start the ICUAdmin7000, click **IrisICUAdmin7000.exe**.

OR

Click on IrisICUAdmin7000 shortcut in start menu or desktop.

The application window will be displayed as shown in the following image.

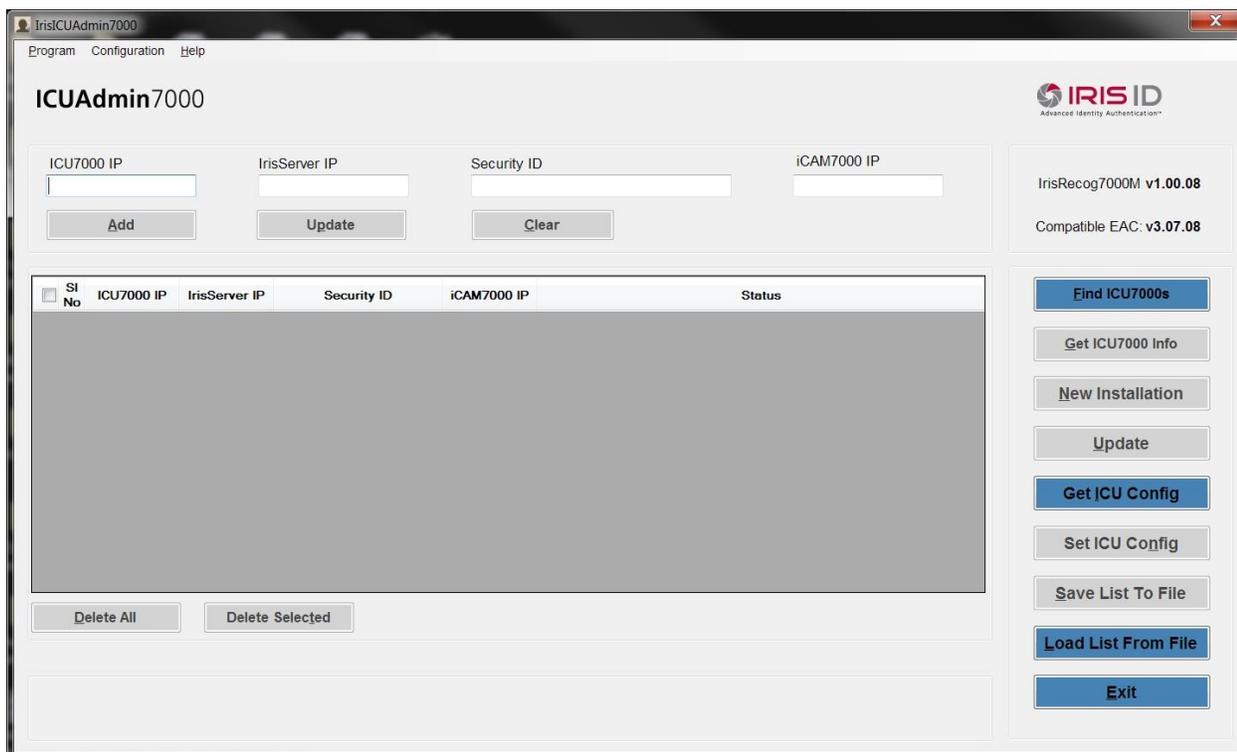
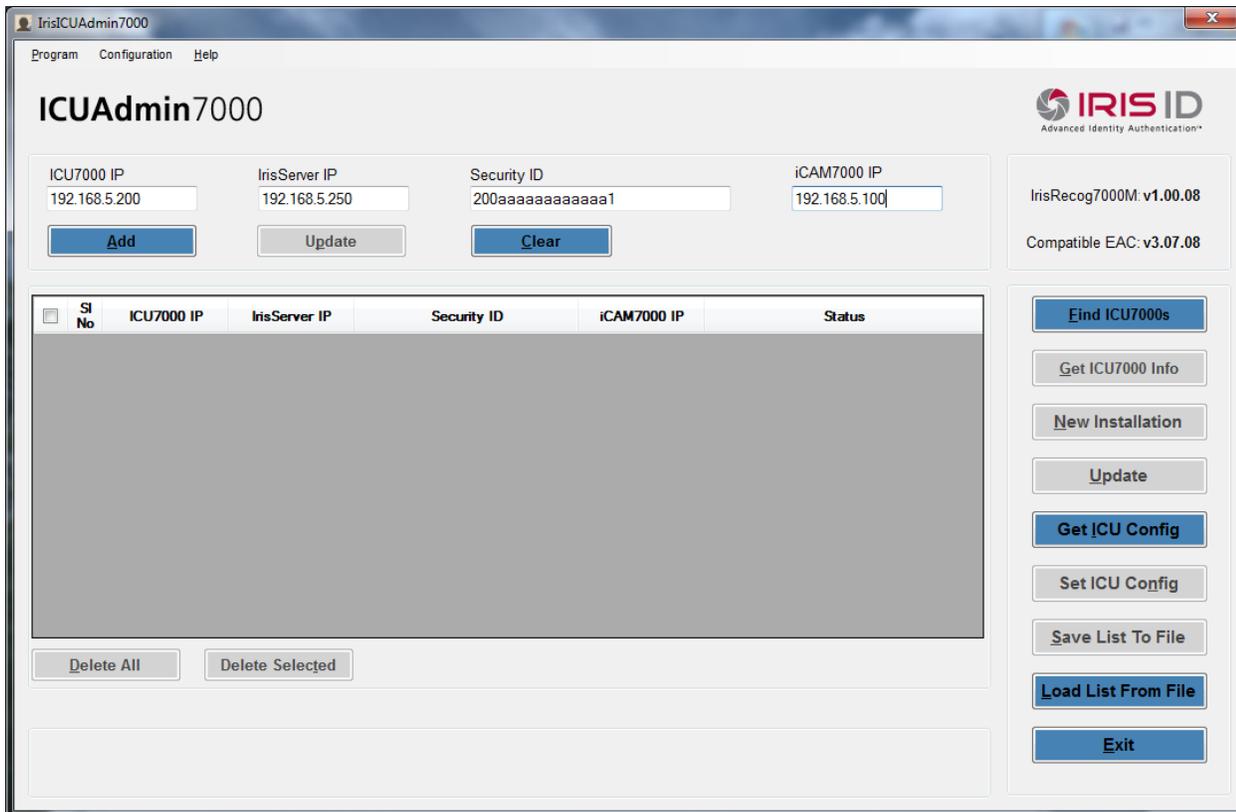
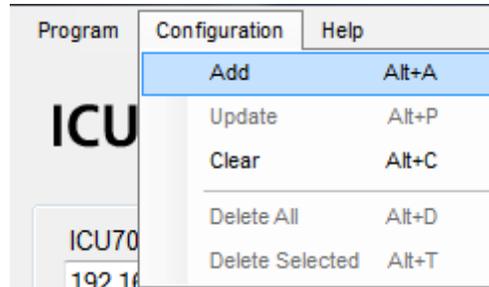


Fig 1

9.2.1 Add

Add option is used to add **ICU7000 IP, IrisServer IP Security ID and iCAM7000 IP** to the list.

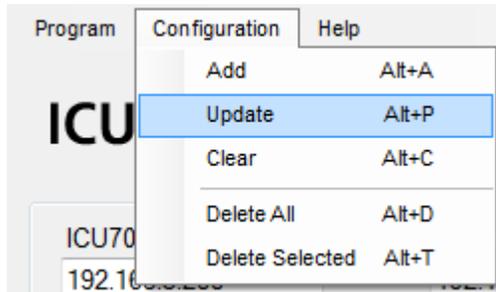
After entering valid **ICU7000 IP, IrisServer IP and Security ID (iCAM7000 IP optional)**, click on **Add** button or select **Add** option from **Configuration** menu.



9.2.2 Update

Update option is used to update the existing ICU7000Admin information. This option is enabled when you select the item from the list.

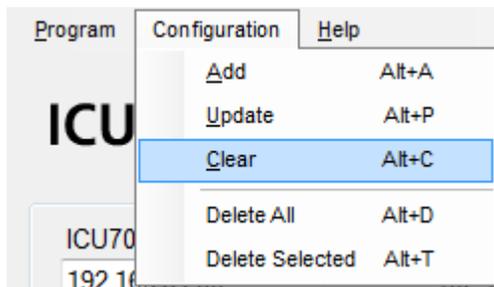
After modifying valid **ICU70007000 IP**, **IrisServer IP** and **Security ID**, click on Update button or select Update option from **Configuration** menu.



9.2.3 Clear

Clear option is used to clear the entered information from the text.

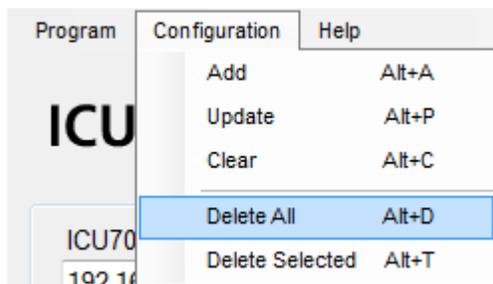
Click on **Clear** button or select **Clear** option from **Configuration** menu.



9.2.4 Delete All

Delete All option is used to delete all the entries from the list.

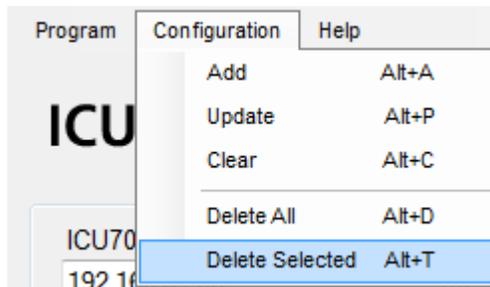
Click on **Delete All** button or select **Delete List** option from Configuration menu.



9.2.5 Delete Selected

Delete Selected option is used to delete all the entries from the list.

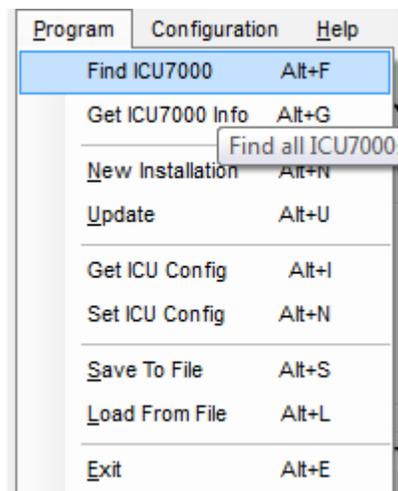
Click on **Delete Selected** button or select **Delete Selected** button from lower Configuration menu.



9.2.6 Find ICU7000s

The FindICU7000 will search the network for available ICU7000 controller units and display them in the list.

Click on **Find ICU7000** button or select **Find ICU7000s** option from **Program** menu.



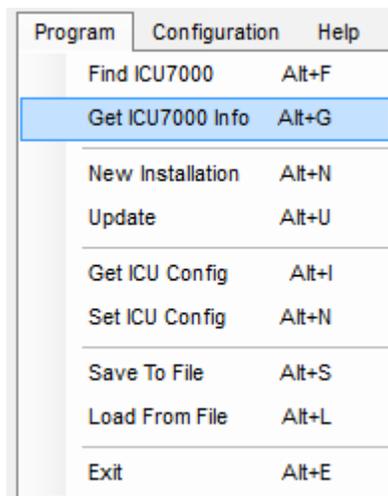
A finding scroll bar will begin when the process is started. In the event that the Find ICU7000 function does not work successfully, enter the IP address data manually.

Note: Network settings, windows firewall, available ports, routers, and anti-virus applications can block the applications ability to find/detect ICU7000s on the network.

9.2.7 Get ICU7000 Info

The GetCU7000 can be used after a Find ICU function has been performed, or after the IP address of a valid ICU on the network has been added to the configuration list. This function allows for the ICUAdmin7000utility to provide the available ICU information such as IrisServer IP, security ID and applicable iCAM7000 IP that is configured for that ICU channel. Select the check box next to the desired ICU IP address.

Click on **Get ICU7000** button or select **Find ICU7000s** option from **Program** menu.

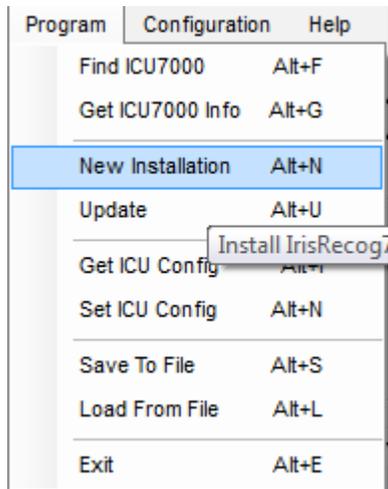


A Get ICU7000 info scroll bar will begin when the process is started. In the event that the Get ICU7000 function does not work successfully, the configuration settings may not be entered in the ICU or available.

9.2.8 New Installation

New installation of iCUAdmin7000 will install IrisRecog7000M software in ICU7000.

Click on **New Installation** button or select **New Installation** option from **Program** menu.



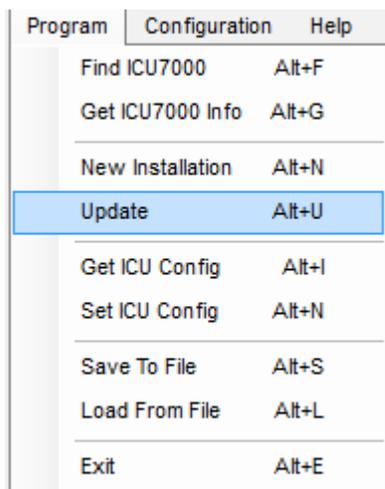
A new installation progress bar will be seen indicating the progress of the installation.

After successful installation, ICU7000 will reboot.

9.2.9 Update

Update function of ICUAdmin7000 will update the IrisRecog7000M software in ICU7000.

Click on **Update** button or select **Update** option from **Program** menu.



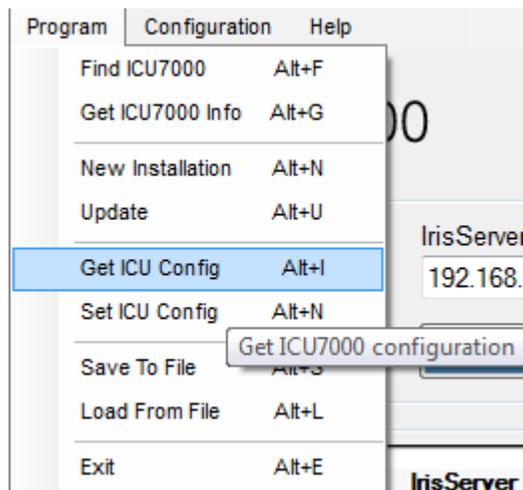
An update progress bar will be seen indicating the progress of the installation.

After successful update, iCAM7000 will reboot.

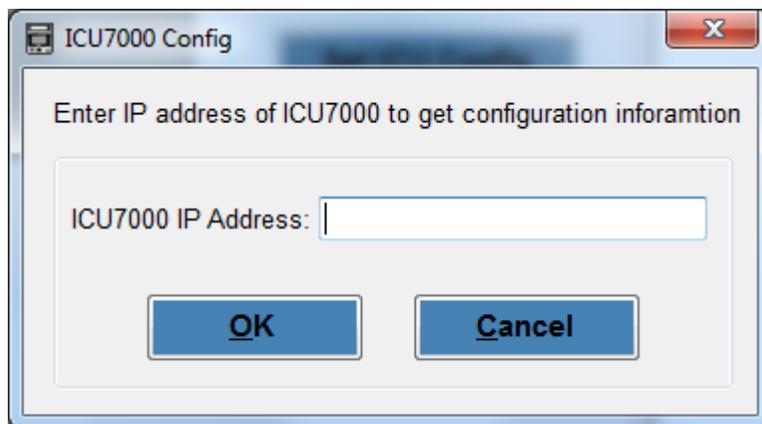
9.2.10 Get ICU Config

Get ICU Config option is used to get the ICU7000 information from an ICU7000 that you wish to save. This saved file is stored as a .dat file.

Click on Get ICU Config from File button or select Get ICU Config option from Program menu.



Enter the IP address of the ICU that is to have the configuration saved from and press OK.

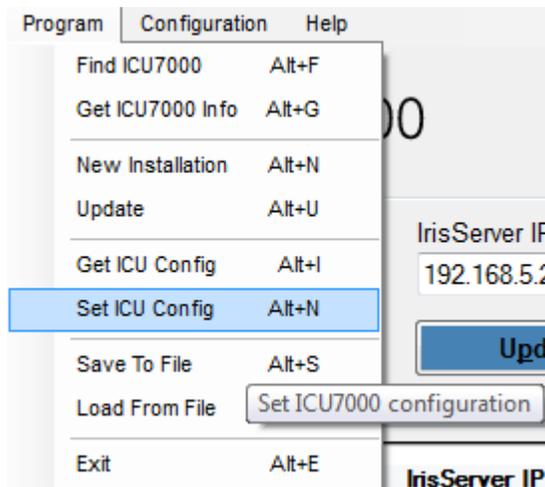


Save the .dat file making sure to provide a name and location path that you will remember in the event it is needed to be used at a later time.

9.2.11 Set ICU Config

Set ICU Config option is used to set a saved .dat file (that was saved using the Get Config File option of this utility) into another ICU7000 listed by IP address in the configuration list.

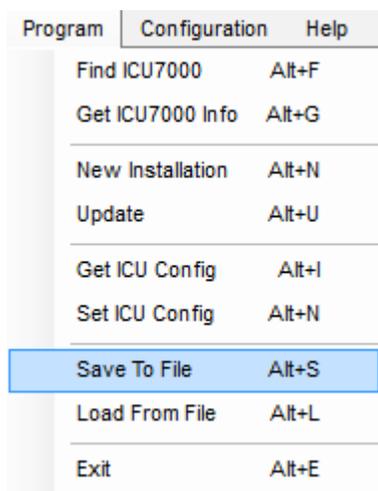
Click on **Set ICU7000 Config** button or select **Set ICU7000 Config** option from **Program** menu.



9.2.12 Save List to a File

Save List To File option is used to save the entered list information to file with .csv format.

Click on **Save List To File** button or select **Save To File** option from **Program** menu.



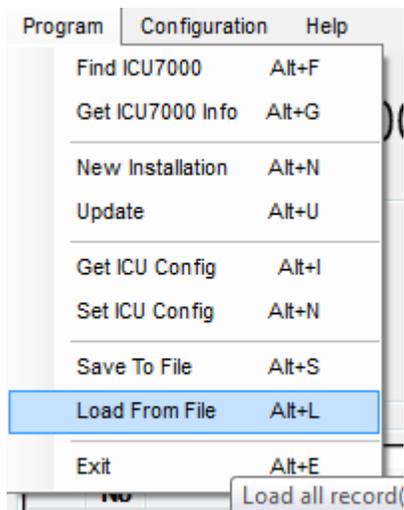
Save the .csv file making sure to provide a name and location path that you will remember

in the event it is needed to be used at a later time.

9.2.13 Load List to a File

Load List From File option is used to load the ICU7000 information from the file which is of .csv format.

Click on Load List From File button or select Load From File option from Program menu.



10. Technical Support

10.1 Technical Assistance

10.1.1 How to receive Technical Support

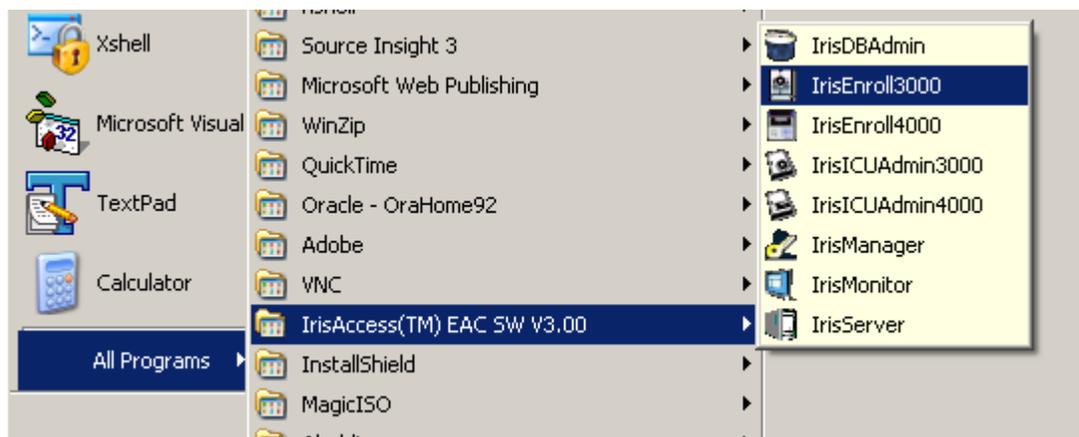
Additional Information and Technical assistance is available on the Iris ID's support web site at www.irisid.com, click on Support & Service then Technical Support.

11. Appendix

11.1 IrisAccess™ IrisEnroll3000

11.1.1 How to Run IrisEnroll3000

To start the **IrisEnroll3000**, click on the **IrisEnroll3000** menu item. The location of the program is shown in the figure below.

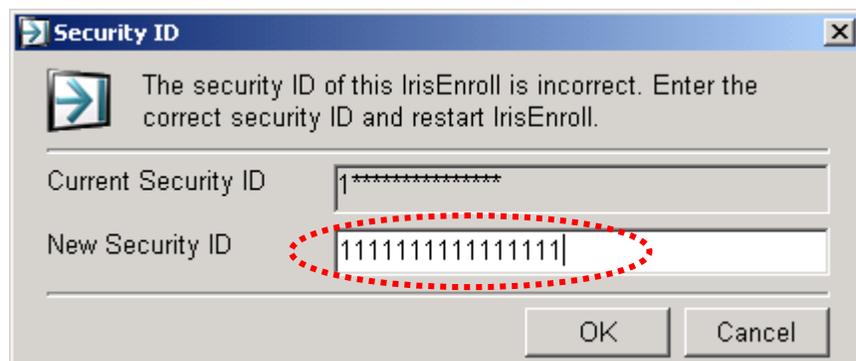


*Note:

IrisServer must be running before starting **IrisEnroll**.

IrisEnroll must first be registered in **IrisManager**.

If the security ID is not identical to the security ID typed in during IrisEnroll registration in IrisManager, the following **Security ID** window is displayed. This window is also displayed the first time IrisEnroll is started.



Enter the security ID of IrisEnroll. The security ID must be identical to the security ID typed in during IrisEnroll registration. Click the OK button.

The following Confirmation window is displayed.

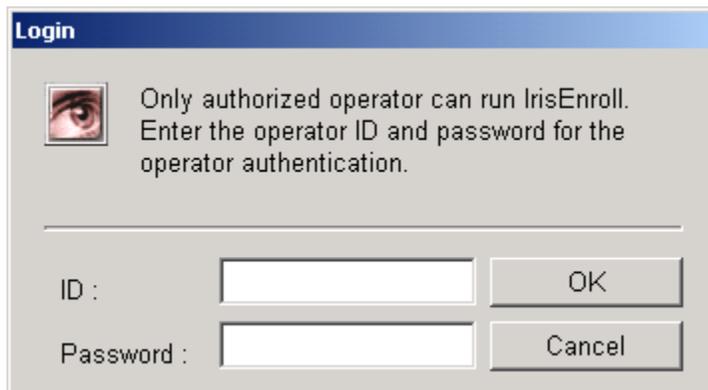


Check if the new security ID is correct and then click the Exit button.

Re-Start IrisEnroll.

11.1.2 How to Login to IrisEnroll3000

2. Successful execution of the **IrisEnroll** will open the following **Login** window for entering the User ID and password required to execute the **IrisEnroll**.
 - ◆ The **IrisEnroll** may only be executed by **Administrators and Operators with IrisEnroll privileges**.



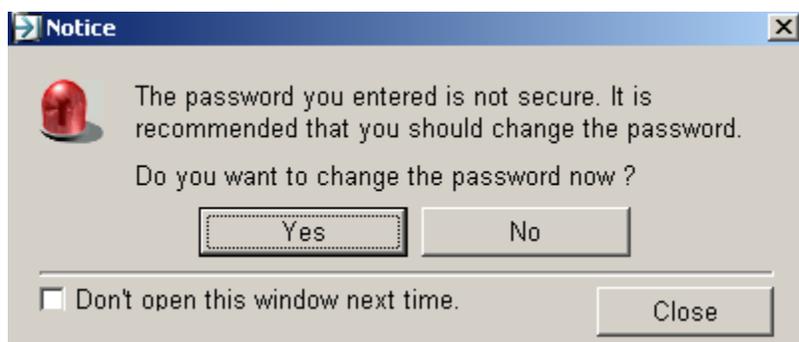
3. Enter the **ID** and **Password** of the operator who has **IrisEnroll** rights and click on the **OK** button.
 - ◆ Default ID and password are "**administrator**" and "**iris3000**" respectively. They can only be changed by an administrator. Refer to the section 2.2.8.2 Modification of the Administrator/Operator.

*

Note:

 If the login to the **IrisEnroll** is successful, then you may see the following **Notice** window,

if the password is not secured. (When you login with the default password “iris3000”)



Click on **No** to continue with the same password.

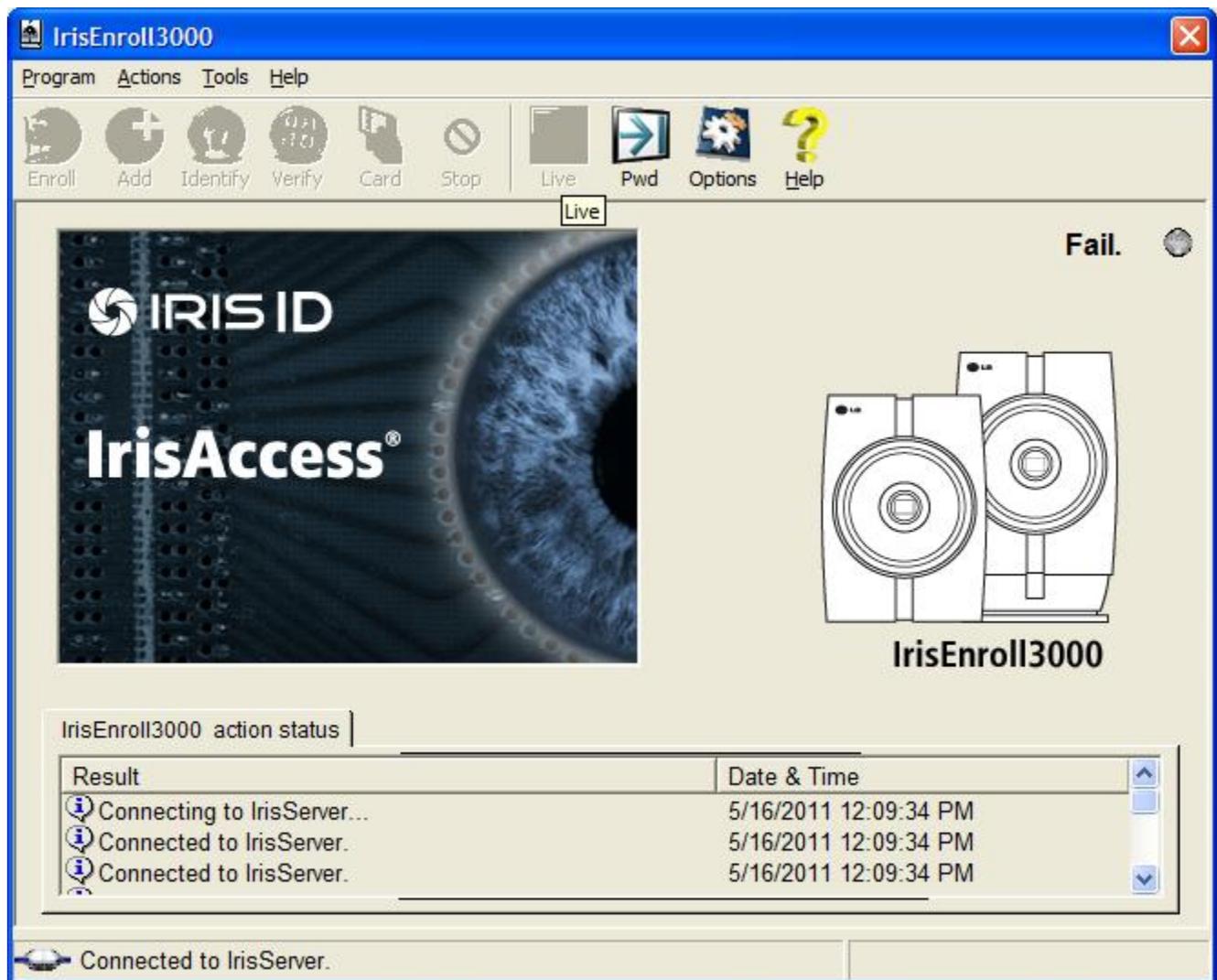
Click on **Yes** to open the following **Password** window to change the password.



Enter the current password in the **Current Password** field. Enter the **New Password** in the **New Password** field and the **Confirm Password** field, then before click on the **OK** button. This will change the password.

The following **IrisEnroll** window will open after changing the password successfully or aborting the password changing operation.

4. The same **IrisEnroll** window will be displayed without the **Notice** window, if the **ID** and **Password** are valid and the password is secured.



11.1.3 Enroll

Enrollment is the process of **adding new IrisCodes** into the system. The records are used during the **identification and verification** process to validate the user for access (entering or existing through the door).

The maximum number of users that can be registered is determined by each EAC S/W version.

*Cautions:

To decrease the “False Reject Rate” (Rejection of an Iris that should be accepted) and generate higher-quality IrisCodes, the user should follow the below recommendation.

- ◆ The user should open his/her eye as widely as possible. For example,



Correct



Incorrect

- ◆ The user should NOT rotate, pan and tilt his face. For example,



Correct



Incorrect



Incorrect



Incorrect

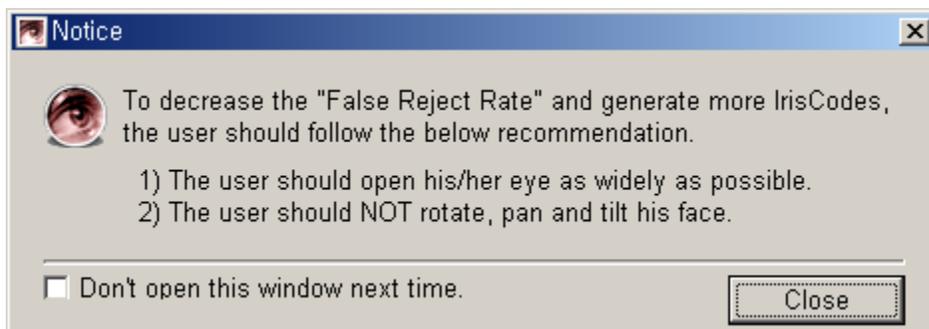
- ◆ Eyeglasses must be removed before enrollment, but may be worn during verification and identification.
- ◆ Contact Lenses with patterns that cover any part of the Iris may not be worn.

Limitation of ambient light in working environment

- ◆ When Fake Eye Detection is not used: 1,000 lx Fluorescent light and 100 lx Incandescent or sunlight.
- ◆ When Fake Eye Detection is used: 500 lx Fluorescent light and 50 lx Incandescent or sunlight.
- ◆ If the ambient light exceeds these limitations, the False Reject Rate will be increased.

The **enrollment** of the user can be performed using the following procedure.

1. Select the **Enroll** Item from the **Actions menu** in the menu bar or select the **Enroll** icon from the tool bar.
2. If you didn't select the "**Don't open this window next time**" check box on the following **Notice** window in previous enrollment, the **Notice** window is displayed. Read the message on the **Notice** window for good enrollment and click on the **Close** button. If you don't want this window to open next time, select the "**Don't open this window next time**" check box and then click on the **Close** button.



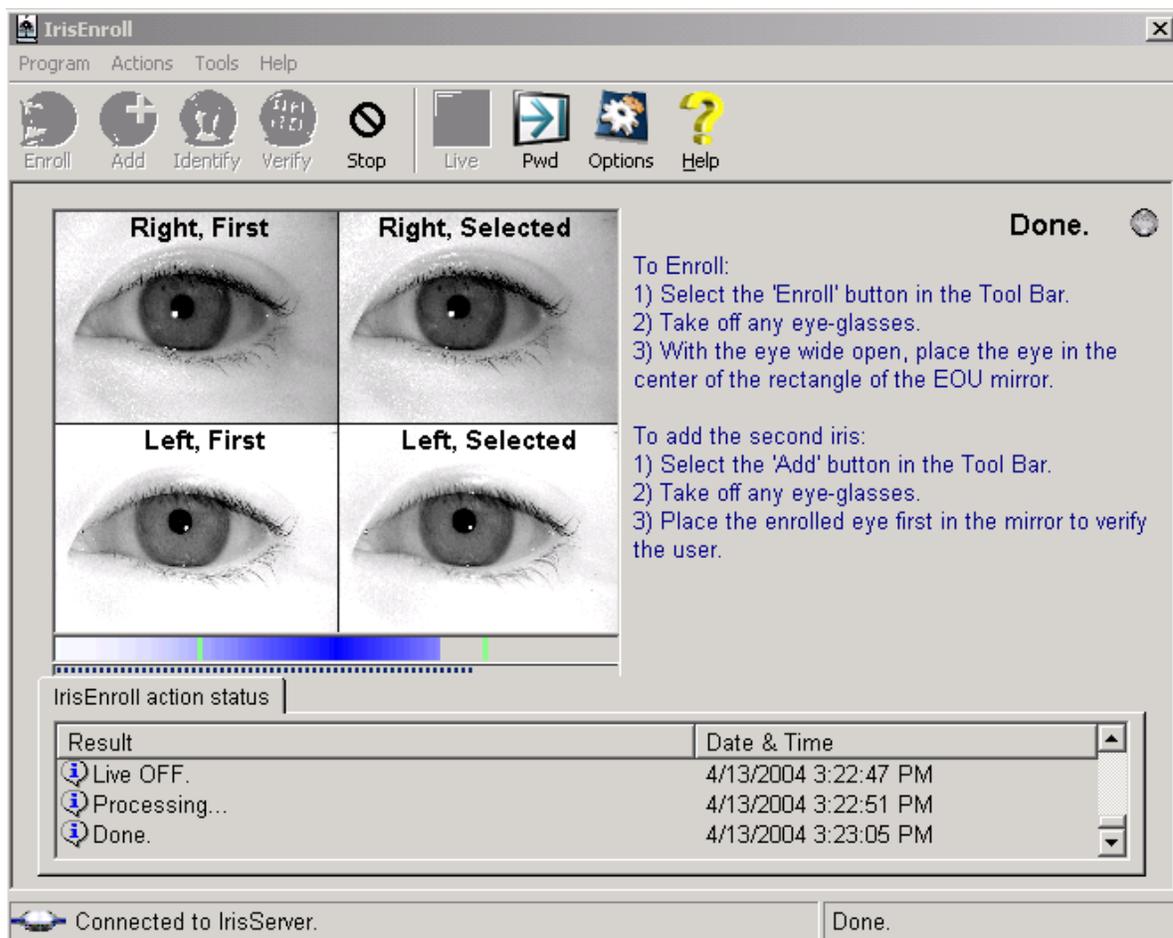
3. With the eye wide open, have the user center their eye in the rectangle on the mirror of the EOU, until the voice message of "Thank you for your cooperation" is heard. Any voice prompts, such as 'Please move back a little' should be followed.
4. If the image is not captured properly for enrollment, the following window opens on the screen.



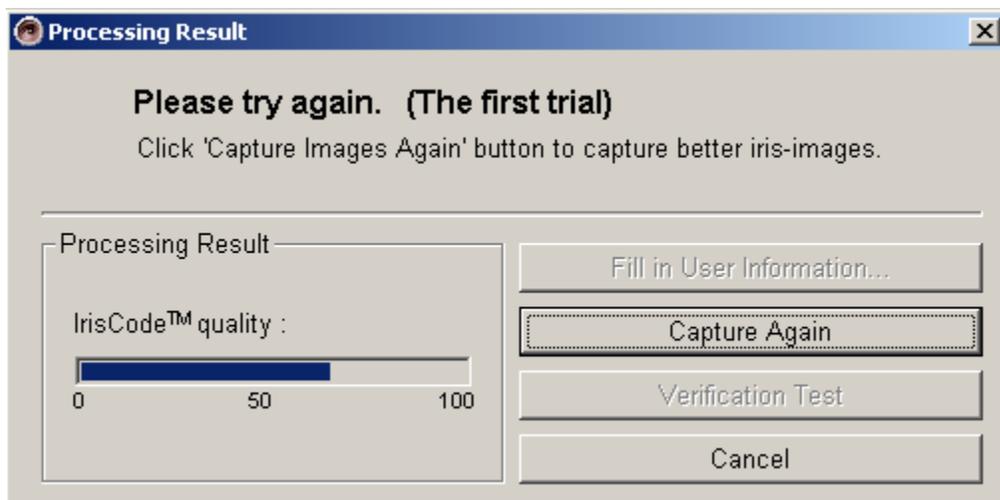
5. If your eye has already been enrolled in Server DB, the following window opens on the screen. In other words, if any iris already exists in the Server database, the iris may not be enrolled again.



6. After getting the Images, four captured images are displayed on the Main window and the quality of the IrisCode created is displayed in the **Processing Result** window.

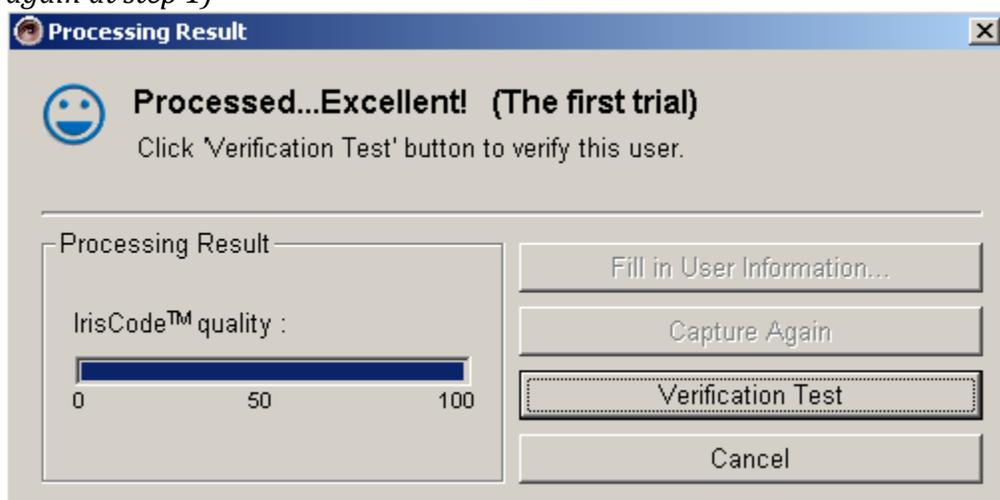


The system will ask to try again if the results of image processing are not of sufficient quality.



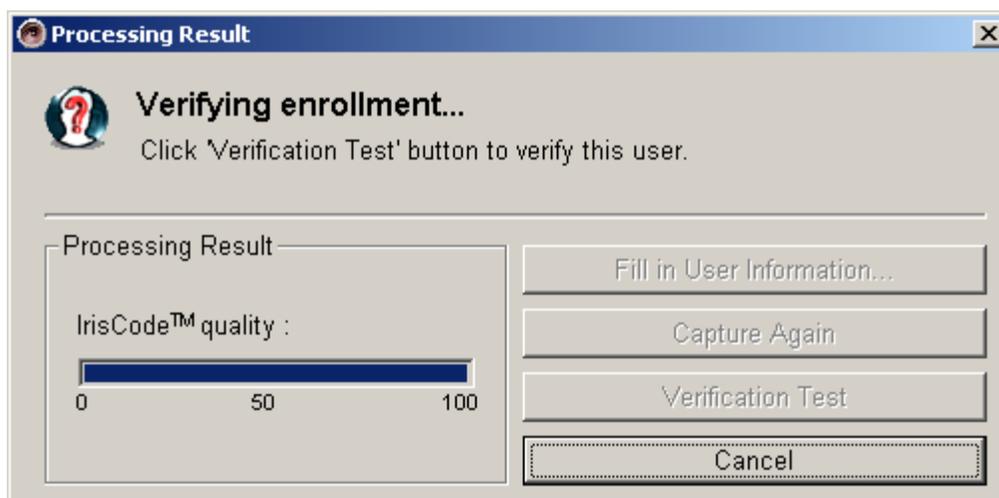
7. Click on the **Capture Again** button in the above box and the system will attempt to enroll the person again. The box below will be displayed if the image was properly captured. (**The system will ask to try again if the image was not captured properly on the second try.*)

It can be tried a maximum of three times. If you do not succeed on the third attempt, begin again at step 1)

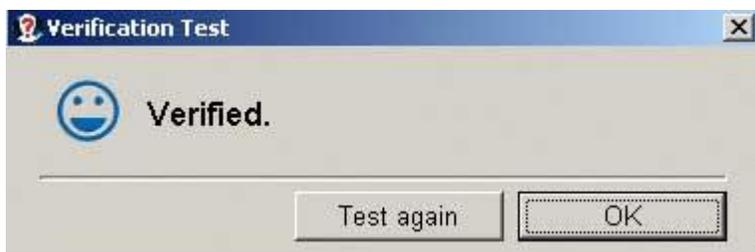


8. You must perform a verification test by clicking on the **Verification Test** button. IrisEnroll will prompt the user to present his/her iris again to the camera while displaying the window below.

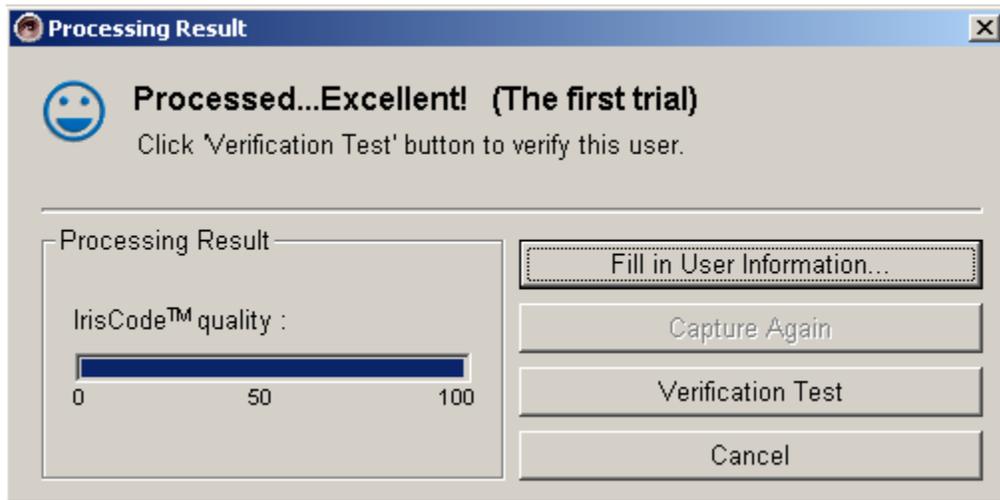
◆ After you click **Verification Test**, look into the center of the mirror of the EOU.



9. Once the verification is complete the window below is displayed.



10. To verify again, you may click the **Test again** button, or click the **OK** button, which will display the window shown below.



11. The User information can be entered on the **User Information** window, which may be opened by clicking on the button labeled **Fill in User Information**.

User Information

Type user ID and then click 'Get user information' button, then the rest of options will be enabled. If the user information already exists in the server DB, the information will be displayed.

* User ID

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

Name

First Name

MI

Last Name

Card

* Card ID

* Card Number

Photo

Delete photo

Gender

Female

Male

* Eye

Left Right

Use warning eye

Left Right

< Back

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

- A. **If the user with the entered User ID does not exist in the Server database**, the message box titled **"User Information is not found"** is shown and the rest of the text boxes will be enabled.

- B. ***If the user with the entered User ID already exists in the Server database, and one of the user's irises is enrolled,*** the user may only enroll the second iris through the "Add" button on the main **IrisEnroll** screen.



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: 123456 Get user information

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

Name

First Name: Brandy
 MI:
 Last Name: Park

Card

None
 * Card ID:
 * Card Number:

Photo

Select Photo...
 Delete photo

Gender

Female
 Male

* Eye

Left Right

Use warning eye

Left Right

Click the 'Next' button to continue.

< Back Next > Cancel

When a user that does not already exist in the Server database is enrolled (Refer item 11.A), the window above is shown.

13. Enter the following information in their respective text boxes.

- a. Enter the **First Name, MI and Last Name of the user.** (Optional)

- b. If the system is used with a card reader and/or access panel, select the card type in the card drop-down. When a card type is selected, the **Card ID** and **Card Number text boxes** will be activated. To complete the registration of card information, **Card ID** and **Card Number** must be filled. If not, the warning window will be displayed.
 - ◆ **Card ID: Card ID is the effective data that is used in verification mode or for Card ID, Wiegand or RS422 output. When the wiegand/RS422 output ports are activated, Card ID is outputted in the configured format after the user is identified.**
 - ◆ **Card Number: Card Number is assigned by the Card Manufacturer. It is commonly printed on the card.**

- c. Select the **Eye** (left/right) from the check boxes.
 - If both the eyes are enrolled, one eye may be assigned as a **warning eye**. If a user is forced to access the door by an unauthorized intruder the user may use the warning eye. The remote unit opens the door as an authorized user, but notifies IrisServer (or IrisMonitor) of the emergency.

- d. Select the **Gender** (Female/Male) from the radio buttons. (Optional)

- e. **Select Photo** (Optional). If you want to delete the registered photo of user, select the **Delete Photo** in the check box.

(If using Wiegand or RS422, the user ID should be a positive integer and the configuration of the ICU should be completed properly. Please refer to section 2.4.2 and 2.4.3 in the document **IrisAccess Software Installation Manual** (Document No. DV002S501)).

User Information

Enter the Department, Position, Home Phone number, Mobile Phone number, Office Phone number, E-mail, Address, Resident Number and descriptions (Memo1-5) of the user.

* User ID: 123456 Get user information

Detail information of the user

Department	Division	Position	Engineer
Phone(Home)	02-526-1234	Phone(Mobile)	019-526-1234
Phone(office)	02-526-1234	E-mail	Brandy@giris.com
Address	Seoul, Korea		
Resident Num	800225-1234567		
Memo 1	Memo1		
Memo 2	Memo2		
Memo 3	Memo3		
Memo 4	Memo4		
Memo 5	Memo5		

< Back Next > Cancel

14. Enter the **Department, Position, Home Phone number, Office Phone number, Mobile Phone number, E-mail, Address, Resident Number** and **descriptions (Memo1-5)** of the user. (All Optional)
15. Click on the **Next >** button to set the User's Access Rights.

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: 1982 Get user information

Assign access rights to the user.

Visitor

Remote Group: All, Group1, Medical, NFC Add

Access Rights:

Remote Group	Time Group	Delete
All	All	

Time Group: All, TG1 Add

A term of validity (mm/dd/yyyy)

Start Date: Delete

Expire Date: Delete

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

< Back Next > Cancel

16. In this window select the check box labeled **Visitor** if the **User** is a **Visitor** with temporary access rights.

17. If the user type is **General User**: (The **Visitor** check box is NOT selected)

- h. Select the **Remote group** of this user.
- i. Click on the **Add** button under the **Remote Group**.
- j. Select the **Time Group** of the user.
- k. Click on the **Add** Button under the **Time group**.

- l. The Selected Remote Group and Time Groups may be viewed in the **Remote Group and Time Group** List in the **Access Rights** section.
- m. **Users** may be removed from **Remote** and **Time Groups** by selecting the **Groups** in the **Access Rights** section and clicking on the **Delete** button.
- n. You may set the **Start Date** and **Expiration Date** for the user. If you do not select a **Start Date** and **Expiration Date** for the user, their **Access Rights** are always valid.

To set the Start Date:

- Press the **Calendar** button next to **Start Date**.
- On the Calendar screen that opens, select the first date that the User's **Access Rights** will take effect.
- Press the **Ok** button to enter the **Start Date**, or Press the **Cancel** button to cancel the date selection.
- Repeat the process for the **Expire Date**

If a **Remote Group** or **Time Group** is selected, the **Detail** button may be pressed to display the **Remote Unit(s)** in the **Remote Group** or the valid times under the **Time Group**.

Remote Name	IP address	Channel ID	Use Type	Description
R137-1	150.140.62.131	1	Identification	
R137-2	150.140.62.132	2	Access In	
R137-3	150.140.62.133	3	Identification	
R137-4	150.140.62.134	4	Access In	

Sunday	Monday	Tues...	Wedn...	Thurs...	Friday	Satur...	Holiday
00:00...	00:00...	00:00...	00:00...	00:00...	00:00...	00:00...	00:00...

Multiple **Remote** and **Time Groups** may be assigned to a single user by repeating steps a - g. A maximum of 10 access rights may be assigned to a single user.

18. If the **User** is a **Visitor**:

- b) Check the check box labeled **Visitor** and enter the visitor information
- c) Select the **Remote group** of the visitor,
- d) Click on the **Add** button under **Remote Group**, to add the **Visitor** to the **Remote Group**.
- e) The selected **Remote Group** will be listed in the **Remote Group** list under **Access Rights**.
- f) You may set the **Start Date** and **Expiration Date** for the user. If you do not select a **Start Date** and **Expiration Date** for the user, their **Access Rights** are always valid. To set the **Start Date**:
 - i. Press the **Calendar** button next to **Start Date**.
 - ii. On the Calendar screen that opens, select the first date that the User's **Access Rights** will take effect.

- iii. Press the **Ok** button to enter the **Start Date**, or Press the **Cancel** button to cancel the date selection.
- g) Repeat the process for the **Expire Date**.
- h) The valid access times (start time and the end time) during the selected valid days for the visitor can be selected by choosing the starting and ending hours and minutes in **Reservation time for Visitor**. Only one Reservation time can be set.

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

All
Group1
Medical
NFC

Access Rights

Remote Group		Delete
All		

A term of validity (mm/dd/yyyy)

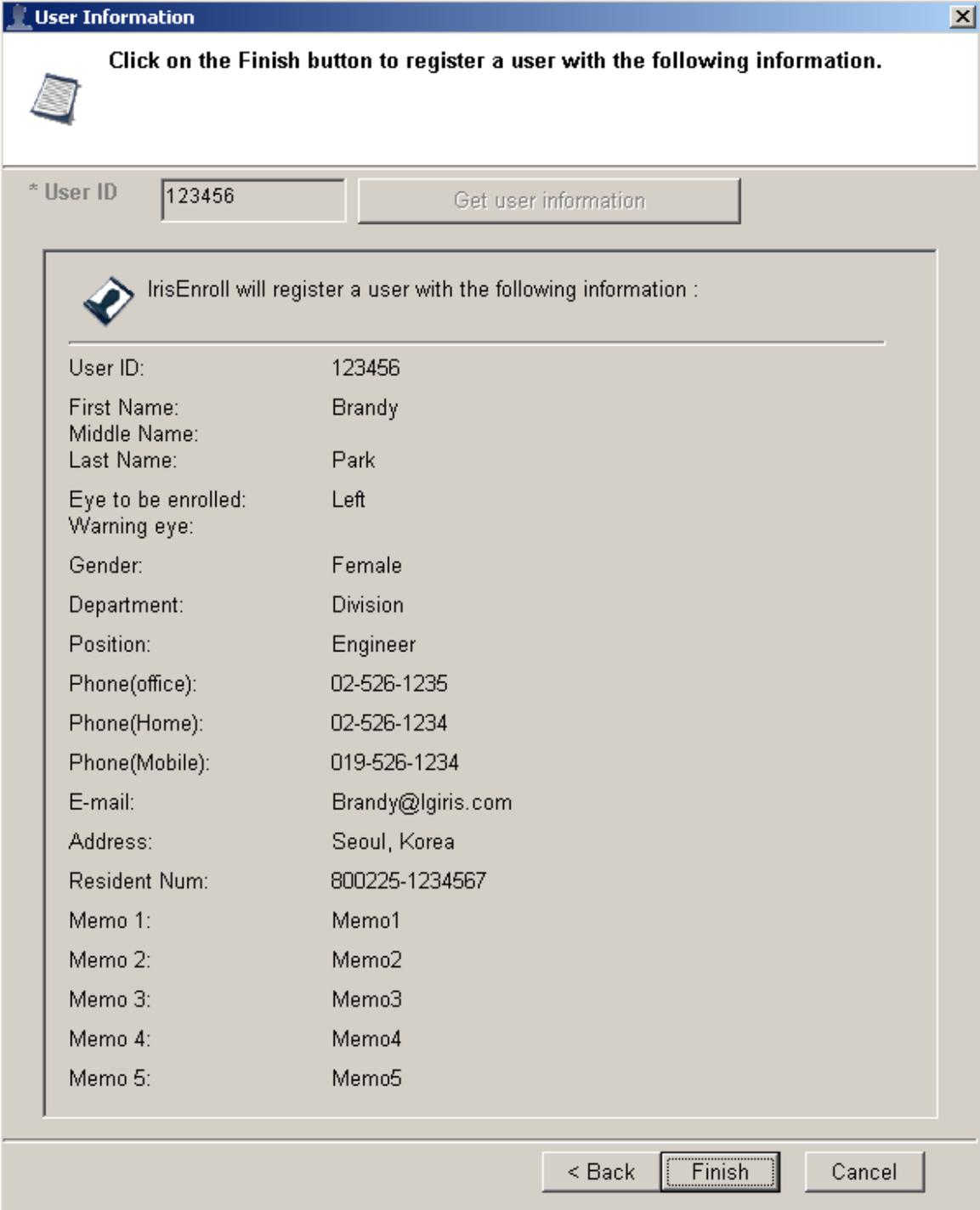
Start Date	<input style="width: 100%;" type="text" value="05/16/2011"/>	Delete	
Expire Date	<input style="width: 100%;" type="text" value="05/28/2011"/>	Delete	

Reservation time for visitor

~

Remote Name	IP address	Channel ID	Use Type	
101-I	172.19.6.40	1	Access In	▲
102-O	172.19.6.40	2	Access Out	
103-I	172.19.6.41	1	Access In	▼

19. Click the **Next** button.



The dialog box titled "User Information" contains the following elements:

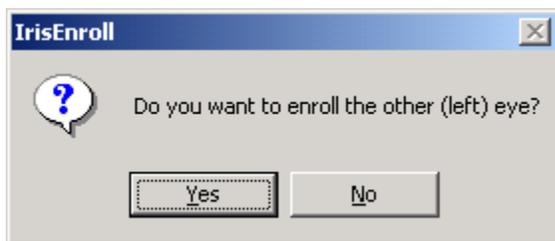
- Header: "Click on the Finish button to register a user with the following information." with a document icon.
- Input field: "* User ID" with the value "123456" and a "Get user information" button.
- Summary section: "IrisEnroll will register a user with the following information :" with an iris icon.
- User details table:

User ID:	123456
First Name:	Brandy
Middle Name:	
Last Name:	Park
Eye to be enrolled:	Left
Warning eye:	
Gender:	Female
Department:	Division
Position:	Engineer
Phone(office):	02-526-1235
Phone(Home):	02-526-1234
Phone(Mobile):	019-526-1234
E-mail:	Brandy@lgiris.com
Address:	Seoul, Korea
Resident Num:	800225-1234567
Memo 1:	Memo1
Memo 2:	Memo2
Memo 3:	Memo3
Memo 4:	Memo4
Memo 5:	Memo5

Buttons at the bottom: "< Back", "Finish", and "Cancel".

20. This window shows a summary of the information of the enrolled user. Click on the **Finish** button.

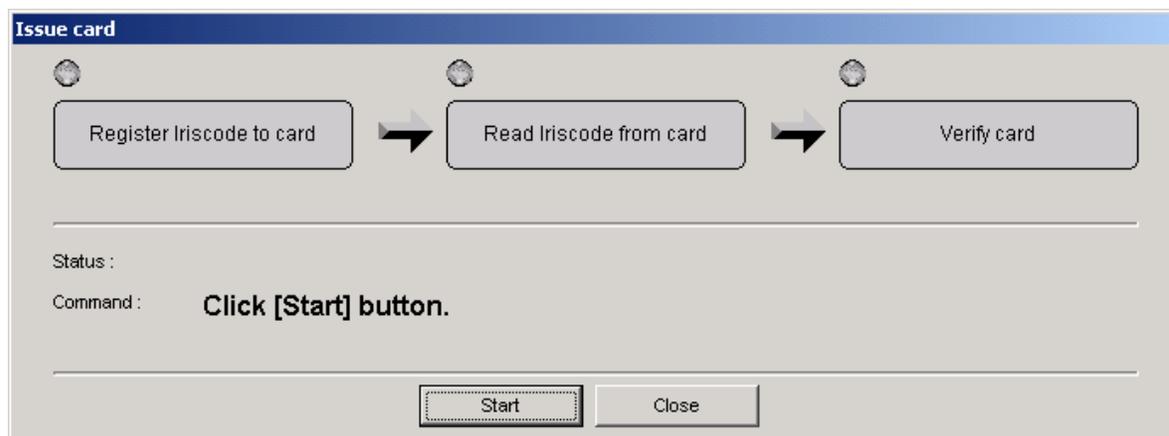
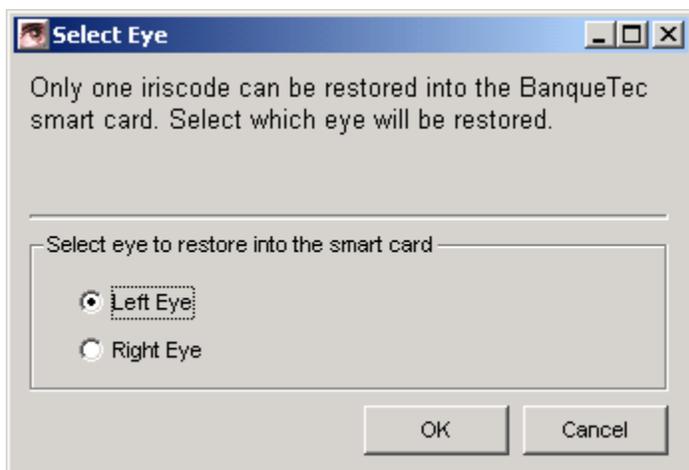
21. When the enrollment is finished, the window shown below opens on the screen. If you want to continue to enroll another eye, click **Yes**, and begin from step 3 above.



22. If the user selected to use a Smart Card, the next window opens. The card must be issued. The card may be issued by carrying out following steps:
- Encryption keys must have already been generated and registered in **IrisServer**.
 - **Use Smart Card** check box in the **Options** window of **IrisEnroll** must be checked.
 - Card combo box in the User Information window must have been set to Smart Card

*Note:

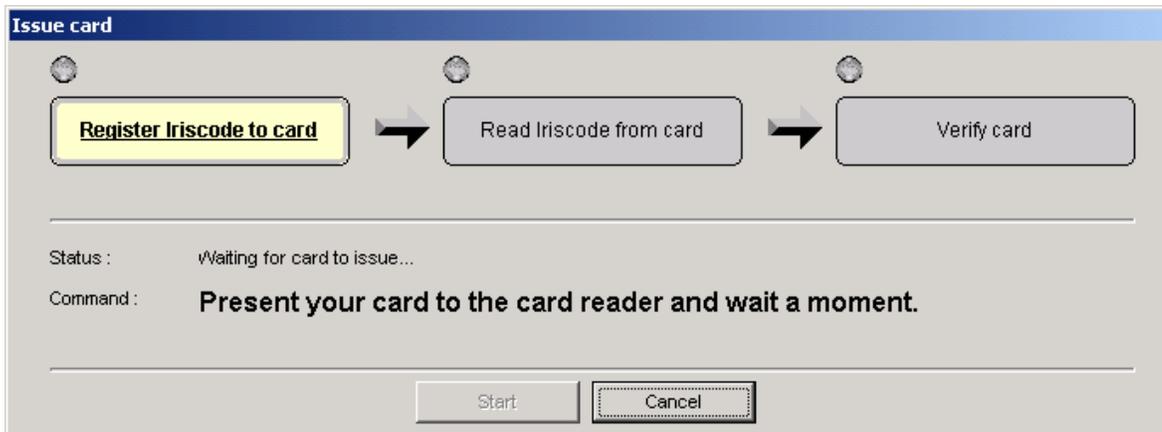
If the user uses a Smart Card of the type "BanqueTec", it is not possible to write both eyes to the BanqueTec type Smart Card. The next window opens after the user enrolls both eyes.



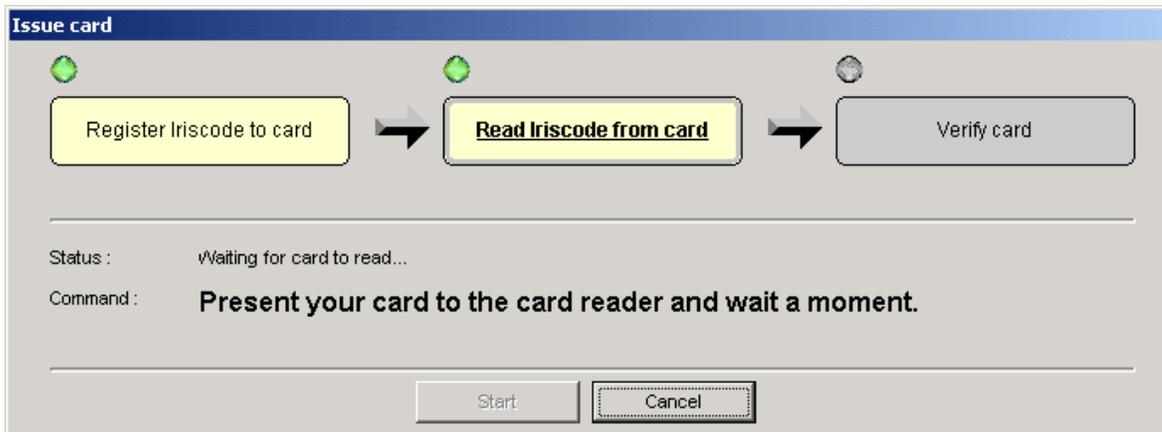
- A. If the operator clicks the “Start” button in the “Issue card” window, the 3 step Smart Card process begins:

Note: Before beginning the Smart Card issuing process, the Smart Card must already be within range of the Smart Card Reader / Writer. If not, an error will occur. If this happens, press the **Ok** button on the error window, place the Smart Card within range of the Smart Card Reader/Writer and press the **Start** button again.

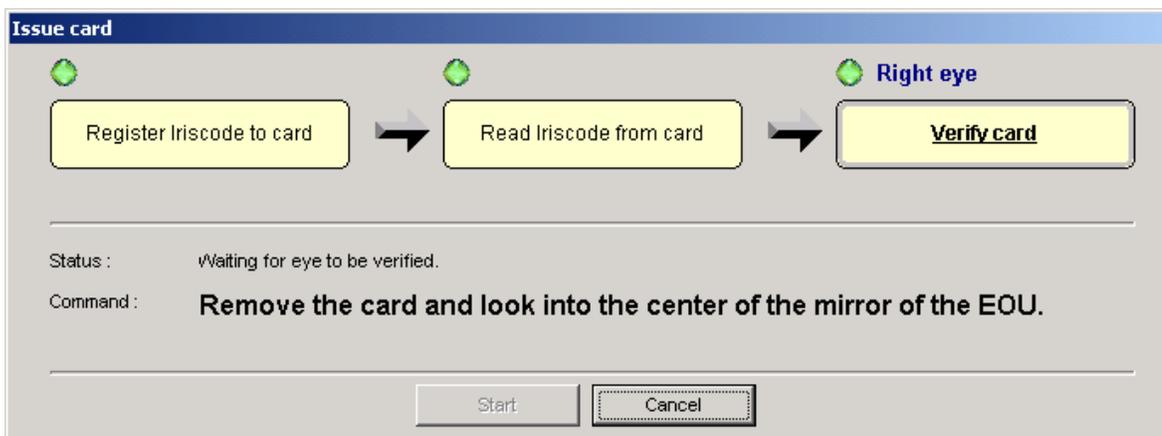
- 1) Register the IrisCode to the card



- 2) Read the IrisCode from card (for verification)



- 3) Verify card by comparing the read IrisCode to a live Iris. The User will be asked to present their eye to the optical camera again.



If the process completes successfully, the following window is displayed.



*Note:

 If the Smart Card type is "HID", it is possible to write both eyes to the Smart Card. The user may issue both eyes on the card by following the process below.

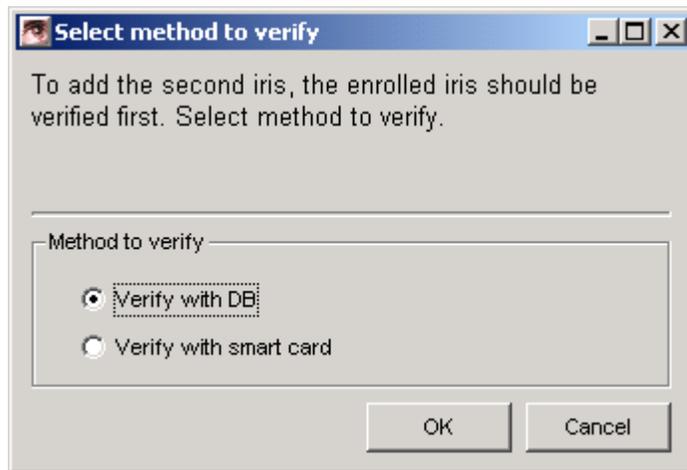
Register IrisCode to card → Read IrisCode from card → Verify one eye → Verify another eye.

11.1.4 Add

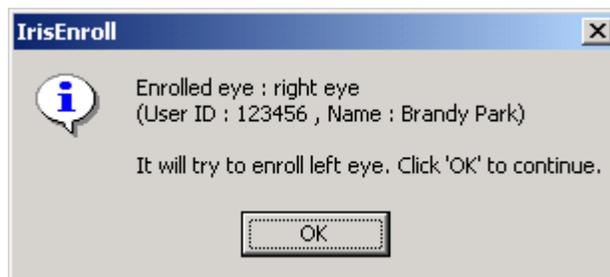
The **Add** feature is used to enroll a second eye when one eye of a user is already enrolled in the Server database.

The **Add** process can be done using the following steps.

1. Select the **Add** Item from the **Actions menu** on the menu bar or select the **Add** icon from the tool bar. The following window will be displayed:



2. To add another eye, the enrolled iris will be verified first. The user can verify her/his iris from either the database or a Smart Card. Select either the **Verify with DB** or **Verify with smart card** button.
3. Have the user verify her/his eye. The next window will open on the screen. Press the OK button and enroll the second eye.



The **User Information** window opens, but the only modification possible is to set **1** eye as the warning eye.

User Information

All fields of user information except for the 'Use warning eye' are not enabled. The operator cannot either enter new information or modify the information, but it is possible for the operator to see the existing information.

* User ID: 1982 Get user information

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

Name

First Name: Ajay
MI:
Last Name: Vishwakarma

Card

Smart Card Use as Prox Card
Enter Card ID
Wiegand Data Length (No of Bits)
* Card ID: 1234567890 Get From iCAM
* Card Number: 12345677890 Get From Card

PIN

**** Show PIN

*** Eye**

Right Use warning eye
 Left Left Right

Photo

Capture Image
Select Photo...
 Delete photo

Gender

Female
 Male

Click the 'Next' button to continue.

< Back Next > Cancel

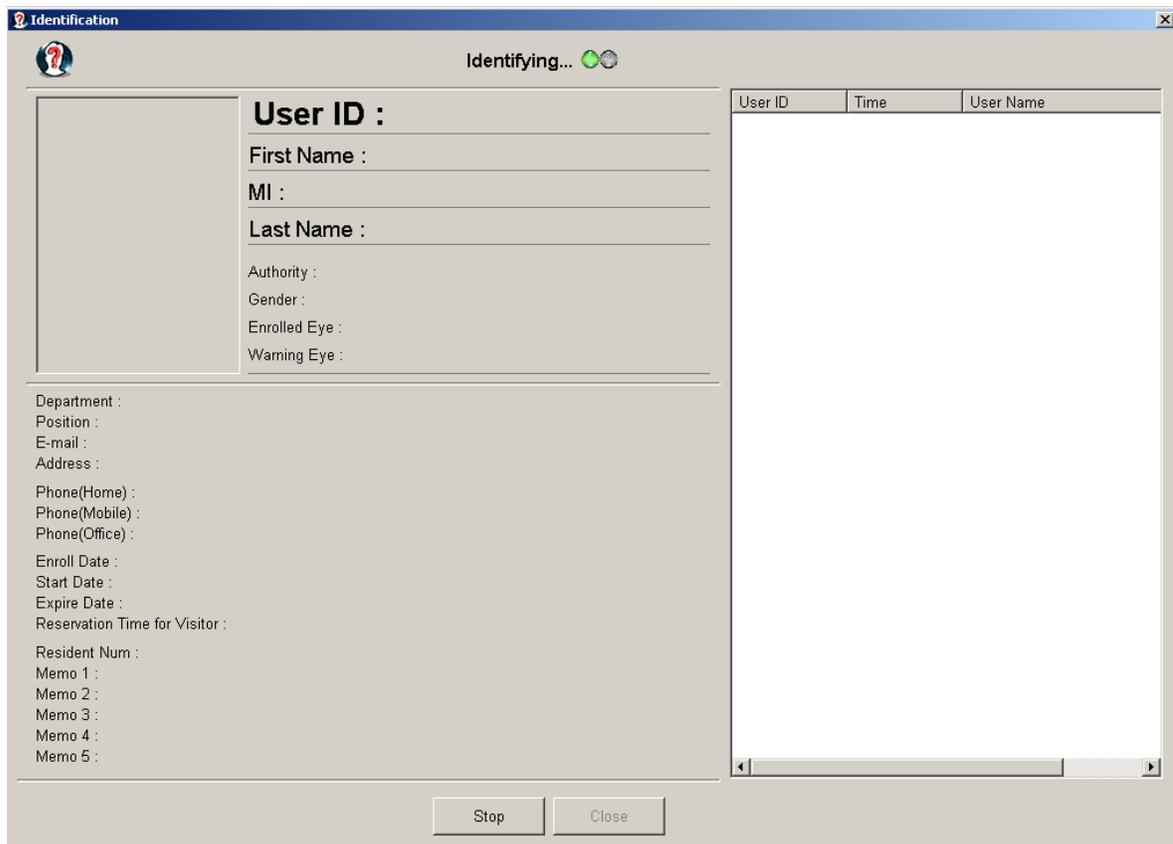
4. Click the **Next** button.

11.1.5 Identify

The **Identify** feature is used to identify a user by comparing the IrisCode™ of the user to all existing IrisCodes™ in the system. (1: N matching)

The Continuous Identification process can be done using the following steps.

1. Select the **Identify** Item from the **Actions menu** in the menu bar or select the **Identify** icon from the tool bar. The following identification window will be displayed.



The screenshot shows a window titled "Identification" with a status bar "Identifying...". The window is divided into several sections:

- User ID :** A large empty text field.
- First Name :** A text field.
- MI :** A text field.
- Last Name :** A text field.
- Authority :** A text field.
- Gender :** A text field.
- Enrolled Eye :** A text field.
- Warning Eye :** A text field.
- Department :** A text field.
- Position :** A text field.
- E-mail :** A text field.
- Address :** A text field.
- Phone(Home) :** A text field.
- Phone(Mobile) :** A text field.
- Phone(Office) :** A text field.
- Enroll Date :** A text field.
- Start Date :** A text field.
- Expire Date :** A text field.
- Reservation Time for Visitor :** A text field.
- Resident Num :** A text field.
- Memo 1 :** A text field.
- Memo 2 :** A text field.
- Memo 3 :** A text field.
- Memo 4 :** A text field.
- Memo 5 :** A text field.

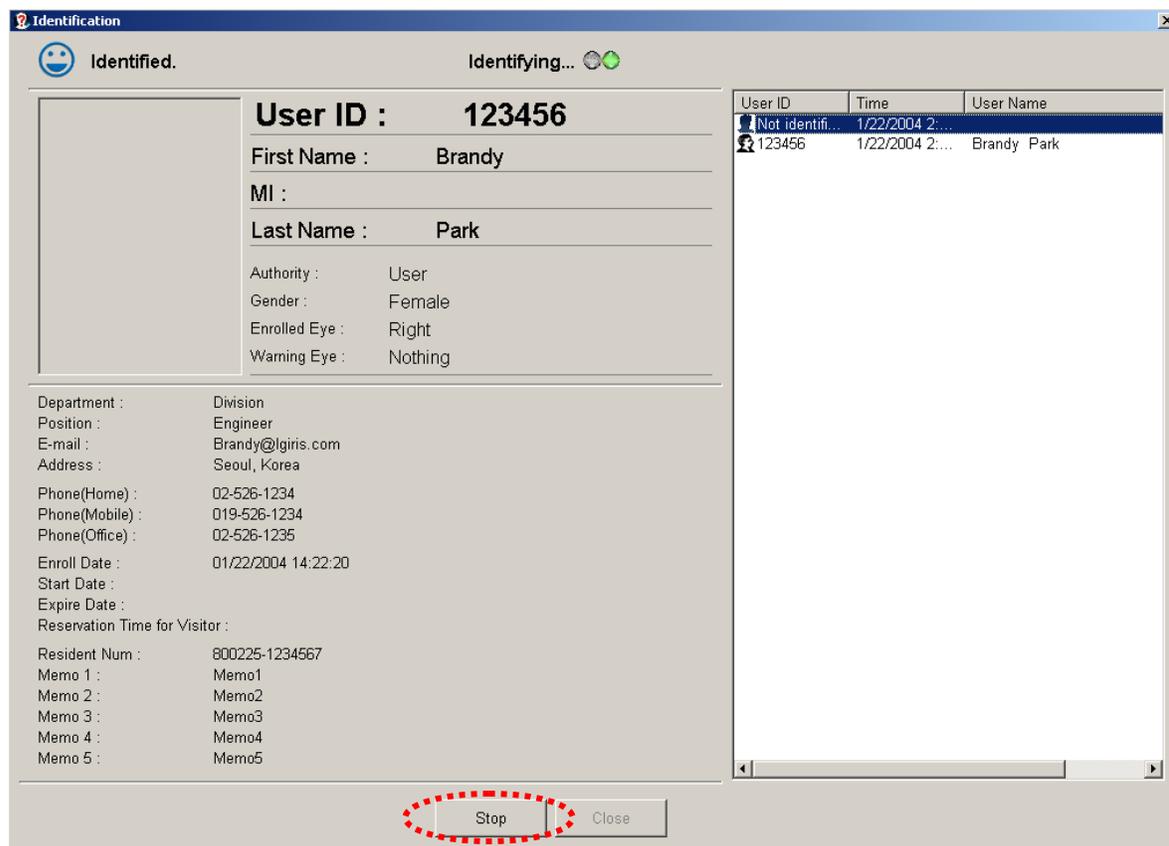
On the right side, there is a table with the following columns:

User ID	Time	User Name
---------	------	-----------

At the bottom of the window, there are two buttons: "Stop" and "Close".

2. Have the User look into the center of the mirror of the EOU.

The IrisCode™ of the user will be generated from Iris images and compared with the existing IrisCode™ in the database. If the IrisCode™ matches with any of the enrolled IrisCodes™, then the user is identified as a valid user. The window after the identification of the sample user is shown below:



If the user's IrisCode™ does not match with an enrolled IrisCode™, then a **'Not Identified'** message will be displayed and all information items in the screen will be cleared.

3. Identification mode runs continuously until the operator clicks the **Stop** button or the **Close** button.

Until the **Stop** button is clicked, the continuous identification process is active. If you click on the **Close** button, the identification window will be closed.

- ◆ **Notice: Information about the identified user to be displayed in the identification window can be selected by checking the check boxes in the option window. (Refer to section 2.3.8.5 Display)**

11.1.6 Verify

Verification is the process of verifying the user, by checking the IrisCode™ of the User with either:

- IrisCode™ of the User from the provided User ID in the database or
- IrisCode™ of the User from the provided IrisCode in the Smartcard

Select the **Verify** Item from the **Actions menu** in the menu bar or select **Verify** from the tool

bar, to open the **Verification** window. **Verify with smartcard** button is enabled only when “Use smartcard” option is checked in the Smartcard window under **Options** menu. (Refer to the Section 2.3.8.6 Smartcard in this manual).

To verify the User by User ID



1. Enter the User ID of the User in the **User ID** field in the **Verification** window
2. Clicking the **Verify** button begins the Iris Image capture process.
3. After you click the **Verify** button, look into the center of the mirror of the EOU.
4. After the Iris image is captured, the result of the verification will be shown in the **Verification** window. A sample of the **Verification** window after a successful verification is shown below.



The image shows a software window titled "Verification" with a blue title bar and a close button. Inside the window, there is a "Verified." status with a smiley face icon. The user information is displayed in a structured format:

User ID :	123456
First Name :	Brandy
MI :	
Last Name :	Park
Authority :	User
Gender :	Female
Enrolled Eye :	Right
Warning Eye :	Nothing

Department :	Division
Position :	Engineer
E-mail :	Brandy@lgiris.com
Address :	Seoul, Korea
Phone(Home) :	02-526-1234
Phone(Mobile) :	019-526-1234
Phone(Office) :	02-526-1235
Enroll Date :	01/22/2004 14:22:20
Start Date :	
Expire Date :	
Reservation Time for Visitor :	
Resident Num :	800225-1234567
Memo 1 :	Memo1
Memo 2 :	Memo2
Memo 3 :	Memo3
Memo 4 :	Memo4
Memo 5 :	Memo5

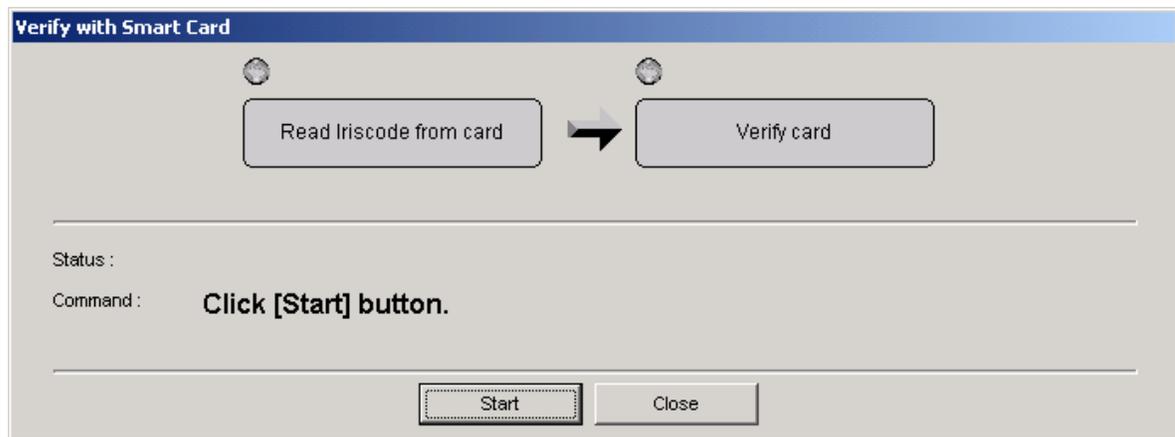
At the bottom of the window, there are two buttons: "Try again" and "Close".

5. If not verified, click on the **Try again** button.
6. If you click the **Close** button, the verification window will be closed.

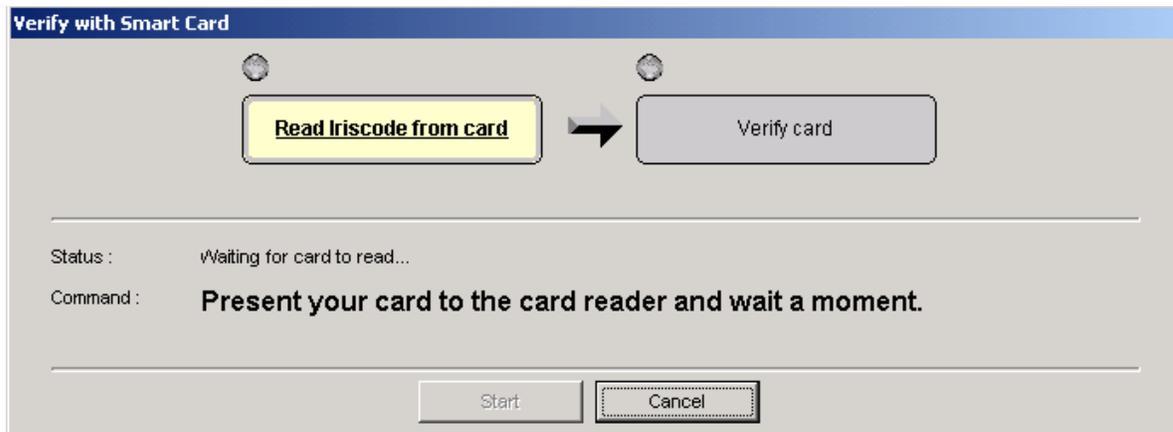
To verify a User with Smart Card



1. Click the **Verify with Smart Card** button in the **Verification** window and the **Verify with Smart Card** window will be displayed.



2. Click the **Start** button and the **Verify with Smart Card** window will begin reading the Smart Card. The Smart Card should be within range of the Smart Card Reader before pressing the **Start** button.



3. Present the Smart Card and wait until the EOU prompts the user to look into the mirror.
4. After the Iris image is captured, the result of the verification will be shown in the **Verification** window. A sample of the **Verification** window after a successful verification is shown below.



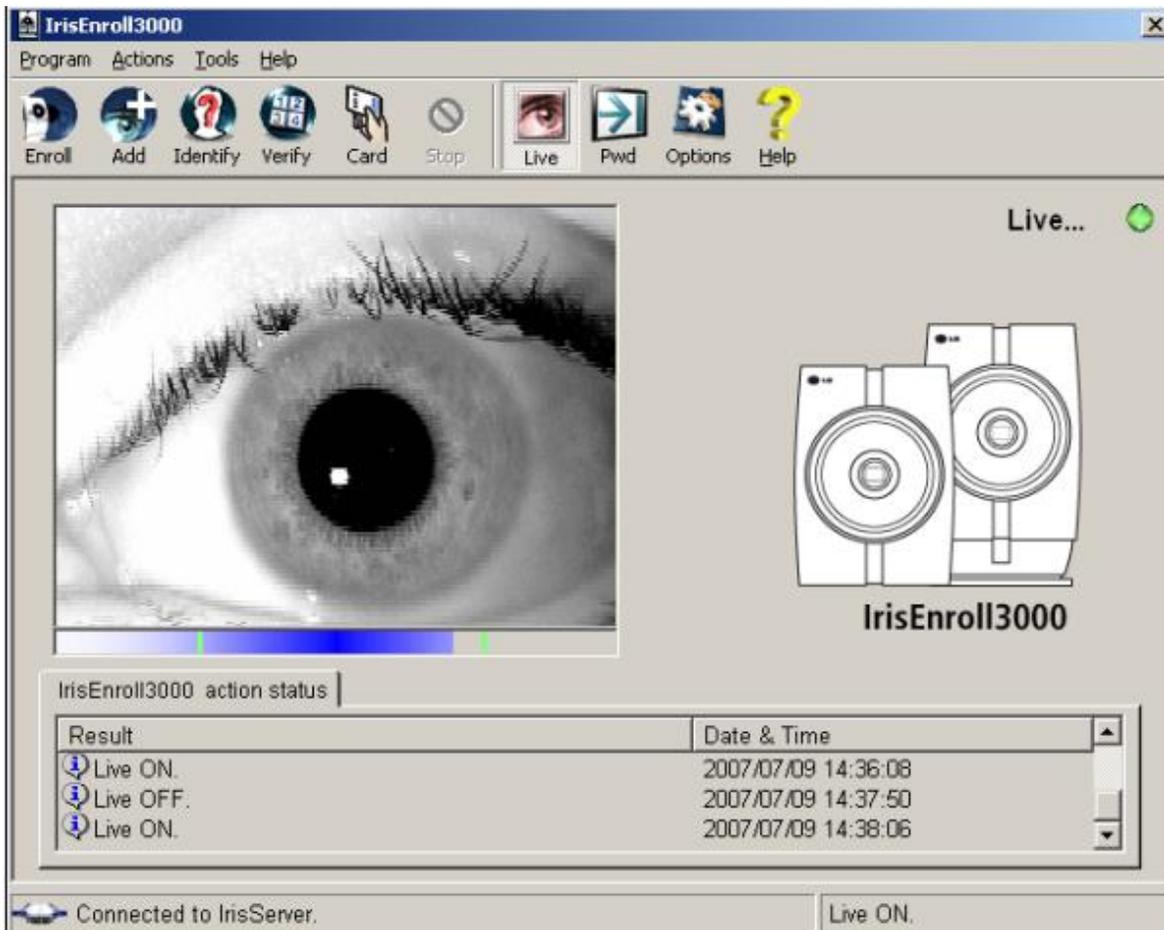
The image shows a software window titled "Verification" with a blue header bar. Inside the window, there is a smiley face icon and the text "Verified.". Below this, a large empty rectangular box is on the left. To its right, user information is displayed in a list format, with labels in bold. The information includes: User ID (123456), First Name (Brandy), MI (blank), Last Name (Park), Authority (User), Gender (Female), Enrolled Eye (Right), and Warning Eye (Nothing). Below this section, a list of fields and values is shown, including Department, Position, E-mail, Address, Phone numbers, Enroll Date, Start Date, Expire Date, Reservation Time for Visitor, Resident Num, and five Memo fields. At the bottom of the window, there are two buttons: "Try again" and "Close".

User ID :	123456
First Name :	Brandy
MI :	
Last Name :	Park
Authority :	User
Gender :	Female
Enrolled Eye :	Right
Warning Eye :	Nothing

Department :	Division
Position :	Engineer
E-mail :	Brandy@lgiris.com
Address :	Seoul, Korea
Phone(Home) :	02-526-1234
Phone(Mobile) :	019-526-1234
Phone(Office) :	02-526-1235
Enroll Date :	01/22/2004 14:22:20
Start Date :	
Expire Date :	
Reservation Time for Visitor :	
Resident Num :	800225-1234567
Memo 1 :	Memo1
Memo 2 :	Memo2
Memo 3 :	Memo3
Memo 4 :	Memo4
Memo 5 :	Memo5

11.1.7 Live View

This functionality is used only to view the live video from the Iris Camera.



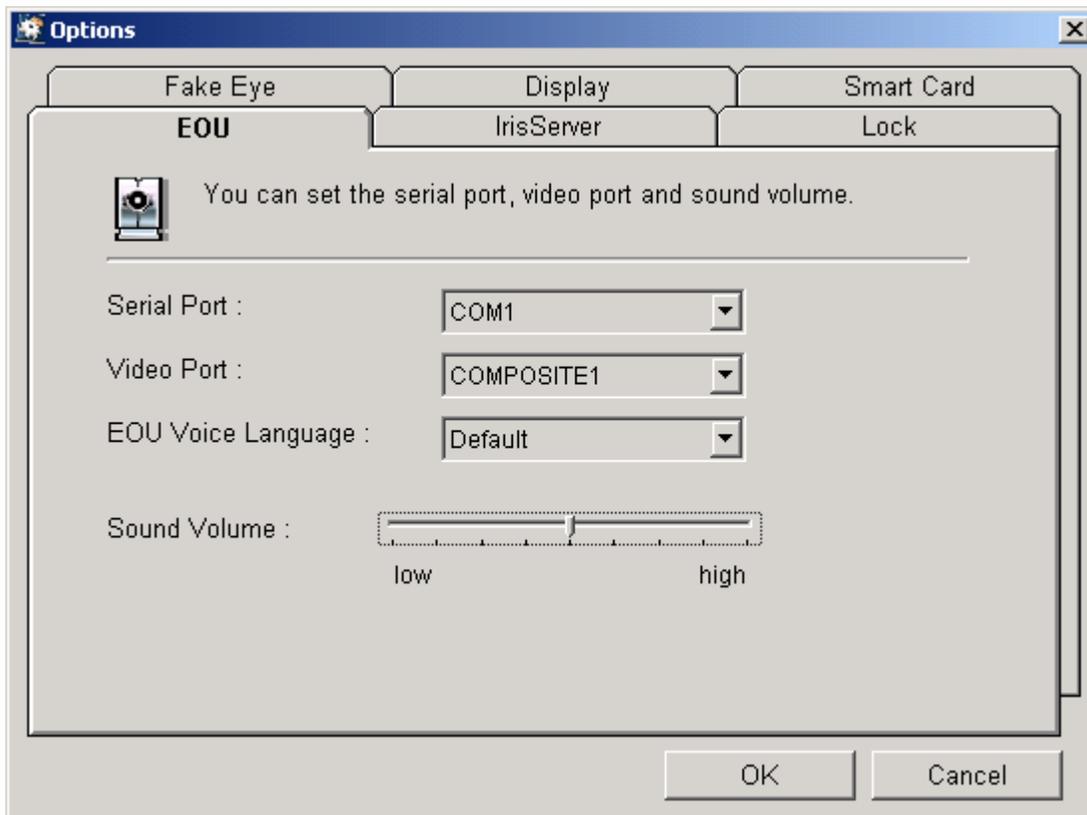
11.1.8 Option Settings

The **Options** Item is used to set various options such as:

1. To set the Serial port, Video port and sound volume of the Enrollment Optical Unit (EOU).
2. To change the IrisServer's IP address.
3. To configure the program lock feature.
4. To enable/disable the fake eye detection.
5. To configure the items displayed in the continuous identification window.

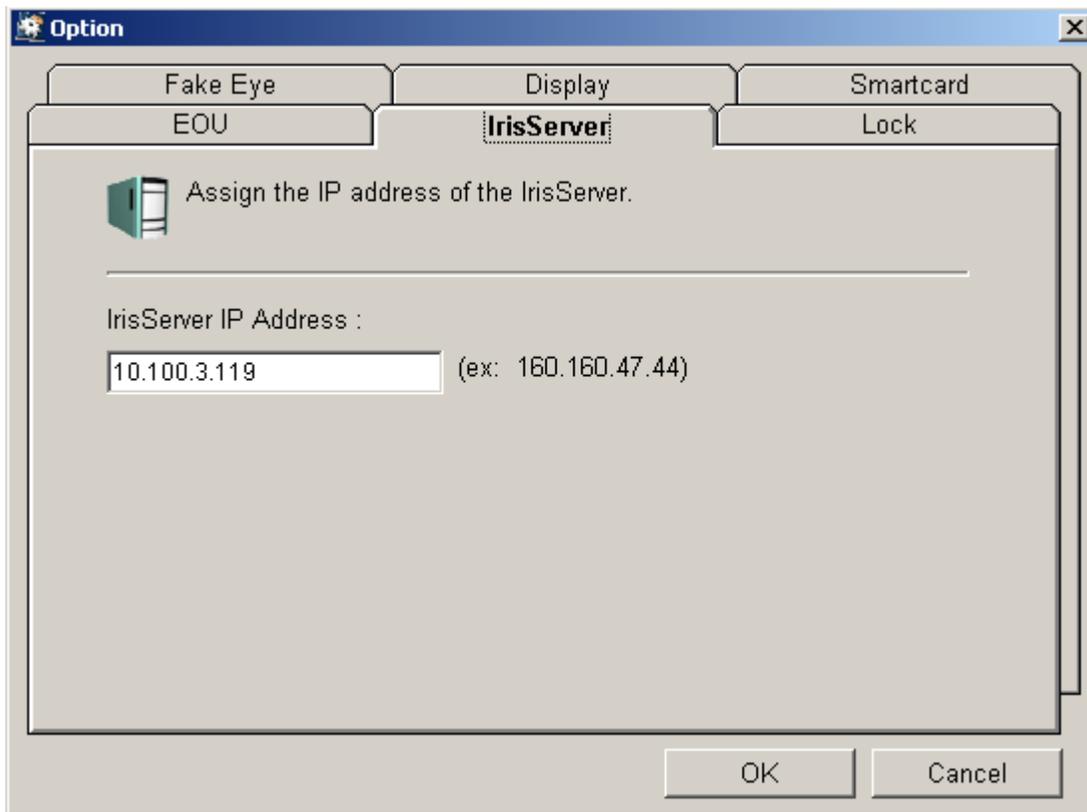
11.1.8.1 EOU Setting

By selecting the EOU tab on the Option dialog box you can set the Serial Port, Video Port and the sound volume as shown below. Default Serial Port and Video Port are "**COM1**" and "**COMPOSITE1**" respectively. Select **EOU Voice Language** – Default or Korean. Select Default unless EOU has the Korean Sound files loaded.



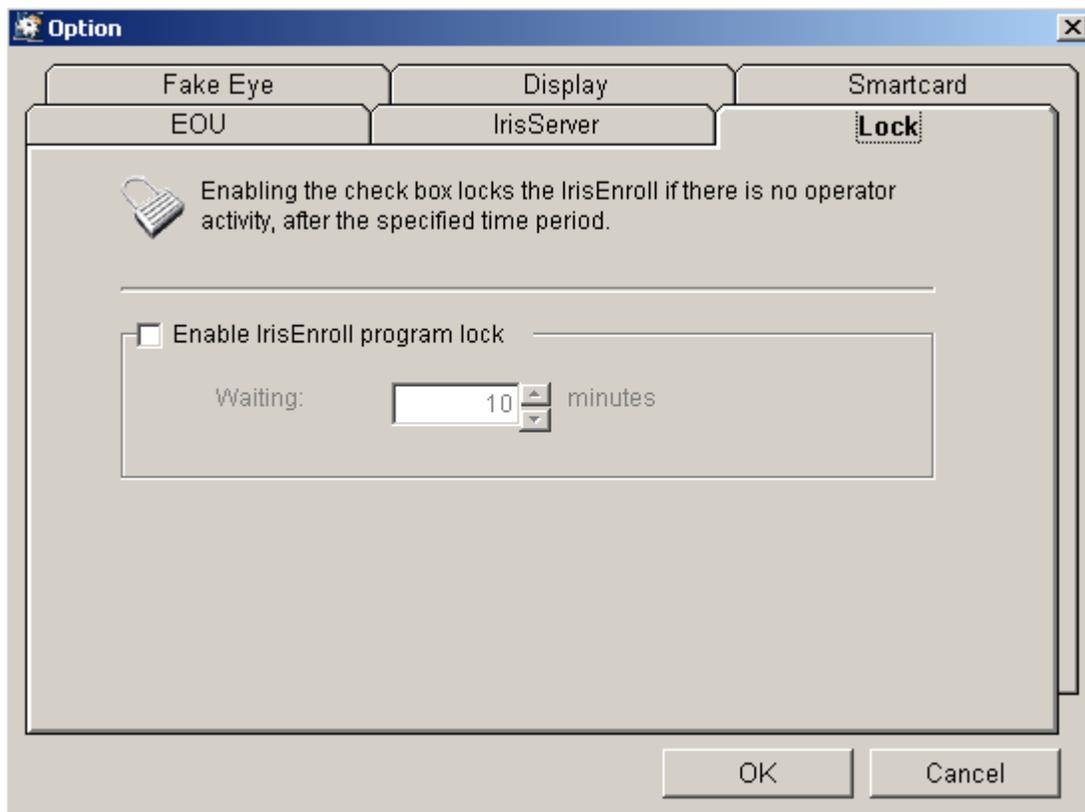
11.1.8.2 IrisServer IP Address

The IrisServer IP Address may be set by selecting the **IrisServer** tab field in the **Options** window and entering the IP Address of the IrisServer. If IrisEnroll is located on the same computer as IrisServer, we recommend setting the IP Address to the loopback address (127.0.0.1).



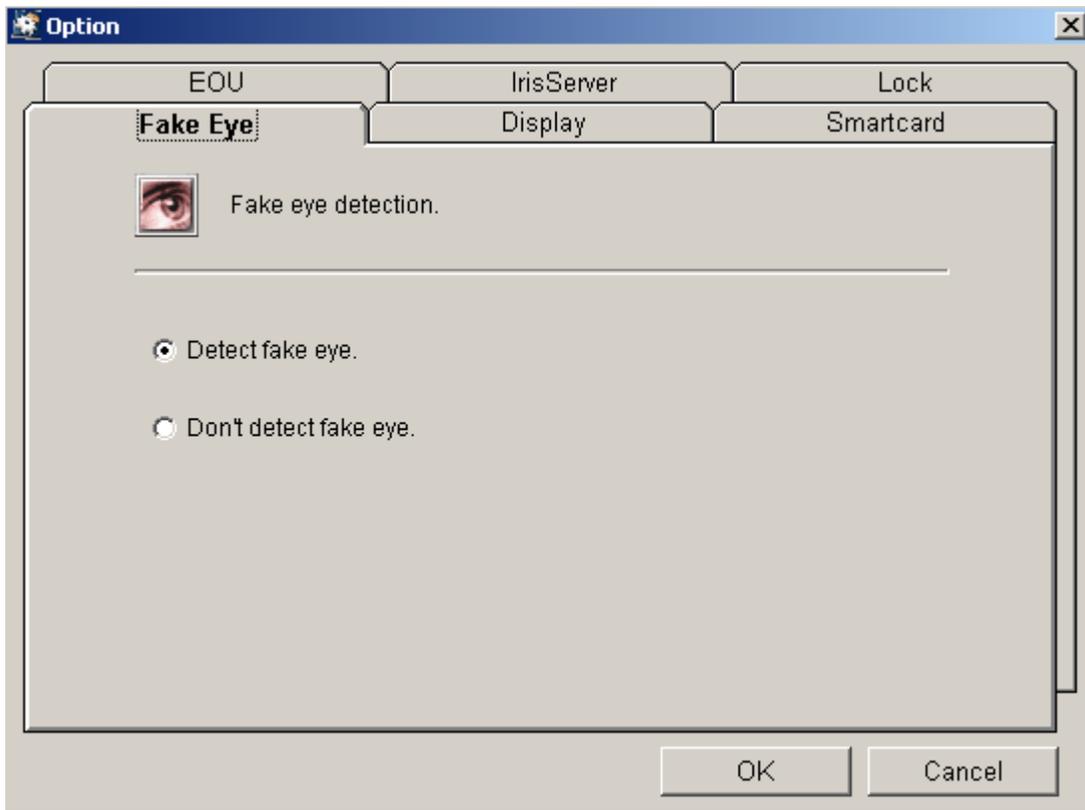
11.1.8.3 Program Lock

The **Program Lock** functionality is used to lock the application if there is no action within the specified time. Once the program is locked, the Operator must re-login to use the application. The **Lock** may be enabled by selecting the **Lock** tab field. Check the check box labeled **Enable IrisEnroll Program lock** to enable the **lock**. To disable the program lock feature, uncheck the check box labeled **Enable IrisEnroll Program lock**.



11.1.8.4 Fake Eye Detection

Fake eye detection can be configured by selecting the fake eye tab of the option window, which will display the following window.



If you want the fake eye detection to be enabled, select the **Detect fake eye** radio button and click the **OK** button. Fake Eyes will be detected when a user tries to enroll, identify or verify.

Fake Eye detection does increase the time required for enrollment, identification or verification, but greatly enhances the security of the system.

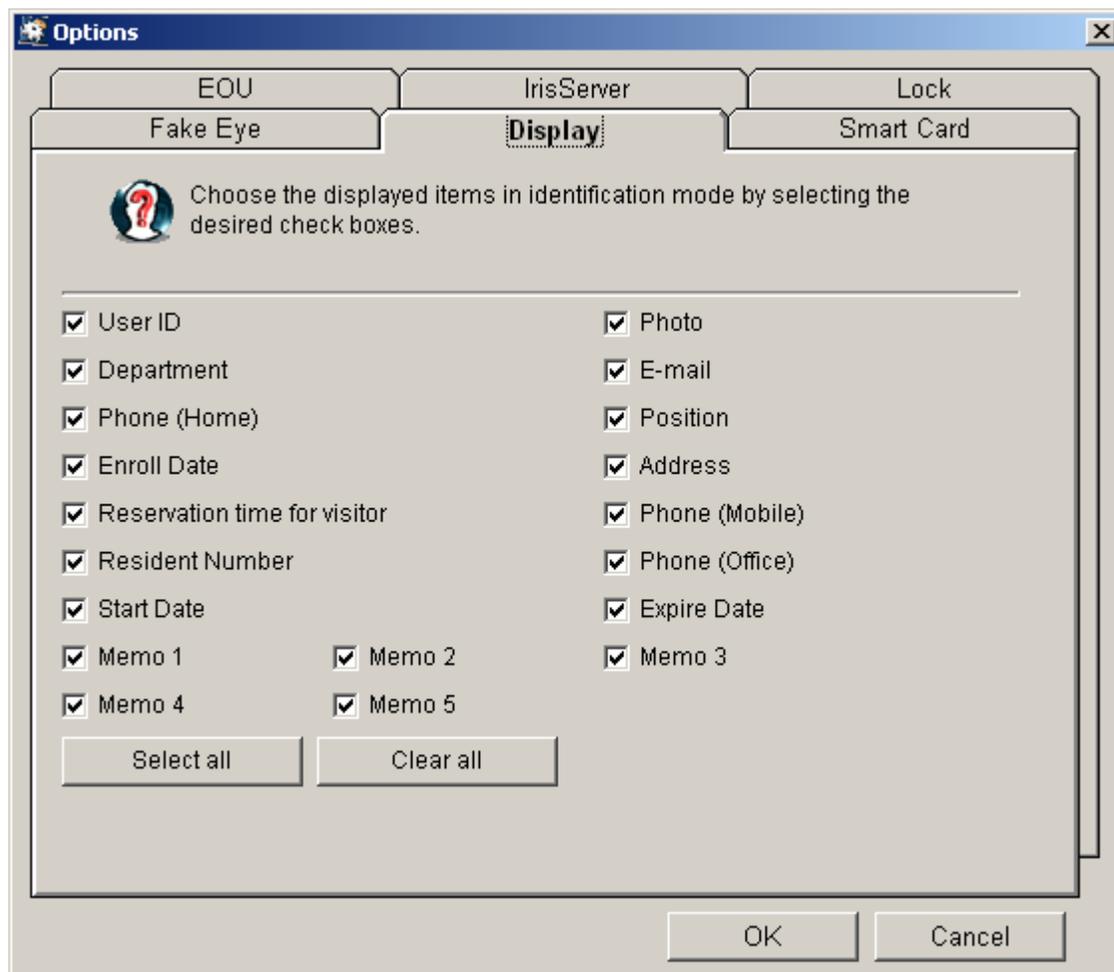
If you don't want the fake eye detection to be enabled, then select the **Don't detect fake eye** option and click the **OK** button. If so, fake eye will NOT be detected when a user tries to enroll, identify or verify.

- ◆ **Caution:** Limitation of ambient light in working environment
 - When Fake Eye Detection is not used: 1,000 lx Fluorescent light and 100 lx Incandescent or sunlight.
 - When Fake Eye Detection is used: 500 lx Fluorescent light and 50 lx Incandescent or sunlight.
 - If the ambient light exceeds the limitation, the False Reject Rate will be increased.

11.1.8.5 Display

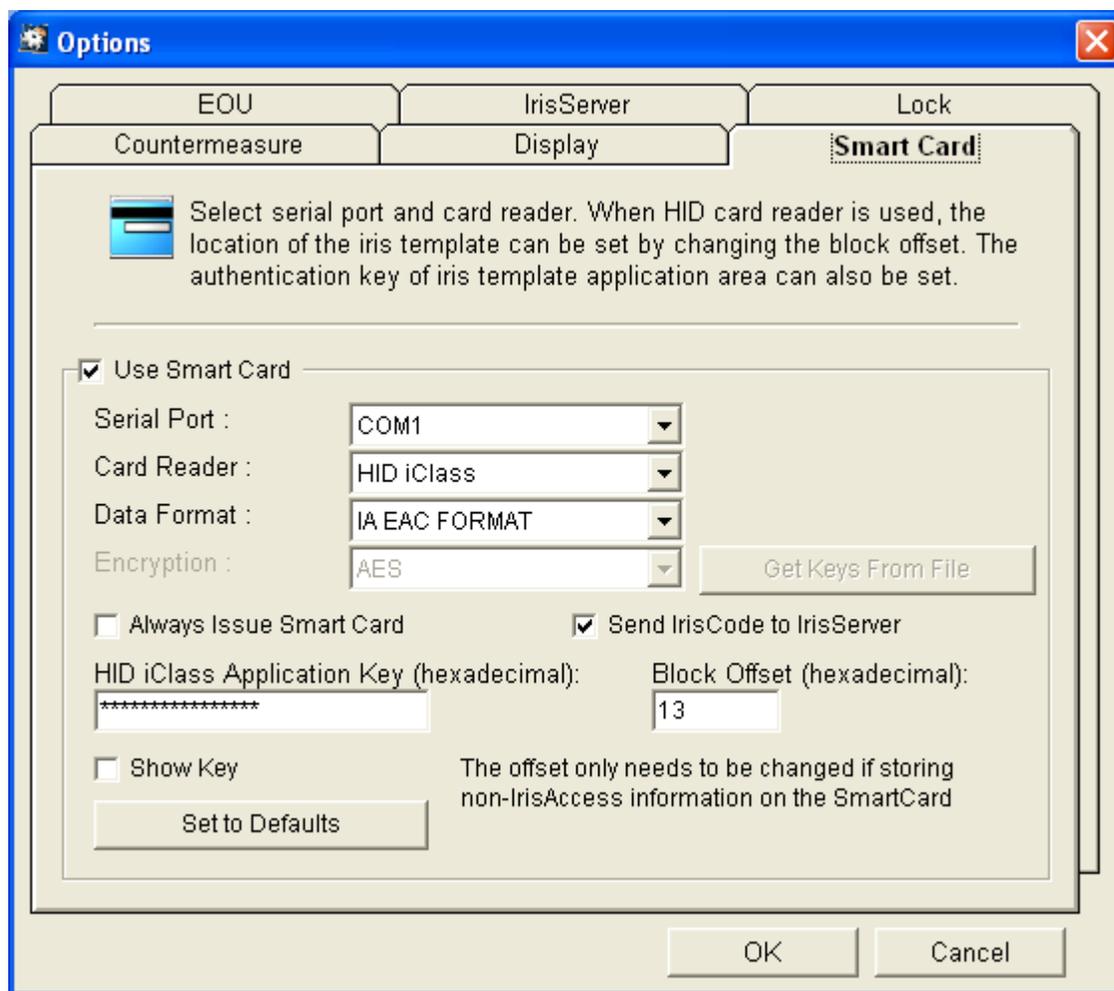
Items to be displayed during the continuous identification mode may be selected by checking check boxes below (Refer to the section 2.3.5 Identify in this manual).

All check boxes are checked by default when **IrisEnroll** program is first installed. If you click on the **Select all** button, all check boxes are checked. If you click on **Clear all** button, all check boxes are unchecked.



11.1.8.6 Smart Card

Selecting the Smart Card tab of the Options window configures the Smart Card reader/writer. Selecting this tab displays the following window.



Selecting the “Use Smart Card” checkbox enables the other Smart Card options. Options to be configured are the serial port to which the reader/writer is attached and the type of Smart Card reader/writer. You may also configure the options “Always Issue Smart Card” and “Send IrisCode to IrisServer”.

By default, “Use Smart Card” and “Always Issue Smart Card” options are deselected.

Serial port of the Smart Card reader/writer should be different than the serial port of the EOU.

If the card reader type is HID, the fields “HID iClass Application Key” and “Block Offset” must be filled. Each value must be entered in hexadecimal format. The length of “HID iClass Application Key” is 8 bytes (16 hexadecimal characters) and the length of “Block Offset” is 1 byte (2 hexadecimal characters). Block Offset needs to be set only if storing non IrisAccess information. The valid values for offset should be in the range of 06~B3. By default “HID iClass Application Key” is masked. To display unmasked key, select “Show Key” check box.

When issuing Smart cards, data format and type of encryption to use may be set in this tab. “Data Format” displays the formats supported for Smart Cards namely, IAEAC and GSC-IS formats. In IAEAC format, encryption keys have to be generated using IrisServer. When set to GSC-IS format, type of encryption may be set to AES, DES, DES3 or no encryption. In each of

these, the encryption key file containing the corresponding encryption key has to be loaded using "Get Keys From File". Once set, the Smart Cards will be issued in the corresponding format with required encryption.

"Get Keys From File" – Click this button to load the file containing the encryption key for the selected encryption type.

"Set to Defaults" – Click this button to set the default values for "HID iClass Application Key" and "Block Offset".

"Always Issue Smartcard" checkbox – When this is checked, IrisEnroll will issue a Smart Card for every user enrolled.

When this is unchecked, the operator can decide whether to issue a card and also the type of card to be issued during the enrollment process. In this case the "Card" combo box on the "User Information" window of the enrollment process provides 3 options to select from, "None", "Smartcard" and "Prox Card".

"Send IrisCode to IrisServer" checkbox – Selecting this checkbox configures IrisEnroll to send the IrisCode to the IrisServer after enrolling the user.

When "Send IrisCode to IrisServer" checkbox is deselected, the IrisCode is **not** sent to the IrisServer after enrolling. This option can be used to save the IrisCode on a Smart Card only instead of the IrisServer.

***Caution:** if the "Card" combo box of the "User Information" window has "None" or "Prox card" selected, the IrisCode will not be saved anywhere.

11.1.9 Password

The current password of the **IrisEnroll** operator may be changed by using this feature.

1. Select the **Change Password** Item from the **Tools** in the menu bar or select the **Pwd** button from the tool bar, to open the following **Password** window.
2. Enter the **current password**.
3. Enter the **New password** and **confirm** the new password.
4. Click on the **OK** button to complete the password change operation.
5. Click on the **Cancel** button to cancel the password change operation.



11.1.10 Security ID

The current security ID of IrisEnroll may be changed by using this feature. The security ID of IrisEnroll may be changed as follows:

1. Select the **Security ID** Item from the **Tools** menu in the menu bar. The following **Security ID** window is displayed.
2. Enter the **New security ID**.
 - ◆ Security ID must consist of 16 characters that are numbers, capital or lower case letters and special characters. The Security ID must match exactly with the Security ID entered in **IrisManager** for this instance of **IrisEnroll**. The Security ID is case-sensitive - upper and lower case letters are considered different (example: 'a' does not match with 'A')
3. Click on **OK** button to complete the security ID change operation.



11.2 IrisICUAdmin3000

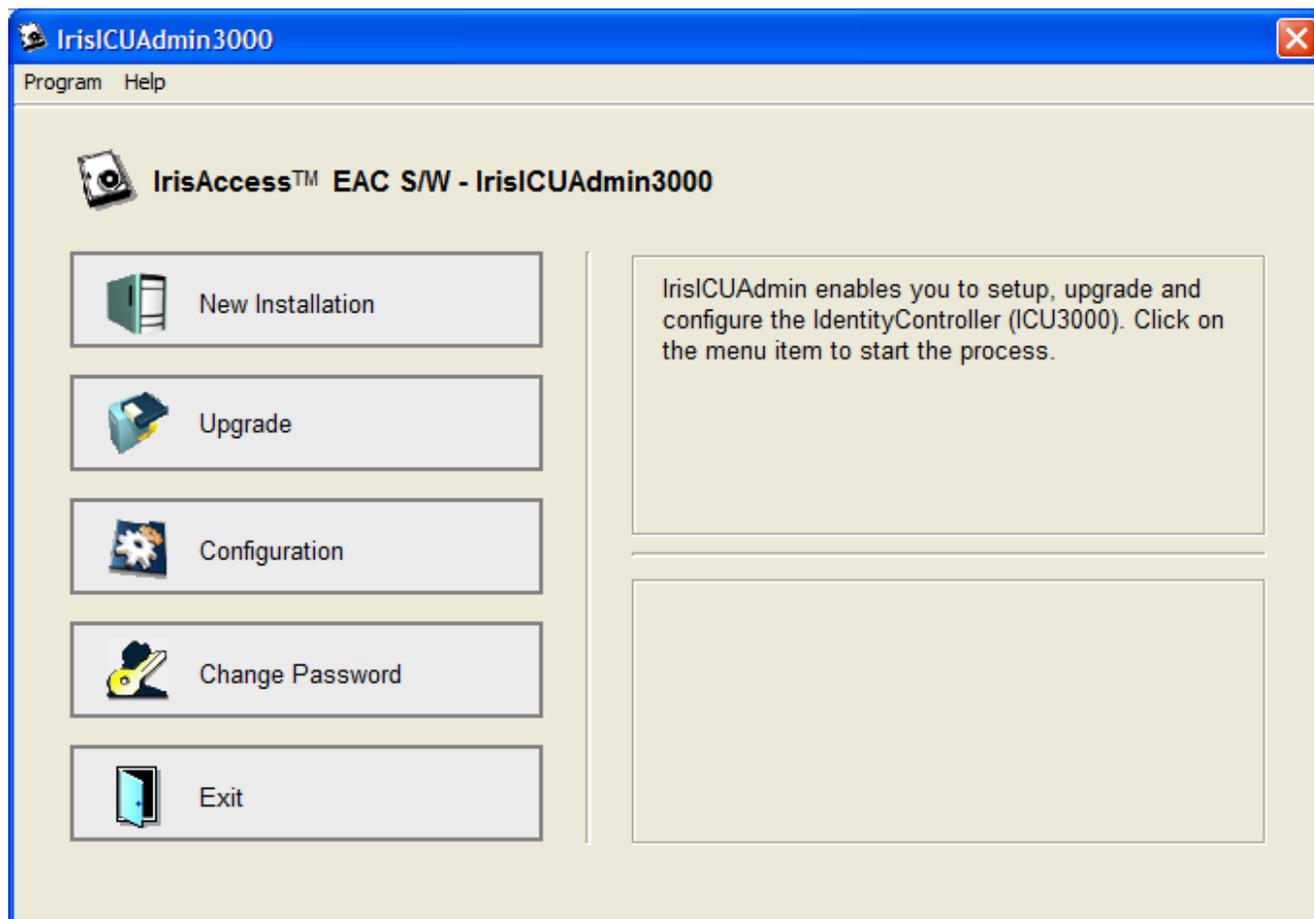
The ICUAdmin3000 application enables you to setup, modify, upgrade, and configure the IdentityController (ICU3000).

11.2.1 How to open IrisICUAdmin3000

To start the IrisICUAdmin3000, click on the IrisICUAdmin3000 menu item. The location of the program is:

<Drive>:\Program Files\Iris ID\IrisAccess\IrisICUAdmin3000.exe

After starting, IrisICUAdmin3000 will open a new window, as illustrated in the following figure:

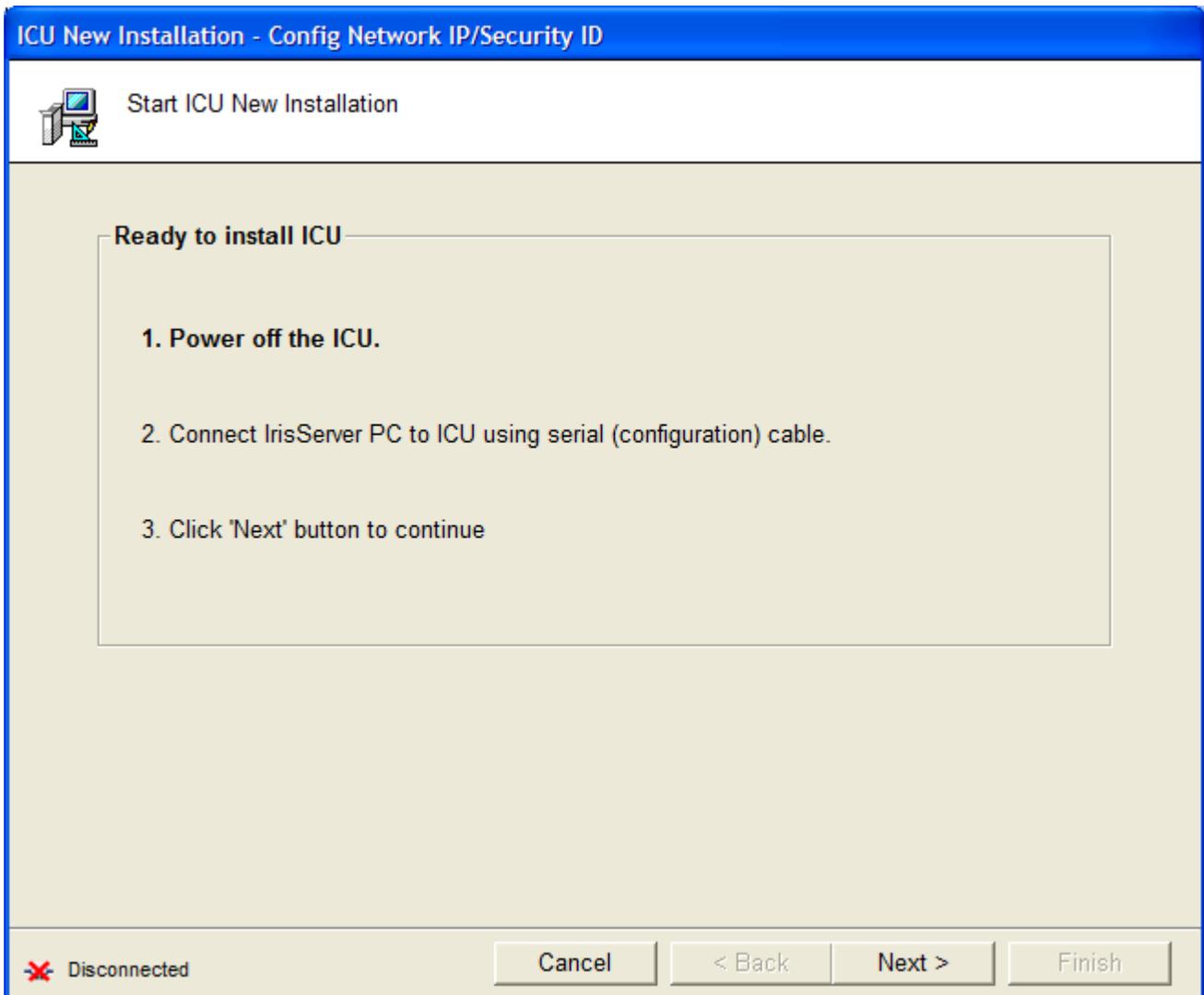


11.2.2 Description of Menu items in IrisICUAdmin3000

- 1. New Installation** – Used for setup and initial configuration of an ICU3000 unit. The use of a provided “ICU Configuration Serial Cable” is needed for use with this option. This cable is required to perform a New Installation setup. (If the cable or use of Serial/Serial to USB is not available, the *ICU Admin Setup Utility program* may be used – available from the Iris ID website at www.irisid.com).
- 2. Upgrade** – Updates the ICU3000 controller unit(s) to the same version of EAC Software that is running/installed on the IrisServer. *Note: This is required after upgrading the iData EAC software version on the server PC.*
- 3. Configuration** – Allows for modification of initially enabled channel settings within the ICU unit. Settings such as Remote unit IP, volume, Wiegand output settings, etc. are available (and configurable per channel per ICU).
- 4. Change Password** – Allows for the password of the ICU unit to be changed. This is often used if the password has been forgotten or is unknown. *Note: The use of a provided “ICU Configuration Serial Cable” (provided with the ICU3000 unit) is required for use with this option. The password will be reset to the factory default if unknown.*
- 5. Exit** – Closes out the application.

11.2.3 The ICUAdmin3000 New Installation Window

Select the “New Installation” button, the following window is displayed on the screen.



Click Next button to continue.

The following screen will appear.

ICU New Installation - Config Network IP/Security ID

Configure Network IP Address

Setting for IrisServer

Server IP Address

Settings for ICU

ICU IP Address ex) 160.160.97.42

Gateway Address ex) 160.160.97.254

Subnet Mask ex) 255.255.255.0

Disconnected

Enter IrisServer IP Address, ICU IP Address, Gateway Address, Subnet Mask and click Next button. A warning message as shown below appears. Click OK and continue installation.

IrisICUAdmin

 ICU will allow the connection from only this Server (172.24.17.68) when Network IP/Security ID Configuration is finished.

It is not recommended to change IP address of this server PC.
If you want to change the IP address, you should setup 'ICU New Installation', again!

The following screen appears next.

ICU New Installation - Config Network IP/Security ID

Configure ROU Security ID

Security IDs

Installed ROU	Security ID			
<input checked="" type="checkbox"/> ROU 1	qqqq	qqqq	qqqq	qqqq
<input checked="" type="checkbox"/> ROU 2	rrrr	rrrr	rrrr	rrrr
<input checked="" type="checkbox"/> ROU 3	ssss	ssss	ssss	ssss
<input checked="" type="checkbox"/> ROU 4	tttt	tttt	tttt	tttt

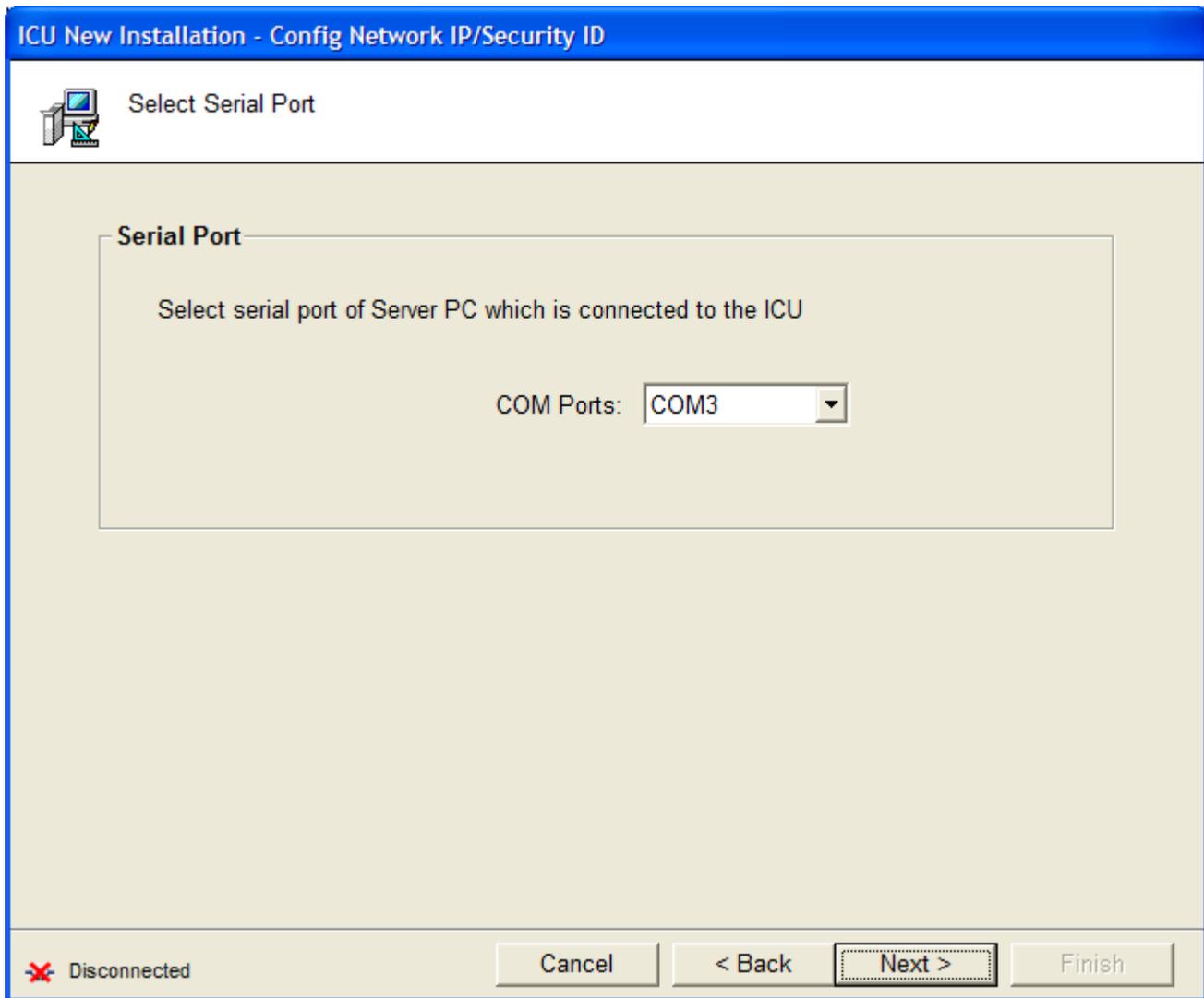
ROU 3 and ROU 4 are available for only 4-channel ICU.

! Only select the ROUs which are installed in this ICU. A unique security ID must be used for each ROU 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.

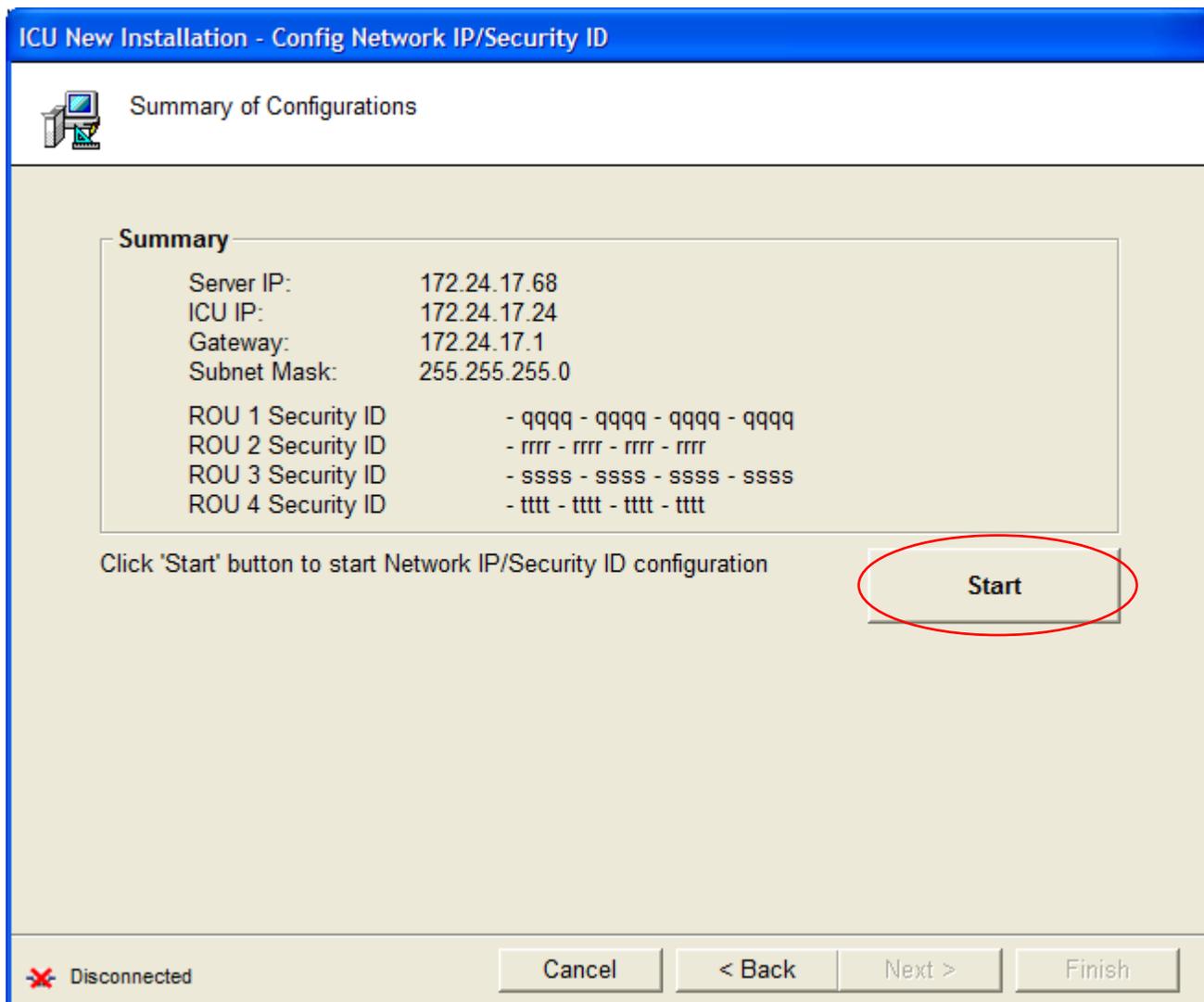
Disconnected

Cancel < Back Next > Finish

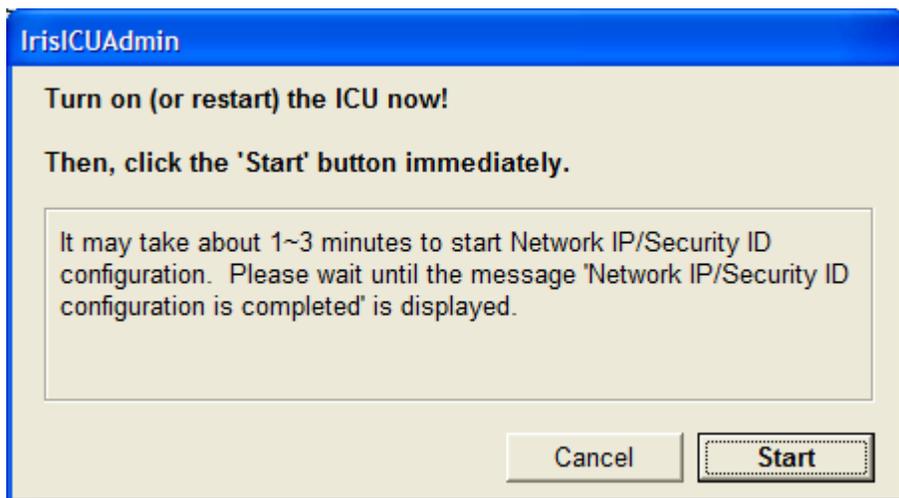
Enter Security IDs for ROU1, ROU2, ROU3 and ROU4. Click on next button. A screen to select serial port appears.



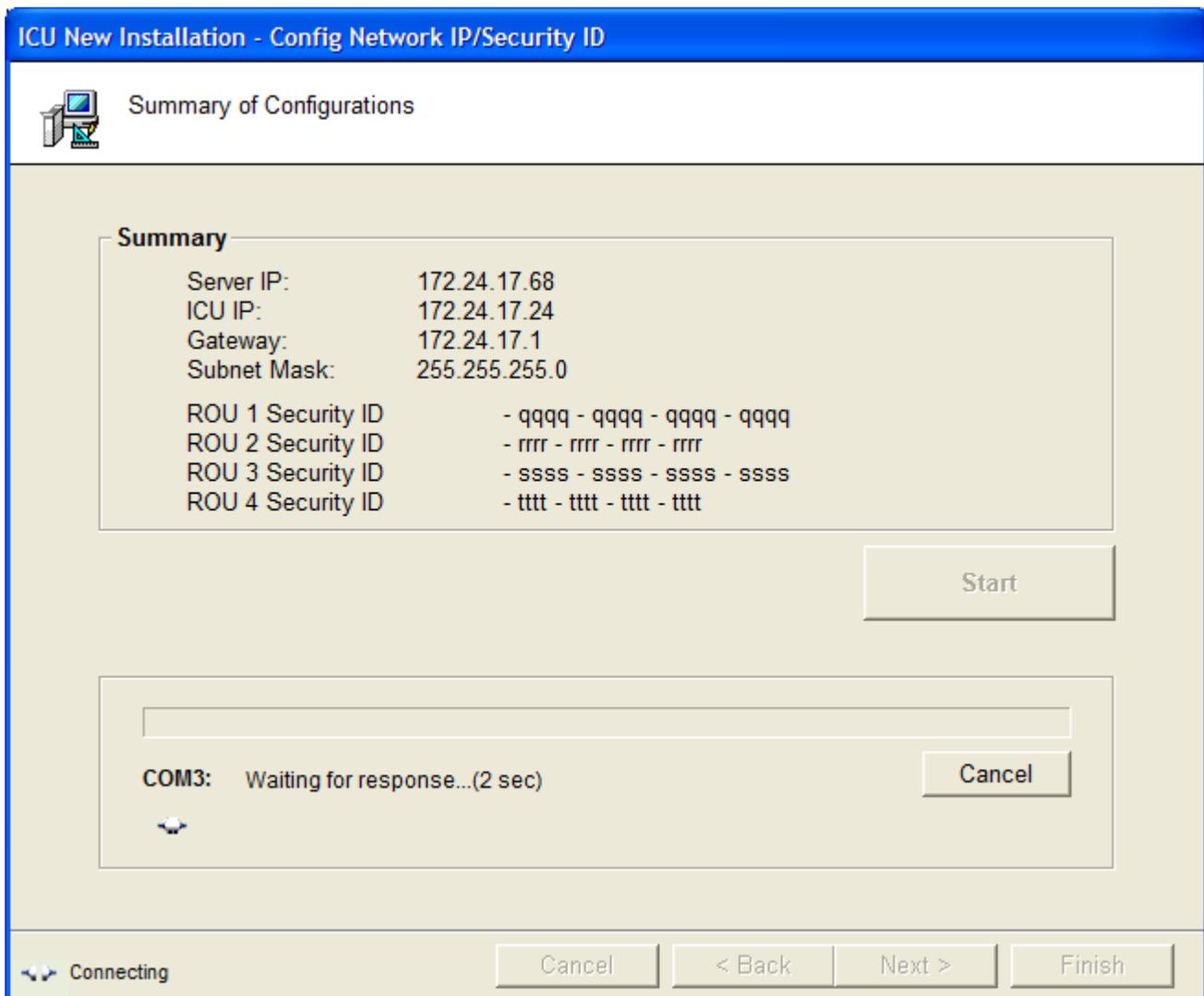
Select the serial port and click Next button. The settings summary screen appears as shown below.



Click on Start button to start new installation.



Click on Start button to start new installation.



11.2.4 The IrisICUAdmin3000 Upgrade Window

Select the "Upgrade" button, the following window is displayed on the screen.

Upgrade ICU EAC S/W

Connect to the ICU (TCP/IP) for EAC S/W Installation

Enter IP address of the ICU

IP Address	172.24.17.24
Password	*****

Click 'Next' button to continue.

Disconnected

Cancel < Back Next > Finish

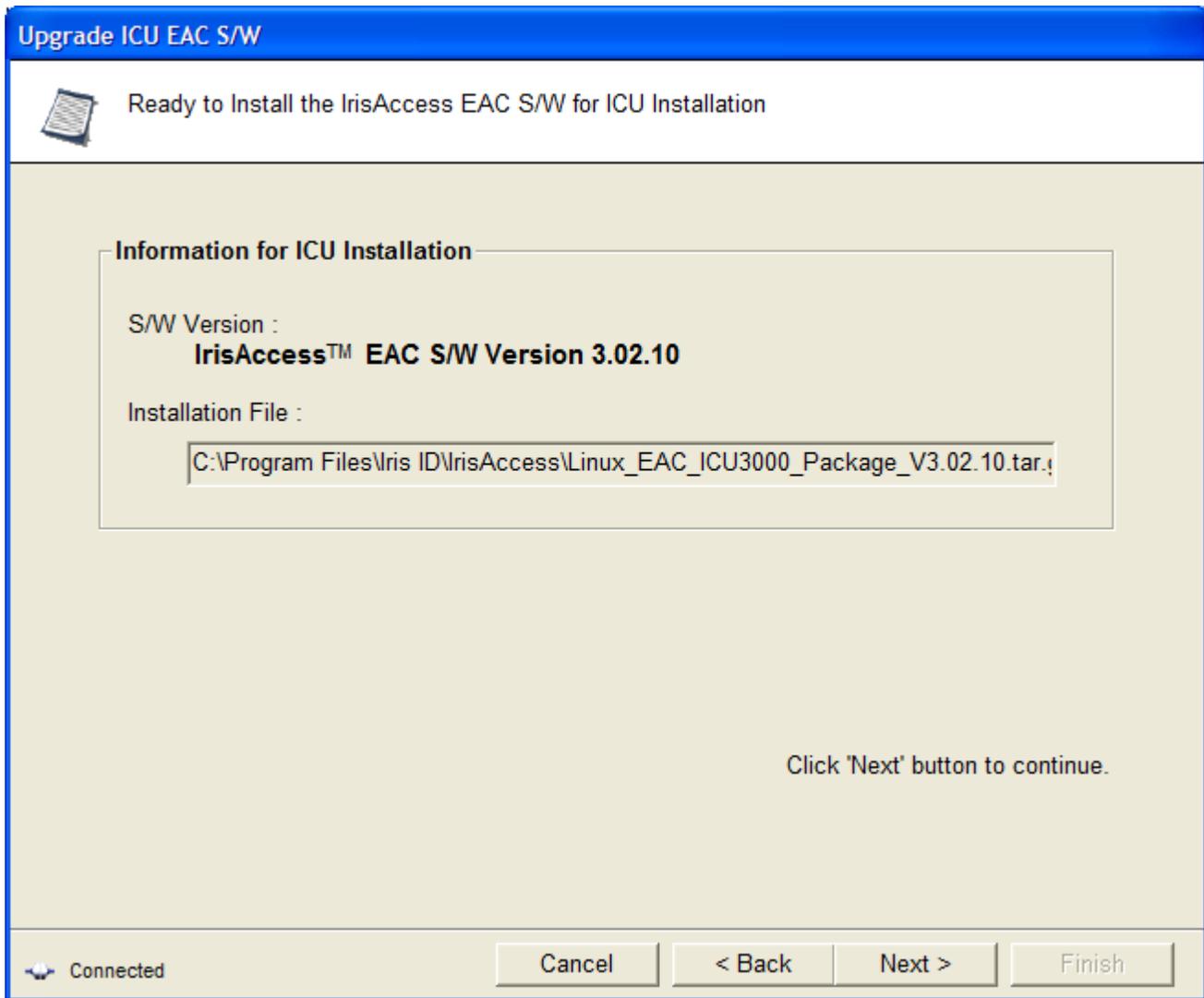
Enter ICU IP Address and password and click on Next button. The following screen will appear.

IrisICUAdmin

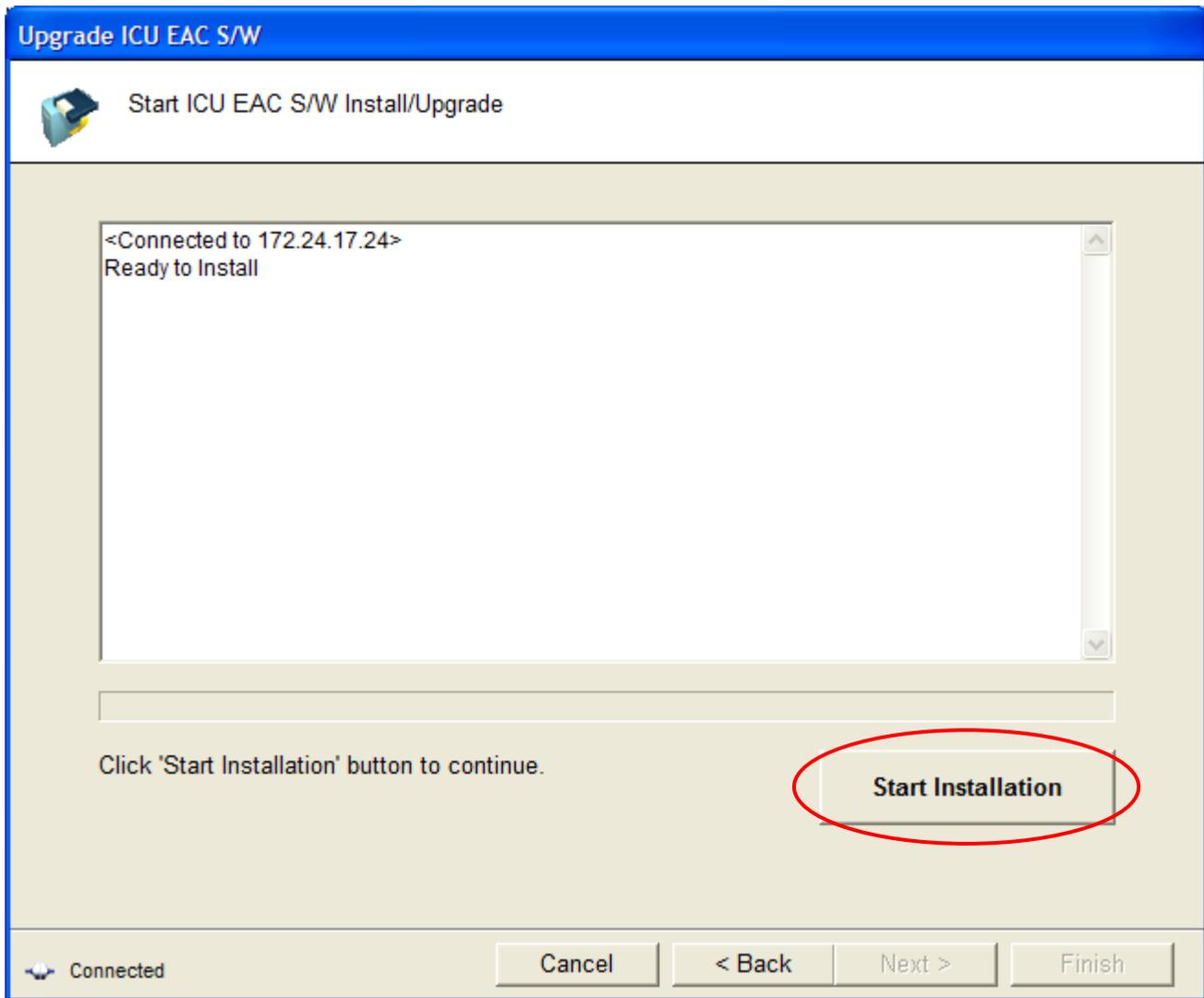
When the ICU is connected, all process on the ICU will be stopped.
Do you want to continue?

Yes No

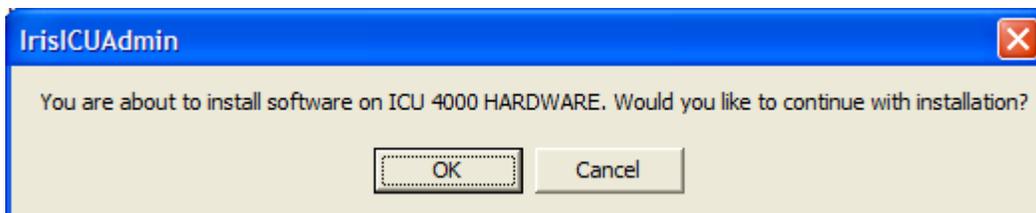
All the process on the ICU will be stopped. Click on Yes button to continue the installation.



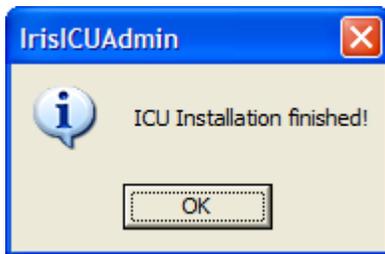
Click on the next Button to continue ICU software upgrade. The following screen appears.



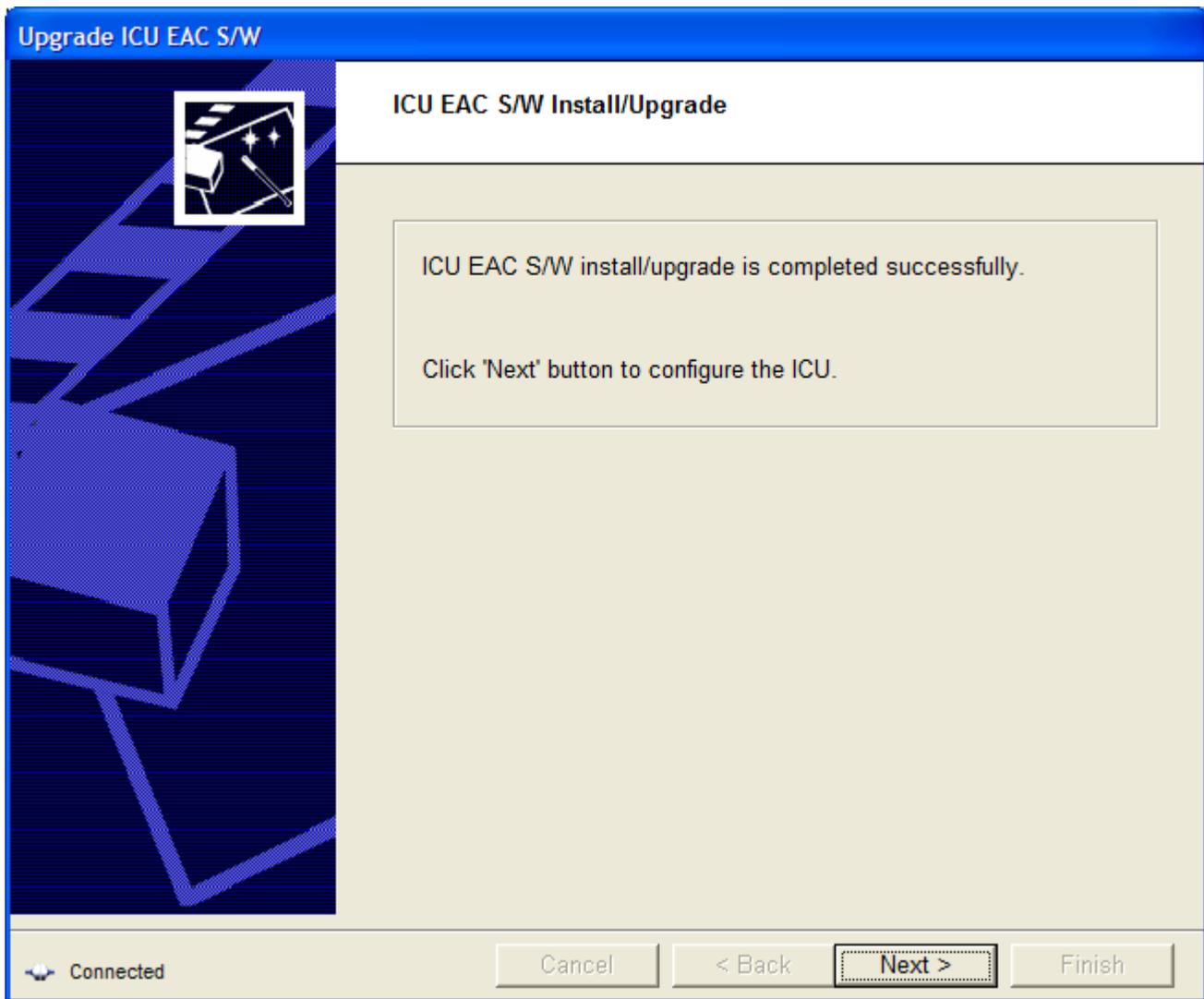
Click on Start Installation button to start upgrading ICU. If IrisAdmin3000 is used to install 3000 software on ICU4000 hardware, following warning appears. Click OK button if you are sure to upgrade the ICU 4000 with 3000 software.



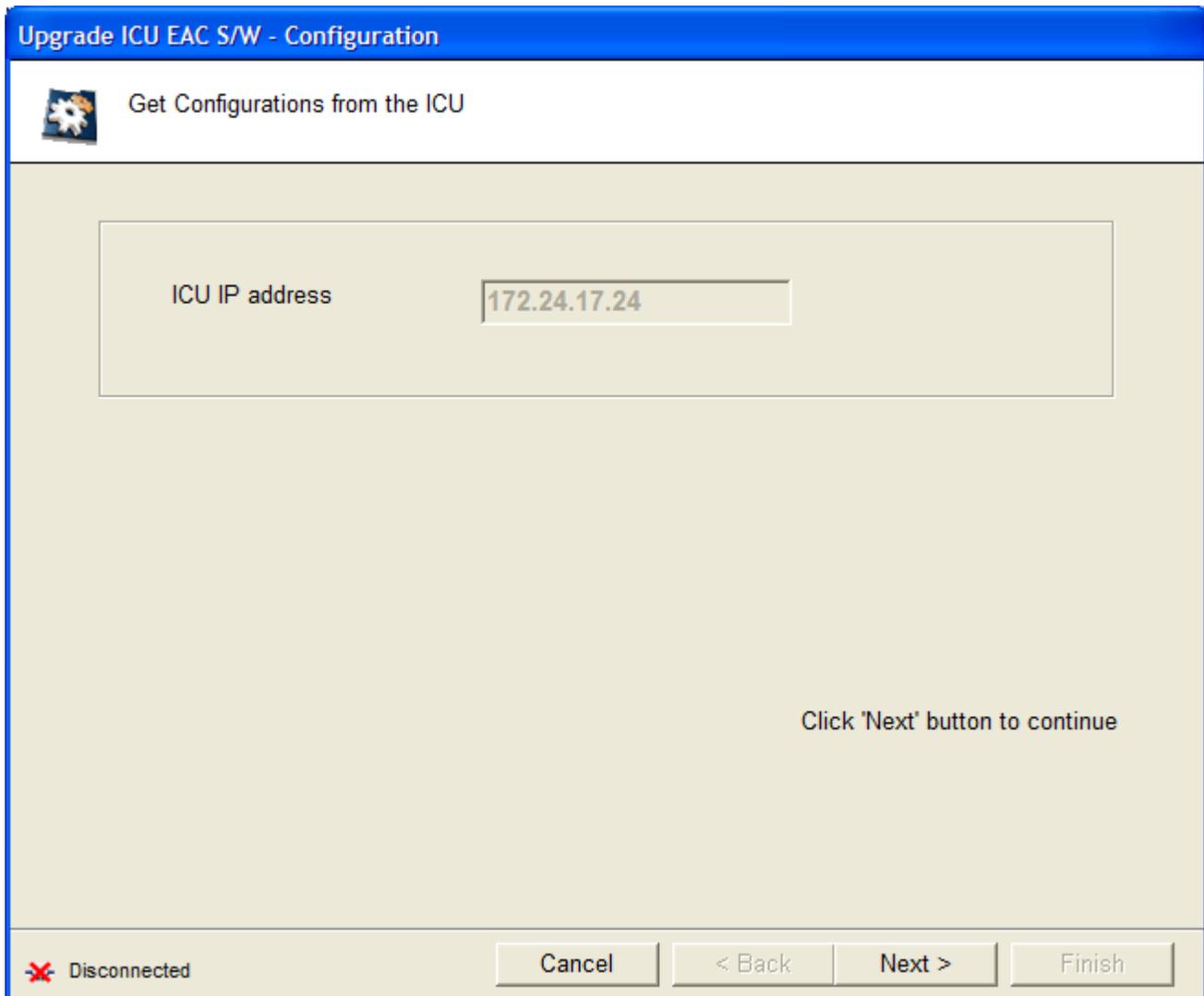
On successful completion following message box appears.



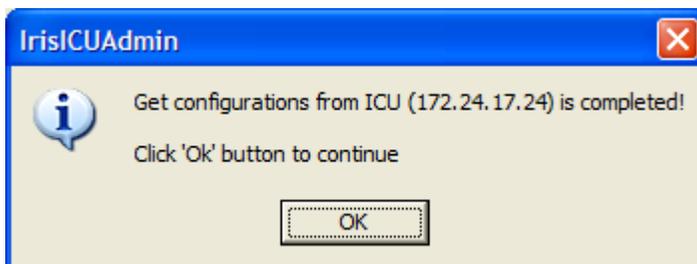
On clicking OK button, following screen appears.



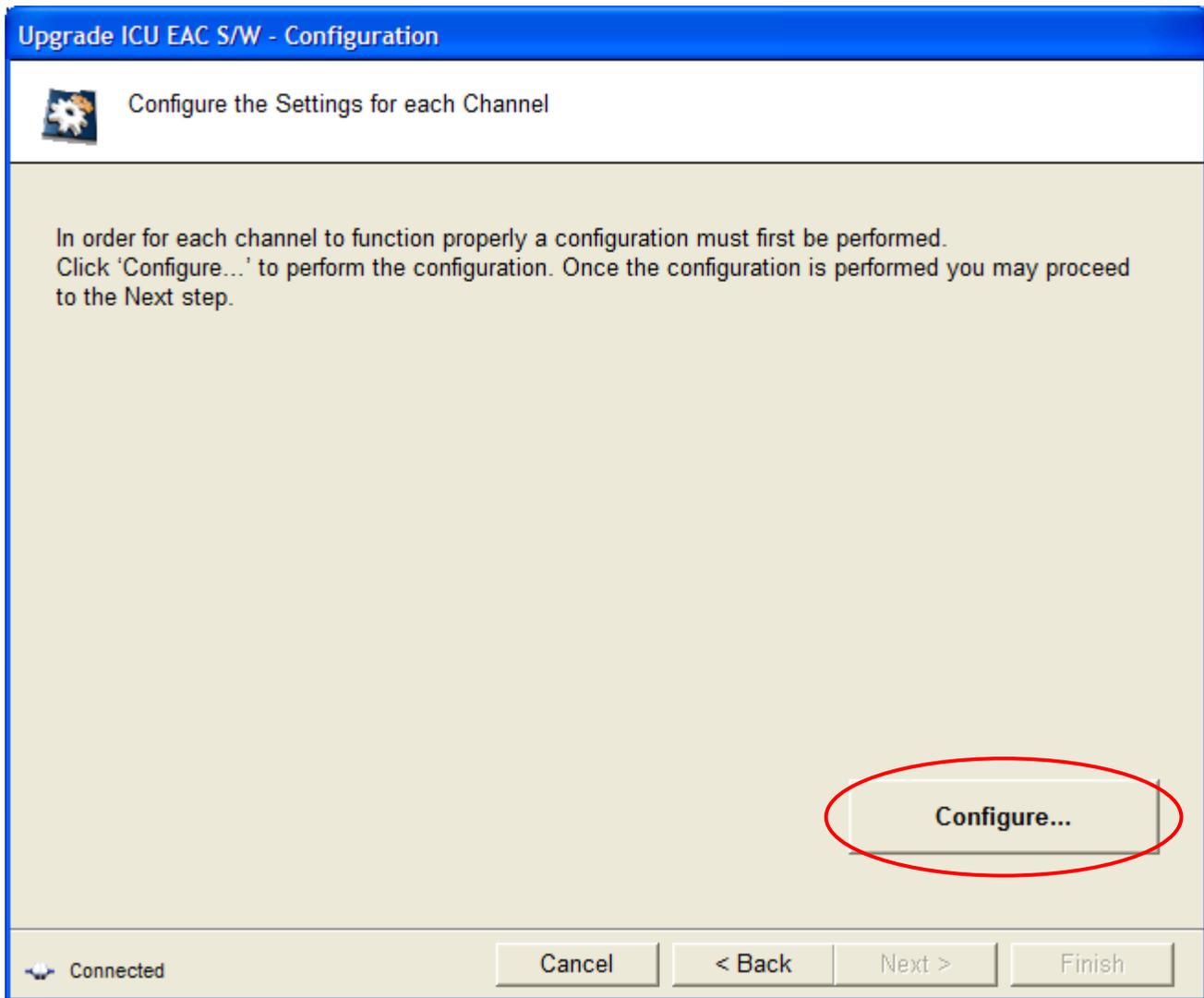
Click on Next button to continue. IrisICUAdmin3000 fetches configuration files from ICU.



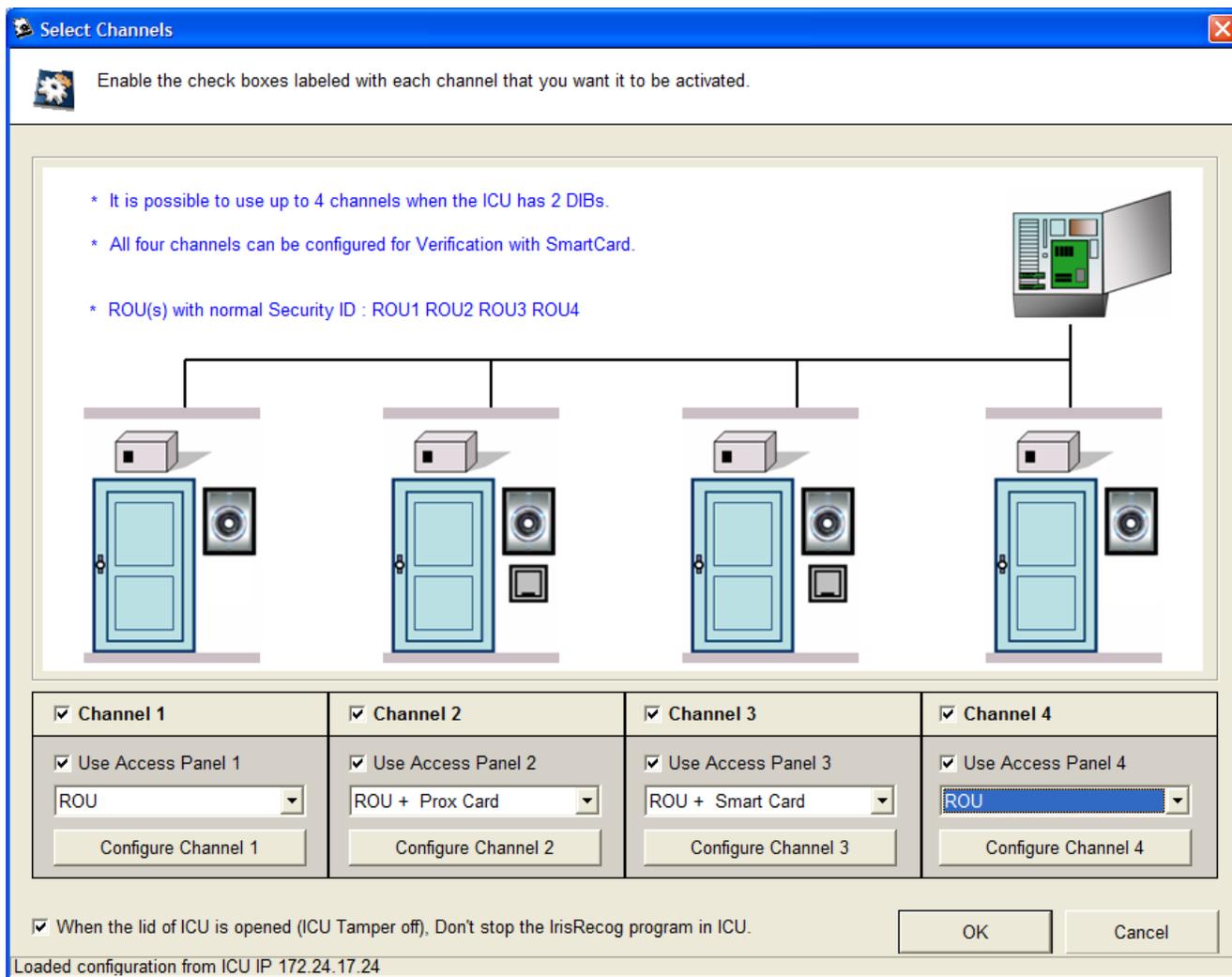
To start fetching configuration files from ICU, click on Next button. On successful completion of fetching configuration files, following message box appears.



Click on OK button to continue.

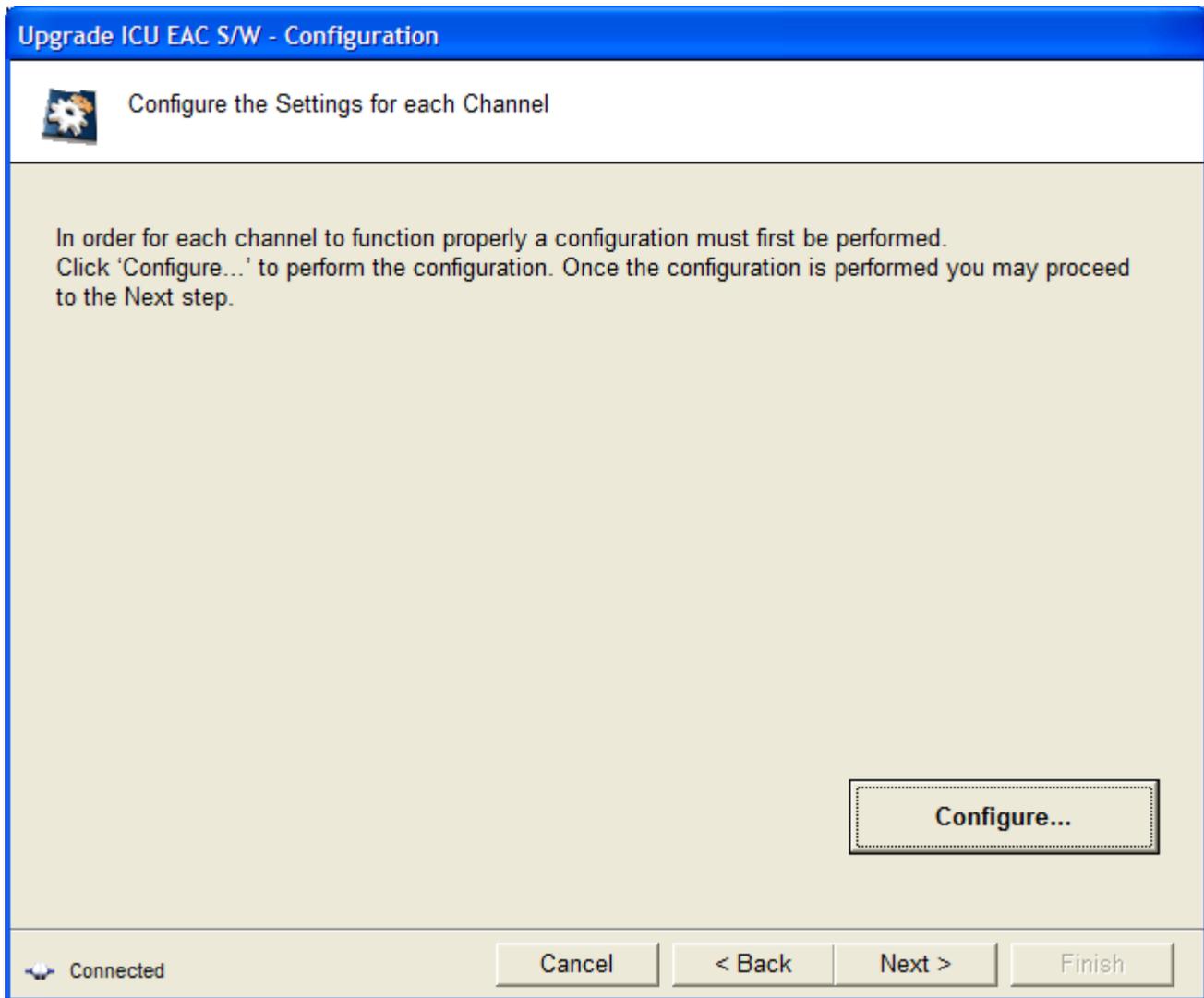


To start configuring ICU channels, click on Configure button. ICU configuration screen appears.

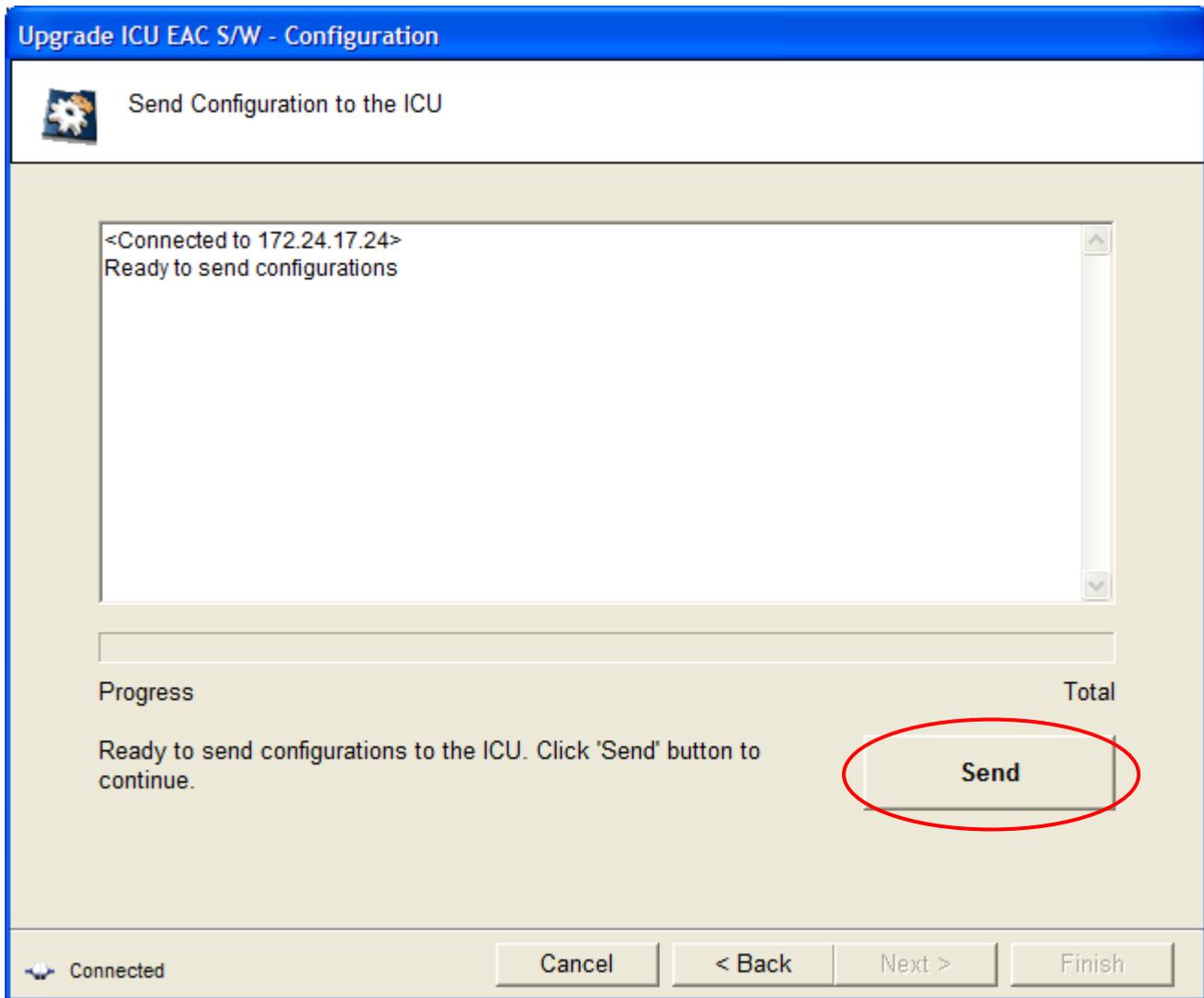


Configure the channels of ICU as required and click on OK button to finish configuration. For more details on configuring ICU, please refer section **2.7.5 The ICUAdmin3000 Configuration Window**.

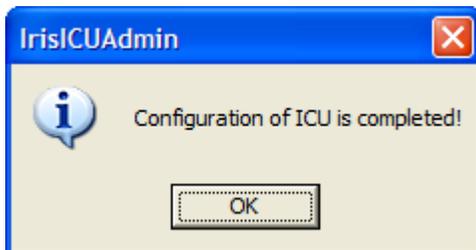
The following screen appears next.



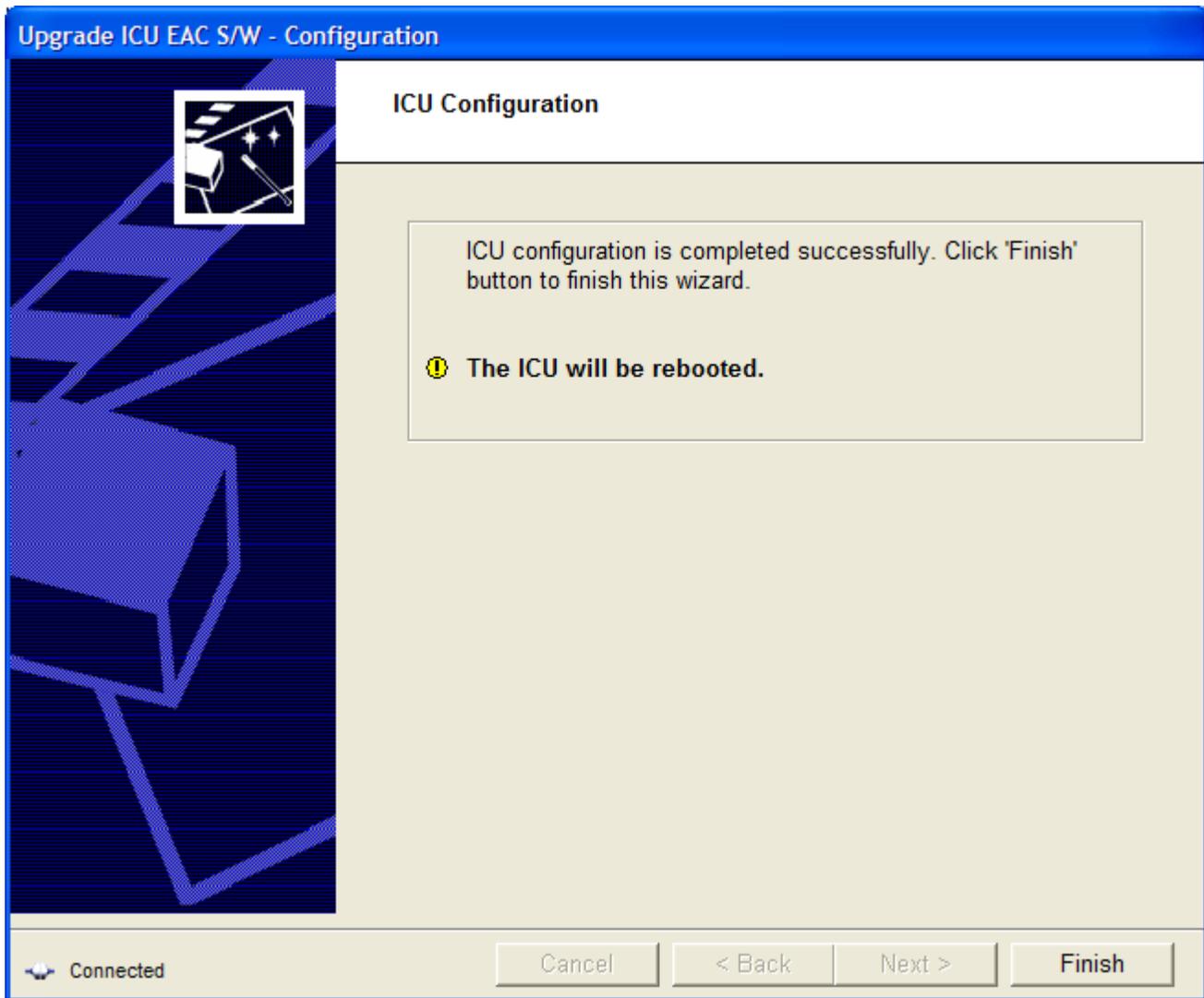
Click on Next button to continue. The following screen appears.



Click on Send button to send configuration to ICU. On successful completion of send configuration, following message box appears.



Click OK to go to the reboot screen.



Click Finish button to complete ICU upgrade process. ICU will restart automatically after clicking Finish button.

11.2.5 The ICUAdmin3000 Configuration Window

ICU Configuration

Before Settings After Settings

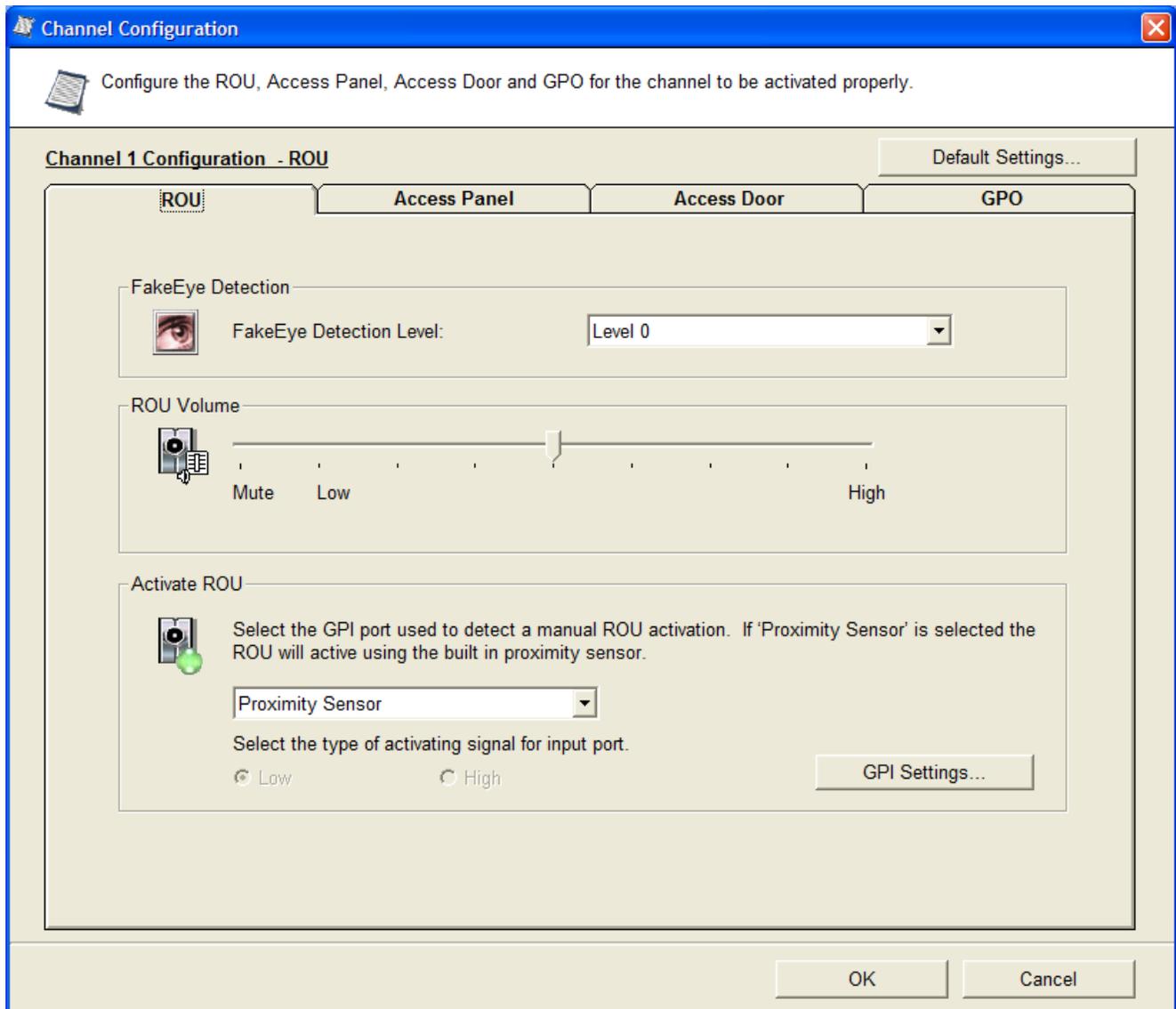
* It is possible to use up to 4 channels when the ICU has 2 DIBs.
 * All four channels can be configured for Verification with SmartCard.

<input checked="" type="checkbox"/> Channel 1	<input checked="" type="checkbox"/> Channel 2	<input checked="" type="checkbox"/> Channel 3	<input checked="" type="checkbox"/> Channel 4
<input checked="" type="checkbox"/> Use Access Panel 1	<input checked="" type="checkbox"/> Use Access Panel 2	<input checked="" type="checkbox"/> Use Access Panel 3	<input checked="" type="checkbox"/> Use Access Panel 4
ROU	ROU + Prox Card	ROU + Smart Card	ROU
Configure Channel 1	Configure Channel 2	Configure Channel 3	Configure Channel 4

When the lid of ICU is opened (ICU Tamper off), Don't stop the IrisRecog program in ICU.

Send Close

Loaded configuration from ICU IP 172.24.17.24



Fake eye detection can be configured by selecting the Fake Eye Detection Level.

If you want the fake eye detection to be enabled, select the **Level 1** option. Fake Eyes will be detected when a user tries to enroll, identify or verify.

Fake Eye detection does increase the time required identification or verification, but greatly enhances the security of the system.

If you don't want the fake eye detection to be enabled, then select the **Level 0**. If so, fake eye will NOT be detected when a user tries to identify or verify.

- ◆ **Caution:** Limitation of ambient light in working environment
 - When Fake Eye Detection is not used: 1,000 lx Fluorescent light and 100 lx Incandescent or sunlight.

- When Fake Eye Detection is used: 500 lx Fluorescent light and 50 lx Incandescent or sunlight.

If the ambient light exceeds the limitation, the False Reject Rate will be increased.

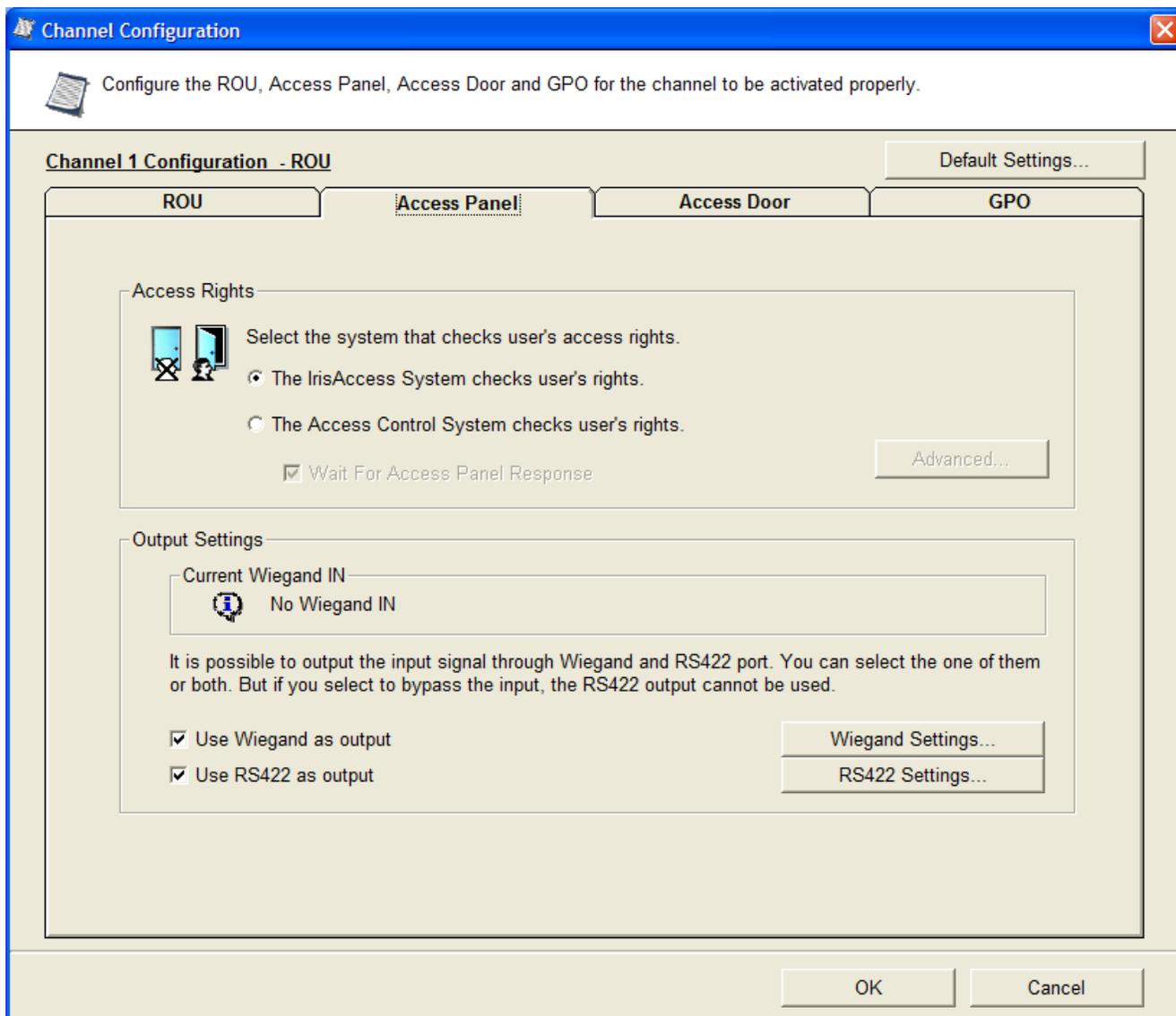
Scroll the ROU Volume bar, to increase or decrease the ROU volume level.

ROU can be activated automatically using proximity sensor or using an external trigger on one of the following GPI pins on DIB.

- ✓ Lock
- ✓ Alarm
- ✓ Egress

When any of the above pins are selected for activating ROU, user must configure the GPI signal after click on GPI Settings button.

Configuration of Access Panel



Access Rights: You can choose the system that checks the user's access rights. Either IrisAccess system checks for user's access rights or an external access control system checks the user's access rights.

If access control system checks user's access rights, Iris Access may/ may not wait for Access control systems response. To configure access control system response, check the **Wait for Access Panel Response** and click on "Advanced" button. This will take you to GPI settings screen.

GPI Settings

You can use 4 ports, 'Lock', 'Status', 'Alarm' and 'Egress' as GPI. The Lock, Egress and Alarm ports may be used to activate ROU or get the result of recognition from Access Panel.

Current GPI Settings

	Lock	Status	Alarm	Egress	GND	NC	COM	OUT
GPI	Accept	Reject						
Activate State	Low	Low	Low	Low				

Activate ROU

Select the GPI port used to activate the ROU. If a GPI port is used to activate the ROU, that port may not be

- None. ROU will be activated using the internal proximity sensor.
- Use signal on Lock port to activate ROU.
- Use signal on Alarm port to activate ROU.
- Use signal on Egress port to activate ROU.

Get the recognition results from Access Panel

When an Access Control System checks user's access rights, select the ports that the IrisAccess System receives the results from Access Control System. Select the GPI port to detect the 'Accept' and 'Reject' signals from Access Panel.

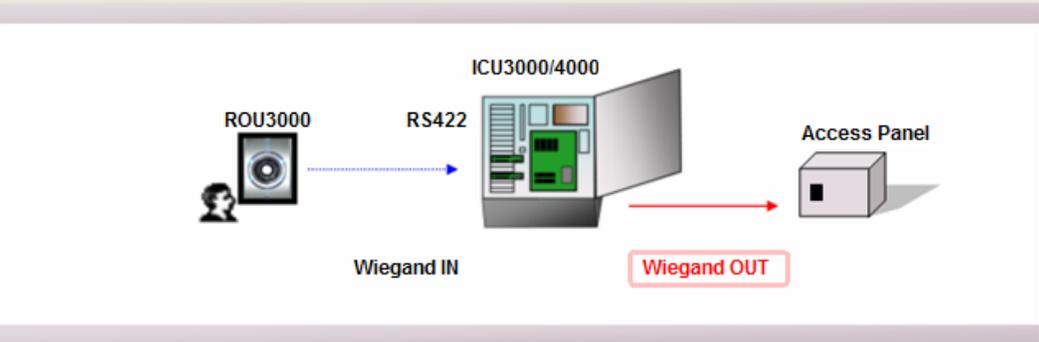
<u>Lock port</u>	<u>Status port</u>	<u>Alarm port</u>	<u>Egress port</u>
<input checked="" type="radio"/> Accept	<input type="radio"/> Accept	<input type="radio"/> Accept	<input type="radio"/> Accept
<input type="radio"/> Reject	<input checked="" type="radio"/> Reject	<input type="radio"/> Reject	<input type="radio"/> Reject
<input type="radio"/> No Use	<input type="radio"/> No Use	<input checked="" type="radio"/> No Use	<input checked="" type="radio"/> No Use

OK Cancel

ON the GPI connector of DCU there are 7 Pins. You can use Lock, Status, Alarm and Egress pins for configuring access panel response. These pins can also be used to configure external input for activating ROU.

Wiegand Setting

Set the format, Active State, Pulse Duration, Bit Period, Total wiegand bits, Start Parity, Stop Parity and Facility code of Wiegand.



Wiegand OUT

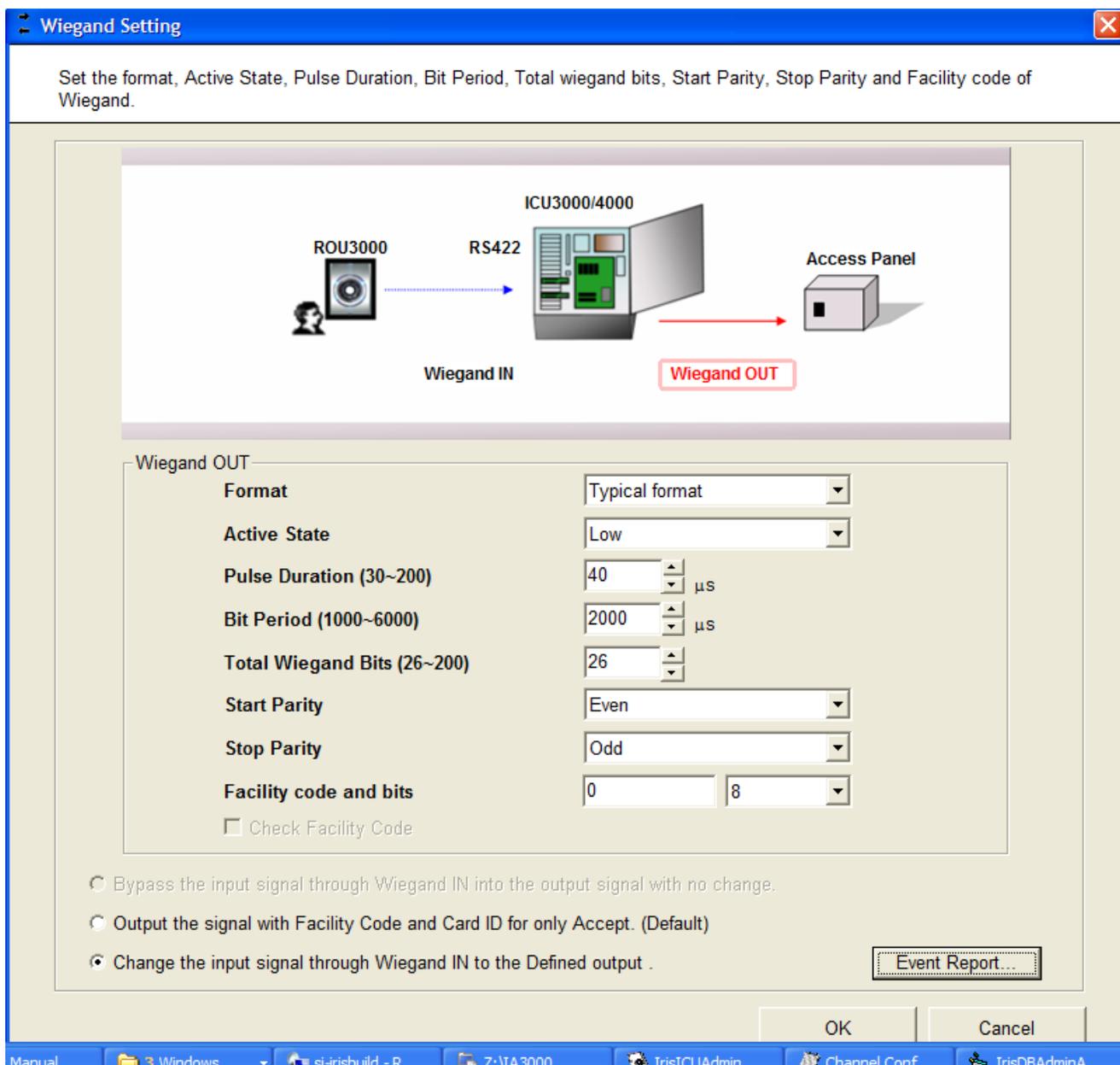
Format	Typical format
Active State	Low
Pulse Duration (30~200)	40 μ s
Bit Period (1000~6000)	2000 μ s
Total Wiegand Bits (26~200)	26
Start Parity	Even
Stop Parity	Odd
Facility code and bits	0 8

Check Facility Code

Bypass the input signal through Wiegand IN into the output signal with no change.
 Output the signal with Facility Code and Card ID for only Accept. (Default)
 Change the input signal through Wiegand IN to the Defined output .

Event Report...

OK Cancel



If you want to bypass signal received on Wiegand IN port to Wiegand out port without any change, then select **“Bypass the input signal through Wiegand IN into the output signal with no change”** option.

If you want to prefix facility code to the card ID received on Wiegand IN port before send it to the Wiegand Out port, then select **“Output the signal with Facility Code and Card ID for only Accept. (Default)”** option.

Signals on Wiegand IN port can be used for other purposes also. To do so, click on the Event Report button. The following screen appears.

Event Reporting to Access Panel

When the following recognition results or System logs occurs, the ICU will send a changed Facility Code output through the Wiegand output of DIB. Set new facility code for each case.

Total Bits - 0-80 bits

0 0 0 0 0 0 0 0 1 1 0 0 1 0 0 0 0 0

15 8 0

The bit Value Starts = 8
Length of Value = 7, Value = 100

Recognition Results

	Total Bits	Start Bit	Value Length	Value (Decimal)
Denied				
Door access trial overtime	16	8	9	1
Live eye check failed	16	8	9	1
Unauthorized - No access authority	16	8	9	1
Warning Eye (Accepted)	16	8	9	1

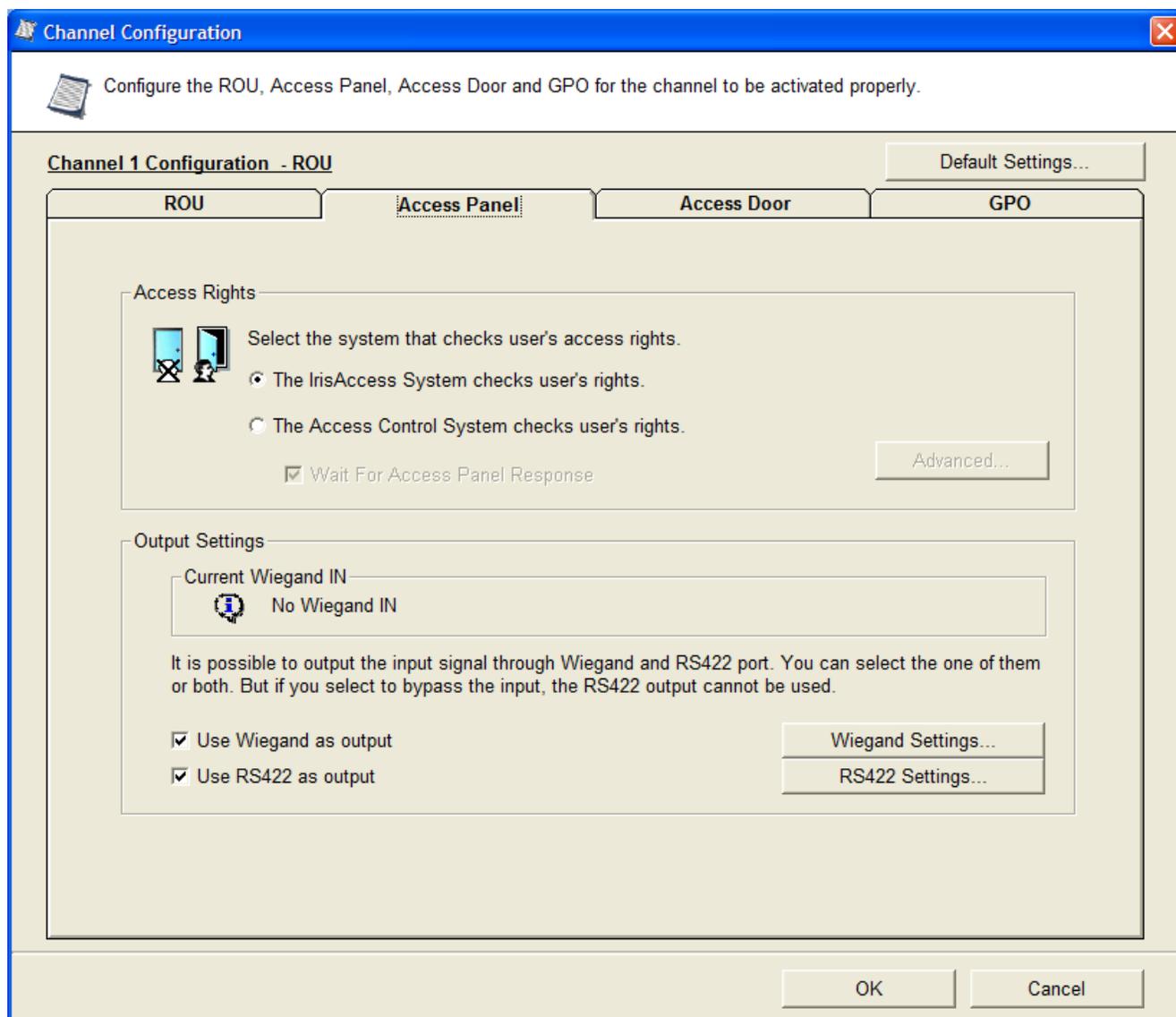
System Logs

Video Connection Error	16	8	9	1
Serial Connection Error	16	8	9	1
IR-LED Failure	16	8	9	1

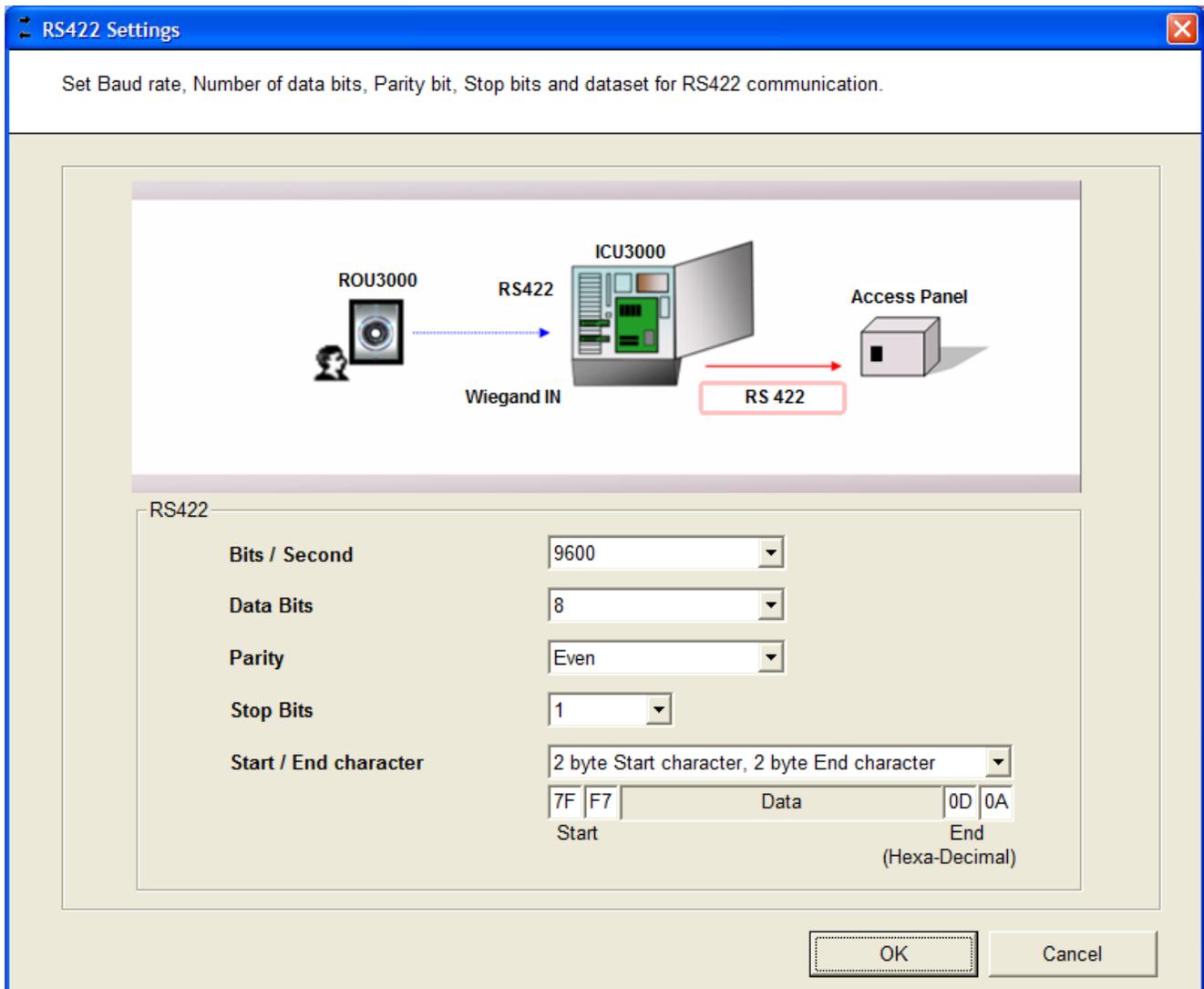
OK Cancel

You can configure Wiegand out signal for each event separately. Configure and click OK button to go back to Wiegand settings page.

Click OK button on Wiegand Settings page to go back to Access Panel configuration screen.



Click on RS422 Settings button to configure RS422 output signals. The following screen appears when RS422 Settings button is clicked.



Configure Bits / Second, Data Bits, Parity, Stop Bits, Start and End character and click on OK button to save settings and go back to access panel configuration page.

Configuration of Access Door

Channel Configuration

Configure the ROU, Access Panel, Access Panel, Access Door and GPO for the channel to be activated properly.

Channel 1 Configuration - ROU Default Settings...

Access Door

Door Open Duration

Door Open Duration (0 ~ 65535 secs) : 3 sec(s)

Door Lock Device Status

Enable to check the Lock Device of a door.

Enable Activate State Low

Door Open Status

Enable to check whether a door stays open for the below 'Check Time'.

Enable

Check Time (0 ~ 255 secs) : 10 sec(s) Activate State Low

Alarm

Enable to get the fire alarm signal. When the fire alarm signal is detected, select how to operate the door.

Enable

Close Activate State Low

Egress Button

When an egress button near the entry area is pushed, the door is opened.

Enable Activate State Low

OK Cancel

Door open duration can be configured to automatically close the door relay.

Door Lock device status: If the door lock fails, event can be sent on Status port of DCU. When a signal is received, an event is raised to the IrisServer and IrisMonitor.

Door Open Status: If the door stays open for more that the Check Time period, a signal is received on the IrisMonitor and GPI port of DCU.

Alarm: Check the Enable check box to get the fire alarm signal is detected on GPI port of DCU. You can choose to open or close the door when the firm alarm signal is detected.

Egress Button: When an egress button near the entry area is pushed, the door is opened. Check the enable check box to enable this feature. The Egree signal is received on Egress port of DCU.

Configuration of GPO

Channel Configuration

Configure the ROU, Access Panel, Access Door and GPO for the channel to be activated properly.

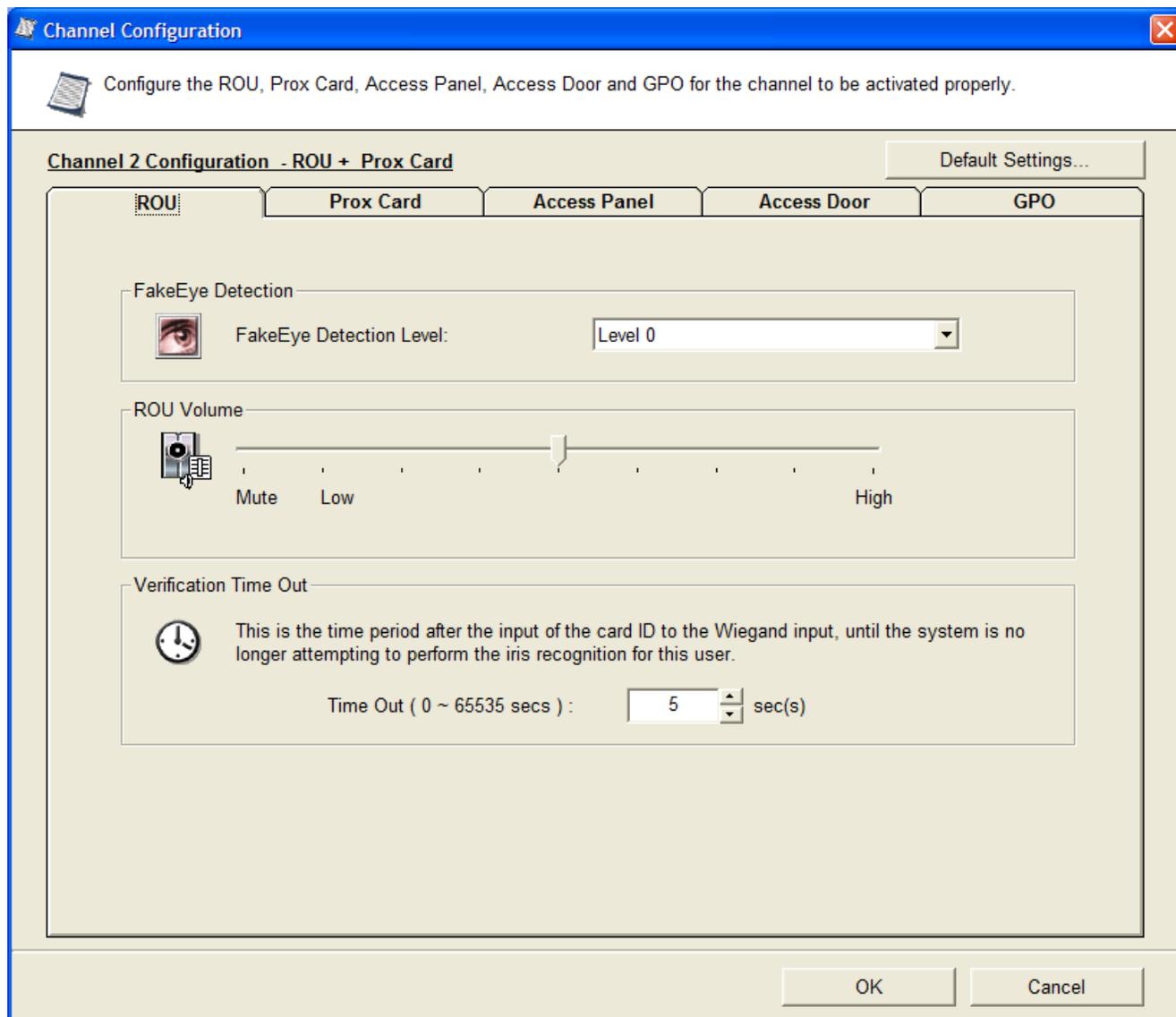
Channel 1 Configuration - ROU Default Settings...

ROU	Access Panel	Access Door	GPO
In the specified state such as followings, a signal can be outputted through two general output ports. Decide the port to which to send the signal, and then select how long time to send the signal.			
<u>When</u>		<u>From Port</u>	<u>During Time Out (0 ~ 65535 secs)</u>
A user is accepted		No	0
A user is denied		No	0
Warning Eye is detected		No	0
The result of matching a card ID is successful		No	0
A door is opened more than the open duration time		No	0
A door is opened without Identification or Verification		No	0
An electromagnetic locking equipment is locked but a door is opened		No	0
Fire Alarm signal is detected		No	0
ICU / DCU Tamper signal is detected		No	0
ROU Tamper signal is detected		No	0

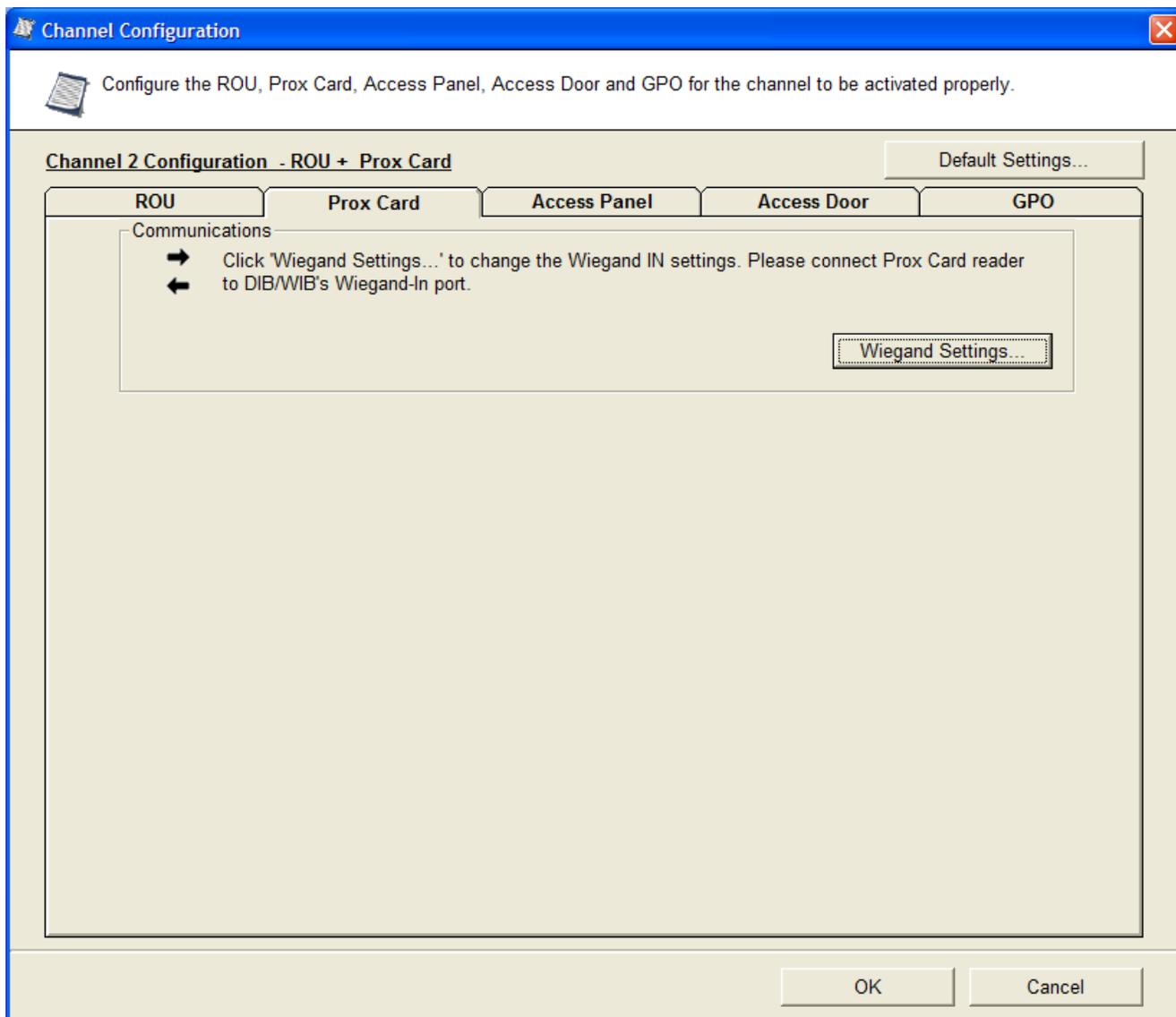
OK Cancel

To output a signal on the GPO port for specified events, select the GPO port and the duration of the signal.

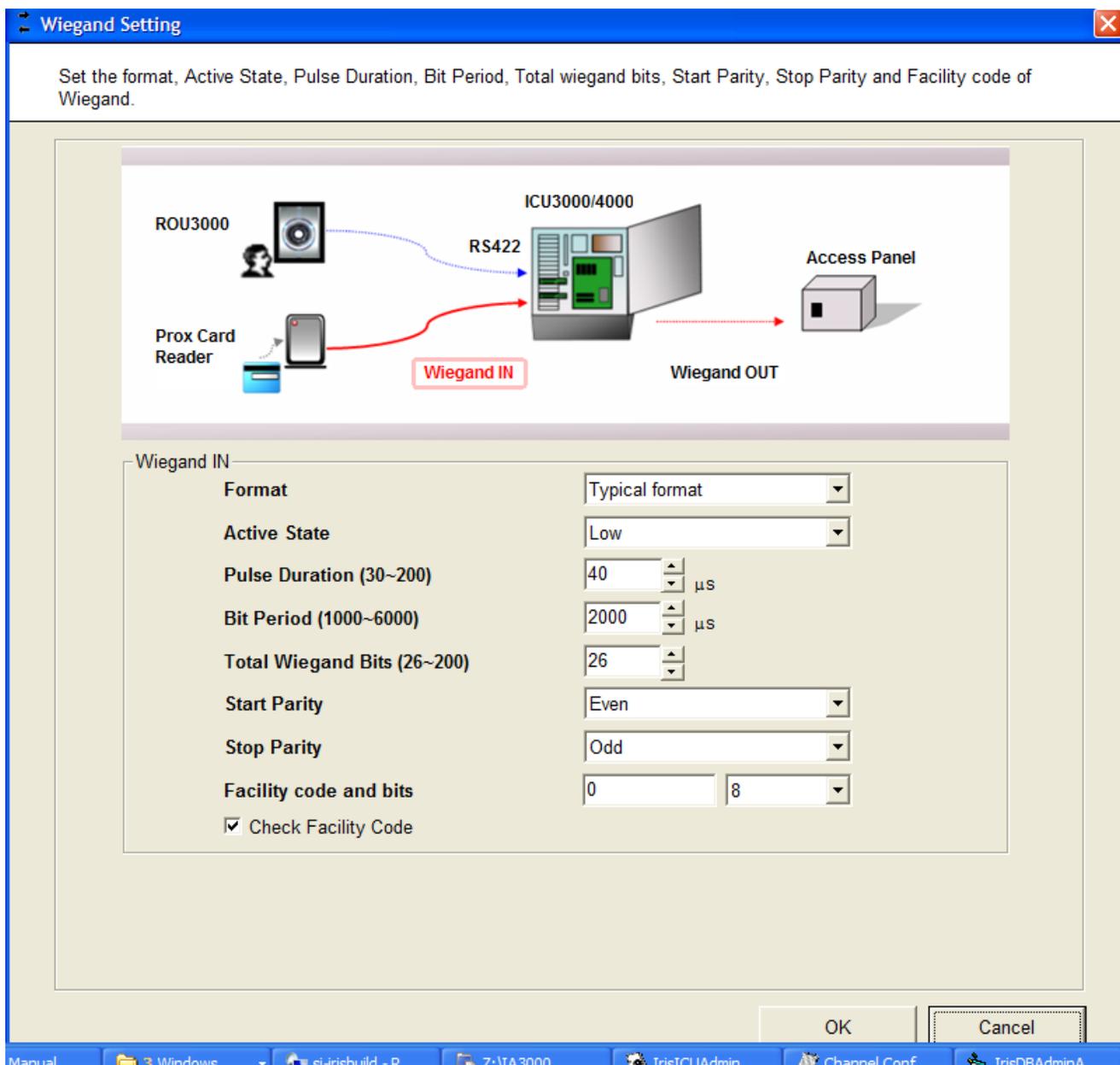
Configuration of Prox Card Mode



Verification timeout can be configured anywhere between (0-65535 sec). If the verification timeout is set to 0, then the time out is set to infinite.



When Prox card is used, Wiegand data is received on the DCU Wiegand IN port from Prox card reader. Configure Wiegand IN, click on Wiegand Settings button. The following screen appears.



The following Wiegand format options are available:

✓ Typical Format

When typical format is selected, the Active State, Pulse Duration, Bit Period, Total Wiegand Bits, Start Parity, Stop Parity and Facility code and bits settings are set automatically to Low, 40 μ s, 2000 μ s, 26, Even, Odd, 0 and 8 respectively.

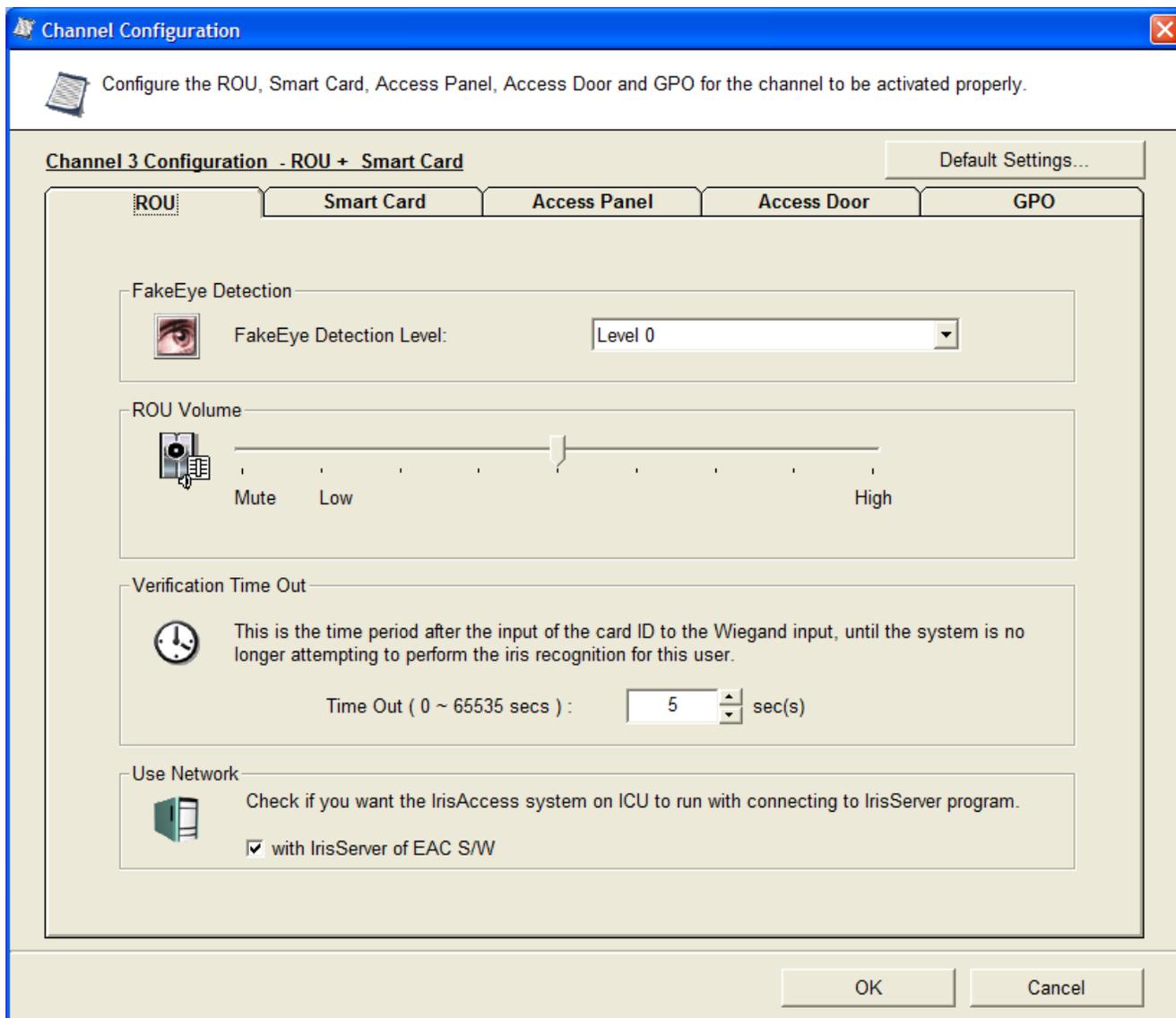
✓ Casi-Rusco 40

When Casi_Rusco 40 format is selected, the Active State, Pulse Duration and Bit Period settings are set automatically to Low, 40 μ s and 2000 μ s respectively. All other settings are disabled.

✓ HID Corporate 1000

When HID Corporate 1000 format is selected, the Active State, Pulse Duration and Bit Period settings are set automatically to Low, 40 μ s and 2000 μ s respectively. All other settings are disabled. If you want to use facility code check the Check Facility Code check box and enter the Facility code in the Facility code box.

Click OK to finish Wiegand IN configuration and go back to main page.



Configuration of Smart Card Mode

Channel Configuration

Configure the ROU, Smart Card, Access Panel, Access Door and GPO for the channel to be activated properly.

Channel 3 Configuration - ROU + Smart Card Default Settings...

Smart Card

The offset only needs to be changed if storing non-IrisAccess information on the SmartCard.

Smart Card Type :

Offset (hexadecimal)

App Key (hexadecimal)

Show Key

Communications

In case of using HID Smart Card, it is supported the Wiegand IN with RS232 to communicate Smart Card Reader and Access Panel. To use Wiegand IN, enable check box labeled with 'Use Wiegand'. Click 'Wiegand Settings...' to change the Wiegand IN settings.

Use Wiegand

Encryption Algorithm

Select the Encryption Algorithm to encrypt the Smart Card

Data format in Smart Card

Encryption Algorithm

Security Keys

Click 'Get Keys...' to get Smart Card keys file. A keys file can be generated in IrisServer.

Show Key

Security Key 1 :

Security Key 2 :

Following type of smart cards are supported by Iris Access.

- ✓ HID iCLASS

Smartcard offset for HID iCLASS smartcard is 13(hexadecimal) by default. You may change it to other value if you are using the same smartcard to store non Iris information. You can also change the smart card application key to your custom application key.

HID iCLASS smart card contains Wiegand data which is read and sent to the Wiegand IN port by iCLASS readers. You can configure Wiegand IN port as shown in **Configuration of Prox Card Mode** section.

- ✓ Indala DESFire
- ✓ BanqTec (BQT BT-815)

Smart card data may be written to smart card in the following format:

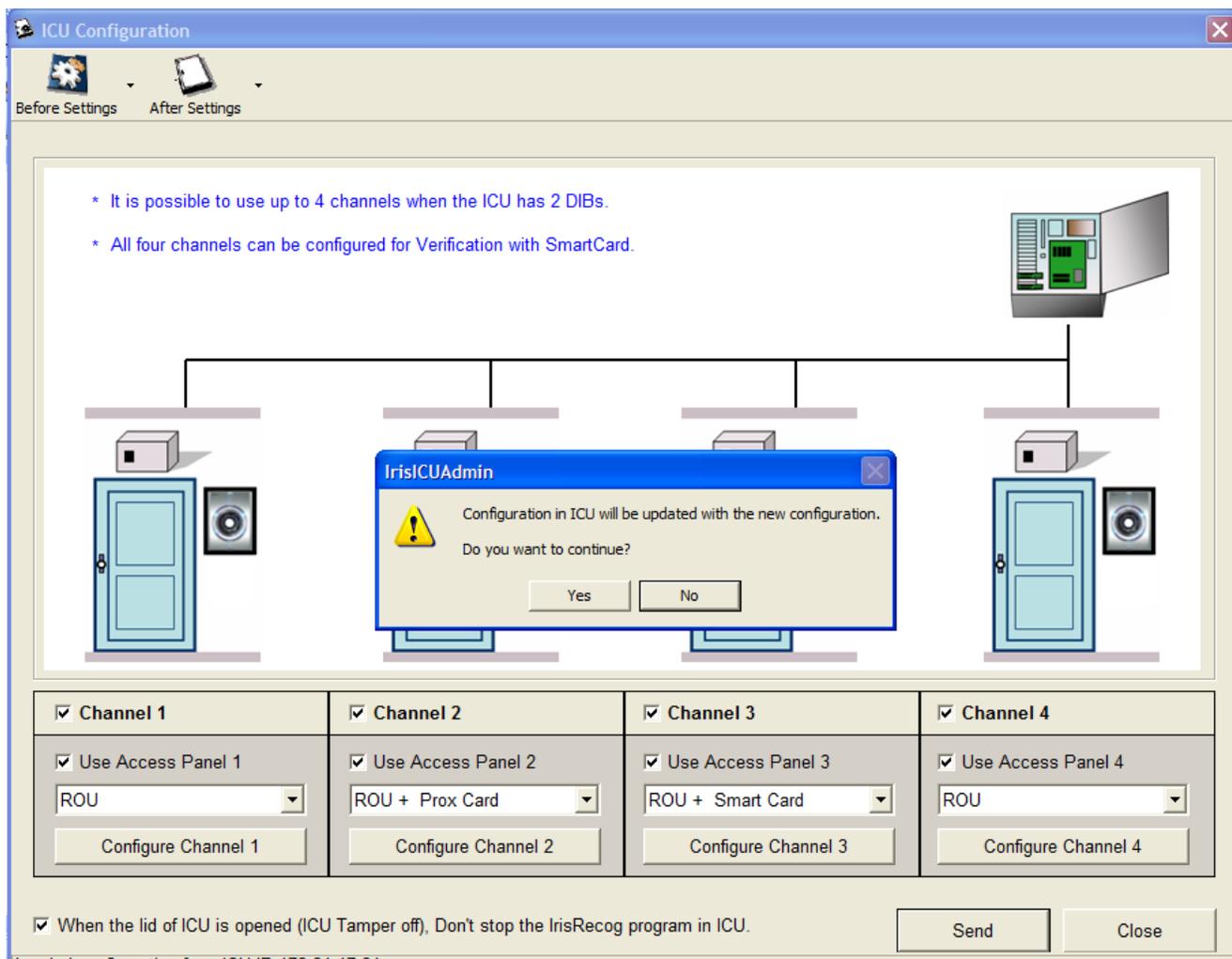
IA EAC format: This format supports Iris Access proprietary encryption algorithm.

GSC-IS format: This format supports AES, DES, DES3 or no encryption.

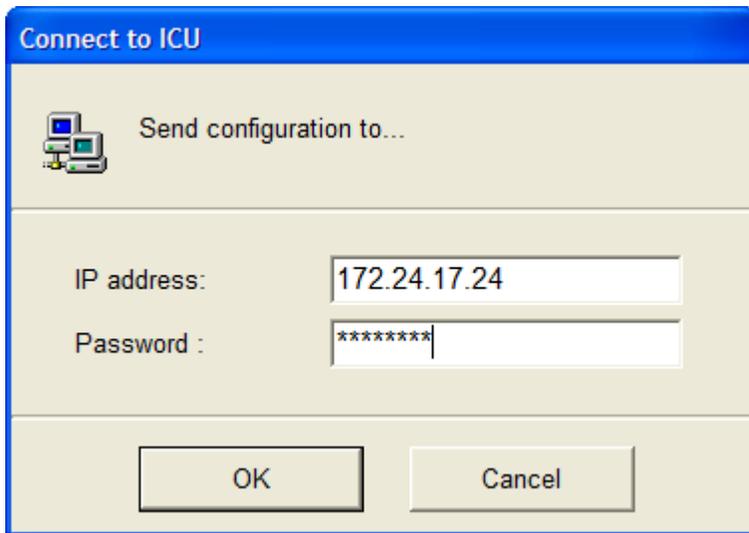
Lenel format: This format supports AES, DES, DES3 or no encryption.

Click on Get Keys button to Load the encryption keys from IrisServer.

Send Configuration to ICU

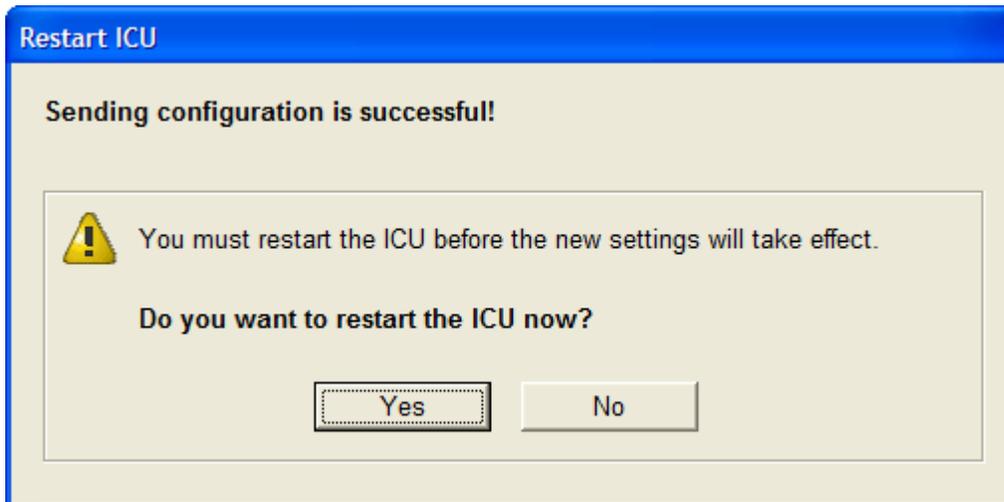


Once all the channels are configured, click on the Send button to send these configurations to ICU. A prompt to enter ICU IP address and password will pop up.



The image shows a Windows-style dialog box titled "Connect to ICU". It has a blue header bar. Below the header, there is a small icon of a computer and the text "Send configuration to...". There are two input fields: "IP address:" with the value "172.24.17.24" and "Password:" with the value "*****". At the bottom, there are two buttons: "OK" and "Cancel".

Enter the ICU IP Address and password and click on OK button. This will send the configuration to ICU. ICU will restart after the configurations are sent to ICU.



The image shows a Windows-style dialog box titled "Restart ICU". It has a blue header bar. Below the header, there is the text "Sending configuration is successful!". There is a yellow warning triangle icon followed by the text "You must restart the ICU before the new settings will take effect." Below this, there is the question "Do you want to restart the ICU now?". At the bottom, there are two buttons: "Yes" and "No".

11.2.6 The ICUAdmin3000 Change Password Window

ICU3000 Change Password

 Connect to the ICU to change password

Enter IP address of the ICU

IP Address	<input type="text" value="172.24.17.24"/>
Password	<input type="password" value="*****"/>

Please check below to reset the ICU password.
Note: ICU configuration cable connection is required.

Reset Password

Click 'Next' button to continue.

 Disconnected

Cancel < Back Next > Finish

IrisICUAdmin

 **1. Power off ICU4000**

2. ICU configuration cable must be connected to reset the password.

OK

ICU3000 Change Password

 ICU3000 Reset Password : Connect to ICU3000 for password reset.

Serial Port

Select serial port of Server PC which is connected to the ICU3000.

COM Ports:

Click 'Start' to reset the password of ICU3000.

Start

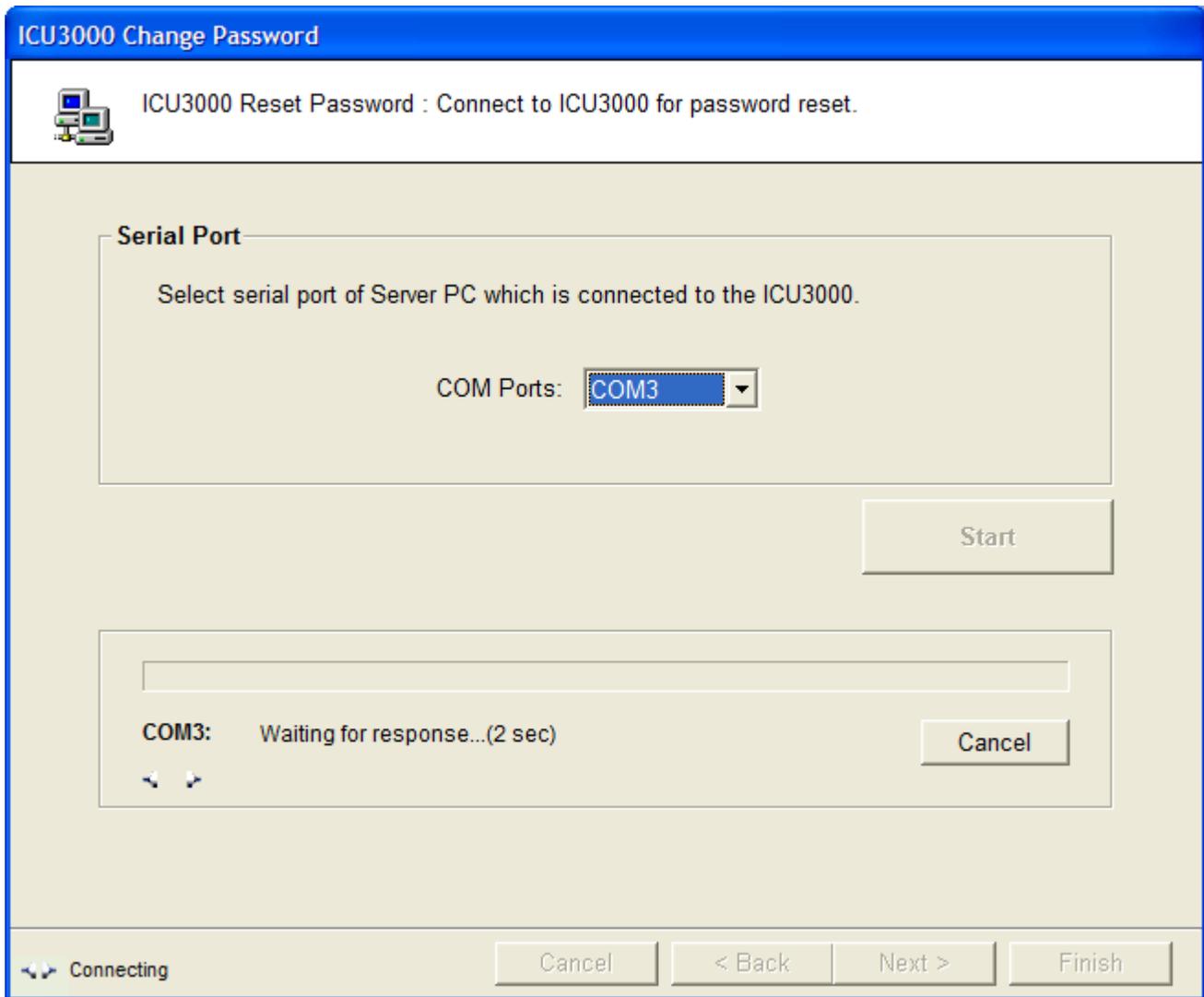
 Disconnected

IrisICUAdmin

Turn on (or restart) the ICU now!

Then, click the 'Start' button immediately.

It may take about 1~3 minutes to start password reset. Please wait until the message 'To reset the password is completed' is displayed.



Change Password

ICU3000 Change Password

 Change Current Password to New Password

New password	*****
Confirm new password	*****

Click 'Next' button to continue.

Connected

IrisICUAdmin 

 The password has been changed

