Air Live®

www.airlive.com

IAR-5000

Internet Activity Recorder

User's Manual

Declaration of Conformity

We, Manufacturer/Importer

OvisLink Corp.
5F., NO.6, Lane 130, Min-Chuan Rd.,
Hsin-Tien City, Taipei County, Taiwan

Declare that the product

Network Security Platform (Firewall)
RS-4000 / IAR-5000
is in conformity with

In accordance with 89/336 EEC-EMC Directive and 1999/5 EC-R & TTE Directive

Clause	Description
■ **EN 55022:1998/A1 :2000/A2:2003**	Limits and methods of measurement of radio disturbance characteristics of information technology equipment
■ **EN 61000-3-2:2000**	Disturbances in supply systems caused by household appliances and similar electrical equipment "Harmonics"
■ **EN 61000-3-3:1995/ A1:2001**	Disturbances in supply systems caused by household appliances and similar electrical equipment "Voltage fluctuations"
■ **EN 55024:1998/A1 :2001/A2:2003**	Information Technology equipment-Immunity characteristics-Limits And methods of measurement
■ **CE marking**	CE

Manufacturer/Importer

Signature：
Name ：**Albert Yeh**
Position/ Title ：**Vice President**

Date：**2006/4/20**

(Stamp)

RS-4000 / IAR-5000 CE Declaration Statement

Country	Declaration	Country	Declaration
cs Česky [Czech]	OvisLink Corp. tímto prohlašuje, že tento RS-4000 / IAR-5000 je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.	**lt** Lietuvių [Lithuanian]	Šiuo OvisLink Corp. deklaruoja, kad šis RS-4000 / IAR-5000 atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
da Dansk [Danish]	Undertegnede OvisLink Corp. erklærer herved, at følgende udstyr RS-4000 / IAR-5000overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.	**nl** Nederlands [Dutch	Hierbij verklaart OvisLink Corp. dat het toestel RS-4000 / IAR-5000 in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
de Deutsch [German]	Hiermit erklärt OvisLink Corp., dass sich das Gerät RS-4000 / IAR-5000in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.	**mt** Malti [Maltese]	Hawnhekk, OvisLink Corp, jiddikjara li dan RS-4000 / IAR-5000 jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
et Eesti [Estonian]	Käesolevaga kinnitab OvisLink Corp. seadme RS-4000 / IAR-5000 vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.	**hu** Magyar [Hungarian]	Alulírott, OvisLink Corp nyilatkozom, hogy a RS-4000 / IAR-5000 megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
en English	Hereby, OvisLink Corp., declares that this RS-4000 / IAR-5000 is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	**pl** Polski [Polish]	Niniejszym OvisLink Corp oświadcza, że RS-4000 / IAR-5000 jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
es Español [Spanish]	Por medio de la presente OvisLink Corp. declara que el RS-4000 / IAR-5000cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.	**pt** Português [Portuguese]	OvisLink Corp declara que este RS-4000 / IAR-5000está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ OvisLink Corp. ΔΗΛΩΝΕΙ ΟΤΙ RS-4000 / IAR-5000 ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.	**sl** Slovensko [Slovenian]	OvisLink Corp izjavlja, da je ta RS-4000 / IAR-5000 v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
fr Français [French]	Par la présente OvisLink Corp. déclare que l'appareil RS-4000 / IAR-5000 est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE	**sk** Slovensky [Slovak]	OvisLink Corp týmto vyhlasuje, že RS-4000 / IAR-5000 spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
it Italiano [Italian]	Con la presente OvisLink Corp. dichiara che questo RS-4000 / IAR-5000 è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.	**fi** Suomi [Finnish]	OvisLink Corp vakuuttaa täten että RS-4000 / IAR-5000 tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen
lv Latviski [Latvian]	Ar šo OvisLink Corp. deklarē, ka RS-4000 / IAR-5000 atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.	Íslenska [Icelandic]	Hér með lýsir OvisLink Corp yfir því að RS-4000 / IAR-5000 er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
sv Svenska [Swedish]	Härmed intygar OvisLink Corp. att denna RS-4000 / IAR-5000 står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.	**no** Norsk [Norwegian]	OvisLink Corp erklærer herved at utstyret RS-4000 / IAR-5000 er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

A copy of the full CE report can be obtained from the following address:

OvisLink Corp.
5F, No.6 Lane 130,
Min-Chuan Rd, Hsin-Tien City,
Taipei, Taiwan, R.O.C.

This equipment may be used in AT, BE, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LV, LT, LU, MT, NL, PL, PT, SK, SI, ES, SE, GB, IS, LI, NO, CH, BG, RO, TR

This device uses software which is partly or completely licensed under the terms of the GNU General Public License. The author of the software does not provide any warranty. This does not affect the warranty for the product itself.

To get source codes please contact: OvisLink Corp., 5F, No. 96, Min-Chuan Rd, Hsin-Tien City, Taipei, Taiwan, R.O.C. A fee will be charged for production and shipment for each copy of the source code.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of
these conditions:
a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
END OF TERMS AND CONDITIONS
How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.
Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is
a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision'
(which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

Copyright

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission.

Trademarks

All products, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

FCC Interference Statement

The **IAR-5000** has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility,
EN 55022/A1/A2, EN 61000-3-2, EN 61000-3-3/A1, EN 55024/A1/A2, Class B.

The specification is subject to change without notice.

Table of Contents

Chapter 1 Introduction **3**
1.1 Functions and Features 4
1.2 Deployment 5
1.3 Front Panel 5
1.4 Packing List 6
Chapter 2 Software Installation **7**
Chapter 3 System **13**
3.1 Admin 16
3.2 Interface IP 18
3.3 Setting 19
3.4 Date/Time 23
3.5 Permitted IP 25
3.6 Logout 26
3.7 Software Update 27
Chapter 4 User List **28**
Chapter 5 IM Management **39**
5.1 Configure 40
5.2 Authentication 42
5.3 Rule 95
Chapter 6 P2P Management **110**
Chapter 7 Record **112**
7.1 Setting 112
7.2 User 114
7.3 Service 119
Chapter 8 Anomaly Flow IP **131**
Chapter 9 Local Disk **135**
9.1 Storage Time 135
9.2 Disk Space 136
Chapter 10 Remote Backup **138**
Chapter 11 Report **146**
Chapter 12 Status **152**

Chapter 1 Introduction

Instead to restrict the access right of communication software, the AirLive brings you a brand new model of Internet Activity Recorder, IAR-5000. It can record the defined service packets in its hard disk, and provide the log to administrator for monitoring. With Sniffer mode or Bridge mode, network administrator will not need to change current network topology, and construct the advanced secure mechanism to protect the confidential information.

1.1 Functions and Features

- **Sniffer and Bridge mode**

  IAR-5000 supports sniffer mode and bridge mode; both installation types will not need to change current network structure. The IM/P2P management is available only at bridge mode.

- **Content Recorder**

  IAR-5000 provides the ability to record the contents of several network communicating programs, such as Mail, Web Mail, IM, HTTP, FTP and Telnet.

- **IM, Web mail signature pattern update**

  The updated process works to update IAR-5000, in order to recognize newest version IM or Web mail and record the contents.

- **Remote Backup**

  The recorded data can be stored at IAR-5000, or remotely to NAS and file server, the privilege user will be able to check the record by browser.

- **IM Authentication**

  It is for Bridge mode only. The administrator can restrict the access right of IM users, unless they pass the authentication. The database types support local database, RADIUS, POP3, and LDAP.

- **IM rule management**

  It is for Bridge mode only. The function is divided with Default Rule and Account Rule. IAR-5000 supports to detect IM account automatically, and offer them the default access rule; if necessary, administrator can also modify the rule per specific account in Account Rule.

- **P2P Management**

  It is for Bridge mode only. The function is divided with Default Rule and Account Rule. IAR-5000 supports to detect P2P account automatically, and offer them the default access rule; if necessary, administrator can also modify the rule per specific account in Account Rule.

- **Privilege user**

  Network administrator can define the privilege user who has the authority to access Internet without recording content.

- **Intrusion detection and notification**

  Administrator can customize the function to block the anomaly flow IP based on the setting, and send out a message to specific account for managing.

1.2 Deployment

- **Bridge Mode**：Link one of the internet recorder's ports to firewall or gateway, the other port connects to the internal network via hub or switch.
- **Sniffer Mode**：Link one of the internet recorder's ports to the mirror port of core switch or any port of the hub.

1.3 Front Panel

Figure 1-1 Front Panel

LED	Color	Status	Description
POWER	Green	On	Power on the device
Hard Disk	Green	Blinking	Data reading / accessing
Port1	Green	Blinking	Sending / Receiving
	Orange	On	100 Mbps
Port2	Green	Blinking	Sending / Receiving
	Orange	On	100 Mbps

Ports:

Port	Description
AC Power	Input voltages ranging from 100 ~ 240 VAC, and with a maximum power output of 85 watts.
Port 1	Use this port to connect to a router, DSL modem, or Cable modem
Port 2	Use this port to connect another ES-4000 device for HA function
Console Port	9-pin serial port connector for checking setting and restore to the factory setting

1.4 Packing List

- ES-4000 Mail Server Appliance
- Installation CD-ROM
- Quick Installation Guide
- CAT-5 UTP Fast Ethernet cable
- CAT-5 UTP Fast Ethernet cross-over cable
- RS-232 cable
- Power code
- Ear x 2
- Screw
- Rubber pad x 4

Chapter 2 Software Installation

Step1. Connecting the administrator's PC and IAR-5000 (port1 or port2) to the same hub or switch , and then use the web browser " IE or Netscape" to connect IAR-5000. The default IP port address in IAR-5000's management interface is http://192.168.1.1。

Step2. The management of IP interface is to fit the company's network environment, so we set the same subnet IP in LAN. If the LAN is not the subnet of IP address192.168.1.0. For example, if the LAN IP is 172.16.0.0 subnet, the administrator should change the management interface of IAR-5000 in the same subnet IP 172.16.0.0, it is easy to manage the device.

Step3. When the administrator enter theIAR-5000's network, enter **User Name** and **Password**. (Figure 2-1)

- **User Name**：admin
- **Password**：airlive
- click **OK**

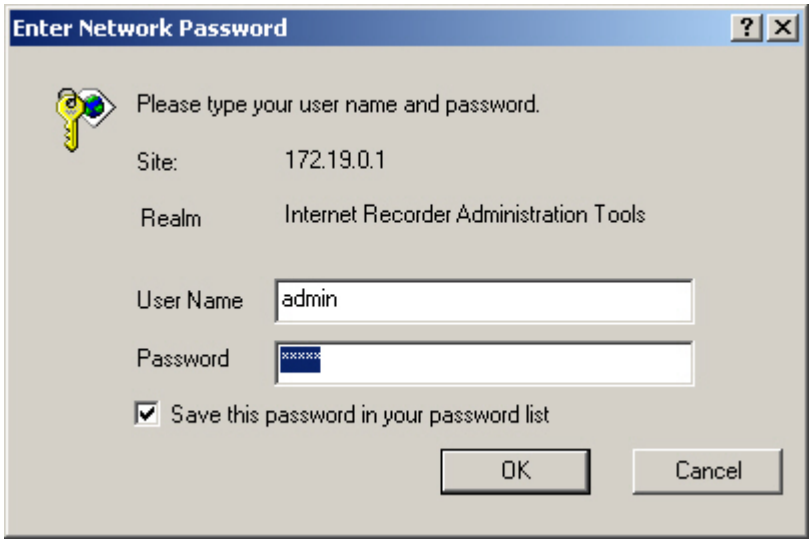


Figure 2-1 Enter the user name and password

Step4. When user is first time to use the IAR-5000 management interface, system will automatically enter **System → Wizard.** It will guide user to make settings, and then click **Next** (Figure 2-2).

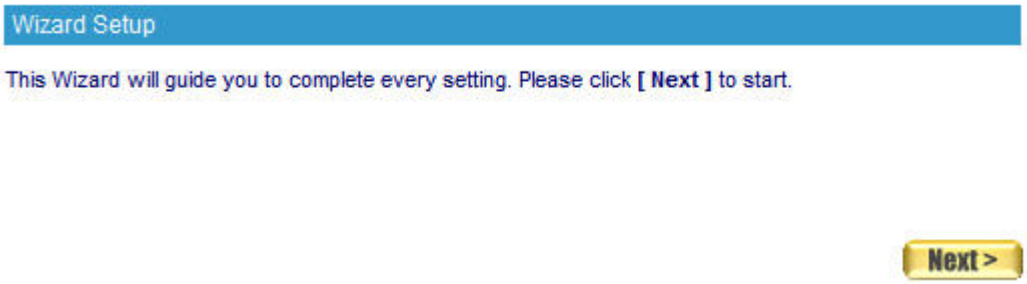


Figure 2-2 Enter the setting wizard

Step5. Select the language (System will change to the selected language automatically) and click **Next** (Figure 2-3).

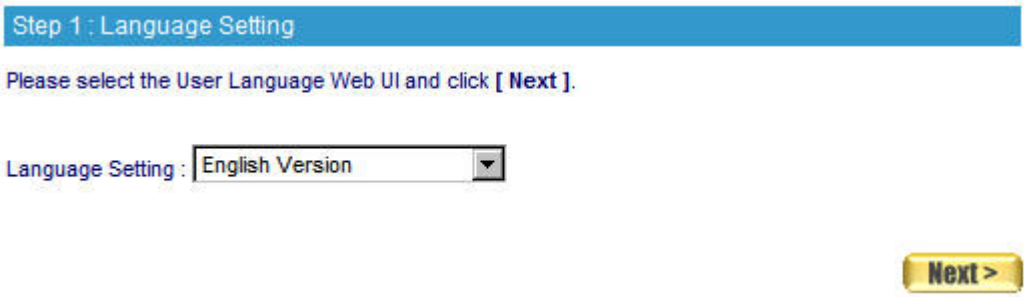


Figure 2-3 Select the language

Step6. Select the correct time zone and enter the time, and click **Next** (Figure 2-4).

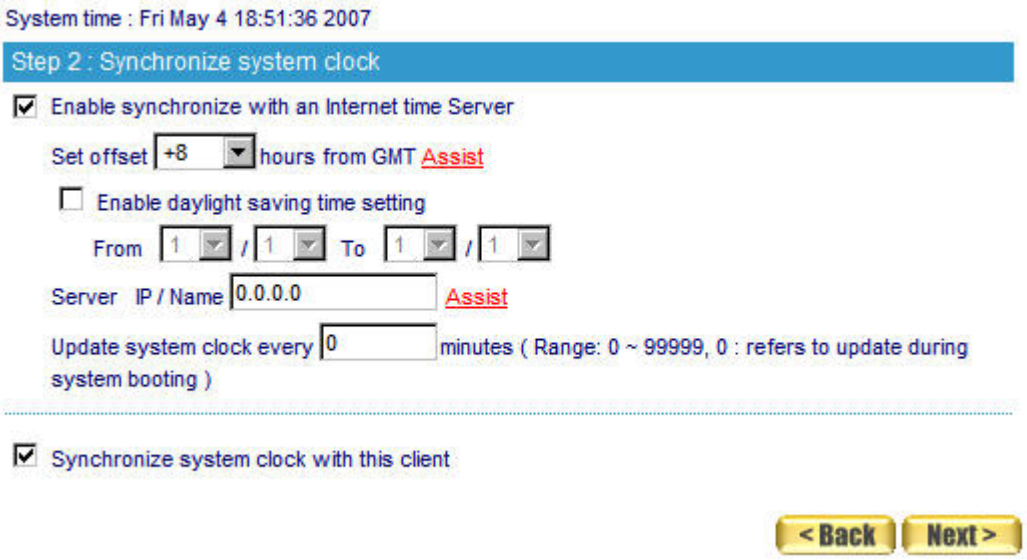


Figure 2-4 Synchronize system clock

Step7. Select the needed **Default Character Encoding,** and click **Next** (Figure 2-5).

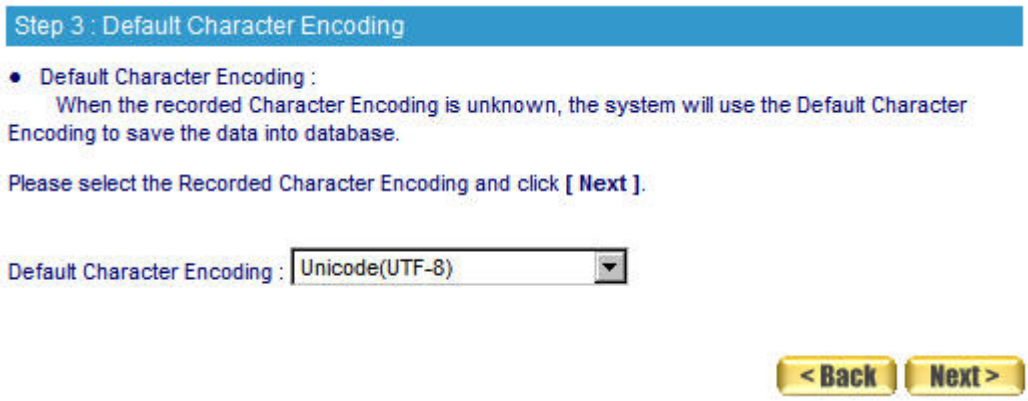


Figure 2-5 Select the default character encoding

When system can not identify the character encoding to save the data into database, it will use the default setting.

Step8. Select the deployment mode in **Network Deployment Mode,** and click **Next** (Figure 2-6).

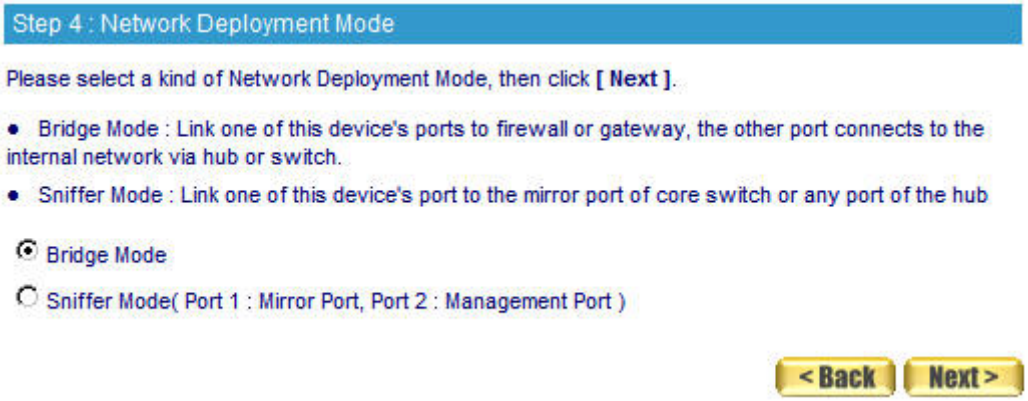


Figure 2-6 Select the Network Deployment Mode

Step9. Select User Name **binds to IP** or **MAC Address**, and click **Next** (Figure 2-7).

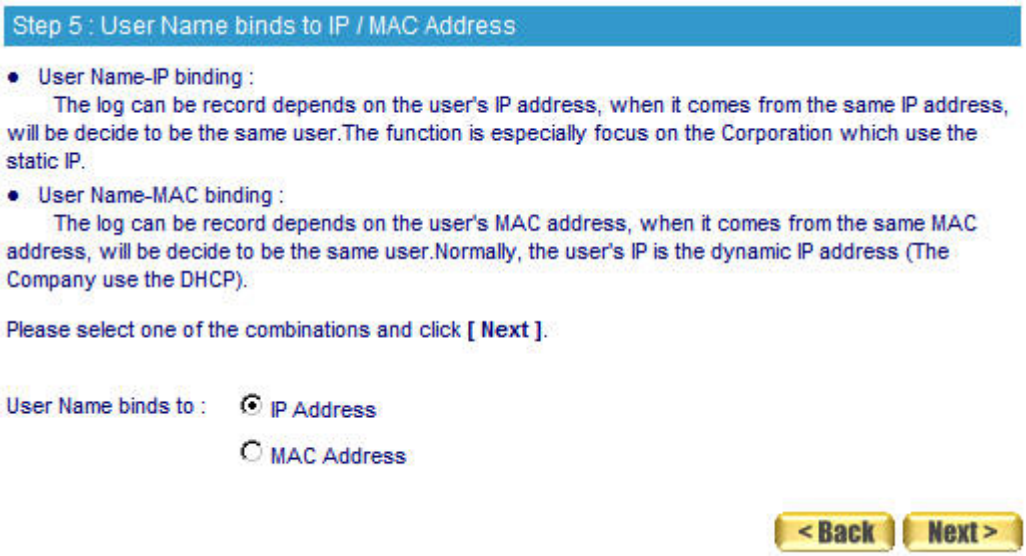


Figure 2-7 Select which method to save the data

User Name – IP binding: The log can be recorded depends on the user IP address, when it comes from the same IP address, will be decided to the same user. This function is usually use for the corporation which use the static IP.

User Name – MAC binding: The log can be recorded depends on the user's MAC address, when it comes from the same MAC address, will be decided to the same user. Normally, user's IP is the dynamic IP address. (Company uses the DHCP)

Step10. Enter the settings in Interface Address (Figure 2-8).

- Enter the available IP (the IP is settled in the same subnet as LAN) to be the IAR-5000 management interface. Set the **netmask, default gateway** and **DNS server** settings.
- If company use VLAN, then it's necessary to select **Enable VLAN of port 1 / 2** and enter the settings.
- Enter the **Downstream** and **Upstream bandwidth** settings.

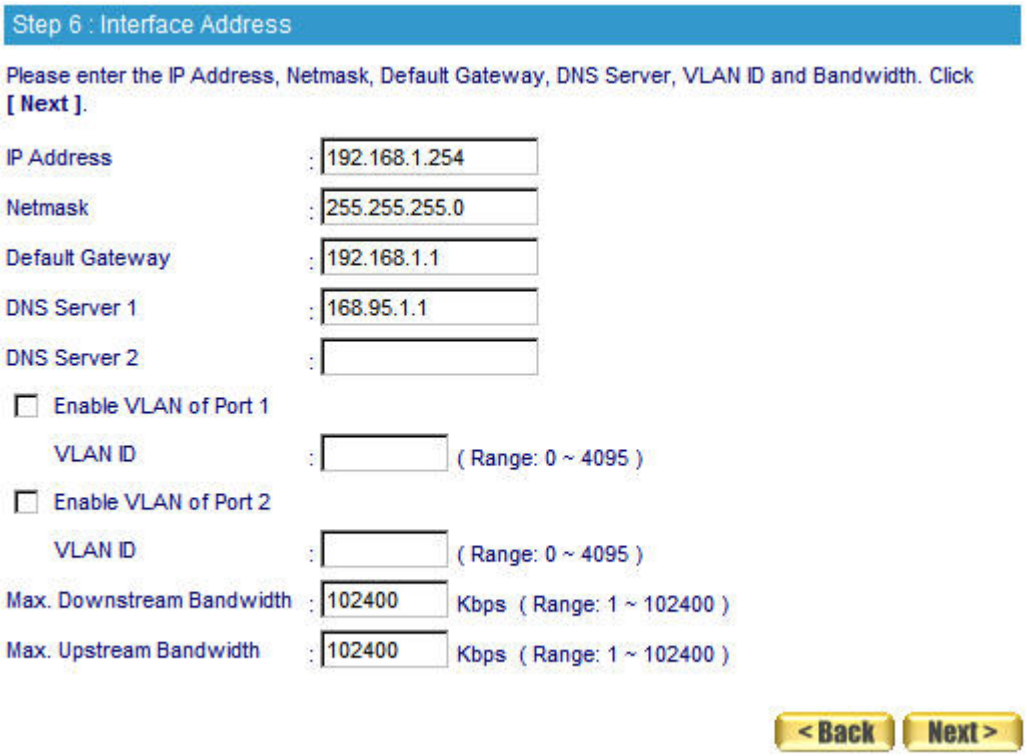


Figure 2-8 Enter the settings in interface address

The management interface address must correspond to the company's environment. Set the IP in same subnet as LAN. If the LAN is not the segment of 192.168.1.x, for example, the LAN is the segment of 172.16.x.x, and then the administrator has to change the management interface IP to 172.16.x.x.

This standard range of virtual IP:

10.0.0.0 ~ 10.255.255.255
172.16.0.0 ~ 172.31.255.255
192.168.0.0 ~ 192.168.255.255

Step11. Enter the subnet information to record, and click **Finish** (Figure 2-9).

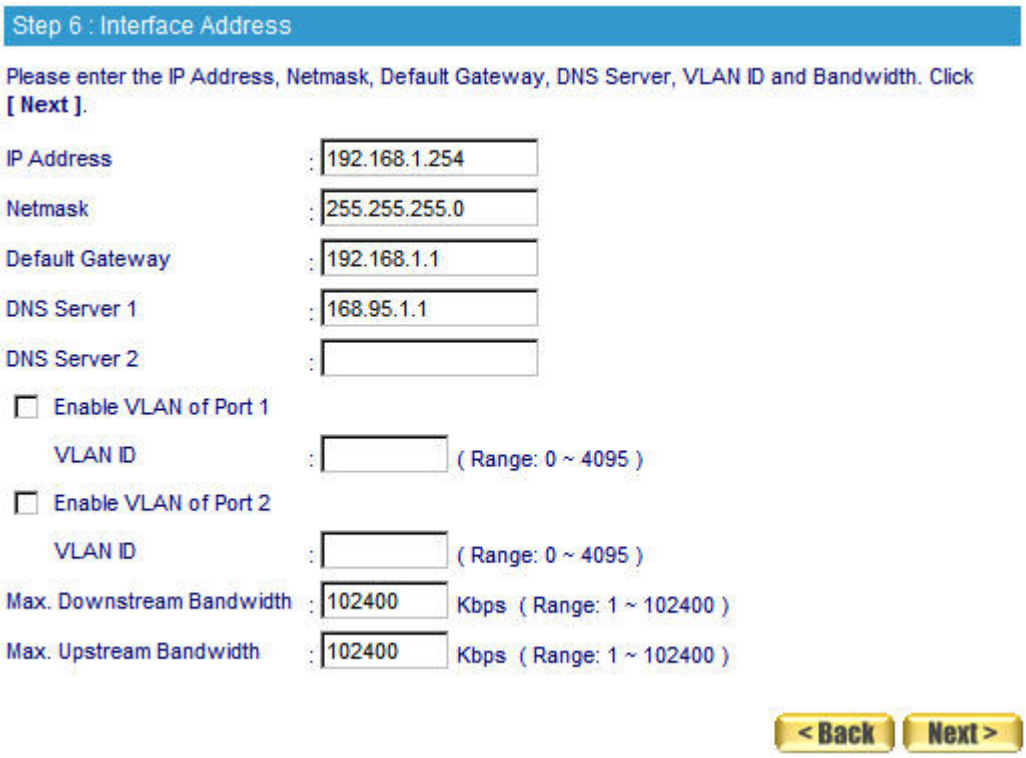


Figure 2-9 Enter the subnet information to record

If we change the interface IP after click **Finish**, then enter the custom interface IP in address column of web browser, so that we can log in to IAR-5000 again.

Step12. In **User List → Logged**, system will shows the default recorded list in the same subnet as the IAR-5000 interface address and the subnet. (Figure 2-10)

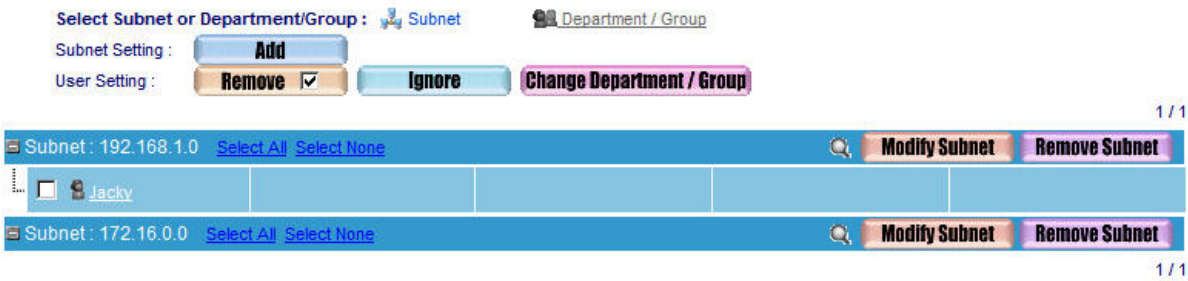


Figure 2-10 Logged list

Chapter 3 System

The so-called system administration refers the competency to manage the IAR-5000. In this Chapter it will be defined to the Admin, Interface IP, Setting, Date/Time, Permitted IPs, Language, Logout and Software Update.

The IAR-5000 is managed by the main system administrator. The main system administrator can add or delete any system settings and monitor the system status. The other group administrator have no competency to modify the system settings (the administrator's name is set by the system main administrator), only can monitor the system status.

Administrator:

Administrator/ Group administrator:

- The name of system administrator and group administrator. Administrator is the default name of system administrator in IAR-5000, and it can not be canceled; otherwise the group administrator can change or cancel it.
- The default system administrator can add or modify the other administrator, and also can decide if the group administrator has the competency to write into main system.
- On the other hand, the group administrator who has the write privilege can modify the competency of default system administrator, or only has the competency to read.
- There must be at least one administrator who has the competency to read and write in IAR-5000.

The default of system administrator in IAR-5000**: Account / password: admin / airlive**.

Privilege:

- The administrator, who has the competency to **read/write,** can change the system settings, monitor the system status, to add and cancel other administrators.
- The administrator, who has the competency to **read,** only can monitor the system status, but has no competency to change any settings.

Password/New Password/Confirm Password:

- To add or modify the main group administrator password.

View Groups:

- The group administrator can divide the internal network into several groups. And he can appoint the specific administrator to view the group but can not view across groups.

Interface IP:

Interface Address:

- The administrator can set the IP login information in IAR-5000.

Ping:

- Enable the function, the user can send Ping (ICMP) packets to Interface.

HTTP:

- Enable this function, the user can login IAR-5000 Web UI through HTTP protocol.

HTTPS:

- Enable this function, the user can login IAR-5000 Web UI through HTTPS protocol.

Download Bandwidth and Upstream Bandwidth：

- The system administrator should set the accurate bandwidth of WAN, in order to be the basic operation of IAR-5000.

Setting：

Internet Recorder Configuration：

- The system administrator can import or export the system settings, or they can also reset the factory setting and format the disk.

E-mail Setting：

- To activate this option, the system administrator will receive the caution message automatically when IAR-5000 is in the unpredictable trouble.

Web Management (Port Number)：

- The system administrator can use the WebUI to manage IAR-5000 anywhere. And the system manager can also change the port number of IAR-5000.

When the port number of HTTP and HTTPS had been changed, if the system administrator wants to log in to WebUI, he must change the WebUI port number. (For example: http://172.20.108.172:8080 and https:// 172.20.108.172:1025)

Log Storage Time

- System administrator can set the log storage time.

Date/Time:

Synchronize system clock:

- This option can synchronize the Date/Time in IAR-5000, the administrator's PC and the WAN server.

GMT:

The international standard time (Greenwich Mean Time: GMT).

Daylight saving time:

- Daylight saving time (also called DST, or Summer Time) is the portion of the year in which a region's local time is advanced by (usually) one hour from its standard official time.

3.1 Admin

Add New Group-Admin

Step1. In admin setting window, click the **New-Group Admin**.

Step2. In add new group-admin window, enter the following information. (Figure 3-1)

- **Group-Admin** set group_admin.
- **Password** enters 12345.
- **Confirm Password** enters 12345.
- In View Groups column, select the permitted group record to see.

Step3. Click **OK** to login the user or click **cancel,** to delete the new group administrator.

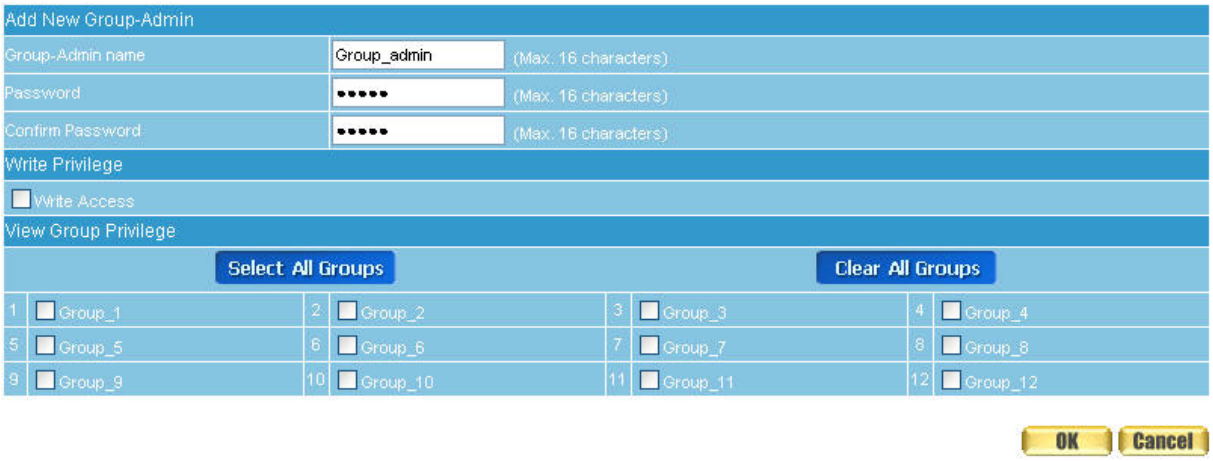


Figure 3-1 Add new group-admin

Change Admin password

Step1. Find the administrator's name that correspond to the right column, then click **modify**.

Step2. Modify admin password or modify group admin password window. And then enter the following information：

- **Password** enters airlive.
- **New Password** enters 52364.
- **Confirm Password** enters 52364. (Figure 3-2)

Step3. Click **OK** to modify the password or click cancel to cancel the setting.

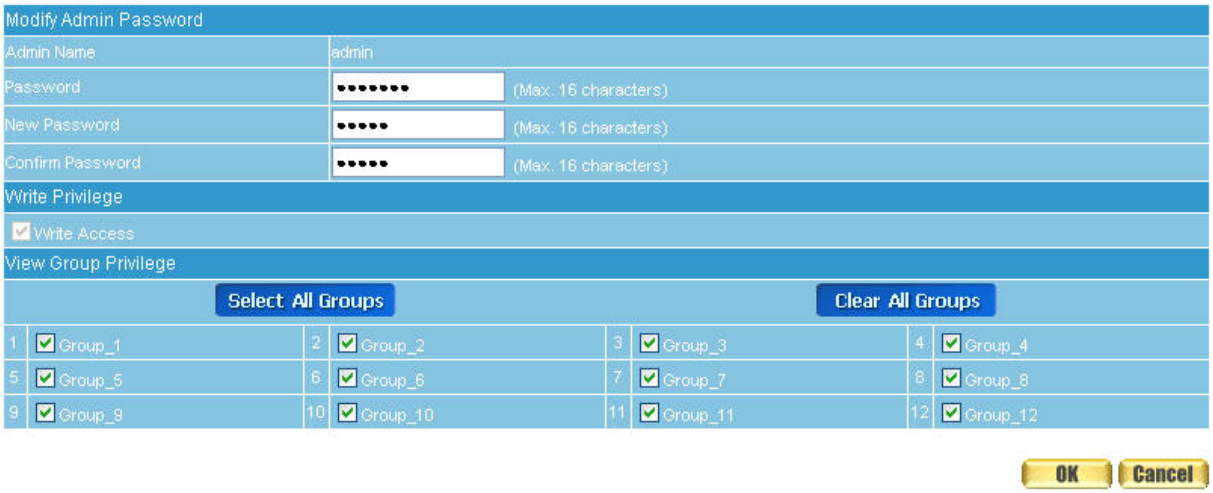


Figure 3-2 To change the admin password

3.2 Interface IP

Step1. In **System → Interface IP**, enter the following setting:

- Enter the available IP of the LAN subnet in **IP Address**, **Netmask and Default Gateway** column.
- Enter **DNS server 1** or **DNS server 2.**
- If necessary, select to enable VLAN feature and provide the VLAN ID based on the setting.
- Enter **Max Downstream Bandwidth** and **Max Upstream Bandwidth**.
  (It depends on the applied flow statistics of the user.)
- Enable the setting of **Ping, HTTP and HTTPS function.**
- Click **OK**. (Figure 3-3)

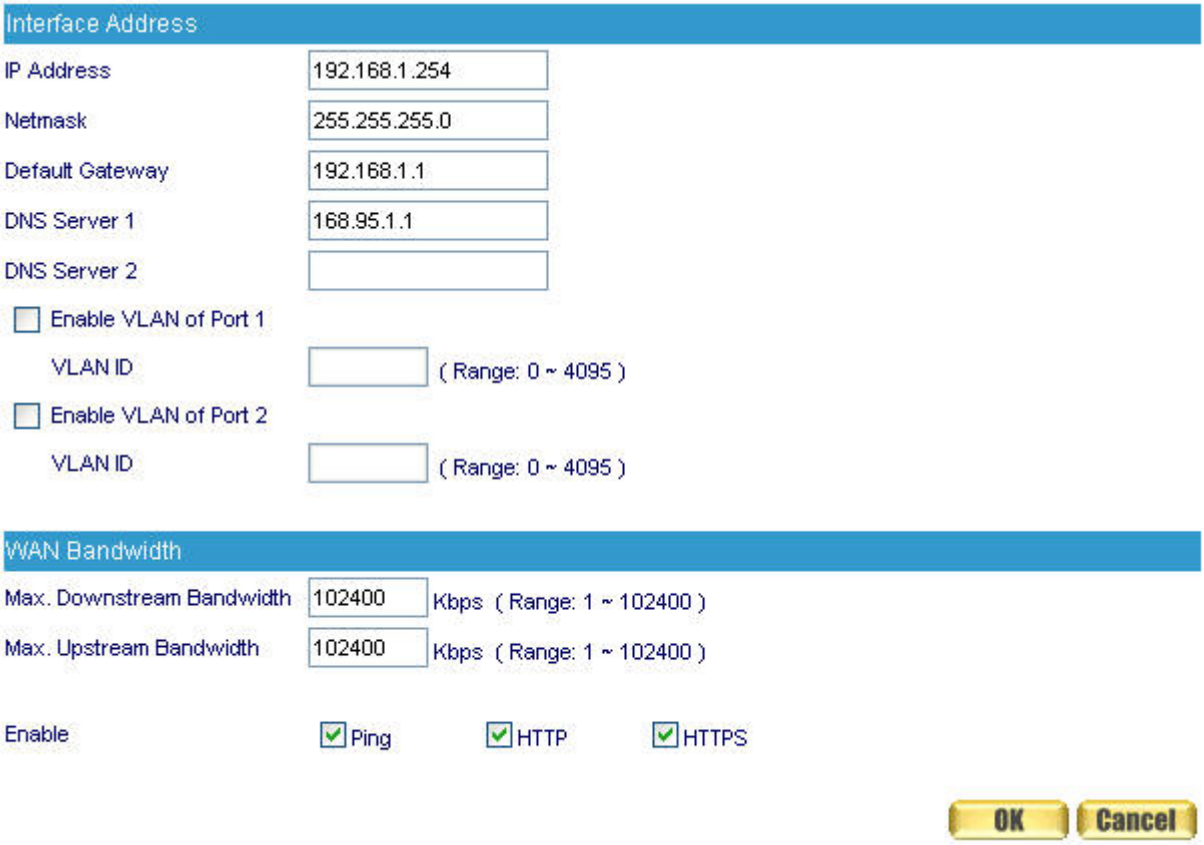


Figure 3-3 The interface IP setting

Please do not cancel HTTP and HTTPS before setting the **Interface IP**, because it will let the system administrator could not enter the WebUI of IAR-5000.

3.3 Setting

Export the configured file

Step1. In **System Setting**, select **Internet Recorder Configuration → Export System setting to client**, and click the **download** button at the right place.

Step2. When it appeared **File Download** window, click **Save** button, and it will show where the file will be saved, then click **Save** button again. The settings of IAR-5000 will be copied to the appointed directory. (Figure 3-4)

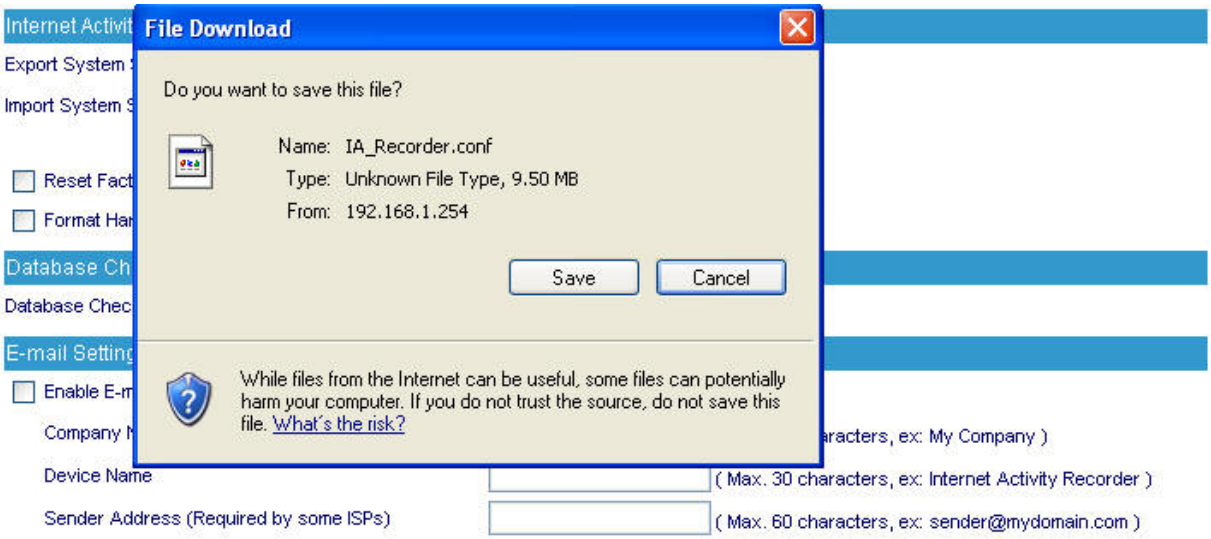


Figure 3-4 Choose where the export file will be saved

Import the configured file

Step1. In **System Setting** window, **Internet Recorder Configuration →Import System Setting from Client**, then click Browse button at right place.

Step2. In **Choose File** window, choose the directory of former saved file in IAR-5000, and choose the correct setting, then click Open. (Figure 3-5)

Step3. Click the lower right OK, the window will closed.

Step4. Click the OK inside the confirm dialogue box, the setting will import to IAR-5000. (Figure 3-6)

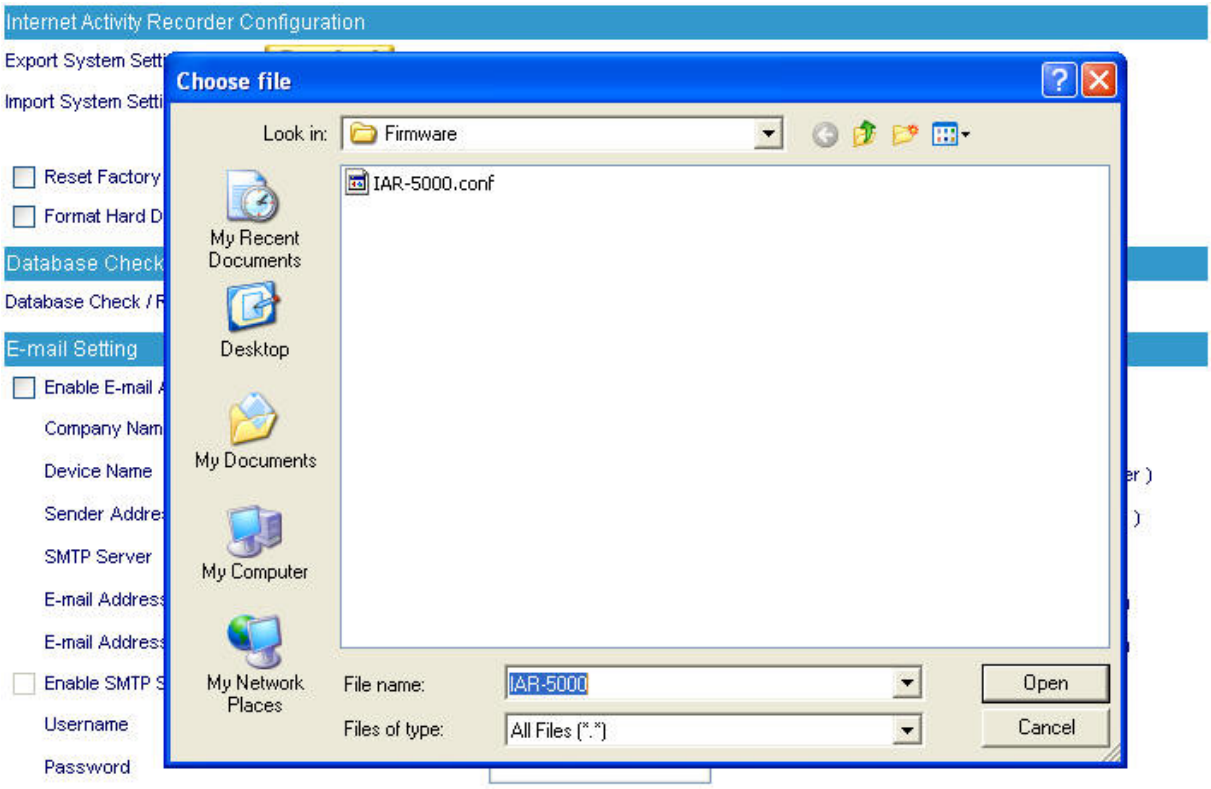


Figure 3-6 Import the file name to the directory to saved

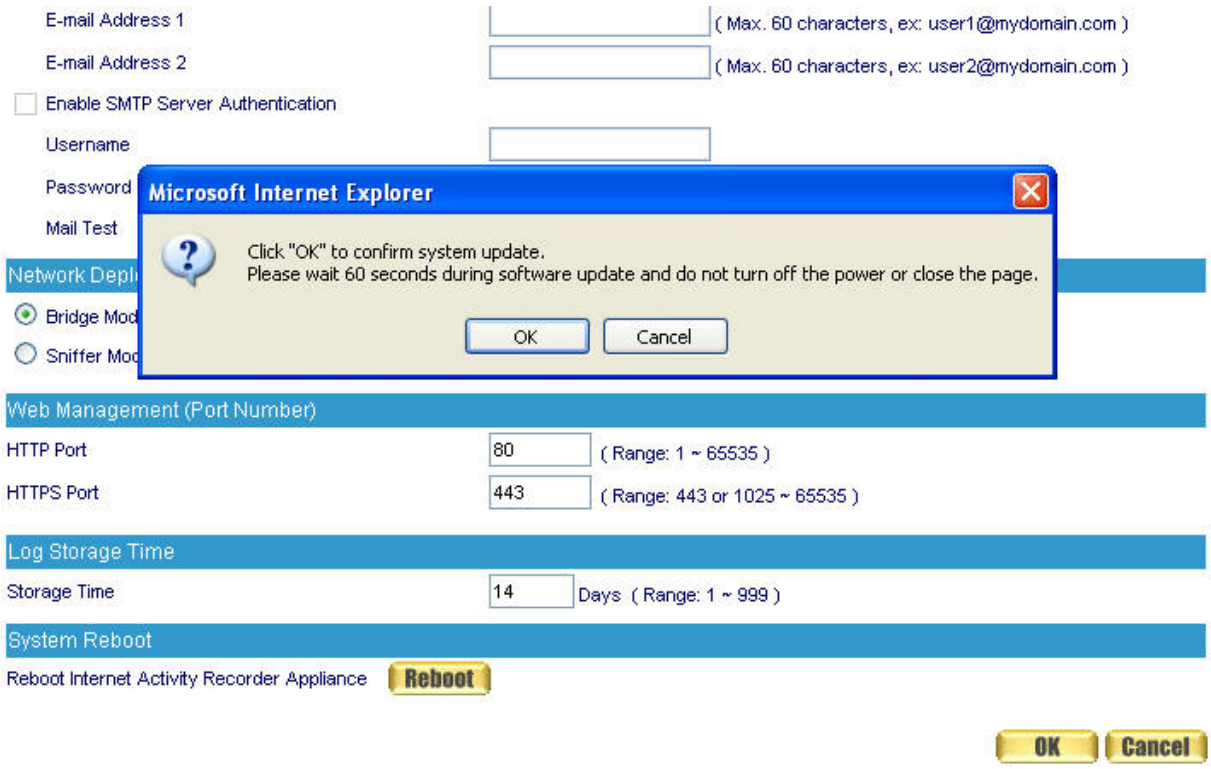


Figure 3-6 Confirm the import setting

Reset Factory Default

Step1. In **System → Setting → Internet Recorder Configuration,** select **Reset Factory Setting** and **Format Hard Disk**.

Step2. Click the **OK** in the lower right, it will restore to the factory setting of IAR-5000 and format the disk at the same time. (Figure 3-7)

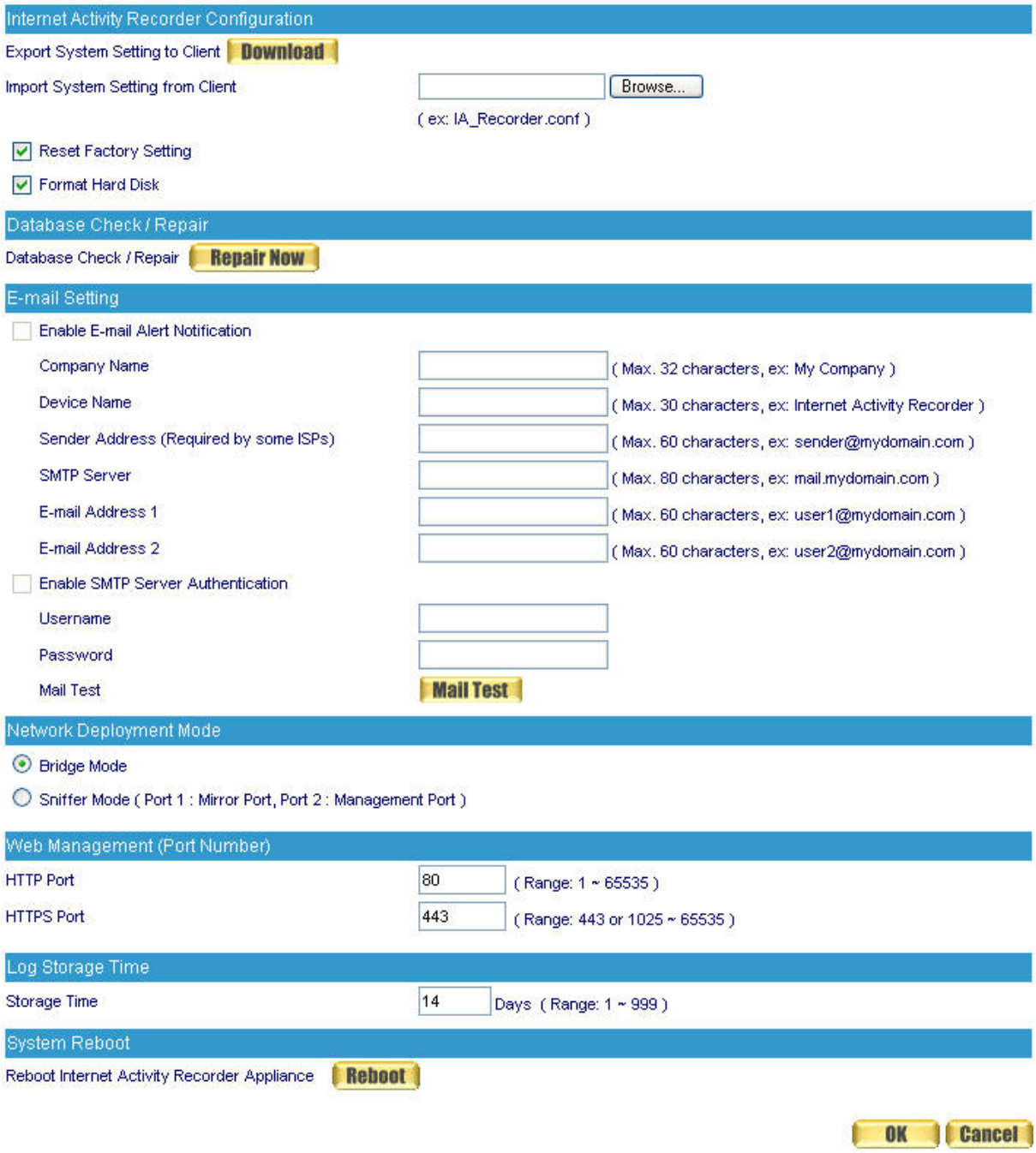


Figure 3-7 Select Reset Factory Setting

Configure Email Notification

Step1. Select **E-Mail Setting → Enable Email Alert Notification.**

Step2. **Company Name,** enter the name of the company which belong the IAR-5000.

Step3. **Device Name,** enter the name of IAR-5000.

Step4. **Sender Address,** sending the e-mail address of the sender.（Some of the ISP have request to enter in the sender address column）

Step5. **SMTP Server,** enter the IP address of the delivered e-mail in SMTP server.

Step6. **E-Mail Address 1**, enter the e-mail address in the first one position to receive the alarm message.

Step7. **E-Mail Address 2**, enter the e-mail address in the second position to receive the alarm message.

Step8. Click the lower right **OK** to set the function of message alarm. (Figure 3-8)

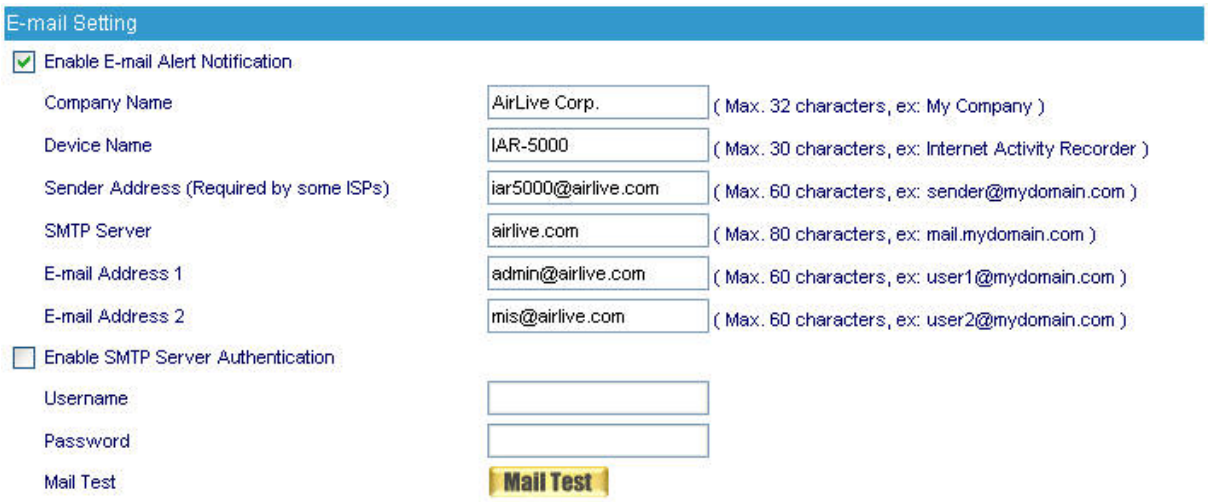


Figure 3-8 Enable the instant mail message alarm of IAR-5000

Select **Enable SMTP Server Authentication** and enter the username and password, then click **Mail Test** button to test E-Mail address 1 and E-Mail address 2, to see if the e-mail sending address can receive the current caution message.

Reboot

Step1. Select **Reboot Internet Recorder Appliance → Reboot** button.

Step2. It will show ”Are you sure to reboot ?“

Step3. Click OK to reboot IAR-5000, or click Cancel to cancel reboot IAR-5000. (Figure 3-9)

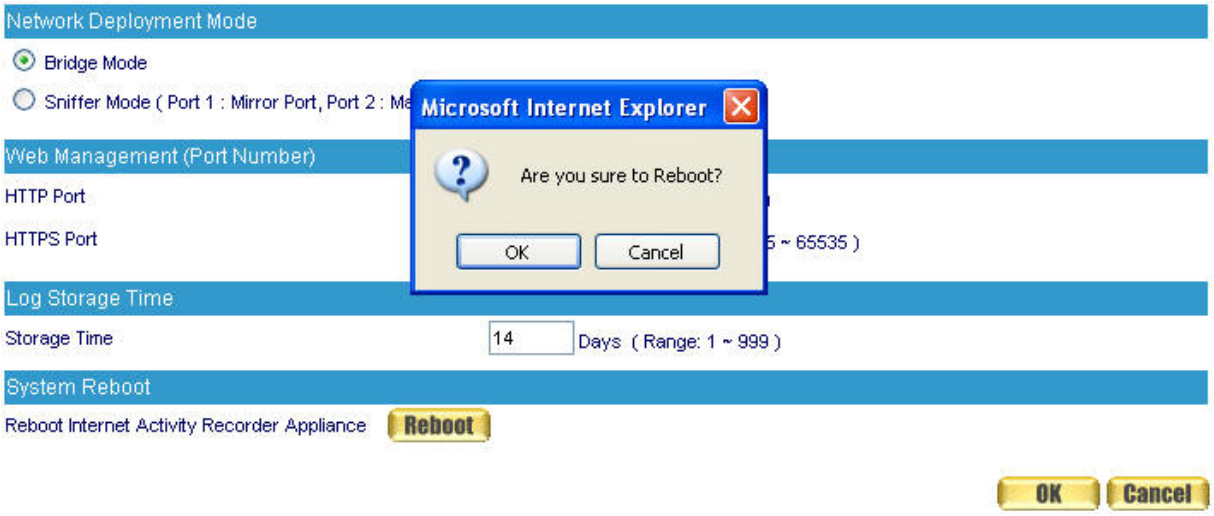


Figure 3-9 Reboot the internet recorder appliance

3.4 Date/Time

Step1. Select **Enable Synchronize with an Internet Time Server.** (Figure 3-10)

Step2. Click **Set Offset Hours from GMT** pull down menu, and choose the correct time.

Step3. Enter the Server IP address into **Server IP/Name**.

Step4. Enter the frequency of the updating time in **Update system clock every minute**.

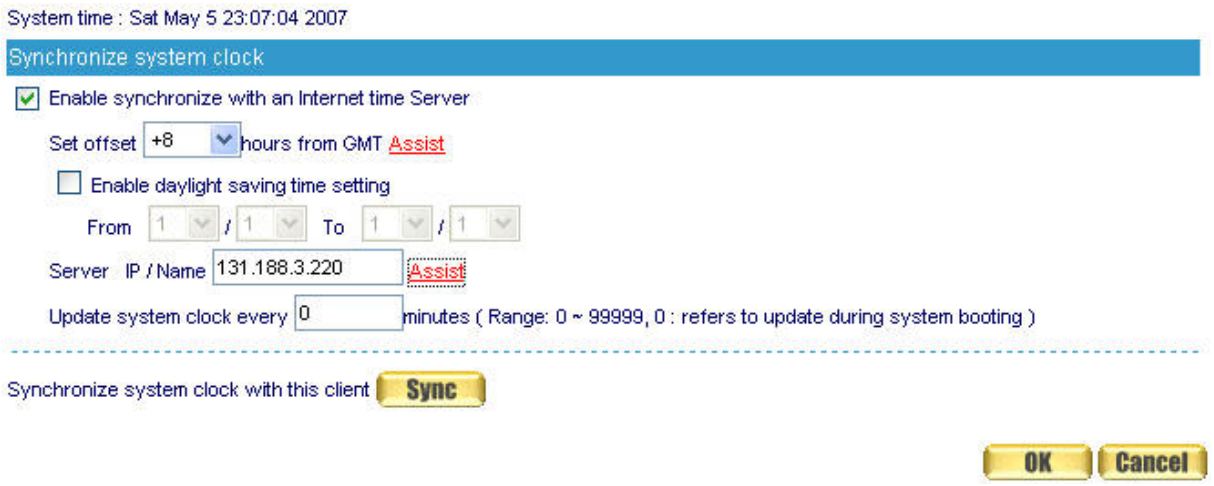


Figure 3-10 System time setting

Select **Synchronize → Sync** button, the system time in IAR-5000, will synchronize to the administrator's computer.

The settings of **Set offset hours from GMT** and **Server IP** can be entered with using **Assist**.

If the local area executes the daylight saving time, then **enable the daylight saving time setting.**

3.5 Permitted IP

Step1. In **System → Permitted IPS → New Entry,** add the new setting: (Figure 3-11)

- **Name** enters master.
- **IP Address** enters 192.168.139.30.
- **Netmask** enters 255.255.255.255.
- **Service** selects Ping, HTTP and HTTPS.
- Click **OK**.
- Complete Permitted IPs settings. (Figure 3-12)

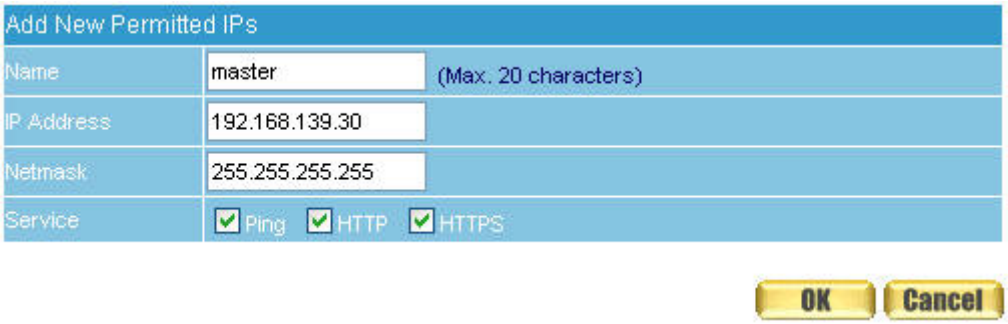


Figure 3-11 The Permitted IPs setting

Figure 3-12 Complete the Permitted IPs setting

If you want the Permitted IPs to be real working, when it must be connected from the administrator to the interface of IAR-5000 WebUI, but the settings of Ping, HTTP and HTTPS all must be canceled. Before you cancel the interface address of HTTP and HTTPS, you have to set the Permitted IPs first or it will not connect to WebUI through the internet.

3.6 Logout

Step1. Click the **Logout** icon in the up right of Web UI, it can let the system administrator to log out from the system admin anytime, and also prevent other person change the settings of IAR-5000. (Figure 3-13)

Figure 3-13 Confirm to logout

Step2. Click **OK**, it shows the logout information. (Figure 3-14)

Figure 3-14 The logout WebUI

3.7 Software Update

Step1. In **System → Software Update**, the user can update the firmware step by step:

- In Version Number, we can know the current version of the software. Go on the internet to gain the newest version of the firmware and download into the storage disk in IAR-5000.
- Click Browse → Choose file, select the newest version of the software.
- Click the lower right OK, it will process the update. (Figure 3-15)

Figure 3-15 Software update

It needs 3 minutes to update the software, and will reboot after updated the system. Please do not turn it off, off line and exit the web page during the update, or it will cause the error in IAR-5000. (It is recommended using the LAN to update.)

Chapter 4 User List

This chapter is about the users can be monitored by the IAR-5000. It can automatic search and add the new users, and the system administrator can add the lists by himself.

Setting

User List Configuration：

- Administrator can export the monitor user list and some related settings to the PC or import these settings into IAR-500.

Department / Group ：

- The administrator can group the users according to the network structure, so that he can manage the system more easily.

The company can be divided into several departments, and part of the user (department) settled in different subnet.

Step1. In **User List → Setting,** set the following settings：

- To set the **Department / Group** depends on the real network deployment.
- Click **OK** (Figure 4-1)

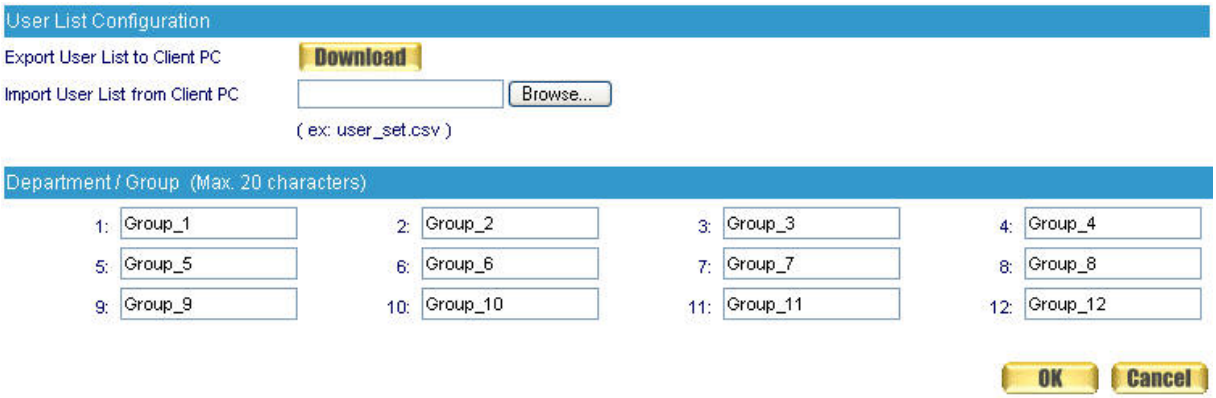


Figure 4-1 Set the user list

Step2. In **User List → Logged**, add the new user.

- Click of 192.168.1.0 subnet and the IAR-5000 will search the new user in the subnet. (Figure 4-2)
- Wait 1~2 minutes until search complete. (Figure 4-3)
- If system administrator wants to search users in specific subnet, set the **search IP range** and click **search.**
- Select the new user to add, click **New User**. (Figure 4-4, 4-5)

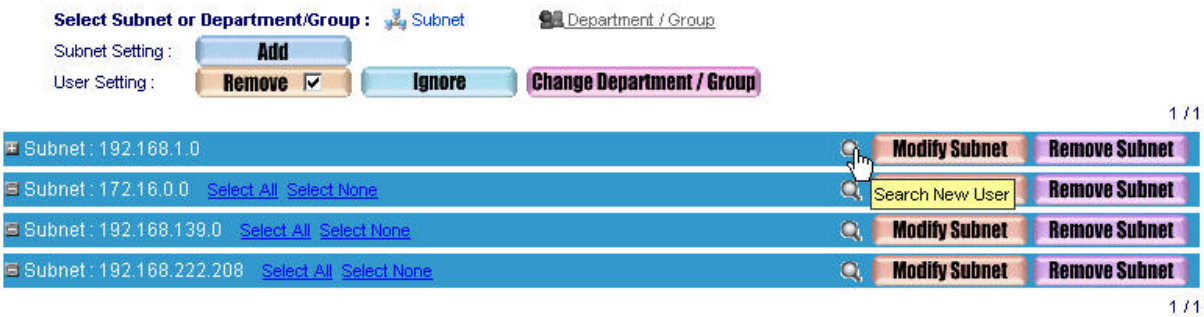


Figure 4-2 Click search new user button

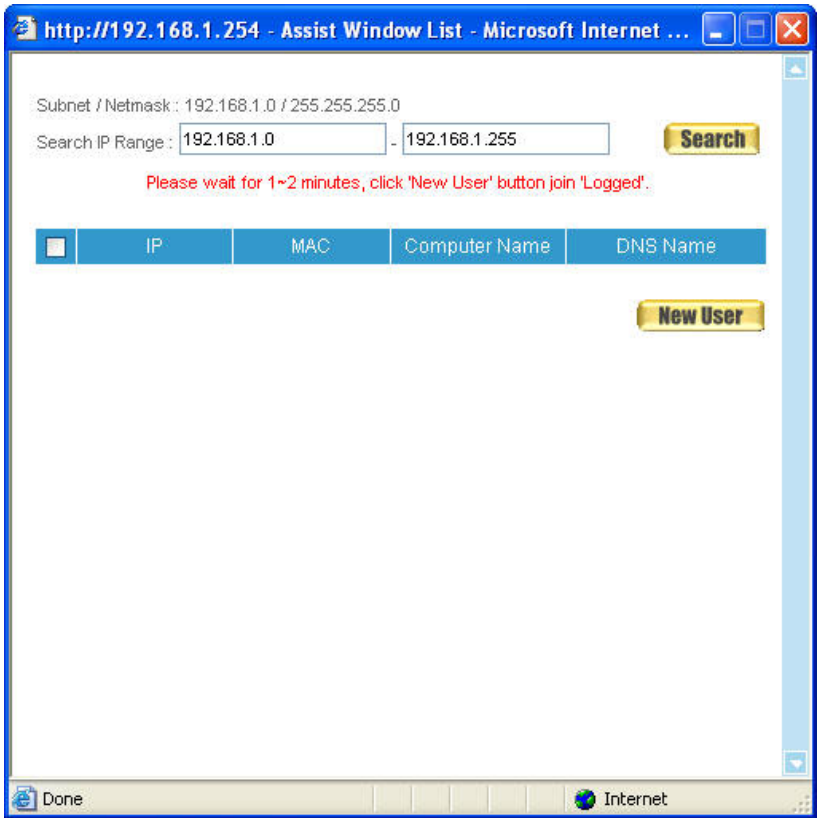


Figure 4-3 Starting to search new user

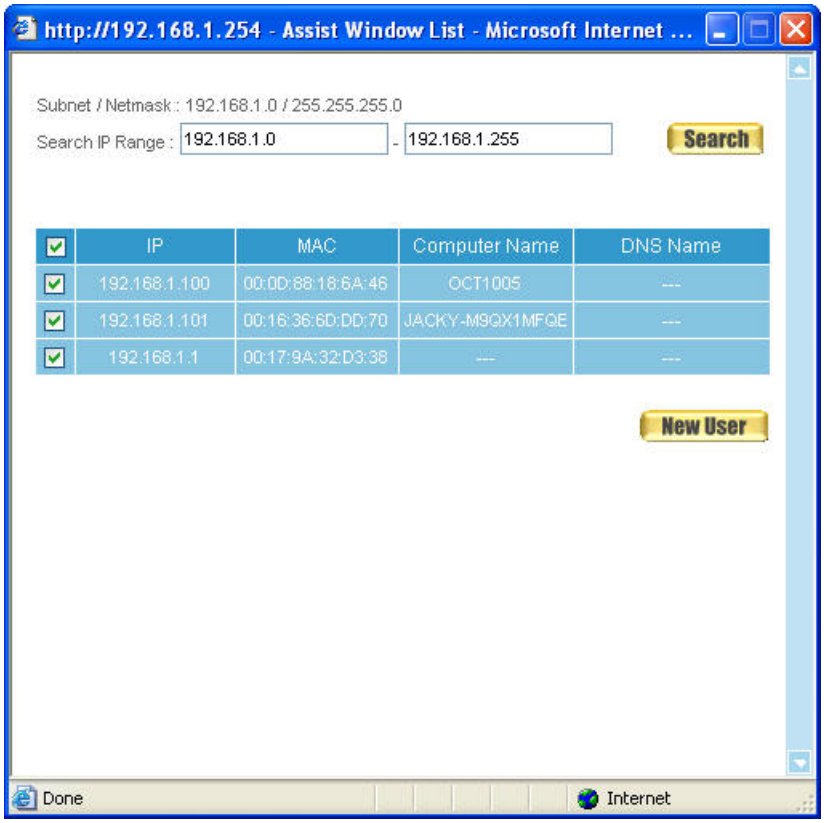


Figure 4-4 Select the new user to add

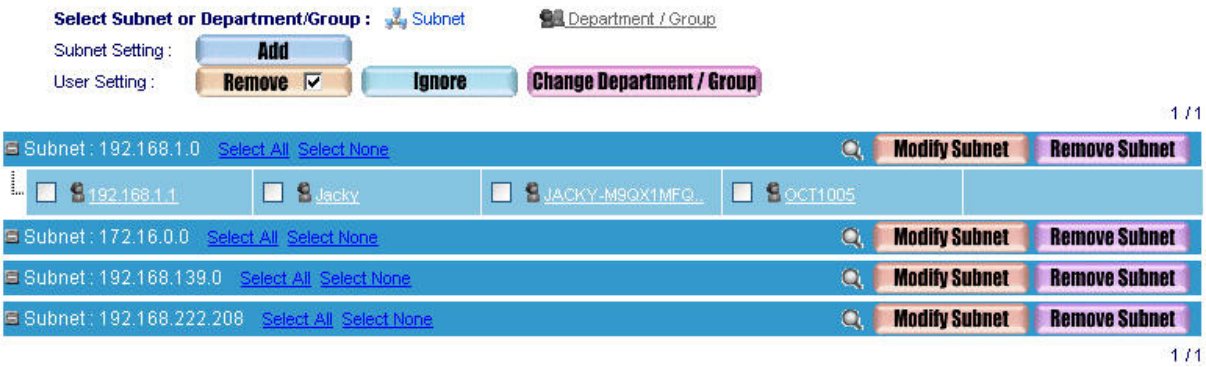


Figure 4-5 Complete to add the new user

After finished the setting of **System → Interface IP**, system will set the subnet to be the **first user group** in **logged user list**, which the interface correspond to.

The IAR-5000 can automatically add the user who has ever used the internet in **logged user list**.

In **System → Interface IP**, if the DNS server set to be the company's internal DNS server, then the IAR-5000 will also look up the user DNS name correspond to the internal DNS server when searching the user list.

When the searched PC has been set the PC or DNS name, then IAR-5000 will use them to apply to user name. The user name priorities are: **PC name → DNS name → IP or MAC** (It depends on the setting of **Record → Setting → User Name binds to IP or MAC address**).

Step3. Modify the user in user list：

- Click User Name of JACKY-M9QX1MFQE
- User Name, enter Jacky_NB.
- Department / Group, select Laboratory.
- Click **OK**. (Figure 4-6, 4-7, 4-8)
- Click **User Name** of OCT1005.
- **User Name**, enter Gateway.
- **Department / Group**, select Device_Room.
- Select **move this user to ignored user list**.
- Click **OK**, then the user will be removed to ignore user list. (Figure 4-9, 4-10, 4-11)
- Repeat the steps to complete modifying the user list. (Figure 4-12)

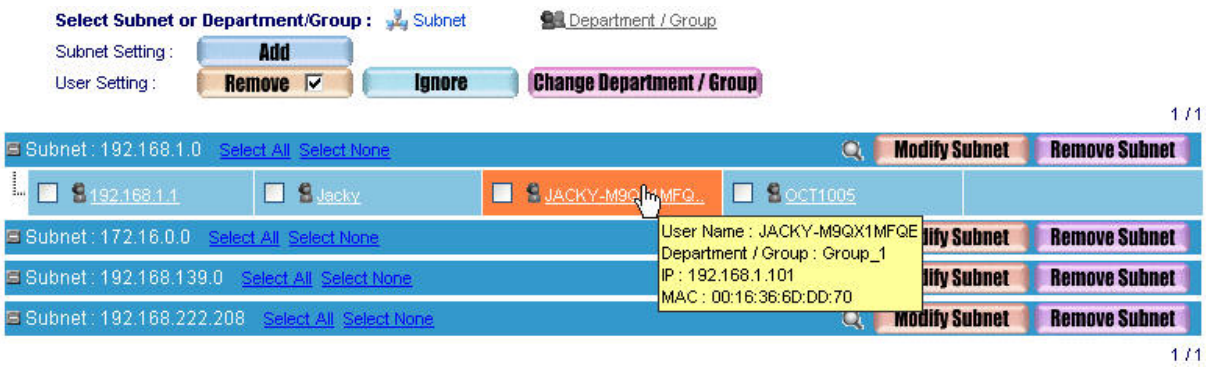


Figure 4-6 Select the user to modify

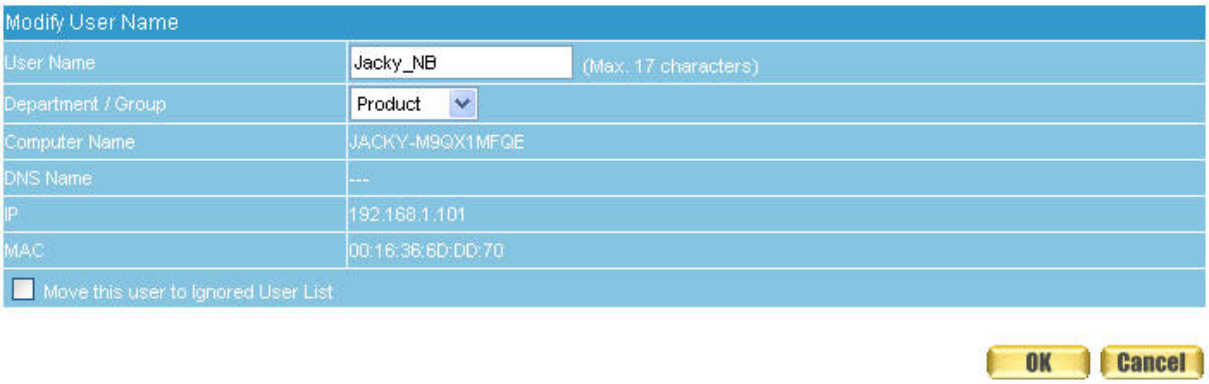


Figure 4-7 Enter the user information to modify

Figure 4-8 Complete to modify the user information

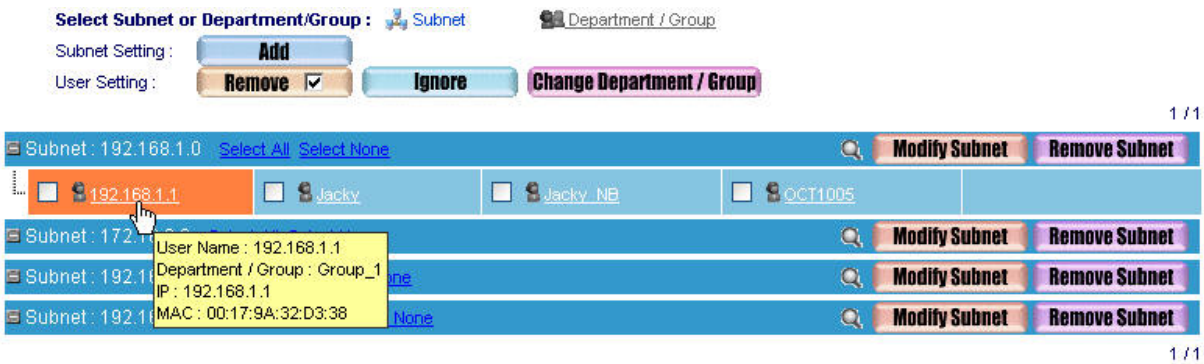


Figure 4-9 Select the user to modify

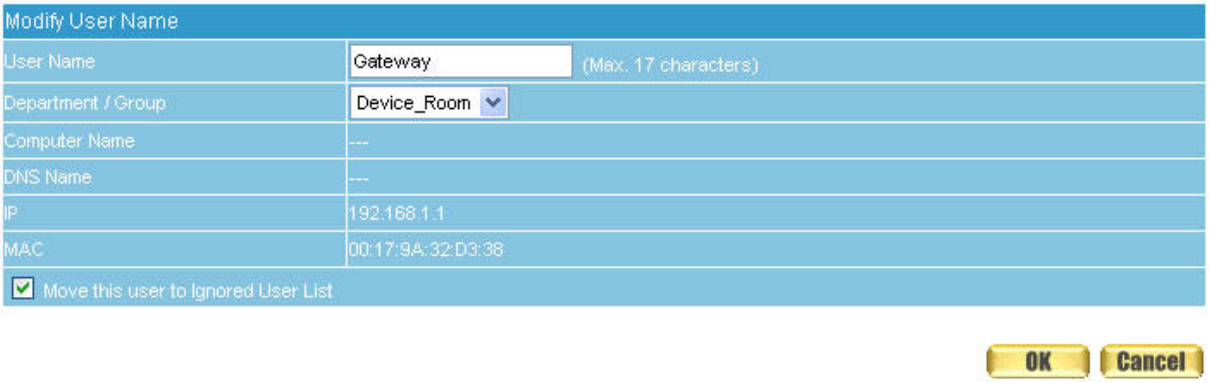


Figure 4-10 Enter the user information to modify

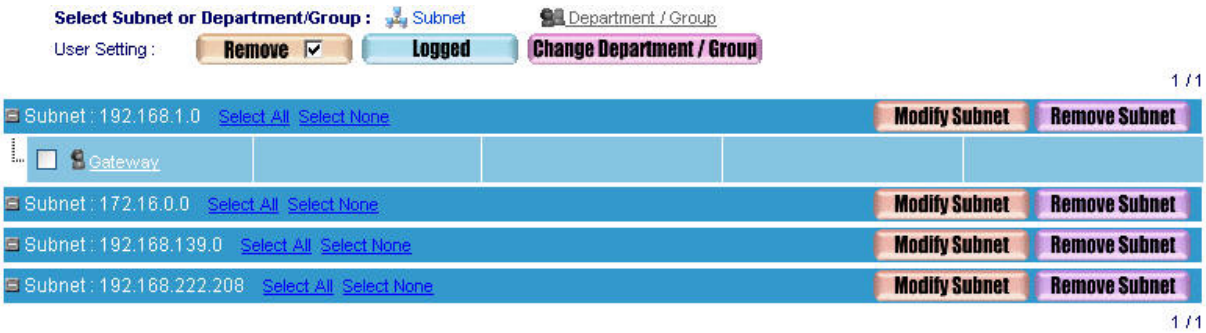


Figure 4 -11 Move the user to ignored user list

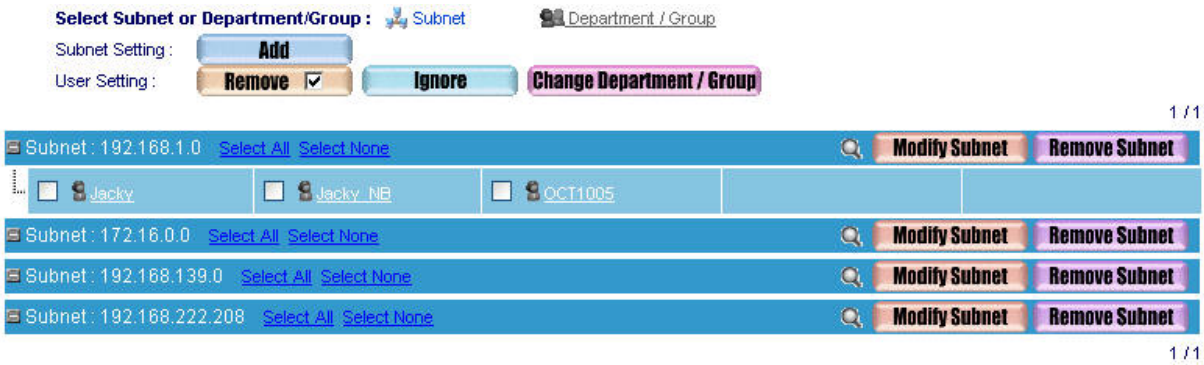


Figure 4-12 Complete to modify the user list

In **Ignored user list**, the system administrator can also select the user to move to **logged user list.**

Step4. In **User List → Logged**, add the new subnet:

- Click **Add.**
- **Subnet**, enter 192.168.139.1.
- **Netmask**, enter 255.255.255.0.
- **Add a New user to this Department / Group**, select R.D.
- Click **OK**. (Figure 4-13)

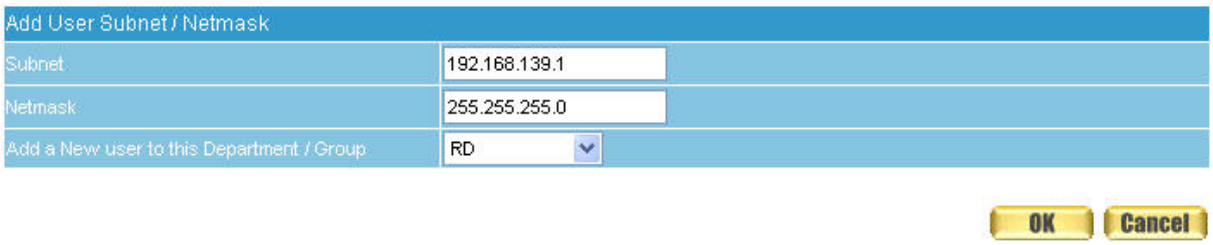


Figure 4-13 Add a new subnet

The **Department / Group** that selected by system administrator, which will become the default **Department / Group** in this subnet.

Step5. Repeat **Step 2** to **Step 4** until finish to set the user list.

Change the user list by import the user list configuration (excel list)

Step1. In **User List → Setting → User List Configuration → Export User List to Client PC →** click Download.

Step2. When it appears **File Download**, click **Save**, choose the position to save the download file, then click **Save** again. The user list settings will be saved in IAR-5000. (Figure 4-14)

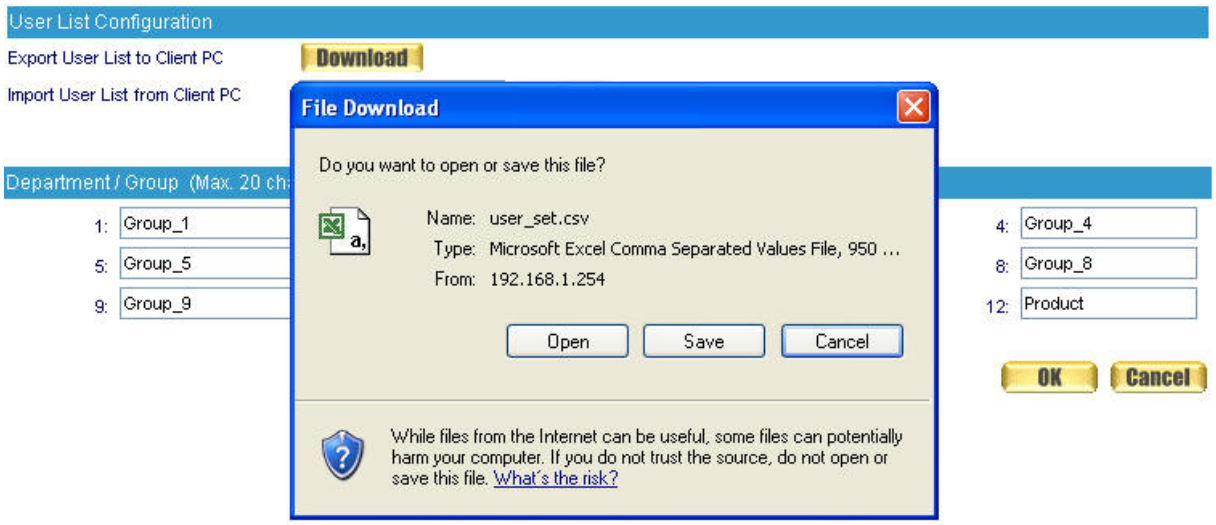


Figure 4-14 Select the position to save the download file

Step3. Use excel to open the user list configuration settings (user_set.csv), and enter the settings to modify.

The way to use the user list：（the contents of user_set.csv）

##					
#Format:					
# ~1	Group_1				
⋮					
##					
Department / Group :					
~1	Internal_Sales				
~2	ales				
⋮					
User List :					
192.168.139.0	255.255.255.0	1			
192.168.139.30	Mail_Server	*	0	00:0C:76:B7:96:3B	11
192.168.139.216	Jacky	Product	3	00:12:0E:2E:CF:DA	10
172.19.0.0	255.255.0.0	9			
172.19.100.10	Hanson	Product	3	00:E0:18:25:F4:BC	9
172.19.100.11	Hans	*	3	00:02:44:8E:B7:C7	9
⋮					

How to use the User List?

The setting of Department / Group：
The User List can set 36 Department / Group

The name of Department / Group

The number of Department / Group

The first subnet

The first range of the subnet

The first default subnet Group

The first subnet information

PC Name

User Name

User's IP

User's Department/Group

User 's MAC

Logged / Ignored Name List

The User's first subnet information

User List

Step4. Change the information of **Department / Group.** (Figure 4-15)

- Change the **8th Department / Group** information, and the original **Customer_Service** will change into **Support.**
- Add the **12th Department /Group** information, and change **Group_12** into **R.D._2**.

Department / Group :	
~1	Internal_Sales
~2	Asian_Sales
~3	European_Sales
~4	American_Sales
~5	Bursary
~6	Human_Resouces
~7	Marketing
~8	Customer_Service
~9	R.D.
~10	Laboratory
~11	Device_Room
~12	Group_12
~13	Group_13

Department / Group :	
~1	Internal_Sales
~2	Asian_Sales
~3	European_Sales
~4	American_Sales
~5	Bursary
~6	Human_Resouces
~7	Marketing
~8	Support
~9	R.D.
~10	Laboratory
~11	Device_Room
~12	R.D._2
~13	Group_13

Figure4 -15 Change the Department / Group information from excel

Step5. To add and modify the user information in the first subnet. (Figure 4-16)

- Change **192.168.1.2**（**Jacky**）**Department / Group** information, and change the **1th Department / Group** into **9th Department / Group.**
- Insert a row under the user list in the first subnet, and enter the new user information in the row.（User IP , User Name, PC Name, Logged / Ignored User List, User MAC, User Department / Group）

User List :						
192.168.1.0	255.255.25	1				
192.168.1.2	Jacky	WRITTER	3	00:D0:59:	1	*
192.168.1.100	*	OCT1005	3	00:0D:88:	1	*
192.168.1.101	Jacky_NB	JACKY-M	3	00:16:36:6		
192.168.1.1	Gateway	---	1	00:17:9A:	11	*

User List :						
192.168.1.0	255.255.25	1				
192.168.1.2	Jacky	WRITTER	3	00:D0:59:	9	*
192.168.1.100	*	OCT1005	3	00:0D:88:	1	*
192.168.1.101	Jacky_NB	JACKY-M	3	00:16:36:6	12	*
192.168.1.1	Gateway	---	1	00:17:9A:	11	*
192.168.1.10	John	PM	6	00:15:5A:	6	*

Figure 4-16 To add or modify the user's first subnet information from the excel

In the Logged / Ignored user information, the **" 0"** number represents **Ignored**, the " 3 " number represents **Logged**.

The **" * "** symbol represents no information in the excel tablet.

Step6. Add the third subnet and user's information. (Figure 4-17)

- Please enter the third subnet basic information under the second subnet user list . （the range of IP, Netmask, and Default Group）.
- Please enter the basic user information under the third subnet.（User IP, User Name, PC Name, Logged / Ignored List, User MAC, User Department / Group）.

192.168.1.1	Gateway	---	1	00:17:9A:3	11
192.168.1.1	John	PM	6	00:15:5A:3	6
172.16.0.0	255.255.25	1			
172.16.0.1	James	*	3	00:18:66:4	7
172.16.0.2	Josh	*	3	00:011:82:	7
172.16.0.3	Marc	Product	3	00:10:72:1	7

Figure 4-17 Add the user's information in the third subnet by excel

There must be one blank row to divide the user list in two subnets.

Step7. Save File（user_set.csv）

Step8. In **User List → Setting**, Click **User List Configuration → Import User List from Client PC →** Browse.

Step9. In the **Choose File** window, select the modified user list setting, then Click Open.

Step10. Click the lower right **OK**, the user list setting files will import into IAR-5000.

Chapter 5 IM Management

IM Management included 3 main parts:

Configure（Login Notice）：

MIS engineer can customize the contents of IM login notice and IAR-5000 can also send the IM login notice to user while he / she use the IM software.

Authentication：

MIS engineer can request user to pass the IM authentication first or IAR-5000 will block the user's IM connection.

Rule：

Default Rule: Can set the default rule of MSN, Yahoo, ICQ and QQ.

Account Rule: Can set different rules for every IM account.

5.1 Configure

MIS engineer can customize the contents of IM login notice and IAR-5000 can also send the IM login notice to user while he / she use the IM software.

Step1. Select which IM notification to be enabled

Step2. In **sender column**, enter the sender name.

Step3. Fill in the notice content and click **OK**. (Figure 5-1)

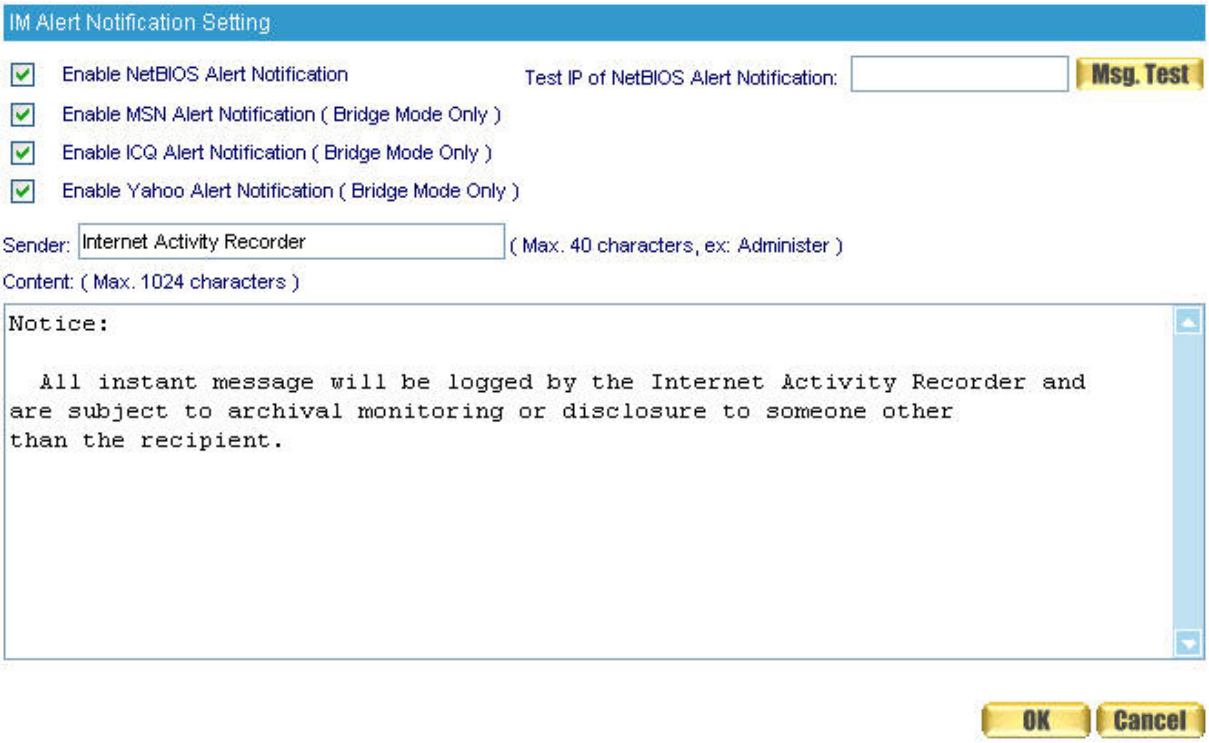


Figure 5-1 IM login notice setting

- **NetBIOS Alert Notification**：

  IAR-5000 will notice user by NetBIOS notification about he processed the IM messages or activities after login to IM software.

- **MSN Alert Notification**：

  IAR-5000 will notice user by msn notification about he processed MSN messages or activities after login to MSN. (**Only available in bridge mode**)

- **ICQ Alert Notification**：

  IAR-5000 will notice the user by ICQ notification about he processed ICQ messages or activities after login to ICQ. (**Only available in bridge mode**)

- **Yahoo Alert Notification**：

  IAR-5000 will notice the user by Yahoo notification about he processed Yahoo messengers or activities after login to Yahoo messenger. (**Only available in bridge mode**)

5.2 Authentication

MIS engineer can request user to pass the IM authentication first or IAR-5000 will block the user's IM connection. And the user does not need to do any authentication once he/she had passed the IM authentication.

Authentication Messages

- MIS engineer can customize the authentication messages. (Figure 5-2) And user will see the authenticaiton messages while he/she login the authenticaiton screen. (Figure 5-3)

User

- It's the built-in mechanism of user authentication.

RADIUS, Remote Authentication Dial-In User Service

- It's kind of remote authentication service of dial-in user.

POP3, Post Office Protocol

- It's the protocol used for receiving e-mails.

LDAP, Lightweight Directory Access Protocol

- It's a kind of directory access Protocol which combined the authentication mechanism of SMTP, POP3, FTP, HTTP and RADIUS etc.

Shared Secret

- The needed authentiction password which is used for IAR-5000 and RADIUS server to process the authentication.

802.1x RADIUS

- 802.1 x RADIUS is used for IAR-5000 to do the authentication process to RADIUS server which contained the wireless network mechanism.

Search Distinguished Name

- It's the identified name of LDAP server.

LDAP Filter

- MIS engineer can assign the specific account of LDAP server.

User Distinguished Name

- It's the needed account used for IAR-5000 to process the authetication to LDAP server.

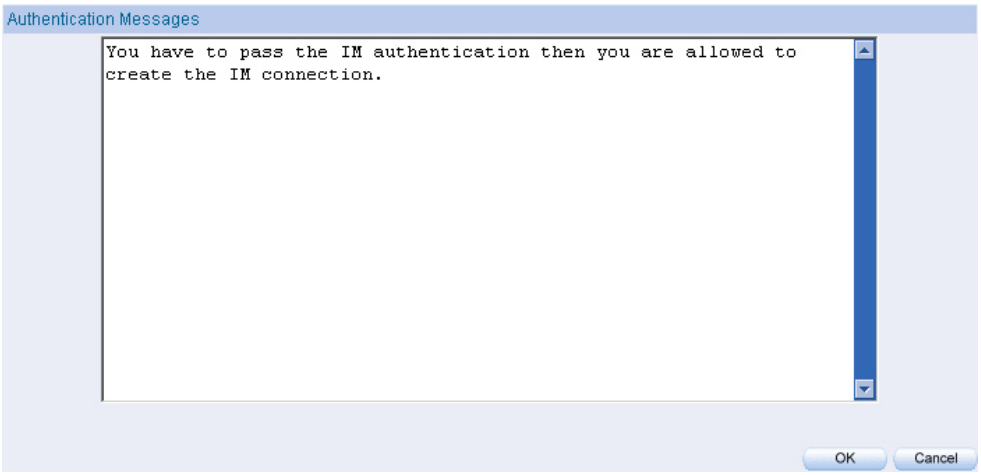


Figure 5-2 Authentication message setting

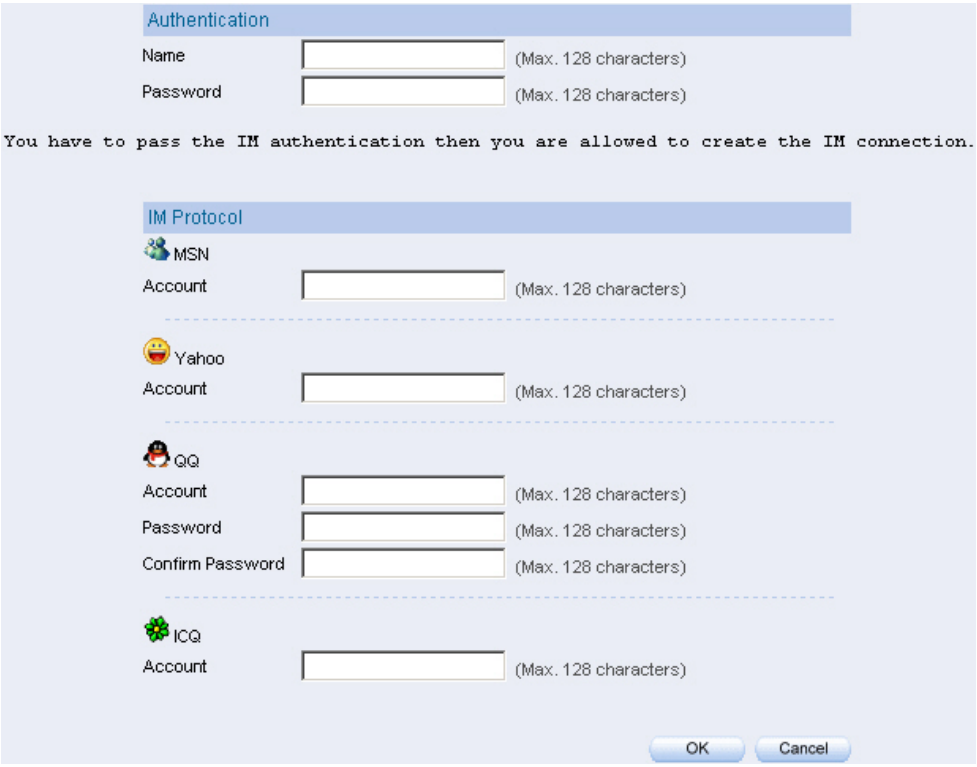


Figure 5-3 User login authentication

How To Use …..

- The Authentication function is only available in Bridge mode. If MIS engineer use Sniffer mode to deploy IAR-5000, then appliance can not block the IM connection and MIS engineer also can not manage the internal user to use IM software. In other words, IAR-5000 can only record the user's IM conversation contents while using Sniffer mode.
- If user's IM account passed the authentication, then there is no more action of IM authentication.
- The Authentication function must apply to Rule function. For exapmle, if MIS engineer want to make rule setting of MSN.

  - MIS engineer select **Rule → MSN → Accept; Always**. It means user can use MSN without passing authentication.

  - MSN MIS engineer select **Rule → MSN → Authentication passed.** That means the user's MSN account need to passed authentication or it will be dropped. (Figure 5-4)

Figure 5-4 User can not login MSN

- MIS engineer can set one authentication accout instead of group of IM accounts to process the IM authentication.
- IAR-5000 provides four built-in authentication mode and also support to RADIUS, POP3 and LDAP server authentication.
- How to log in authentication interface?
  - Open the browser, and then type "http://IAR-5000 interface/auth". For example, http://192.168.1.1/auth

Internal user must pass the IM authentication then he/she is allowed to create MSN connection. (Use the built-in user authentication)

Step1. Add authentication user in **Authentication → User.** (Figure 5-5)

Authentication-User Name	Configure
joy	Modify Remove
john	Modify Remove
jack	Modify Remove

New Entry

Figure 5-5 Set the authentication user

Step2. Select **IM Management → Rule → Default Rule → Accept : Authentication passed and MSN Message not encrypted.** (Figure 5-6). Click **OK**.

Default Setting of IM Rule (Bridge Mode Only)

MSN

- Accept : MSN Message not encrypted
- Drop : MSN Message encrypted
- Accept : Authentication passed and MSN Message not encrypted
- Drop : Authentication failed or MSN Message encrypted
- Accept : Authentication passed
- Drop : Authentication failed
- Accept : Always
- Drop : Always

Figure 5-6 Default IM rule setting

Step3. If the internal user wants to use MSN, then he/she must apply the use privilege of MSN from IM authentication management interface. The management interface is：”http:// IAR-5000 interface/auth”, default setting is http://192.168.1.1/auth：

- Enter the Name and Password.
- Enter the MSN account. (Figure 5-7)
- Click OK. (Figure 5-8)

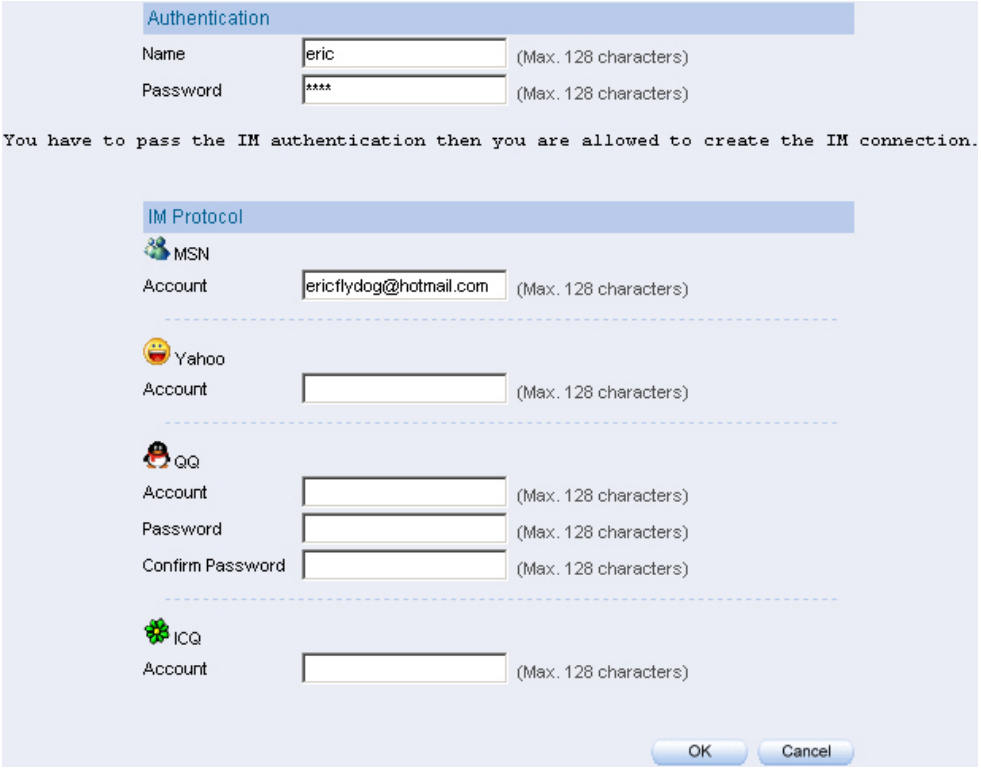


Figure 5-7 Authentication setting

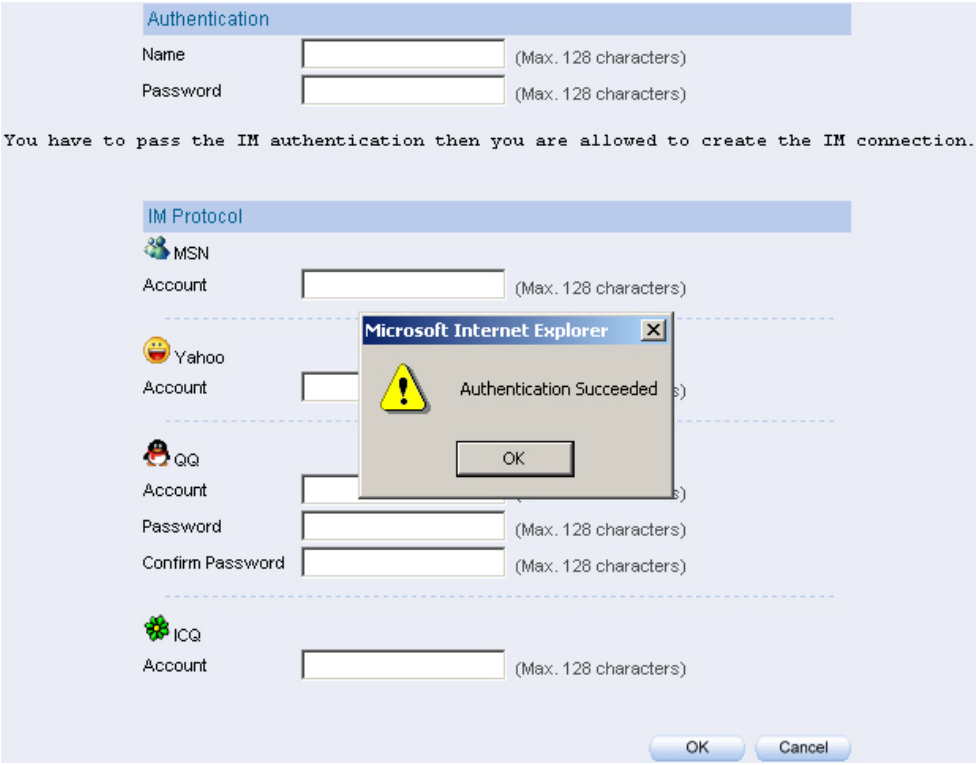


Figure 5-8 Authentication success

Step4. User can use the authenticated MSN account and there is no more authentications to process in the future.

Internal user must pass the IM authentication then he/she is allowed to create Yahoo connection. Use external RADIUS Server authentication. (Windows 2003 built-in authentication)

Deployment of Windows 2003 RADIUS Server

Step1. **Click Start → Control Panel → Add / Remove Programs**, select **Add / Remove Windows Components**, then it shows the **Windows Components Wizard.**

Step2. Select **Networking Services**, then click **Details**. (Figure 5-9)

Figure 5-9 Windows components wizard

Step3. Select **Internet Authentication Service.** (Figure 5-10)

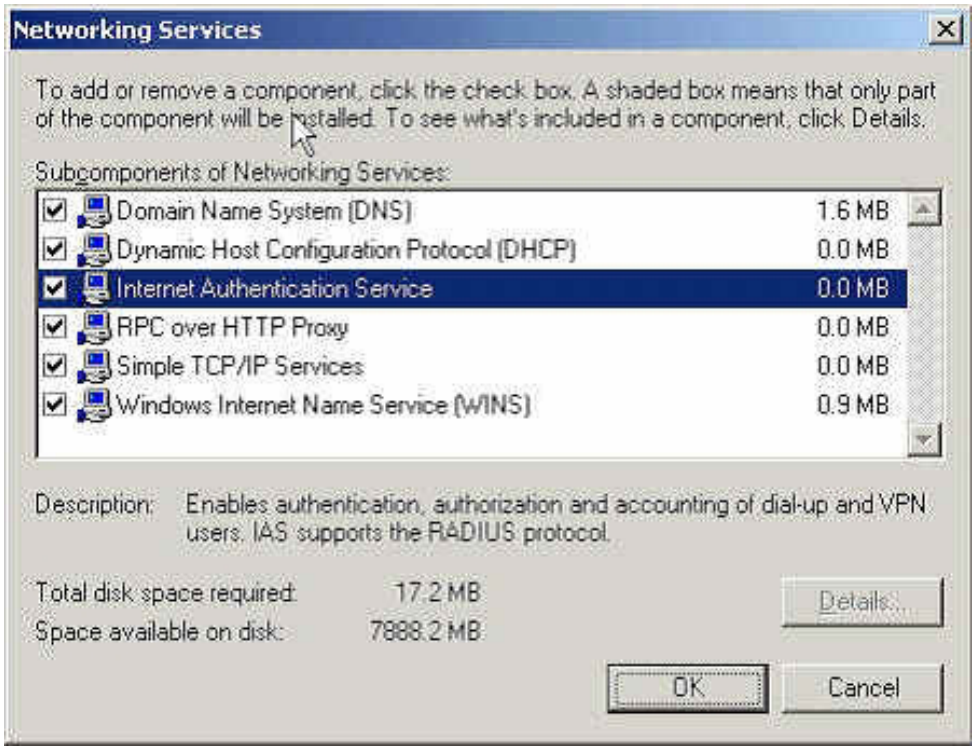


Figure 5-10 Add new network authentication service components

Step4. Click **Start → Control Panel → Administrative Tools**, select **Network Authentication Service.** (Figure 5-1)

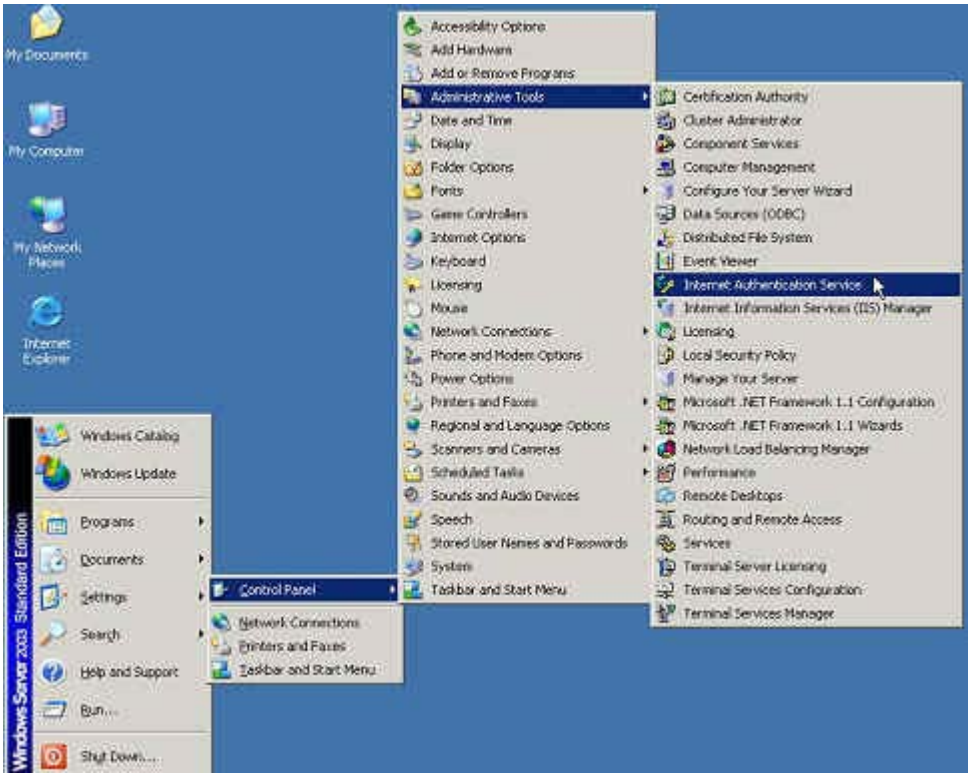


Figure 5-11 Select network authentication service

Step5. Right click **RADIUS Clients → New RADIUS Client.** (Figure 5-12)

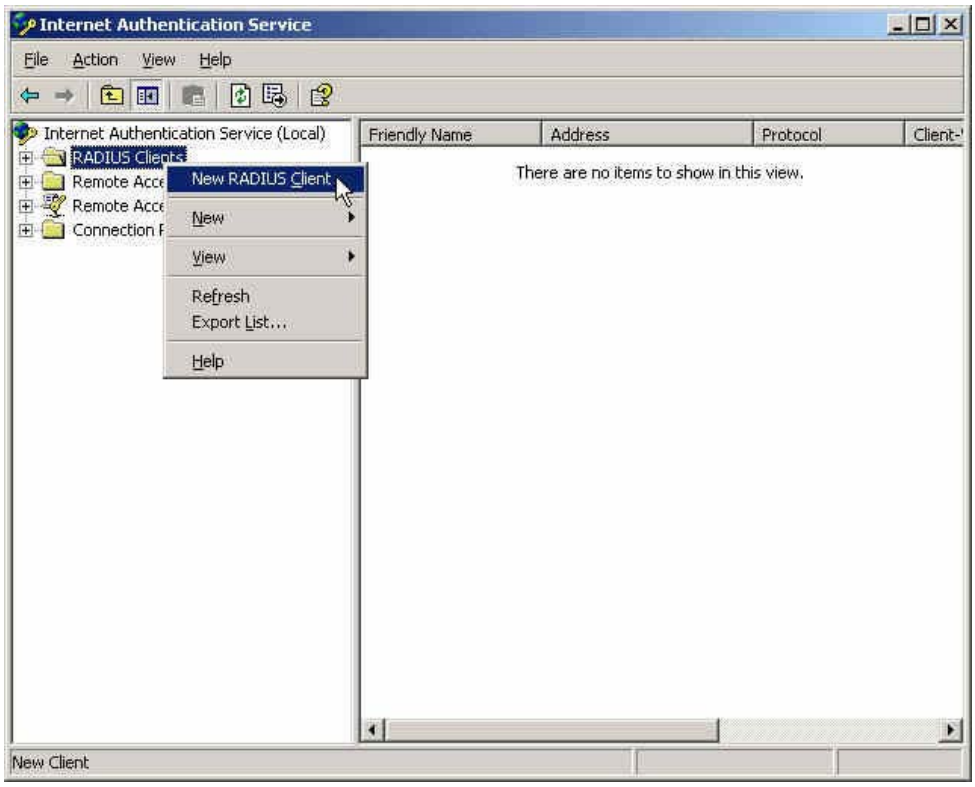


Figure 5-12 Add new RADIUS client

Step6. Enter the **Name and Client Address** (It is the same as IAR-5000 IP Address). (Figure 5-13)

Figure 5-13 Add New RADIUS client name and IP address setting

Step7. Select **RADISU Standard**, enter the Shared secret and Confirm Shared secret. (It must be the same setting as RADIUS in IAR-5000). (Figure 5-14)

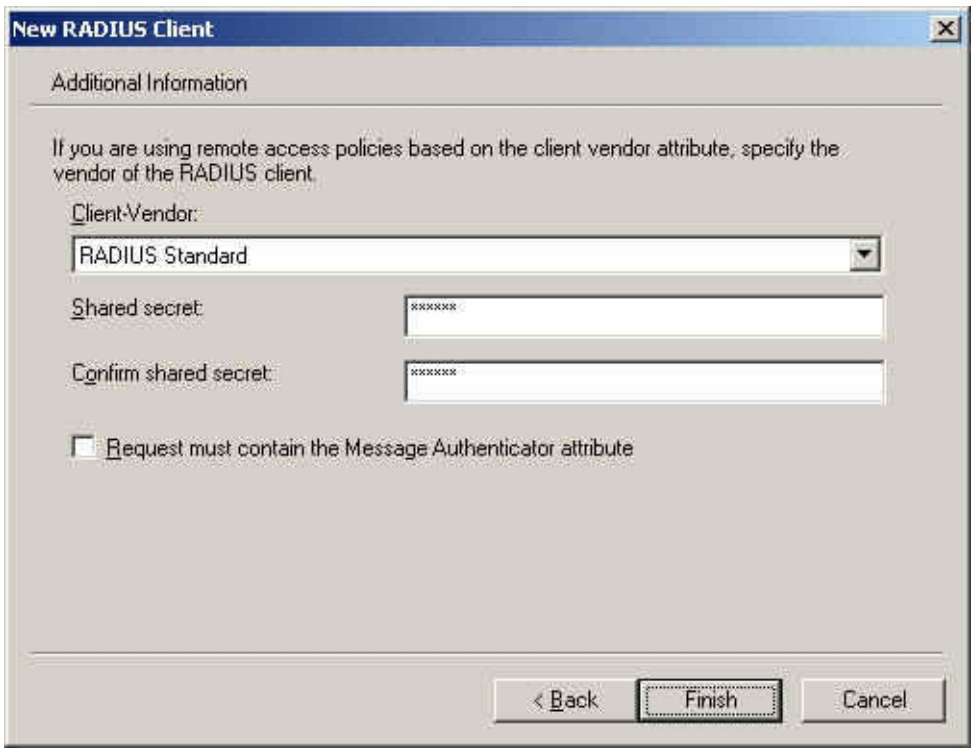


Figure 5-14 Add new RADIUS client-vendor and shared secret

Step8. Right click on **Remote Access Policies→ New Remote Access Policy** (Figure 5-15)

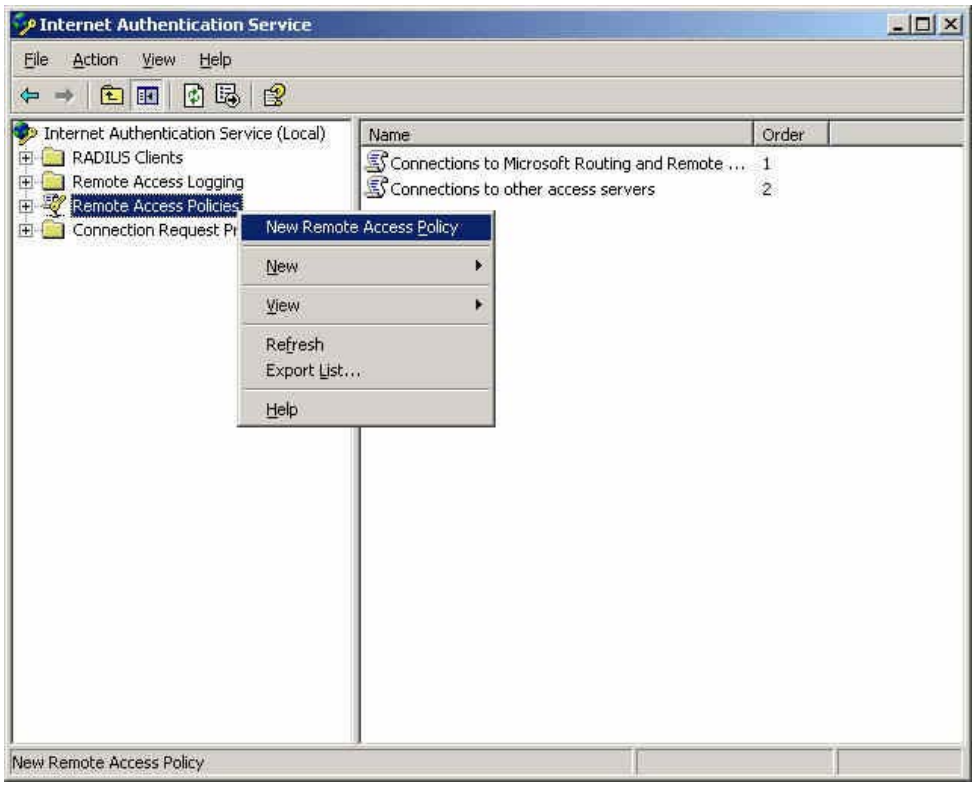


Figure 5-15 Add new remote access policies

Step9. Select **Use the wizard to set up a typical policy for a common scenario**, and enter the **Policy name.** (Figure 5-16)

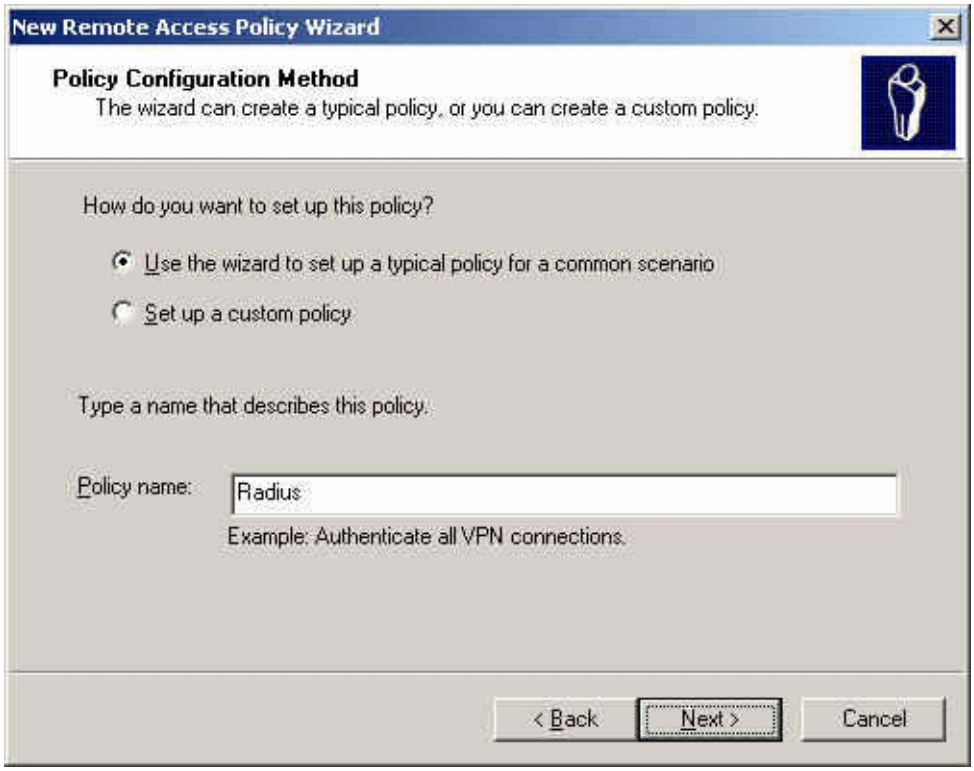


Figure 5-16 Add new remote access policies and policy name

Step10. Select **Ethernet**. (Figure 5-17)

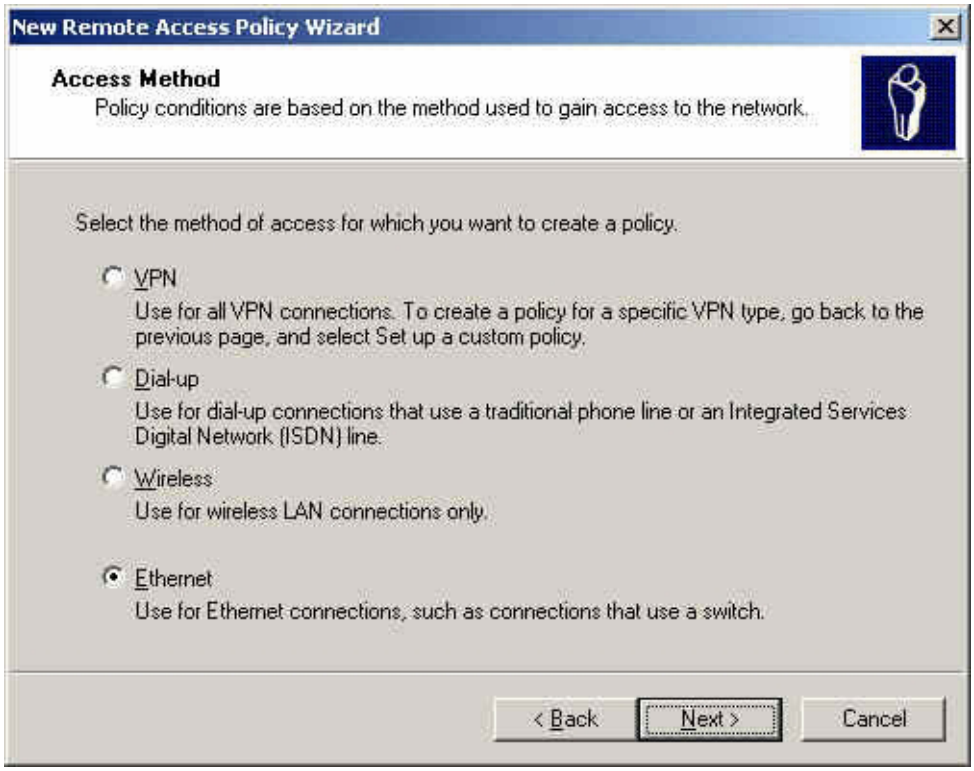


Figure 5-17 The way to add new remote access policy

Step11. Select **User.** (Figure 5-18)

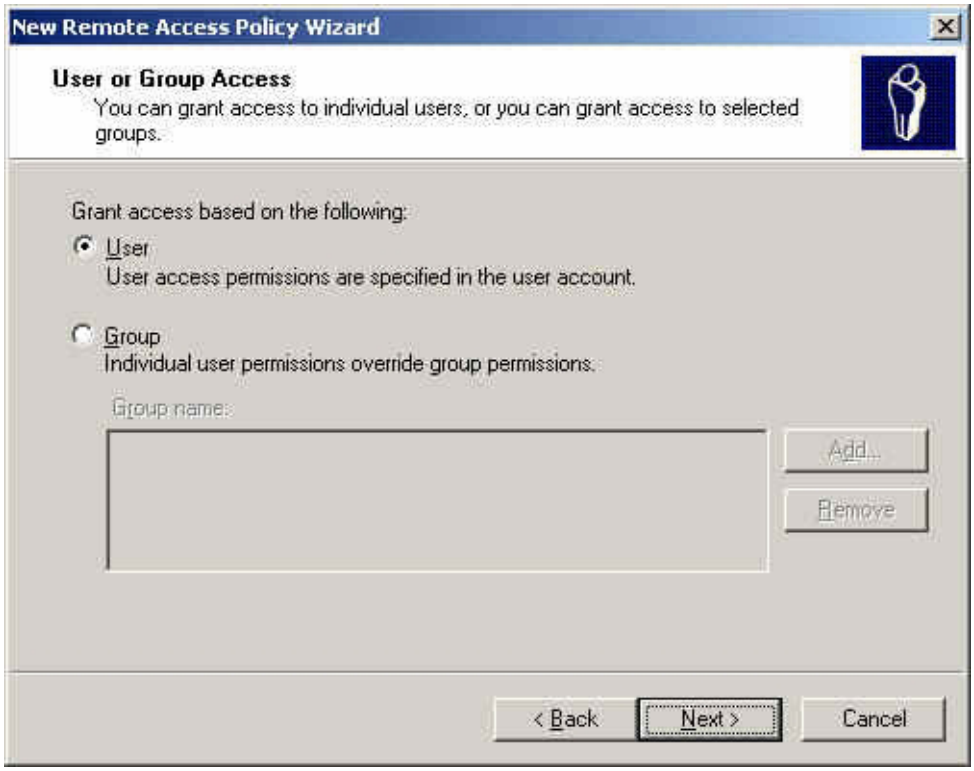


Figure 5-18 Add new remote access policy user and group

Step12. Select **MD5-Challenge**. (Figure 5-19)

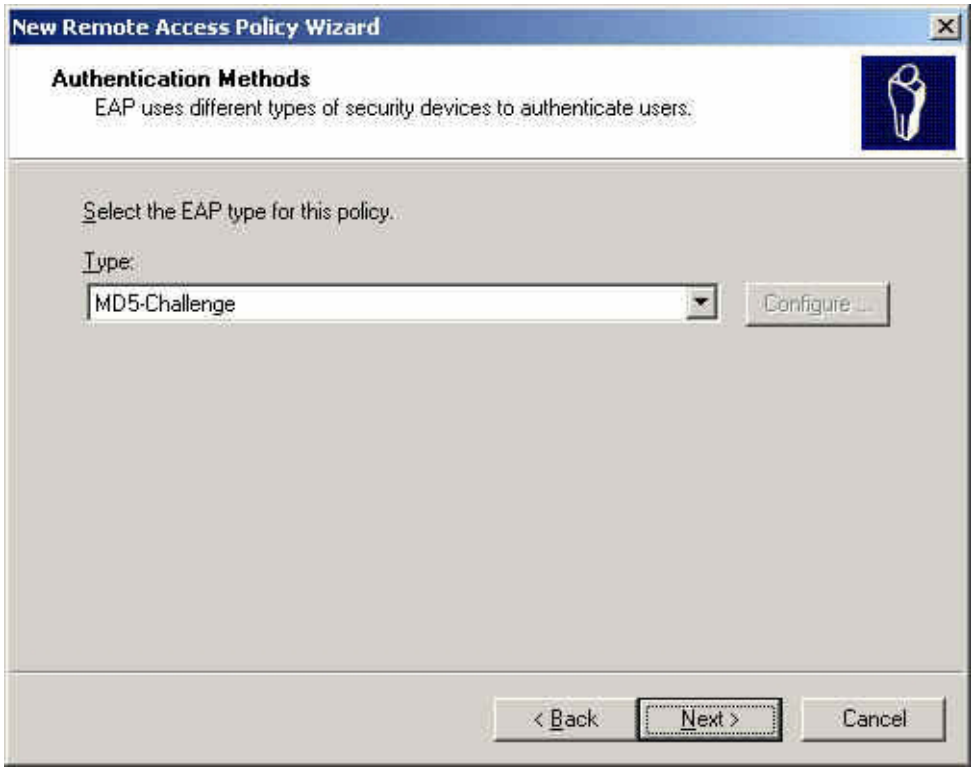


Figure 5-19 The authentication of add new remote access policy

Step13. Right click on the **Radius → Properties** (Figure 5-20)

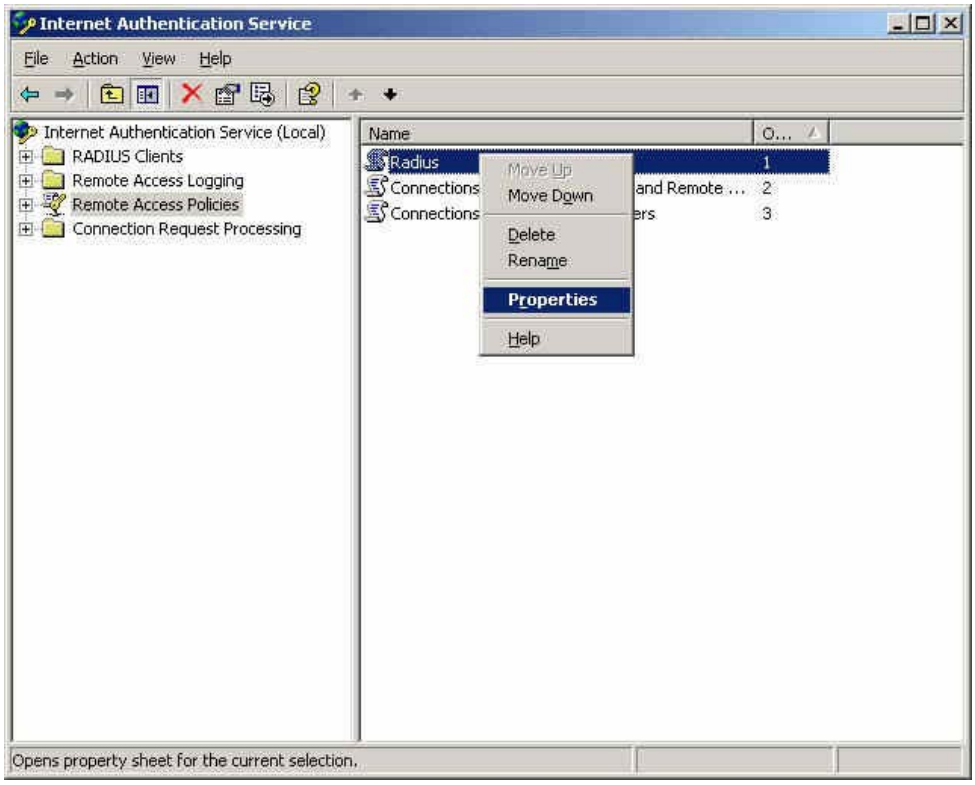


Figure 5-20 The network authentication service setting

Step14. Select **Grant remote access permission**, and **Remove** the original setting, then click **Add**. (Figure 5-21)

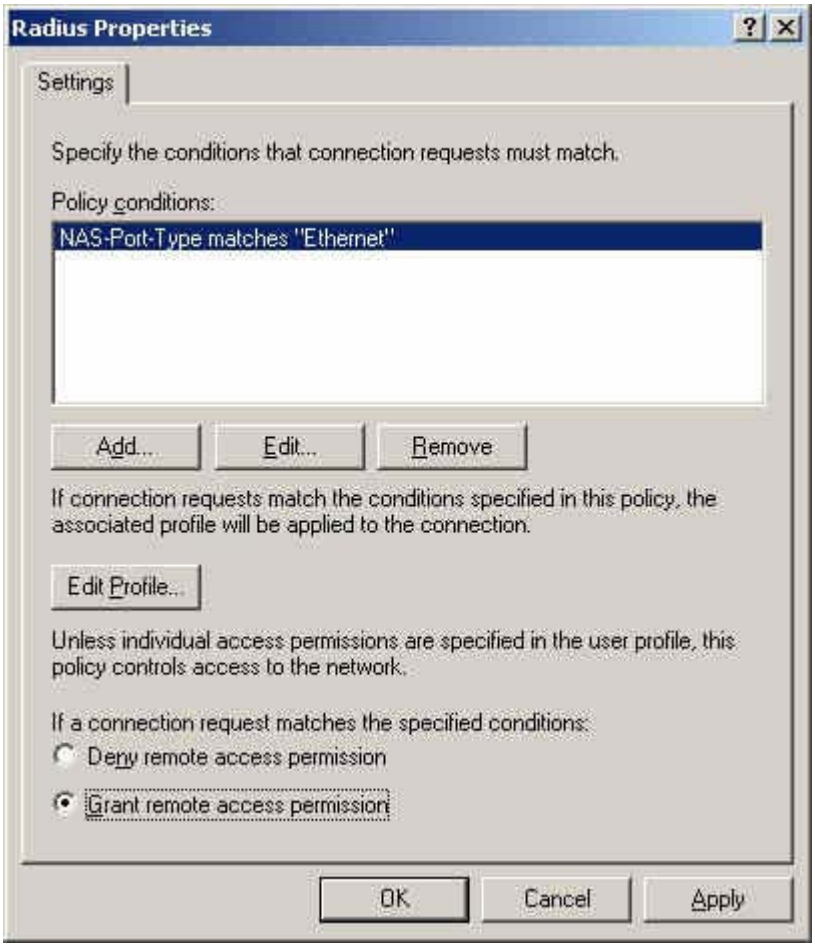


Figure 5-21 The RADIUS properties settings

Step15. **Add Service-Type**. (Figure 5-22)

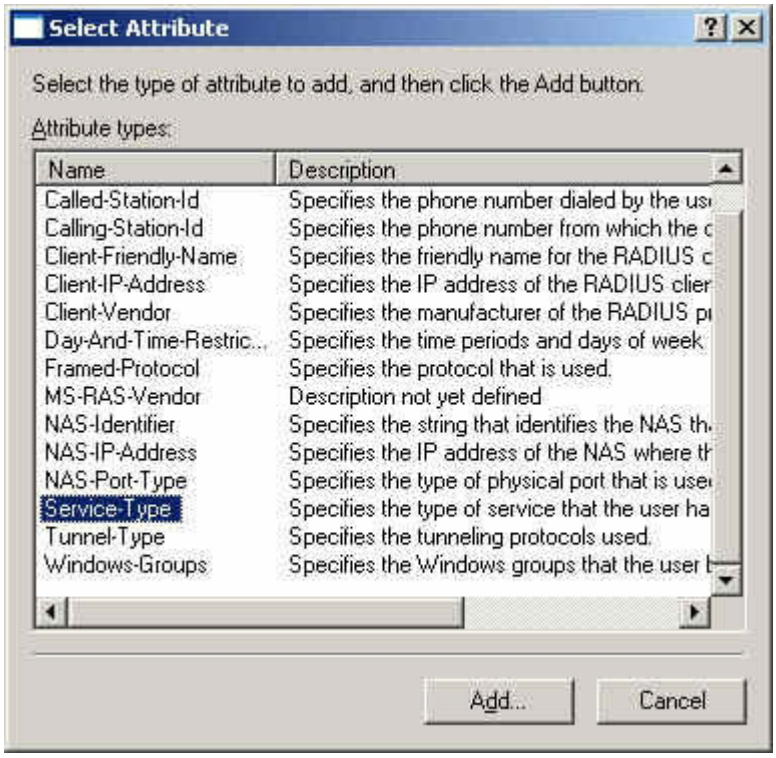


Figure 5-22 Add new RADIUS properties attribute

Step16. **Add Authenticate Only** from the left side. (Figure 5-23)

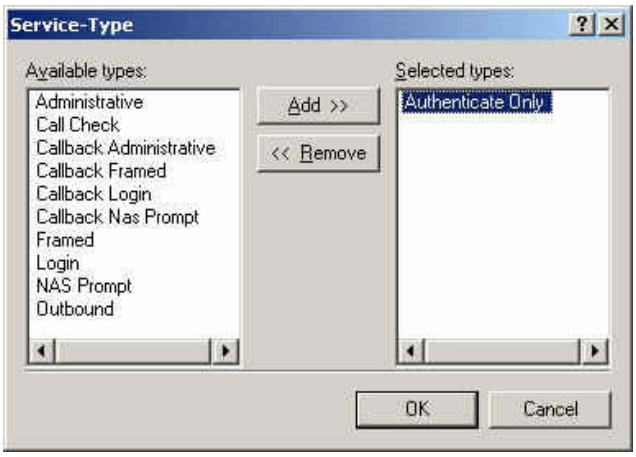


Figure 5-23 Add RADIUS properties service-type

Step17. Click **Edit Profile,** select **Authentication**, and check **Unencrypted authentication (PAP, SPAP)**. (Figure 5-24)

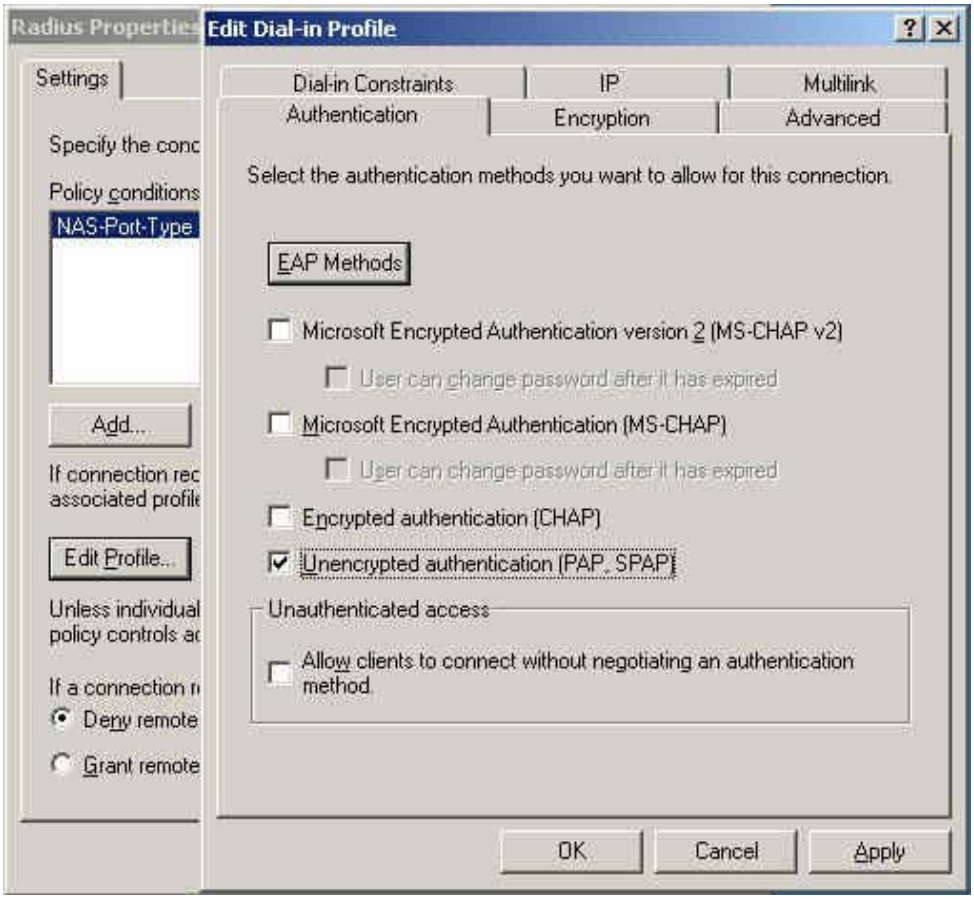


Figure 5-24 Edit RADIUS service-type dial-in property

Step18. **Add Auth User**, click **Start → Setting → Control Panel → Administrative Tools**, select **Computer Management.** (Figure 5-25)

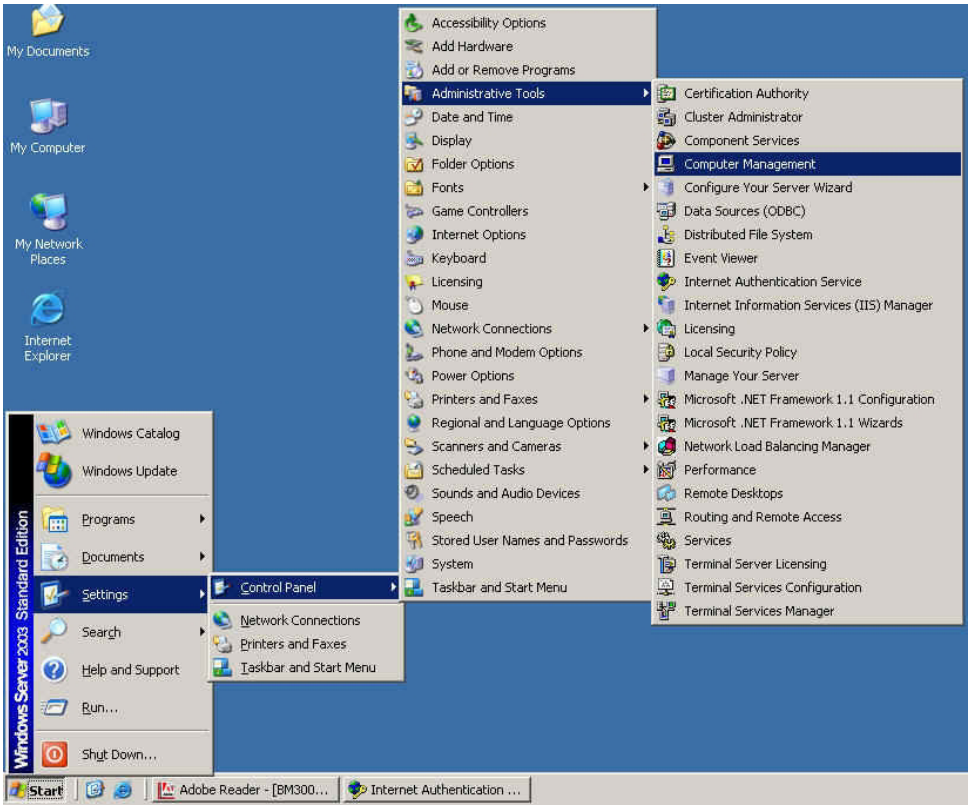


Figure 5-25 Enter computer management

Step19. Right click on **Users**, select **New User**. (Figure 5-26)

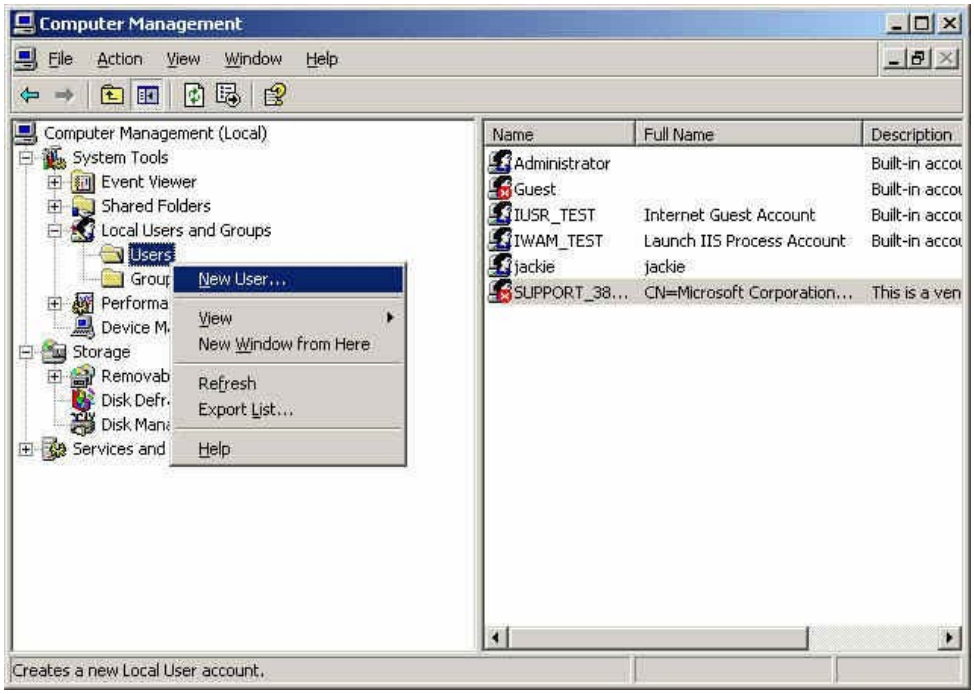


Figure 5-26 Add new user

Step20. Complete the Windows 2003 RADIUS Server settings.

Step21. In **Authentication → RADIUS** function, enter **IP**, **Port** and **Shared Secret**. (The setting must be the same as RADIUS server). (Figure 5-327)

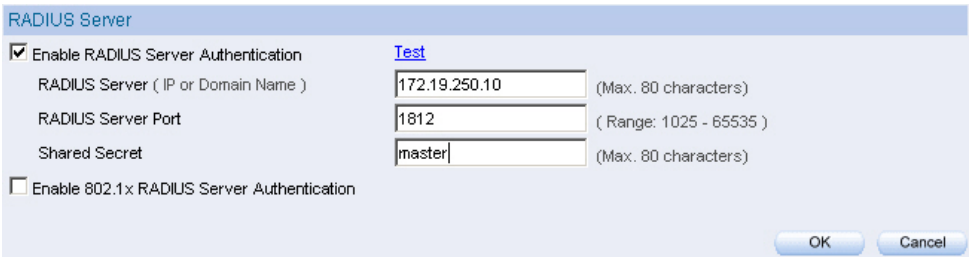


Figure 5-27 The RADIUS server setting

Click **Test**, it can detect if the IAR-5000 and RADIUS server can real working.

Step22. Select **IM Management → Rule → Default Rule → Yahoo → Accept : Authentication passed.** (Figure 5-28)

Figure 5-28 Default IM rule

Step23. If the internal user wants to use MSN, then he/she must apply the user privilege of MSN from IM authentication management interface. The management interface is http://IAR-5000 interface/auth. Default setting is http://192.168.1.1/auth.

- Enter the Name and Password.
- Enter the Yahoo account. (Figure 5-29)

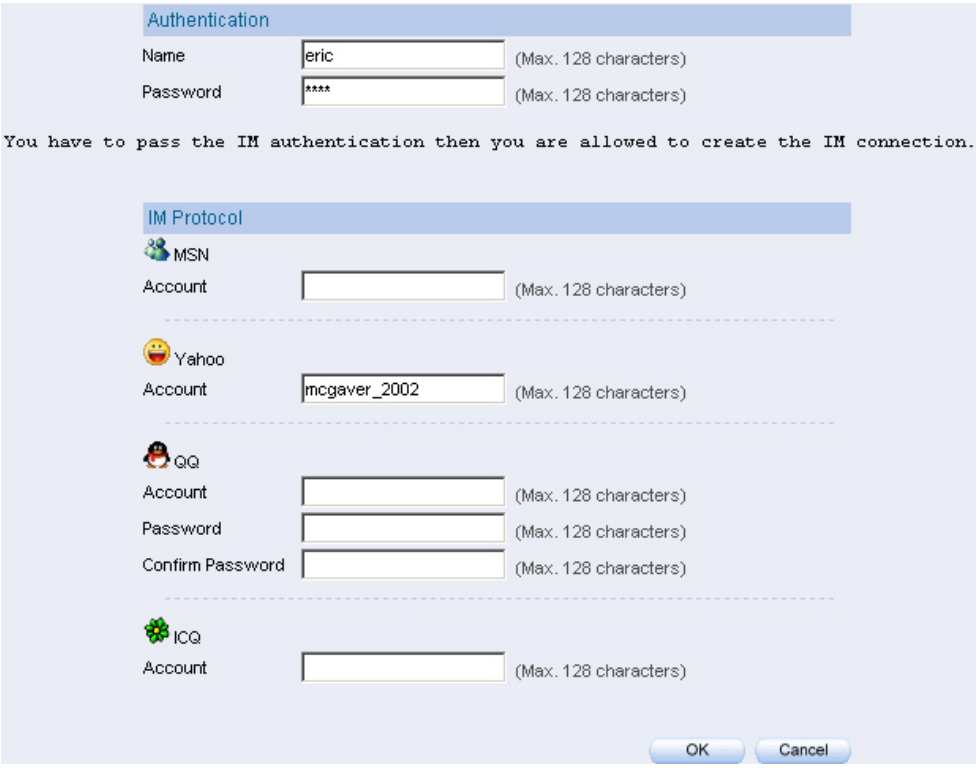


Figure 5-29 Authentication setting

◆ Click **OK.** (Figure 5-30)

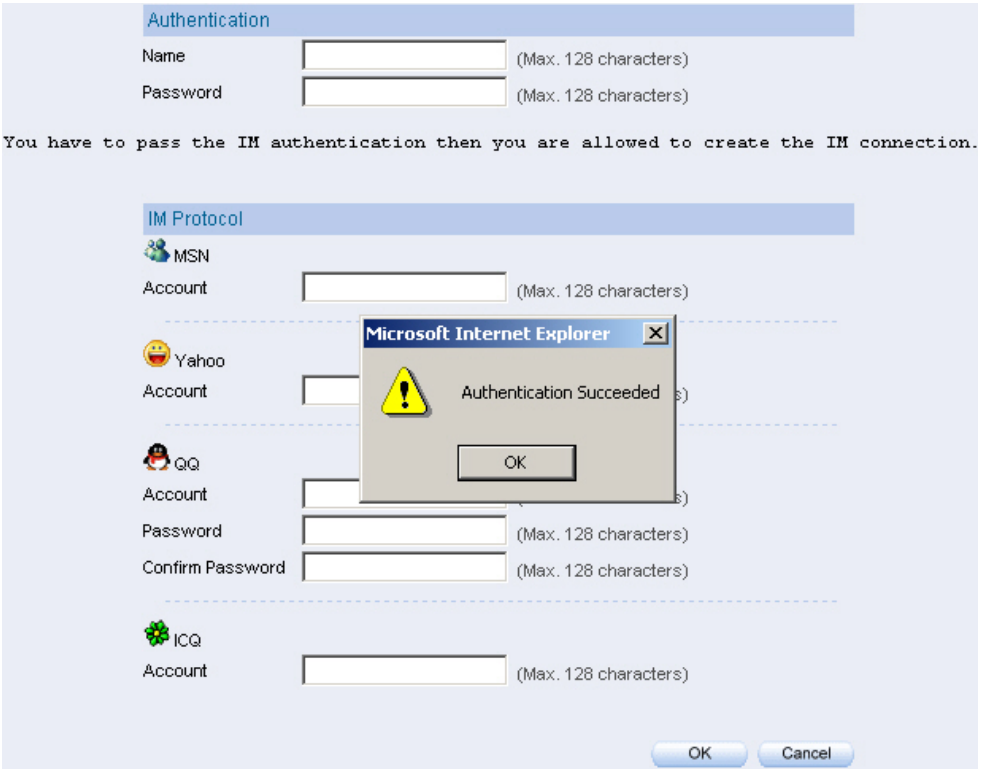


Figure 5-30 Authenticated successful

◆ User can use the authenticated Yahoo account and there is no more authentication to process.

Internal user must pass the IM authentication then he / she is allowed to create QQ connection. (Use external POP3 Server authentication)

Step1. Select **Accept : Authentication passed and QQ Password valid** in **IM Management → Rule → Default Rule → QQ.** (Figure 5-31)

Figure 5-31 Set the QQ default rule

Step2. Enter the POP3 setting in **Authentication → POP3**：(Figure 5-32)

Figure 5-32 POP3 setting

Click Test, to see if IAR-5000 can connect to POP3 Server properly.

Step3. If the internal user wants to use QQ account, then he/she must apply the use privilege of MSN from IM authentication management interface. The management interface is http: //IAR-5000 interface/auth. Default setting is http://192.168.1.1/auth.

- Enter the POP3 Server account name and password. (It is the mail account and password that used for receiving e-mails.)
- Enter QQ account (Figure 5-33)

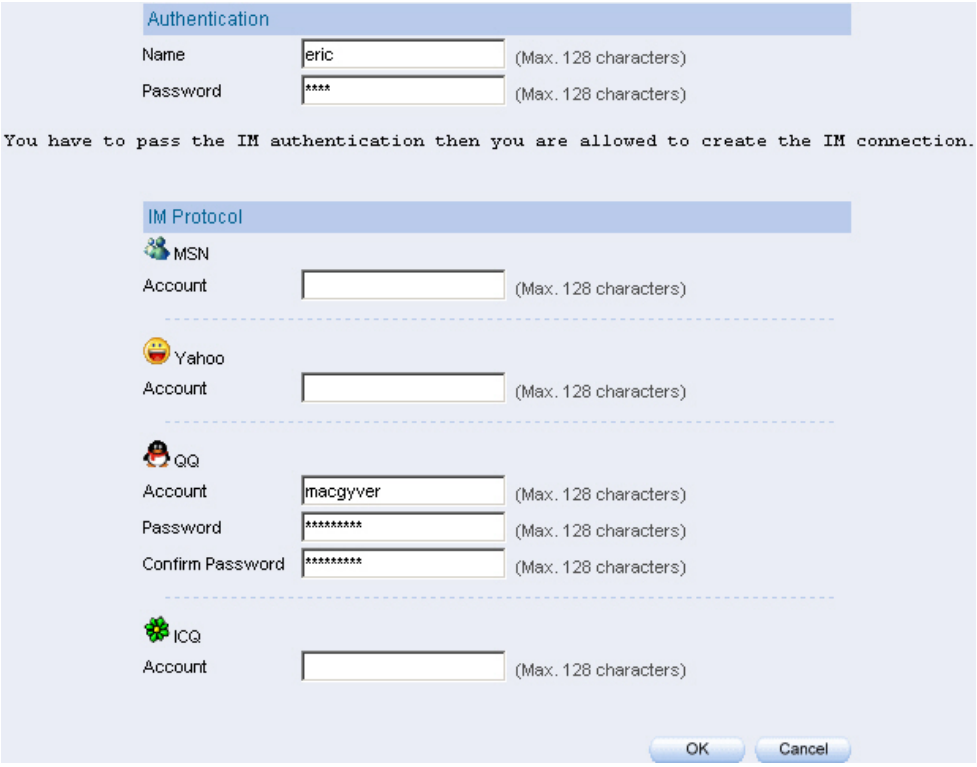


Figure 5-33 Enter the QQ account and password

◆ Click **OK**. (Figure 5-34)

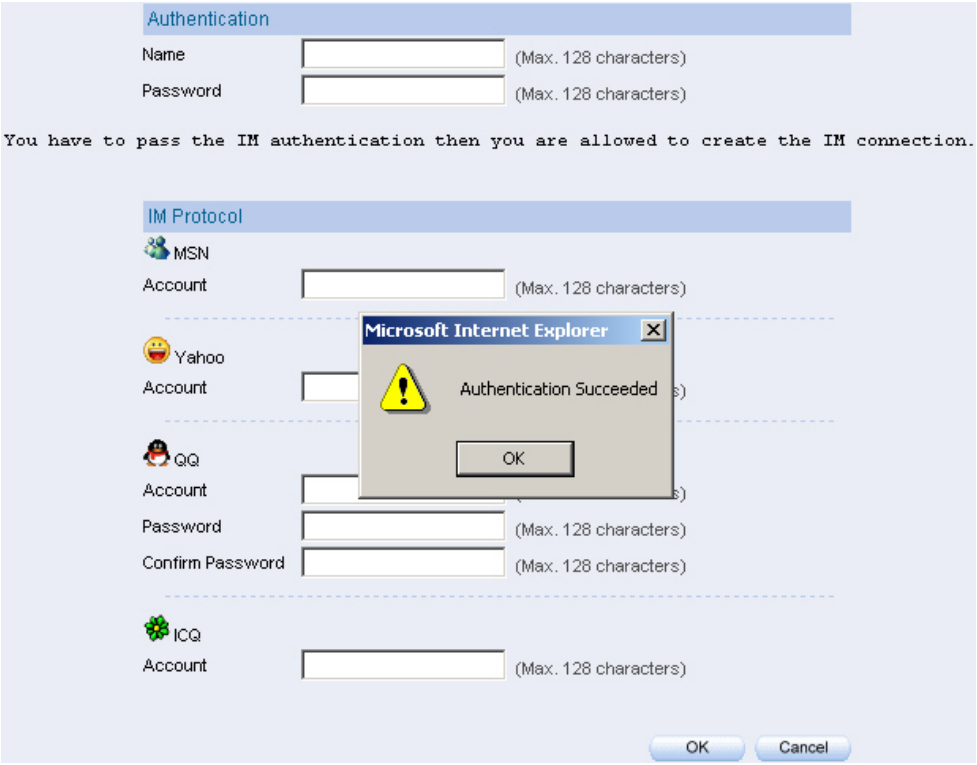


Figure 5-34 QQ account authenticated succeed

Step4. User can use the authenticated QQ account and there is no more authentication to process in the future.

Internal user must pass the IM authentication then he/she is allowed to create ICQ connection. Use external LADP Server authentication. (Windows 2003 Server built-in authentication)

Windows 2003 LDAP Server Deployment

Step1. Click **Start → Program → Administrative Tools → Manage MIS engineer Server.**

Step2. In **Manage MIS engineer Server** window, click **Add or remove a role → Configure MIS engineer Server Wizard**. (Figure 5-35)

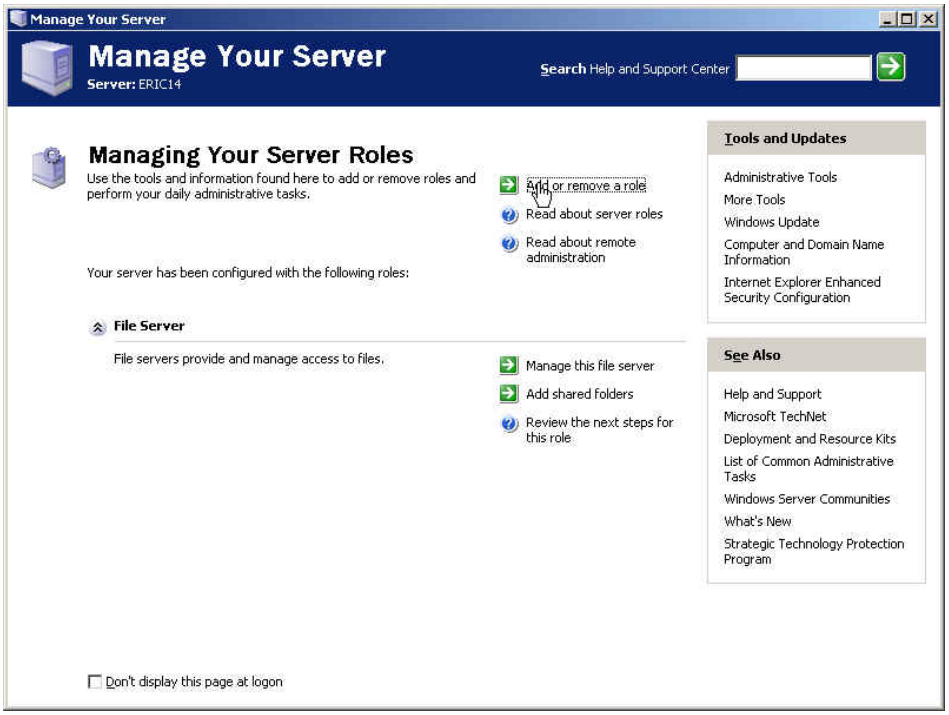


Figure 5-35 Click add or remove a role

Step3. In **Preliminary Steps** window, click **Next.** (Figure 5-36)

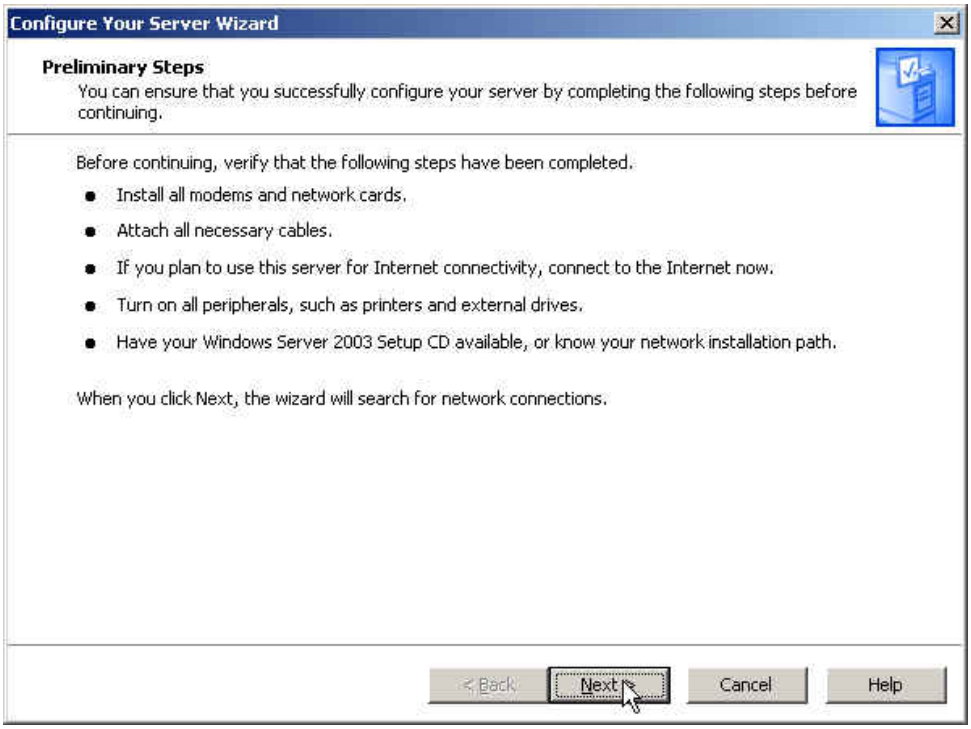


Figure 5-36 The Preliminary steps Web UI

Step4. In **Server Role** window, select **Active Directory** and click **Next**. (Figure 5-37)

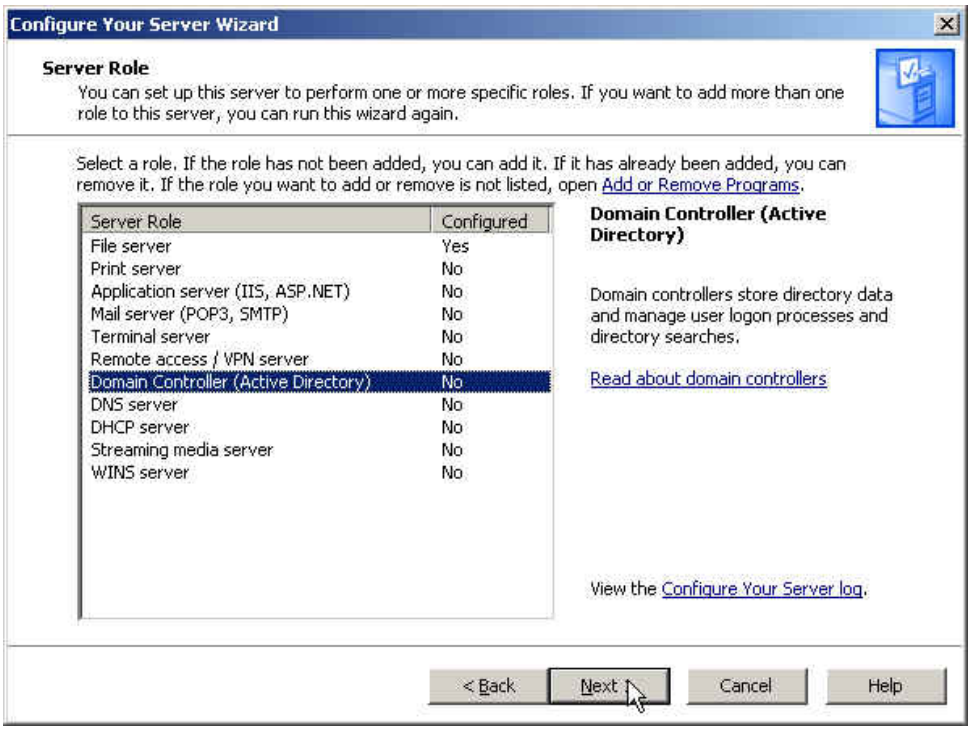


Figure 5-37 The server role window

Step5. In **Summary of Selections** window, click **Next**. (Figure 5-38)

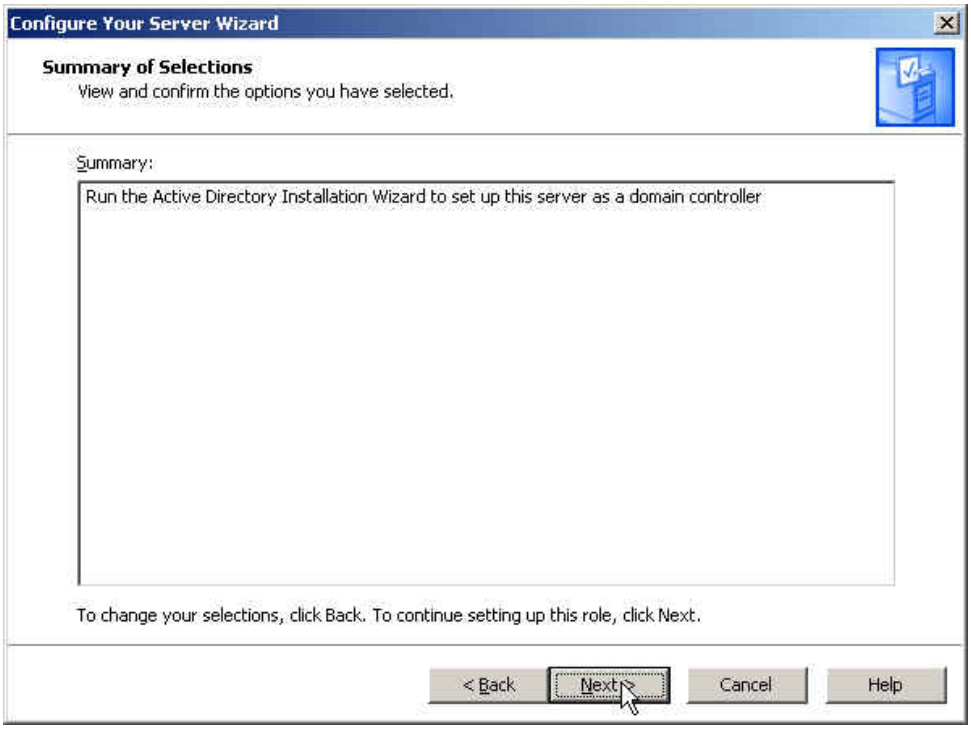


Figure 5-38 The summary of selections window

Step6. In **Active Directory Installation Wizard** window, click **Next**. (Figure 5-39)

Figure 5-39 Active directory installation wizard

Step7. In **Operating System Compatibility** window, click **Next**. (Figure 5-40)

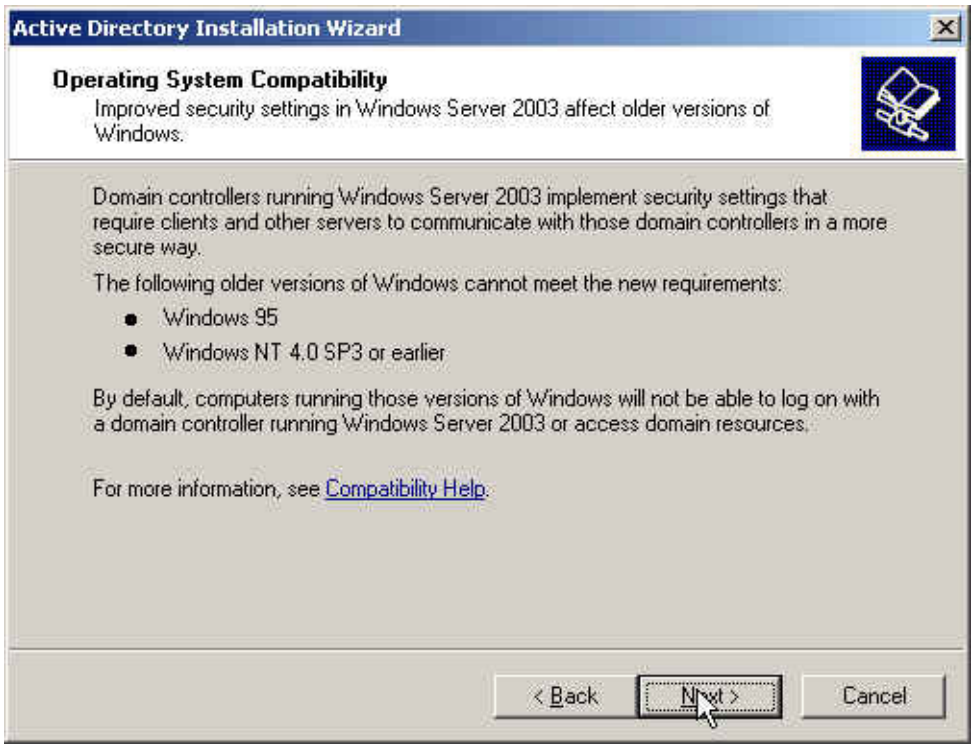


Figure 5-40 The operating system compatibility window

Step8. In **Domain Controller Type** window, select **Domain controller for a new domain**, click **Next**. (Figure 5-41)

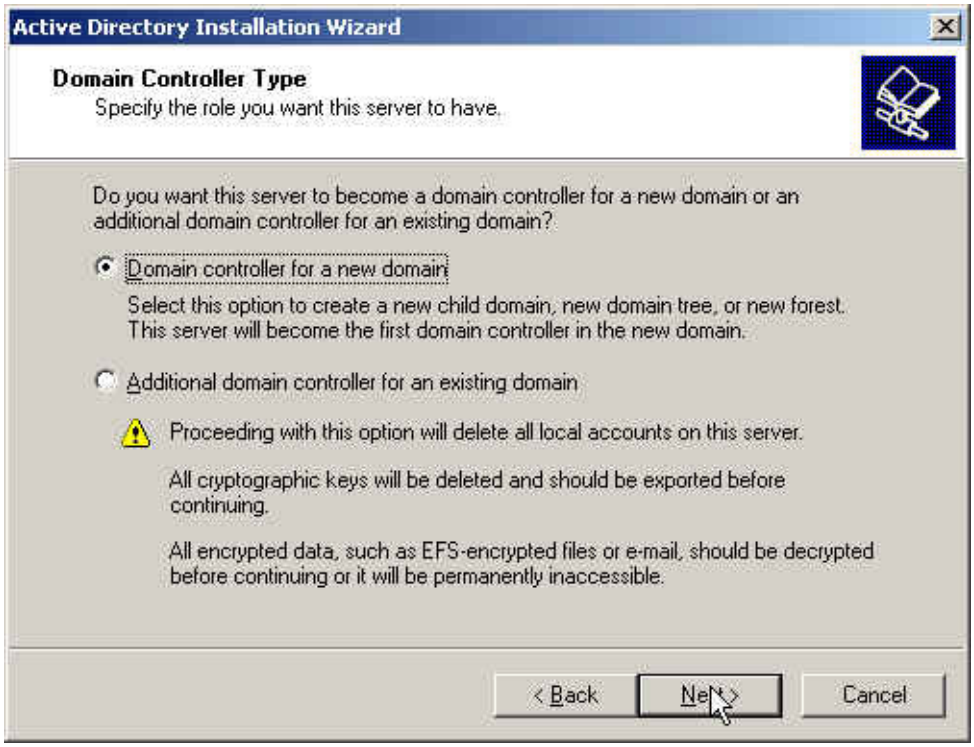


Figure 5-41 The domain controller type window

Step9. In **Create New Domain** window, select **Domain in a new forest**, click **Next**. (Figure 5-42)

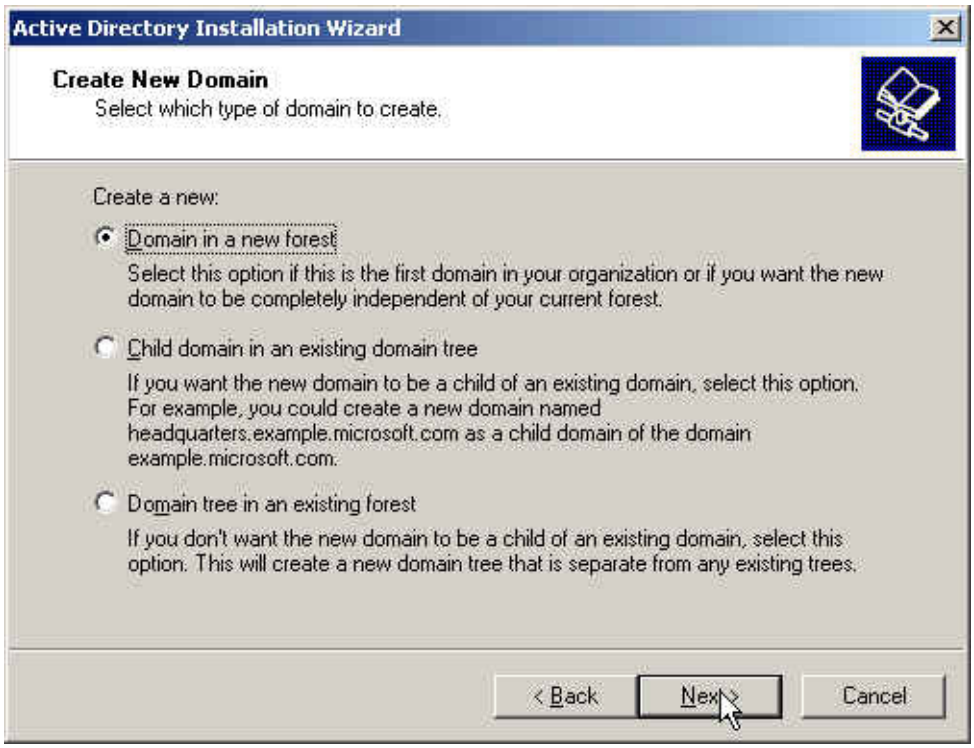


Figure 5-42 Create new domain window

Step10. In **New Domain Name** window, enter the **Full DNS name for new domain**, click **Next.** (Figure 5-43)

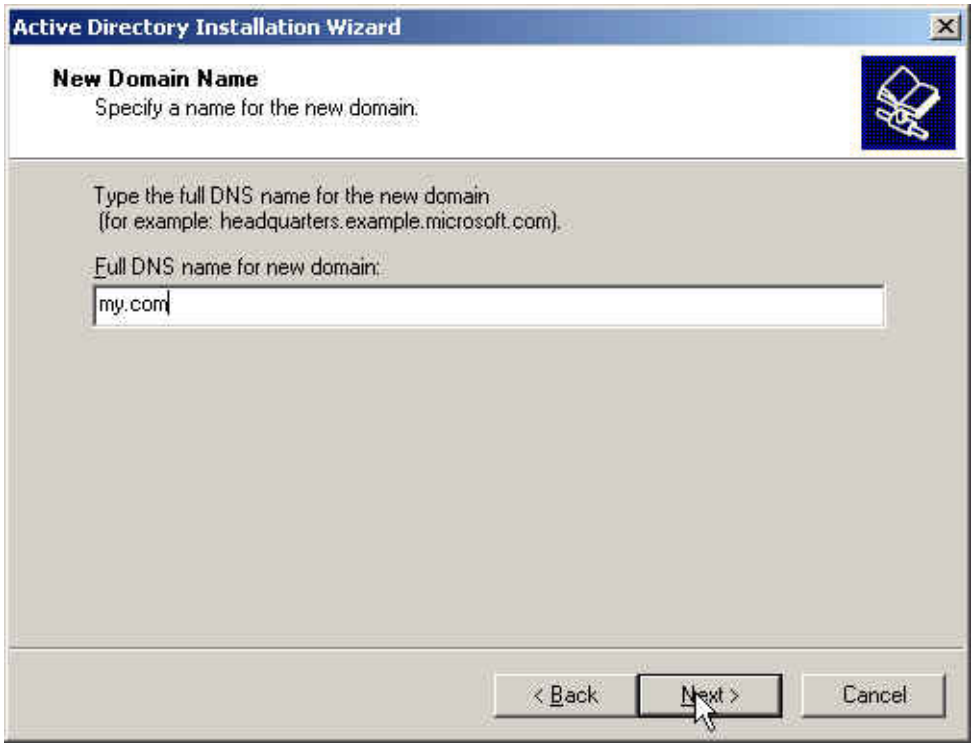


Figure 5-43 The new domain name window

Step11. In **NetBIOS Domain Name** window, enter the **Domain NetBIOS name**, click **Next**. (Figure 5-44)

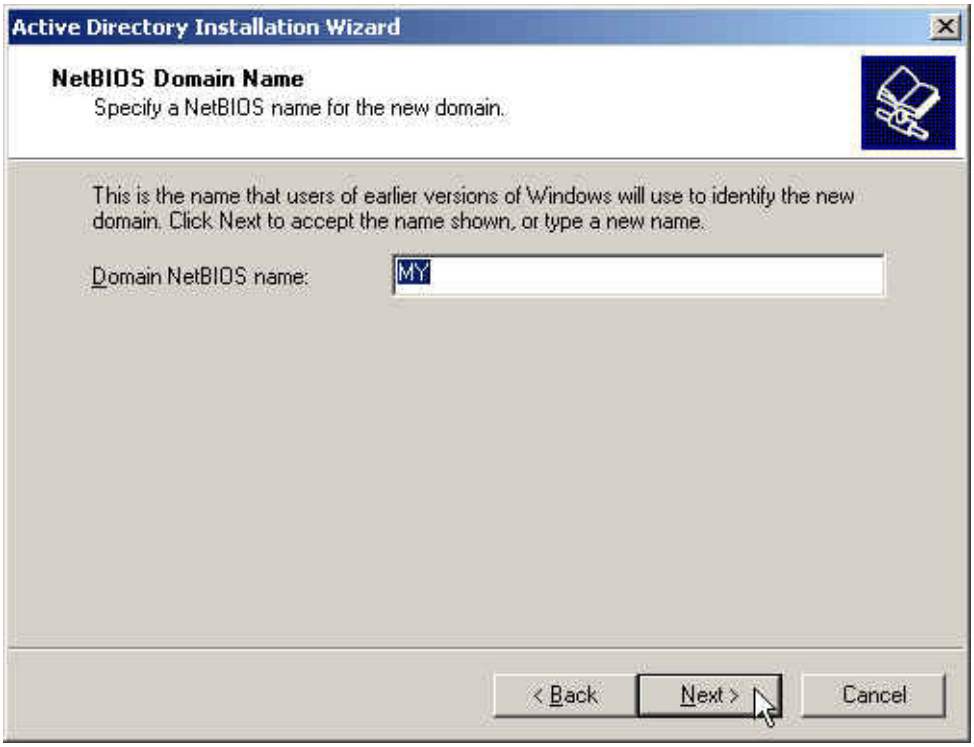


Figure 5-44 The NetBIOS domain name window

Step12. In **Database and Log Folders** window, enter the routes of **Database folder** and **Log folder**, click **Next**. (Figure 5-45)

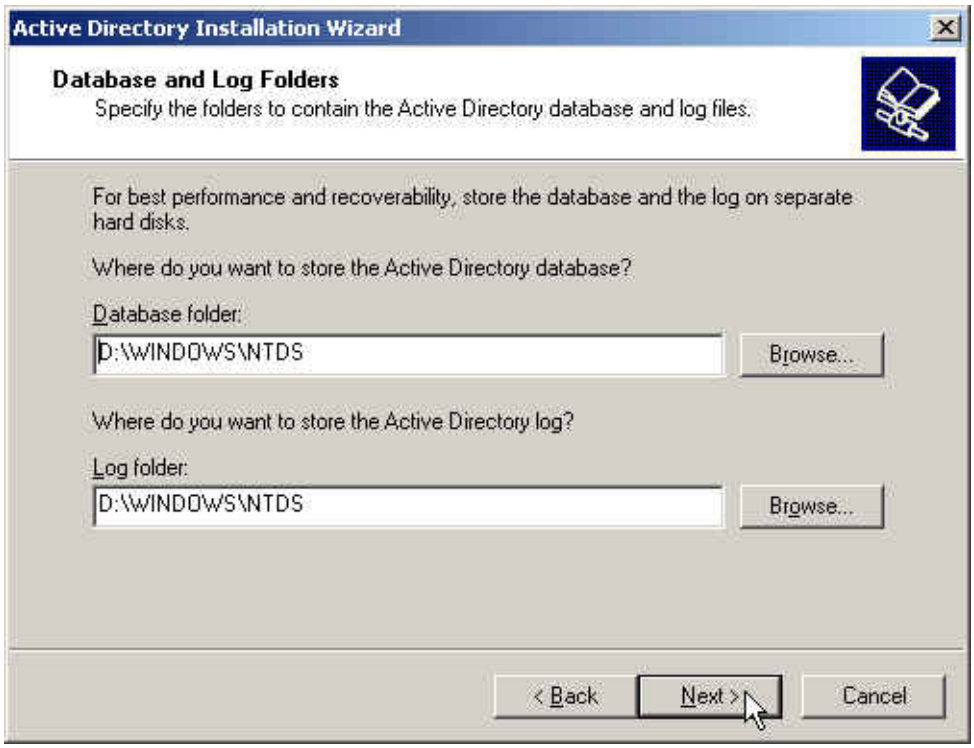


Figure 5-45 The database and log folder window

Step13. In **Shared System Volume** window, enter the **Folder location**, click **Next**. (Figure 5-46)

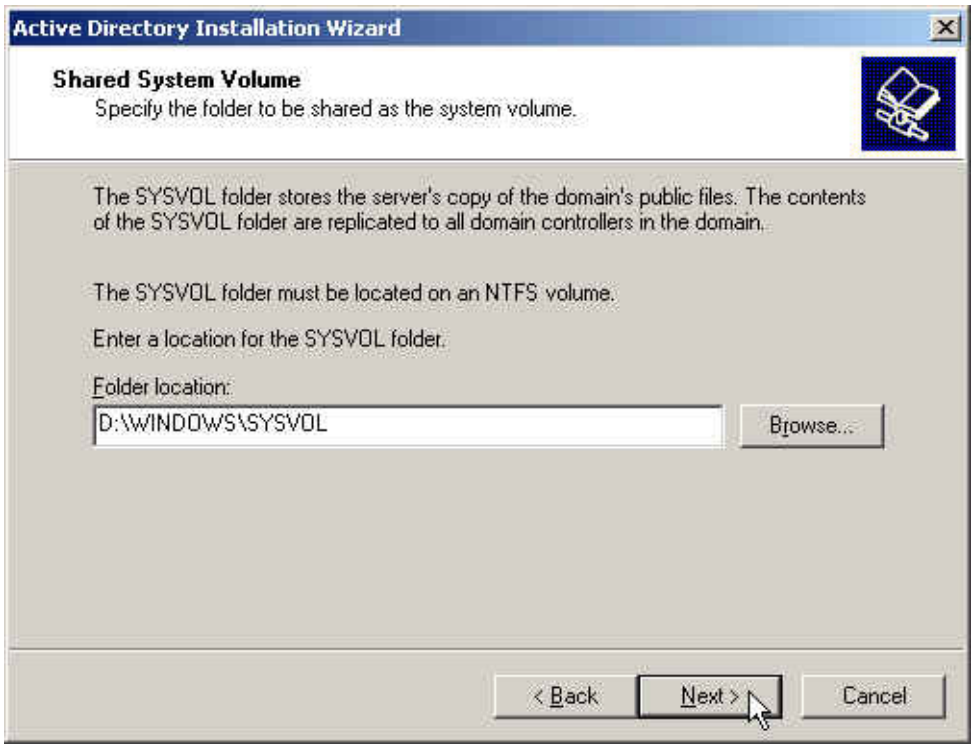


Figure 5-46 The shared system volume window

Step14. In **DNS Registration Diagnostics** window, select **I will correct the problem later by configuring DNS manually (Advanced)**, click **Next**. (Figure 5-47)

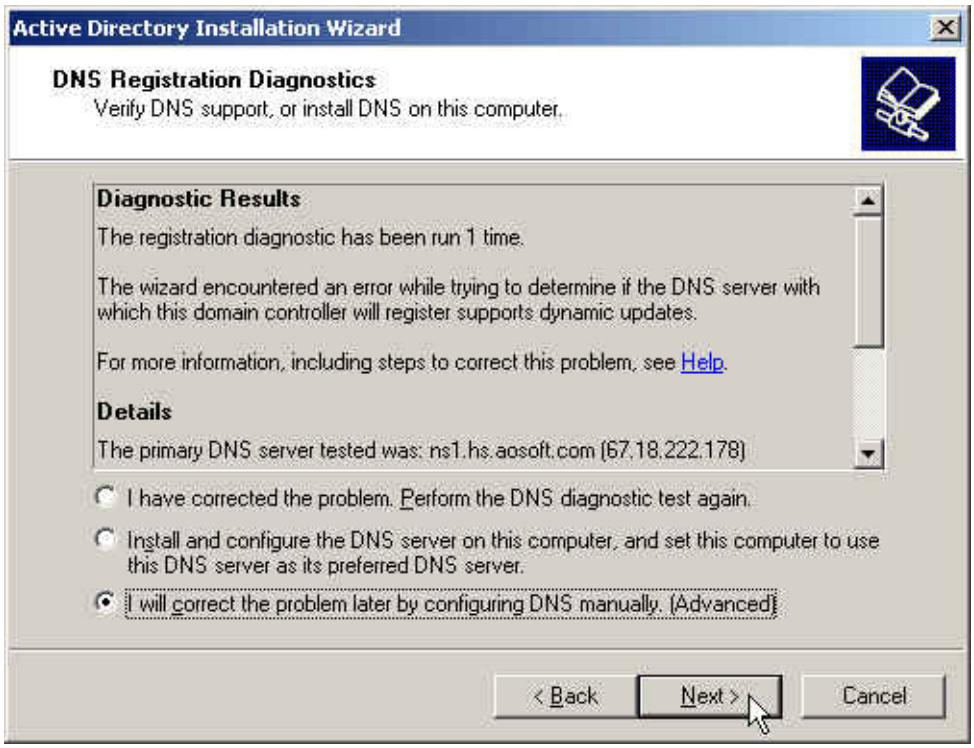


Figure 5-47 The DNS registration diagnostics window

Step15. In **Permissions** window, select **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems**, click **Next**. (Figure 5-48)

Figure 5-48 The permissions window

Step16. In **Directory Services Restore Mode Administrator Password** window, enter the **Restore Mode Password** and **Confirm password**, click **Next**. (Figure 5-49)

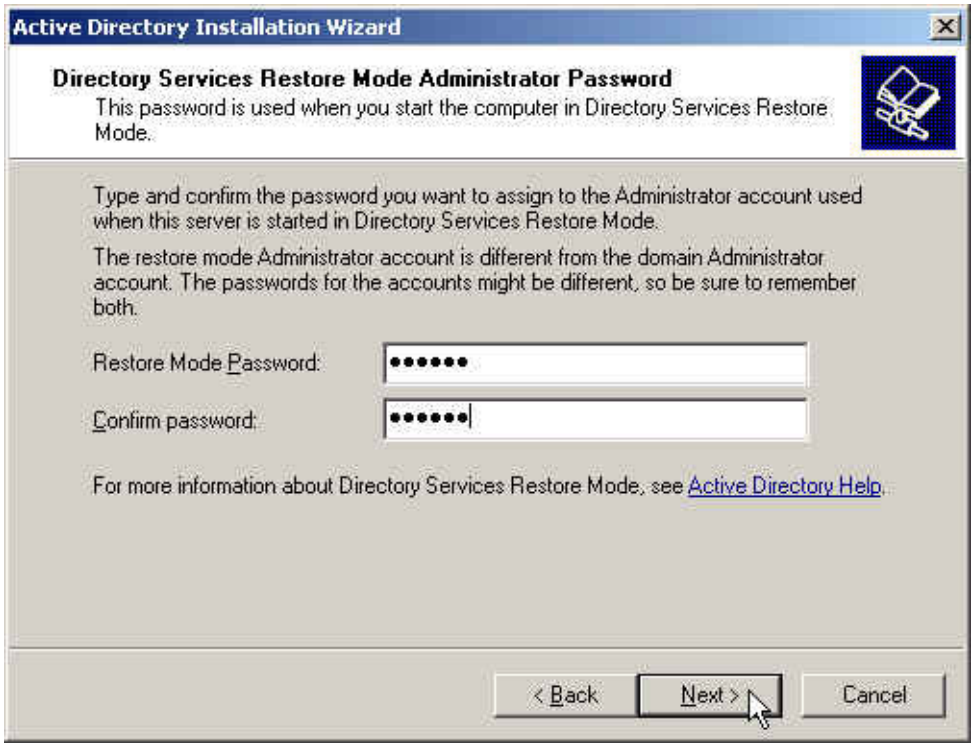


Figure 5-49 The directory services restore mode administrator password window

Step17. In **Summary** window, click **Next**. (Figure 5-50)

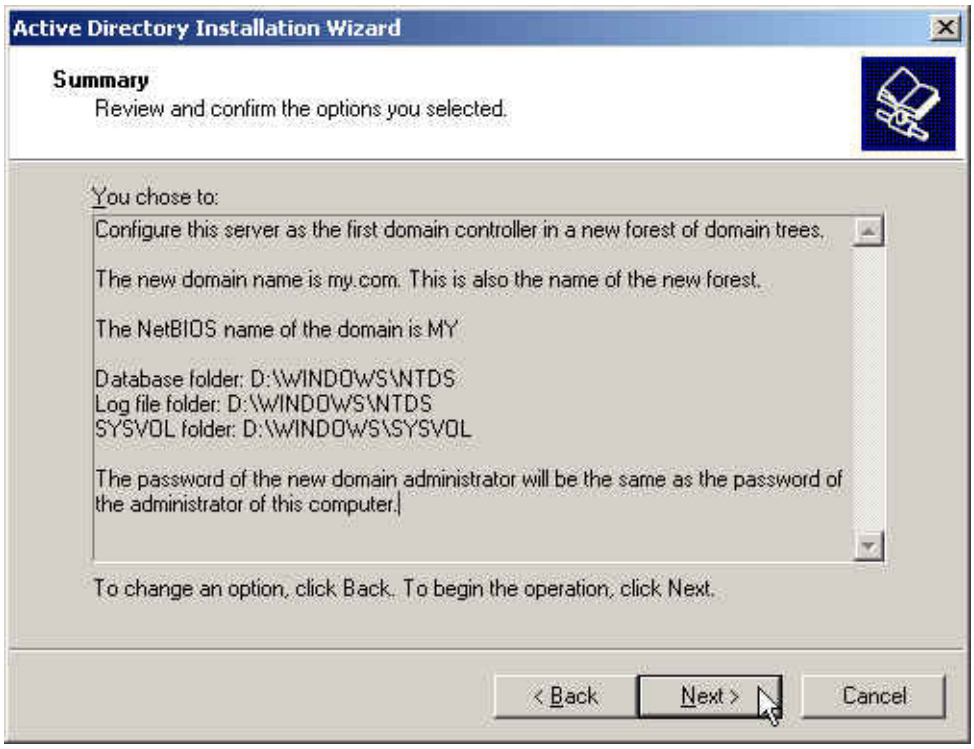


Figure 5-50 The summary window

Step18. Complete the Active Directory installation wizard. (Figure 5-51)

Figure 5-51 Complete the active directory installation wizard

Step19. Click **Start → Programs → Administrative Tools → Active Directory Users and Computers**. (Figure 5-52)

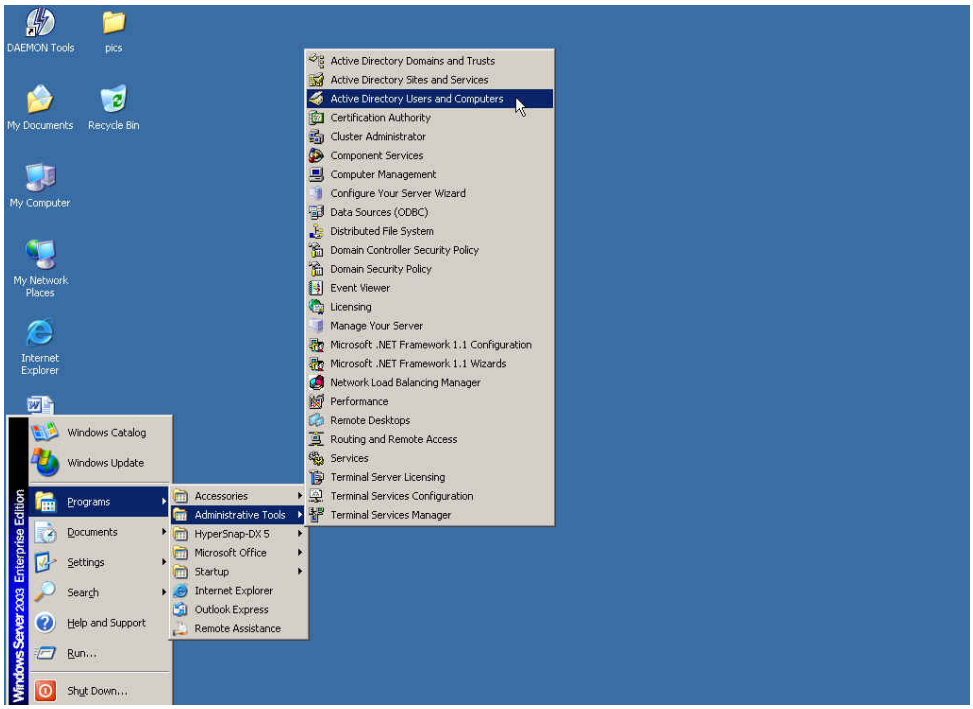


Figure 5-52 Enable active directory users and computers

Step20. In **Active Directory Users and Computers** window, right click on the **Users**, select **New → User**. (Figure 5-53)

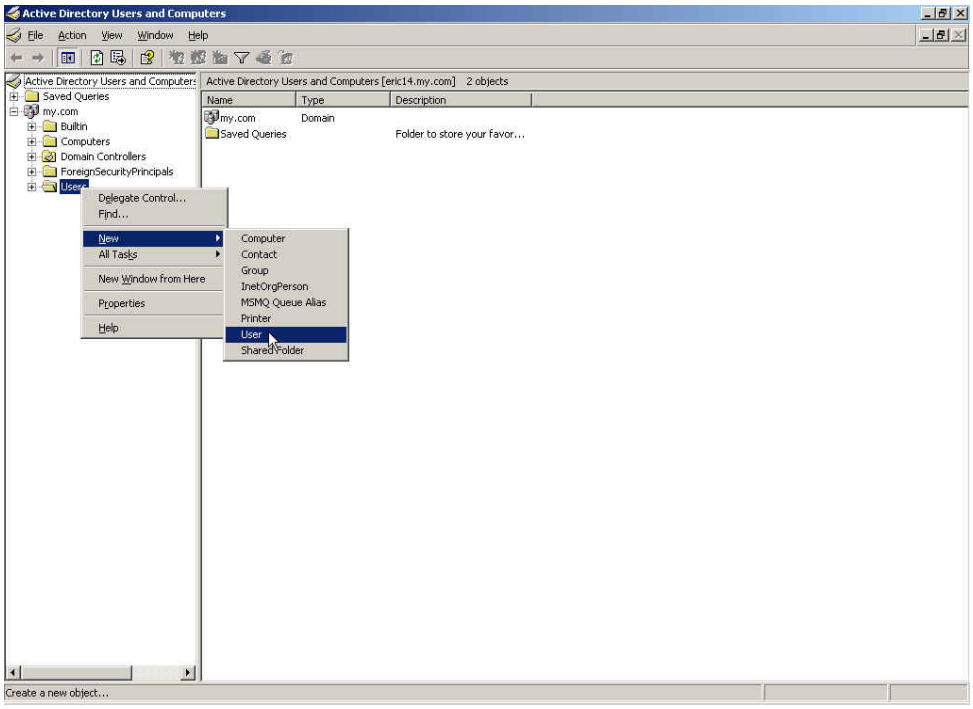


Figure 5-53 Add new active directory user

Step21. In **New Object–User** window, enter the settings, click **Next**. (Figure 5-54)

Figure 5-54 The new object – user setting window 1

Step22. In **New Object –User** window, enter the password, click **Next**. (Figure 5-55)

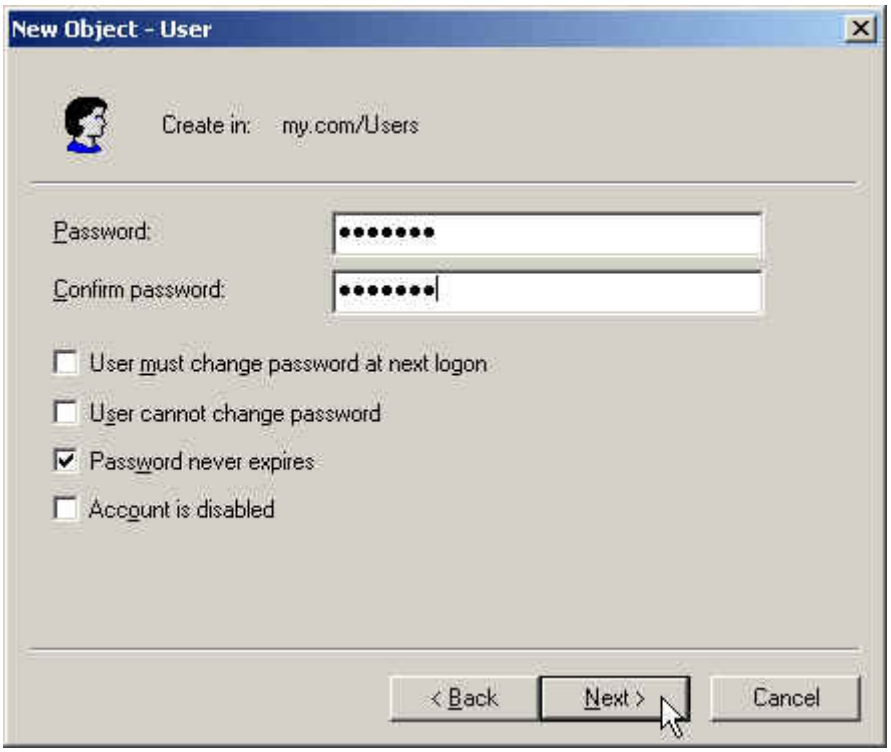


Figure 5-55 The new object – user setting window 2

Step23. Complete to add the user. (Figure 5-56)

Figure 5-56 Complete to add the user

Step24. Select **IM Management → Default Rule → ICQ → Accept** : **Authentication passed**. (Figure 5-57)

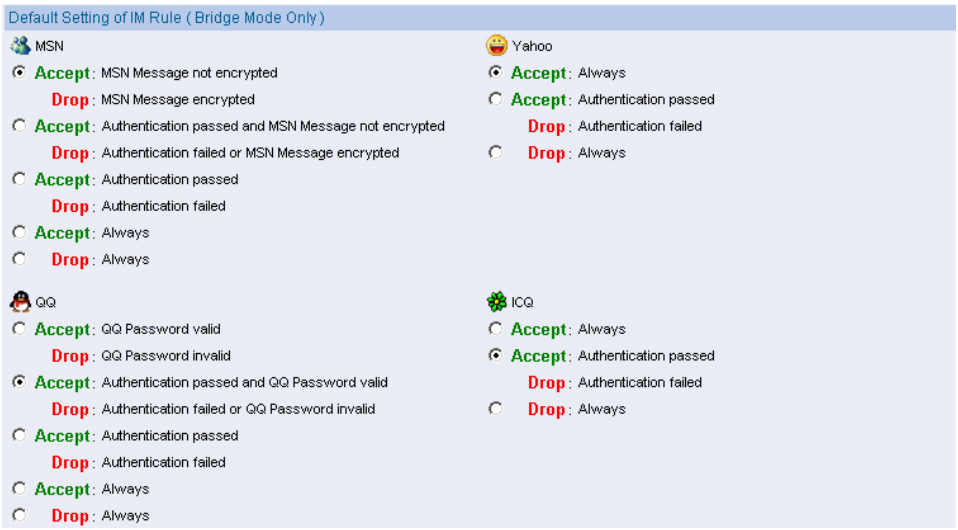


Figure 5-57 The default rule setting of IM

Step25. In **Authentication → LDAP**, enter the following setting：(Figure 5-58)

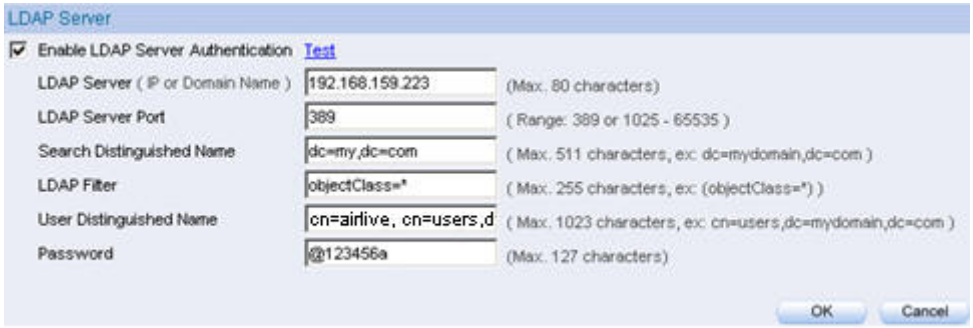


Figure 5-58 The LDAP Server setting

Click **Test**, it can detect if the IAR-5000 and LDAP server is real working.

Step26. Internal user type http://IAR-5000 interfac/auth in address cloumn of browser. For example, http://192.168.1.1/auth. :

- Enter the authentication name and password.
- Enter ICQ account.
- Click **OK**. (Figure 5-59)

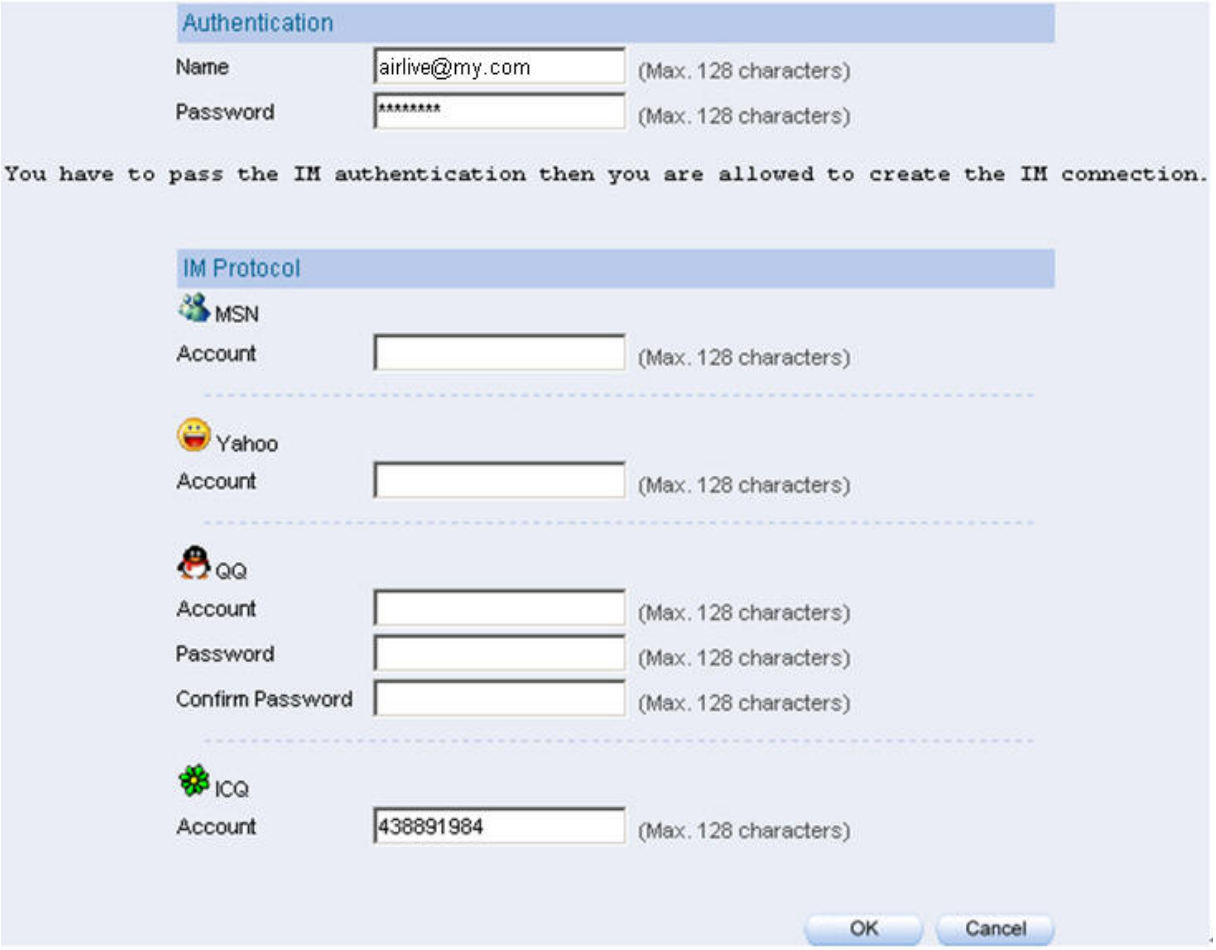


Figure 5-59 ICQ authentication setting

Step27. User can create the ICQ connection after authenticated. (Figure 5-60)

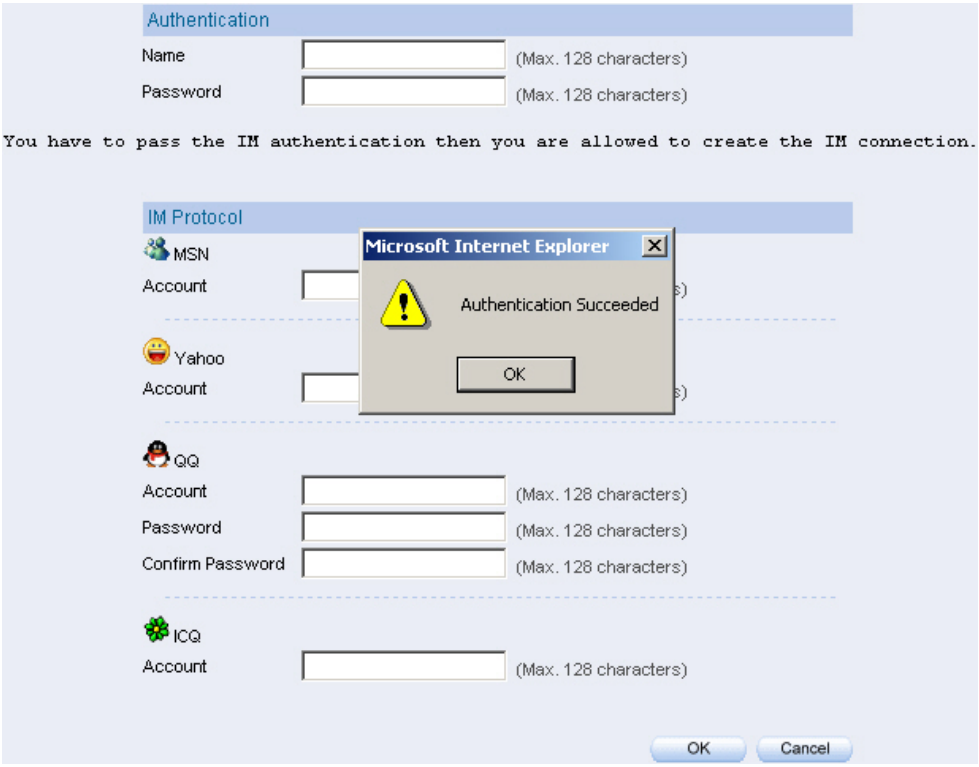


Figure 5-60 Authenticated succeed

5.3 Rule

Default Rule

MIS engineer can make the default IM rule for MSN, Yahoo, ICQ and QQ. When IAR-5000 detects new IM account and it will put the new account in Default Rule. On the other hand, MIS engineer can separately set the IM rule for every IM account in Account Rule, and the IM account will not affected by Default Rule.

Default Rule (For MSN, Yahoo, ICQ, QQ, Skype and Web Mail.)

- **Accept ：Always**
  Everyone can freely use the IM account.
- **Accept : Authentication passed / Drop : Authentication failed**
  User must to pass the authentication first then he/she can use the IM account.
- **Drop : Always**
  No one can use the IM account.

MSN Special Default Rule

IAR-5000 can not record the encrypted MSN contents. MIS engineer can choose to block the MSN encrypted contents.

Types of MSN Rule：

- **Accept : MSN Message not encrypted / Drop : MSN Message encrypted**
  - Anyone can freely use MSN by normal way to send message.
  - IAR-5000 will block MSN while user send message by encrypt MSN message.
    Accept : Authentication passed and MSN Message not encrypted /
    Drop: Authentication failed or MSN Message encrypted
  - User can use MSN only if the MSN account passed authentication and MSN message not encrypted.
  - IAR-5000 will block the MSN if MSN not passed authentication or even though MSN passed authentication but its contents encrypted.

QQ Special Default Rule

QQ send messages by encryption function. If IAR-5000 has user's QQ account and password then it can decrypt and record the QQ messages. There are two ways that user can type his/her QQ account and password.

1. If MIS engineer request user to use QQ by authentication, then user must type needed information in IM authentication management interface. The management interface is http://IAR-5000interface/auth. The default setting is http://192.168.1.1/auth.
2. If MIS engineer request user to use QQ without authentication, then user must type their QQ account and password in Add New QQ Account management interface. The Add New QQ Account management interface is http://IAR-5000 interface/qq. For example, the default setting is http://192.168.1.1/qq.

Types of QQ Rule

- **Accept : QQ Password valid / Drop : QQ invalid**

  User must type the correct QQ account and password in Add New QQ Account interface then he/she can use the QQ account. If it's not correct then IAR-5000 will block the QQ account.
- **Accept: Authentication passed and QQ Password valid / Drop: Authentication failed or QQ Password invalid.**
  - User must type the correct QQ account and password and authentication user name and password in IM authentication management interface.
  - IAR-5000 will block the QQ if user's QQ account did not pass the authentication and user type incorrect QQ account and password.

If user select IM Management → Rule → Default Rule → QQ → Accept: Always or Accept: Authentication passed then IAR-5000 only record when user use the QQ but can not record the QQ messages.

Apply the use privilege of QQ messenger from IAR-5000

The system administrator can find there is one user who does not has the use privilege of QQ messenger from the record in IAR-5000.

Step1.

◆ In **Record → Service → IM**, there is one QQ record can not be recorded normally. (Figure 5-61)

Figure 5-61 Found the QQ account which can't be recorded

◆ Click the QQ record, it can not correctly shows the QQ message contents. (Figure 5-62)

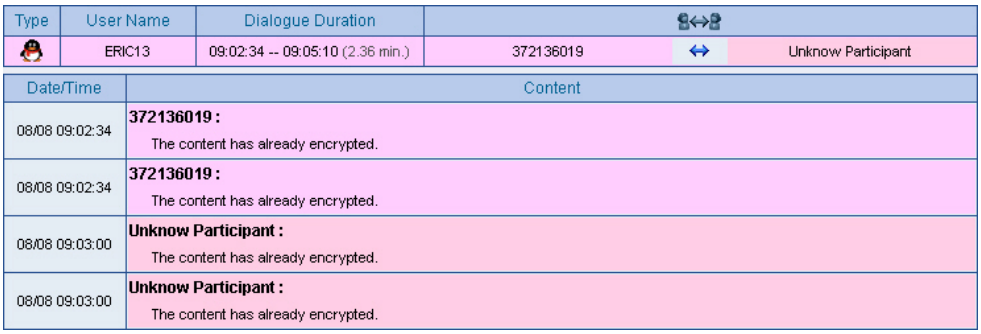


Figure 5-62 IAR-5000 can not record QQ message

◆ In **IM Management → Rule → Account Rule,** it shows the uncertificated QQ account. (Figure 5-63)

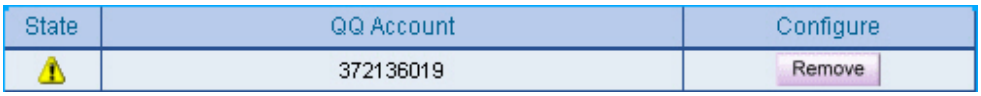


Figure 5-63 Found the uncertificated QQ account

Step2. Request the user to apply to modify his QQ password from IAR-5000：

◆ Enter the address of http://192.168.1.1/qq_accounts in browser (enter the string of " **/qq_accounts** "at the end of IAR-5000 interface IP address), then it shows the interface of **Add New QQ Account** (Figure 5-64)

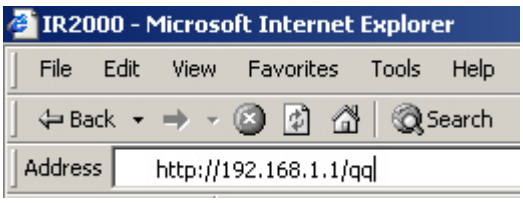


Figure 5-64 Enter Add New QQ Account interface

◆ User must enter the QQ ID and password, then click **Test**, to see if all of them are correct. (Figure 5-65)

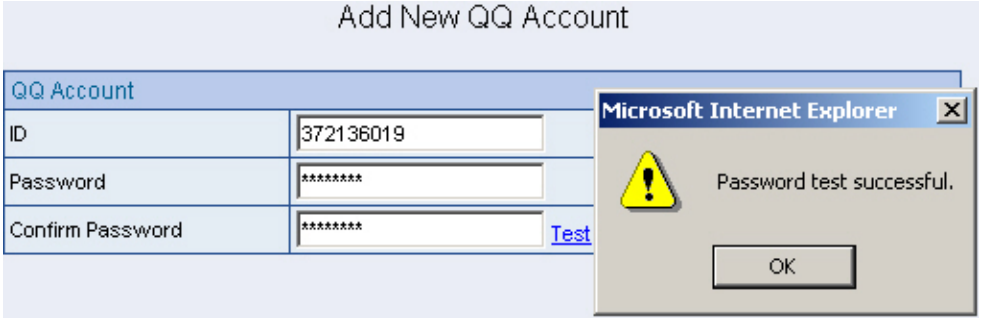


Figure 5-65 Test QQ account

◆ Click OK to complete the application of QQ account. (Figure 5-66)

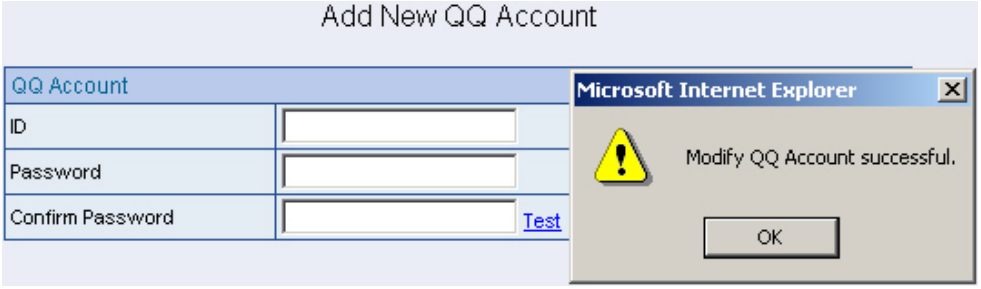


Figure 5-66 Add new QQ account successfully

Step3. In **IM Management → QQ Account**, the administrator can see all the QQ account list. (Administrator can not get user's QQ password.) (Figure 5-67)

State	QQ Account	Configure
✓	372136019	Remove

Figure 5-67 Password authenticated succeed

Step4. IAR-5000 can record the QQ contents successfully. (Figure 5-68, 5-69)

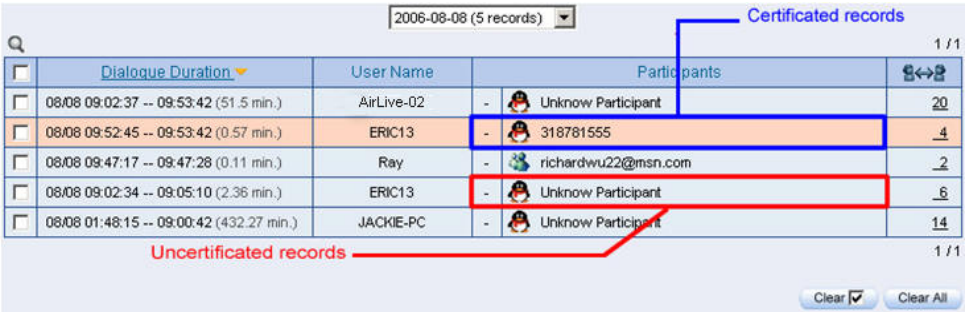


Figure 5-68 Can record the QQ contents

Type	User Name	Dialogue Duration			
	ERIC13	09:52:45 -- 09:53:42 (0.57 min.)	372136019	↔	318781555

Date/Time	Content
08/08 09:52:45	**eric :** log in successfully!
08/08 09:53:05	**318781555 :** ya i know i know
08/08 09:53:06	**318781555 :** ya i know i know
08/08 09:53:42	**eric :** i can's see you

Figure 5-69 Record the QQ contents successfully

User had changed QQ password then applied the modify privilege of QQ password from IAR-5000.

Step1. The user's QQ password is not correct. (Figure 5-70)

State	QQ Account	Configure
✗	372136019	Remove

Figure 5-70 The QQ password is wrong

Step2. Request user to apply to modify his/her QQ password from IAR-5000.

◆ Enter the address of http://192.168.1.1/qq_accounts in browser (enter the string of " **/qq_accounts** "at the end of IAR-5000 interface IP address), then it shows the interface of **Add New QQ Account**. (Figure 5-71)

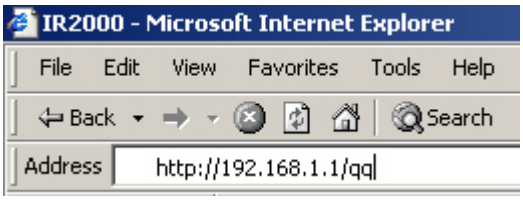


Figure 5-71 Enter Add New QQ Account interface

◆ User must enter the QQ ID, original password, new password and confirm password. (Figure 5-72)

Modify QQ Account

(Please fill Old Password form)

QQ Account	
ID	372136019
Old Password	********
Password	**********
Confirm Password	********** Test

OK

Figure 5-72 Enter the old password, password and confirm password

◆ Click **OK** to complete to modified the QQ password. (Figure 5-73)

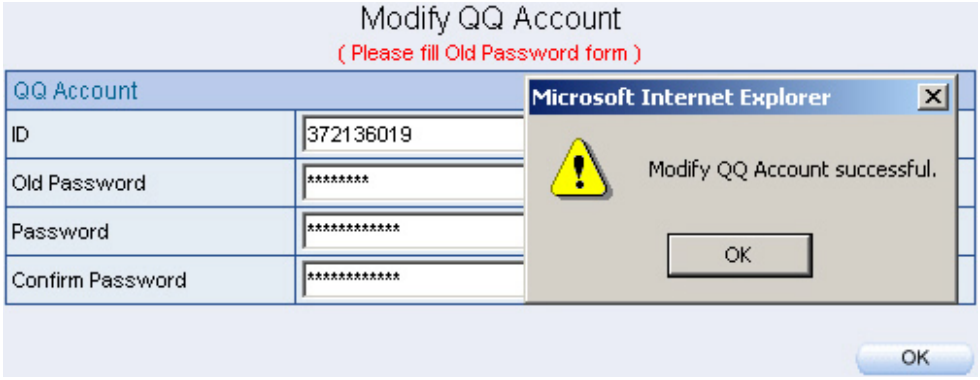


Figure 5-73 Complete to modify the QQ password

Step3. When the user re-login QQ, the IAR-5000 will auto complete the QQ account authentication.

Step4. In **IM Management → QQ Account,** the system administrator can see the user's QQ account has certificated. (Administrator can not get the QQ password.) (Figure 5-74)

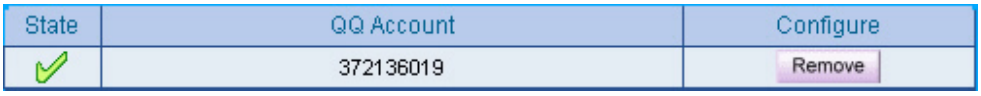


Figure 5-74 QQ account authenticated succeed

Step5. IAR-5000 can record the QQ message contents. (Figure 5-75, 5-76)

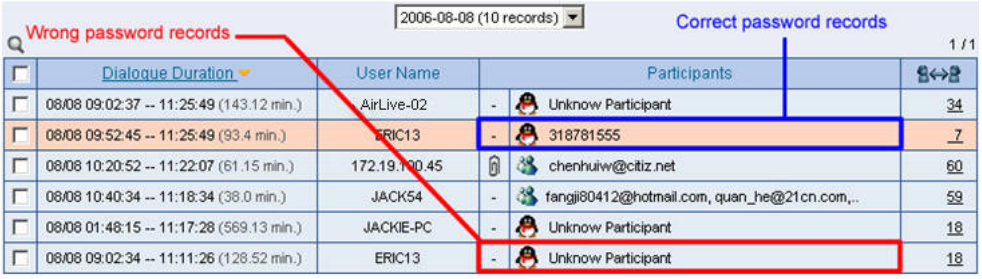


Figure 5-75 Record the QQ message contents successfully

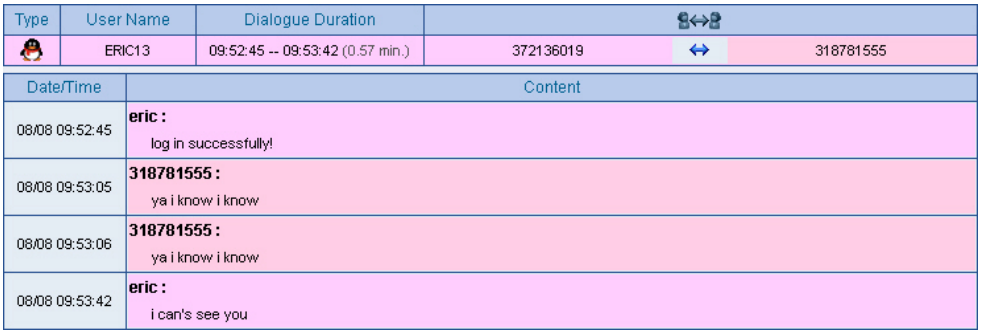


Figure 5-76 Record the QQ message contents successfully

To modify the IM account information by importing the User Account List Configuration (Excel list)

Step1. Download the User Account List Configuration file.

◆ Click **Download** near **Export Account Rule to Client PC** in **IM Management → Rule → Default Rule**. (Figure 5-77)

Figure 5-77 Download the user account list configuration

◆ In **File Download** dialogue box, click **Save**. Then assign the saved location and click **Save** again. (Figure 5-78)

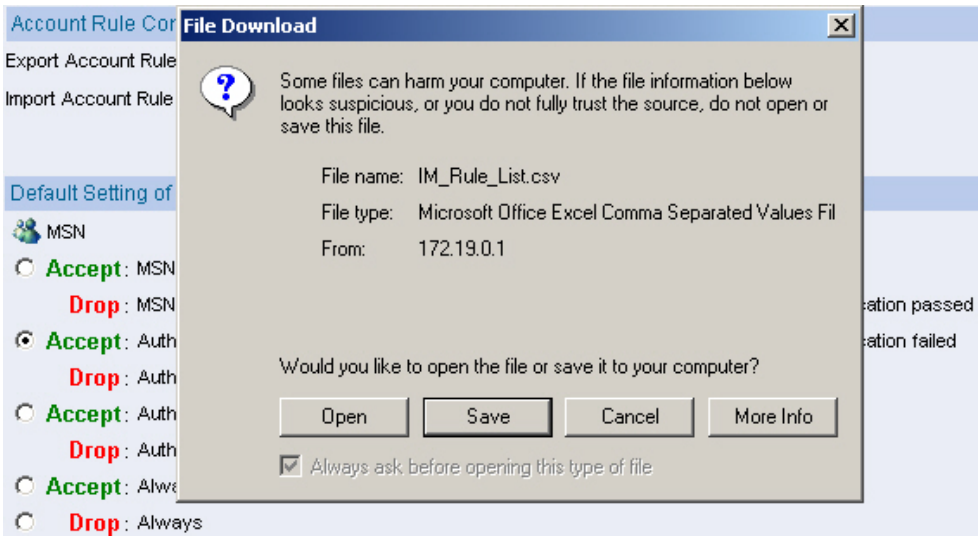


Figure 5-78 Select the location to save the rule list

Step2. Open the user account list by Excel.（IM_Rule_List.csv）

```
#############################################################
#Format:
#
IM_Type        Account                    Rule        AuthName        IP              MAC              AuthType
#
#
#############################################################

MSN      airlive_test01@hotmail.com  Default  sales      172.19.50.24  00:0C:29:8A:BB:46  USER
MSN      airlive_test02@hotmail.com  Default  account    172.19.70.201 00:0A:48:0C:A6:20  -
MSN      airlive_test03@hotmail.com  Accept   account    172.19.50.26  00:0A:48:0C:A6:20  -
MSN      airlive_test04@hotmail.com  Drop     support    172.19.70.204 00:05:5D:95:5B:C6  -
Yahoo     airlive_test01             Default  support    172.19.70.202 00:0A:48:0C:A6:20  USER
Yahoo     airlive_test04             Default  support    172.19.70.204 00:05:5D:95:5B:C6  POP3
QQ                     539236964     Default  -          172.19.70.203 00:05:5D:95:5B:C6  -
QQ                     539330473     Default  sales      172.19.50.25  00:0B:DC:29:8A:CC  -
QQ                     539337471     Default  sales      172.19.70.203 00:05:5D:95:5B:C6  -
ICQ                    292420150     Default  -          172.19.50.26  00:0A:48:0C:A6:20  -
```

"#" means the description

IM Software

IM Account

Types of Rule

User IP Address

IM Account Authentication method

Authentication Name

User MAC Address

Step3. Assume that MIS engineer want to modify one MSN account：

◆ To modify the rule type and change **Default** to **Accept** ：

MSN	airlive_test01@hotmail.com	Default	sales	172.19.50.24	00:0C:29:8A:BB:46	USER
MSN	airlive_test01@hotmail.com	Accept	sales	172.19.50.24	00:0C:29:8A:BB:46	USER

◆ To modify the IP and MAC address：

MSN	airlive_test01@hotmail.com	Accept	sales	172.19.50.24	00:0C:29:8A:BB:46	USER
MSN	airlive_test01@hotmail.com	Accept	sales	172.19.52.30	00:0C:29:8A:BC:9A	USER

◆ If MIS engineer want to add one IM account, just add one row and type the related information.

Yahoo	airlive_test03	Default	-	172.19.70.204	00:05:5D:95:5B:C6

◆ Complete the modification and save the file.

Step4. Click **Browse** near **Import Account Rule form Client PC** in **IM Management → Rule → Default Rule.** Import the file and click **OK.** (Figure 5-79)

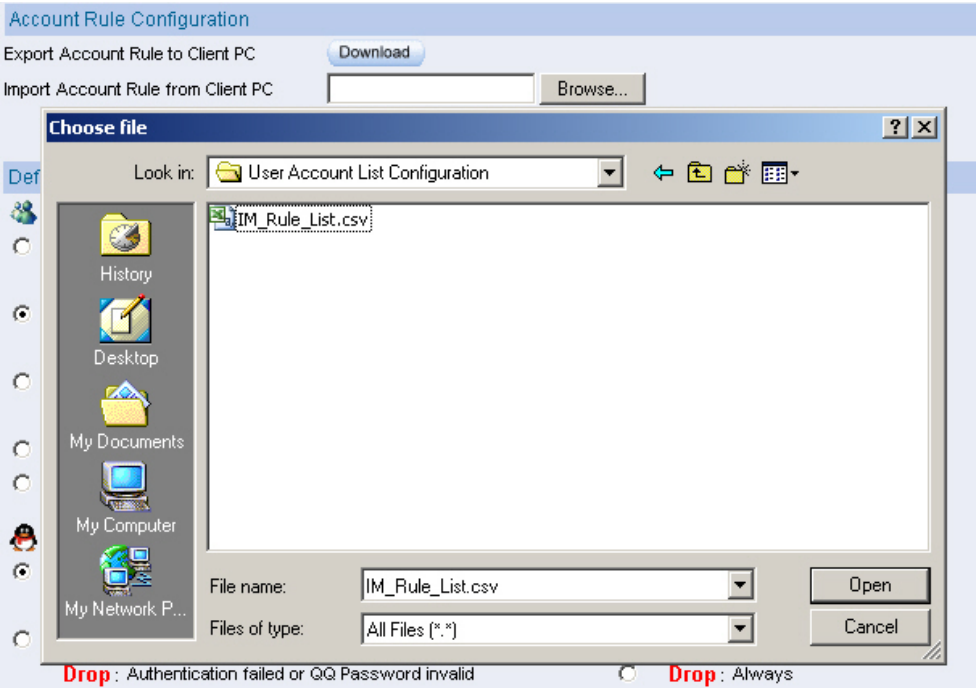


Figure 5-79 Select the location to save the file

Step5. Now the IM account information in IAR-5000 is the modified document edited by MIS engineer.

The CSV files can only modify the already existed IM account content or add new IM account, **but can not remove the IM account.** In other words, if MIS engineer remove one of the IM accounts in csv file and upload it, then the removed IM account still existed.

MIS engineer does not need to modify the authentication method in csv file. It is because if MIS engineer has enabled the IM authentication mechanism, then user must set the related IM account information to pass the IM authentication. And the IM authentication method is determined by authentication IM account and password. So that means it is useless for MIS engineer to set any authentication method of USER, POP3 or LDAP in the csv file. For example, there is an IM account not passed the authentication, even though MIS engineer set the authentication method of USER in csv file, but user can still enter the related POP3 information and pass the IM authentication in IM Management Interface.

Account Rule

Types of Account Rule：

- Default Account：

  When IAR-5000 detects new IM accounts, it will define them to **Default Rule** and these accounts are **Default Account.** On the other hand, MIS engineer can **separately** set the IM account to be **Accept Account** or **Drop Account.**

- Accept Account

  MIS engineer can assign the IM account to be **accepted account** so that user can use the accepted account to log in IM software without affecting by Default Rule.

- Drop Account

  MIS engineer can assign the IM account to be **Drop Account** so that user can not use the Drop Account to log in IM software. Drop Account will not affected by Default Rule.

Icon	Name	Description
	Authentication Passed	Every IM account has a portrait and that means the IM account is not certificated. But if system added an icon of certification near the portrait and that means the IM account is certificated.
	Password Correct	It means the applied QQ account and password were passed the authentication and IAR-5000 can record the contents of this authenticated QQ account.
	Password Uncertificated	User has not applied the QQ account from IAR-5000 or even though he has already add the QQ account but not certificated yet. IAR-5000 can not record the contents of uncertificated QQ account.
	Password Incorrect	The user's QQ account and password can not pass the authentication. IAR-5000 can not record the contents of the QQ account.

IAR-5000 can inspect if the stored QQ account and password are correct once user login QQ account.

To Modify the IM Account Rule：

Step1. Select IM accout to be moved to other position. Click **OK**. (For example, select one MSN accout and click **To Accept** , to move the MSN account to **Accept Accout**.) (Figure 5-80, 5-81)

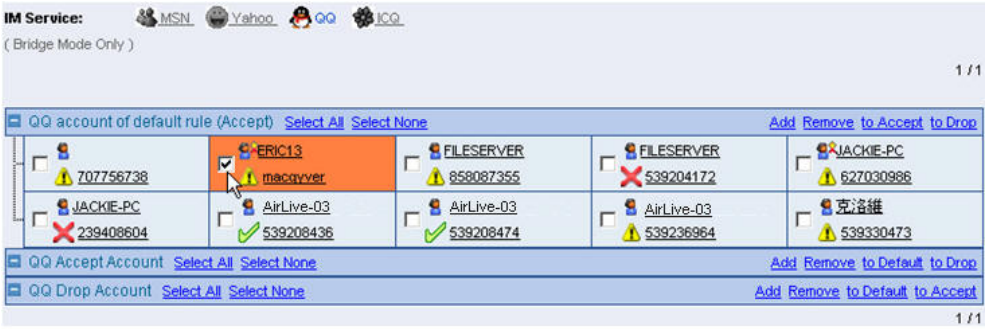


Figure 5-80 Select IM account

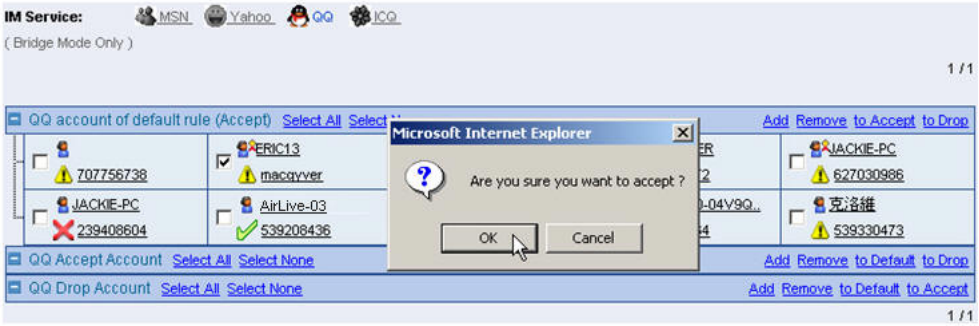


Figure 5-81 Confirm to move the account to accept account

Step2. Complete to move the IM account to accept account. (Figure 5-82)

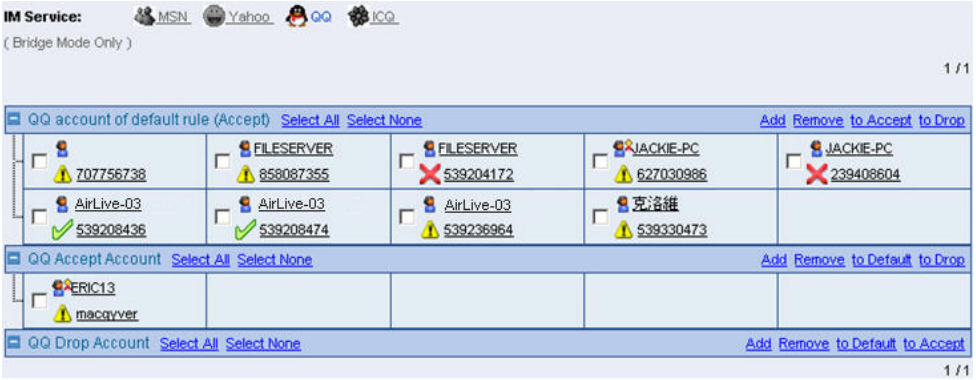


Figure 5-82 The account has been removed to accept account

Remove IM Account：

- Select the IM account and click **Remove**.

Add IM Account：

Step1. Select which IM service to add in IM Service function. For example, **MSN**. Click **Add** at the right column in **MSN Account of Default Rule**. (Figure 5-83)

Figure 5-83 Add MSN account of default rule

Step2. Enter the related information in the column of **Add Account Policy**. (Figure 5-84)

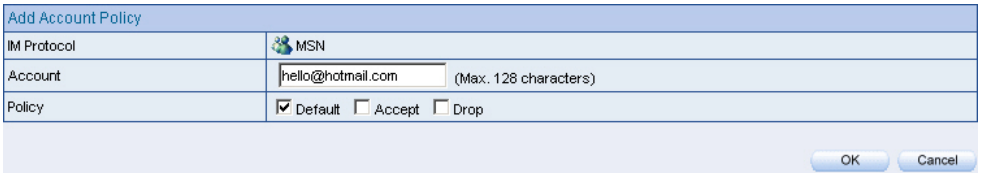


Figure 5-84 Enter the related information

Step3. Complete to add a MSN account to default rule. (Figure 5-85)

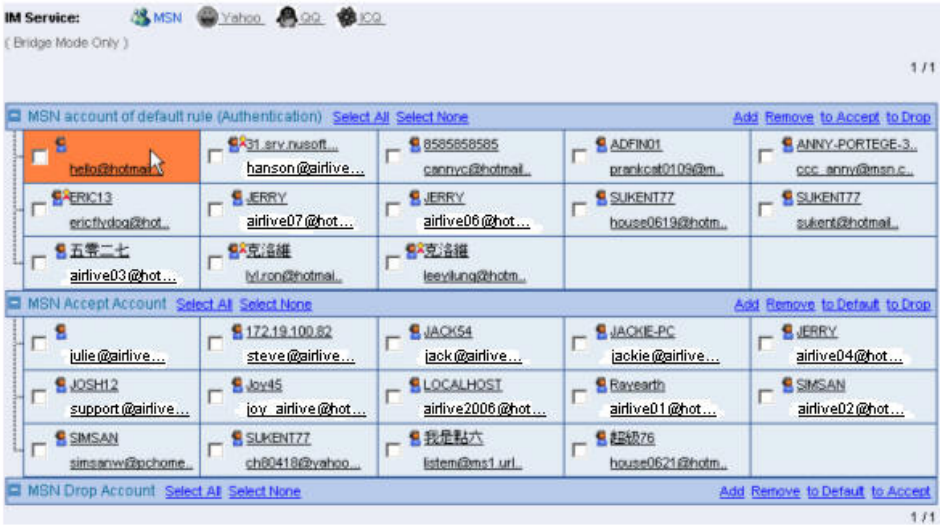


Figure 5-85 Complete to add the MSN account of default rule

Chapter 6 P2P Management

Default Rule

MIS engineer can make the default P2P rule, and he can also separately set the P2P rule for every P2P account in **User Rule**, and the P2P account will not affected by **Default Rule**.

Default Rule (Figure 6-1)

- **Accept ：Always**

  Everyone can freely use the IM account.

- **Drop : Always**

  No one can use the IM account.

Figure 6-1 P2P Management Default Rule

IAR-5000 can manage the access right of P2P software type, including eDonkey, Bit Torrent, WinMX, Foxy, KuGoo, ApplieJuice, AudioGalaxy, DirectConnect, iMesh, MUTE, Thunder5

User Rule (Figure 6-2)

Types of User Rule：

- Default Account：

  When IAR-5000 detects new P2P accounts, it will define them to **Default Rule** and these accounts are **Default Account.** On the other hand, MIS engineer can **separately** set the P2P account to be **Accept Account** or **Drop Account.**

- Accept Account

  MIS engineer can assign the P2P account to be **accepted account** so that user can use the accepted account to log in P2P software without affecting by Default Rule.

■ Drop Account

MIS engineer can assign the P2P account to be **Drop Account** so that user can not use the Drop Account to log in P2P software. Drop Account will not affected by Default Rule.

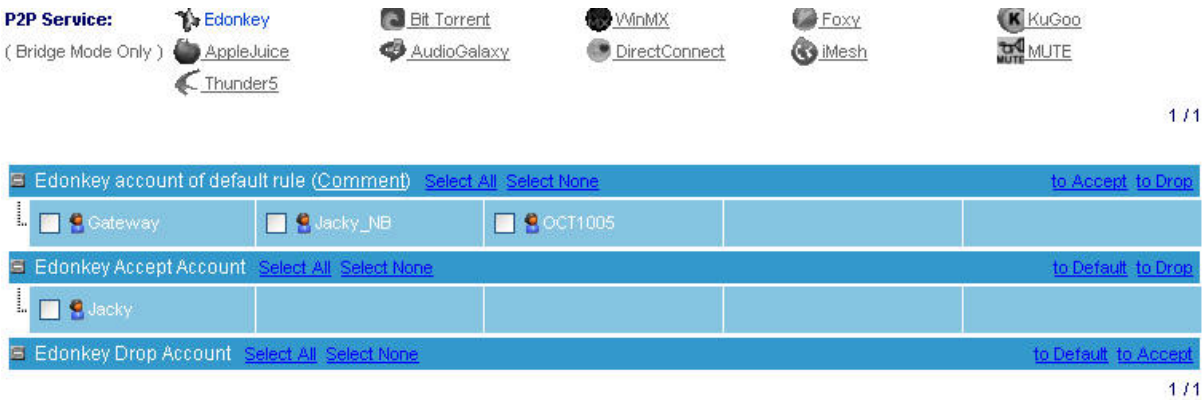


Figure 6-2 P2P Management User Rule

P2P management only can provide or deny P2P Account the access right, but it can not create or remove P2P account in P2P Management.

Chapter 7 Record

IAR-5000 can record the user's internet activities, and administrator easy to manage all of the information by clearly group / department division. And assure the data transmission security and monitor the employee's internet activities. In other words, IAR-5000 can prevent the employee to use the network resources to access private activity via internet.

7.1 Setting

Service Definitions

- The IAR-5000 can auto online update every service definitions without disconnecting, if the internet service provider changed transmission mode.
- IAR-5000 can auto online update the service definitions every one hour. Or click Update Now , the IAR-5000 can instant update the service definitions.

User name binds to IP / MAC address

- The log can be record depends on the user's IP address, when it comes from the same IP address, will be decide to be the same user. The function is especially focus on the Corporation which uses the static IP.
- The log can be record depends on the user's MAC address, when it comes from the same MAC address, will be decide to be the same user. Normally, the user's IP is the dynamic IP address (The Company use the DHCP).

When internal user want to link to the internet by IAR-5000 in front of the router, the MAC address of packets will be replaced in rounter's MAC address, then sent to IAR-5000. It's better to use the user name binds to IP address.

LAN to LAN record setting

- The IAR-5000 can record the transfer data records in LAN. (The data transfer process must pass through IAR-5000). It is suitable for the employee link to internet through company's internal proxy server.

The maximum entries to be displayed on the page

- In **Record** option, user can assign how much data to display in the page.

Default Character Encoding

- When the administrator does not specify which character encodes to use, then IAR-5000 will use default character encode to display the records.

HTTP cache setting

- System administrator can choose to enable the http cache setting, as IAR-5000 process the http recording.

  Enable HTTP cache：IAR-5000 can record the browsed web pages by saving the whole web page contents, but it also wastes more disk space.

  Disable HTTP cache：IAR-5000 can record the browsed web pages by saving the address links. The system administrator only can see the modified web pages if they've been modified. It only wastes less disk space to save these records.

7.2 User

IAR-5000 can record the user's internet activities, and administrator easy to manage all of the information by clearly group / department division. And assure the data transmission security and monitor the employee's internet activities. In other words, IAR-5000 can prevent the employee to use the network resources to access private activity via internet.

Monitor the internet record of the specific User

Step1. In **Record → User → Logged**, can select the division of user.（Click subnet or department / group）.(Figure 7-1, 7-2）

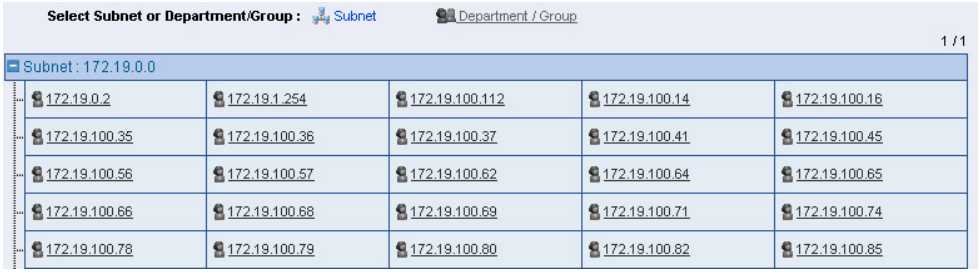


Figure 7-1 Select subnet classification

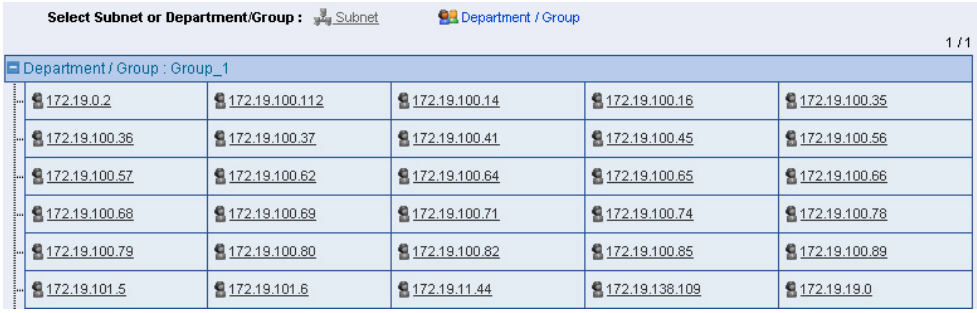


Figure 7-2 Select department / group classification

Step2. Click the user to see (For example, use the **subnet 192.168.1.0**, **User of Jacky**), it shows the service record. (Figure 7-3)

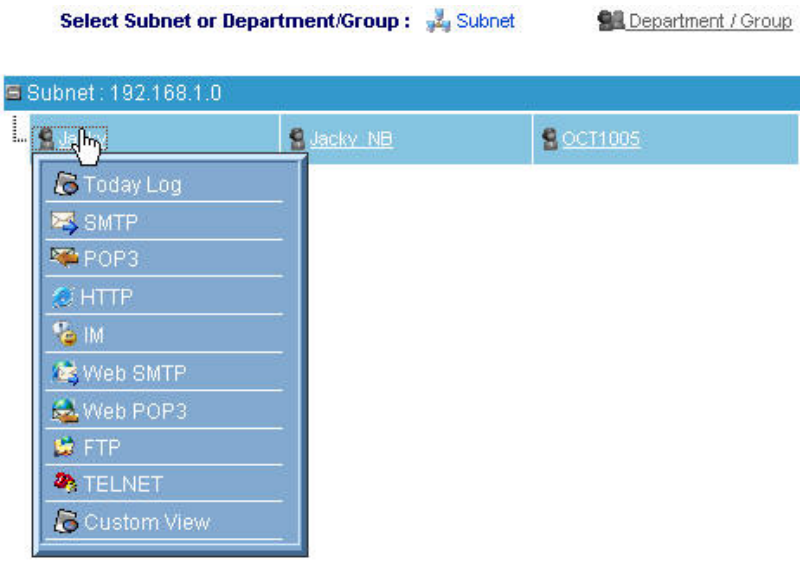


Figure 7-3 The service types of specific user

Step3. Click **Today Log**, to know what kind of internet activities has done by the employees.

Step4. Click the **event**, to know the content of the internet activities done by the user. (For example, HTTP)

Step5. Click **SMTP**, to know what kind of e-mail has sent by the user in SMTP service.

Step6. Click the record, it will show e-mail contents, and forward the mail to the specific mail box. And you can choose to open or save the attached file. (Figure 7-4)

Figure 7-4 The e-mail contents sent by the user

Step7. Click **POP3**, to know what kind of e-mail has received by the user in POP3 service.

Step8. Click the record, it shows the e-mail contents, and users can also forward this e-mail to the specific e-mail box. The user can also choose to open or save the attachment. (Figure 7-5)

Figure 7-5 The e-mail contents received by the user

Step9. Click **HTTP**, to know which web page did the user browsed.

Step10. Click the record, it shows the web page.

Step11. Click **IM**, to know who has made the conversation with the user. The number at right side represents the frequency of the conversation. (Figure 7-6)

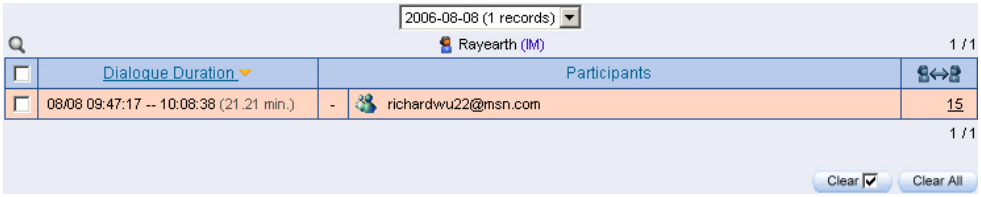


Figure 7-6 The user‘s MSN service record

Step12. Click the number of **15** at the right side, then it shows the conversation contents.

Step13. Click **Web SMTP**, to know what kind of E-Mail has the user sent in Web SMTP.

Step14. Click the recorded subject, then it shows the e-mail contents, and it can be opened or saved.

Step15. Click **Web POP3**, to know what kind of e-mail has the user received in Web POP3.

Step16. Click the **Subject**, it shows the e-mail contents.

If the mail included the attached file, but user only read the mail content from Web POP3 records without downloading the attached file. Then IAR-5000 will only notice the user about the mail has attached file and also its file name.

Step17. Click **FTP**, to know what kind of files has the user upload or download.

Step18. Click the record, it shows **File Download** window, and choose to open or save. (Figure 7-7)

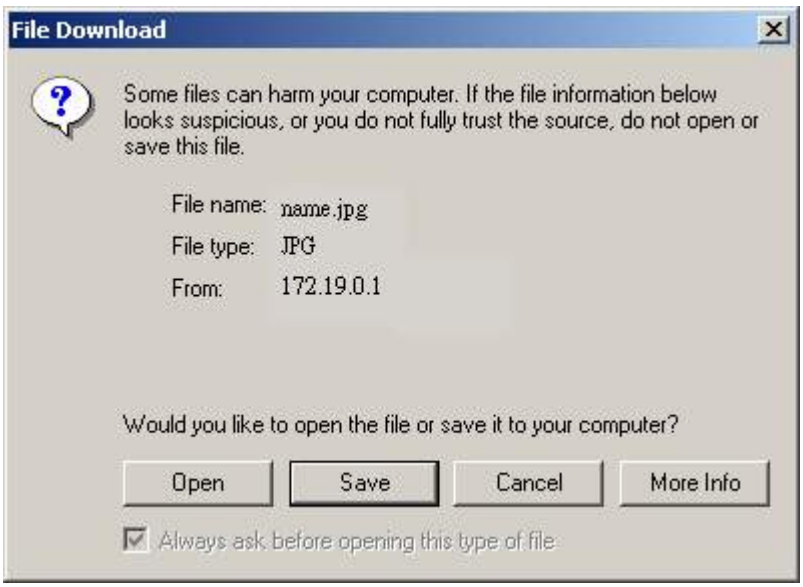


Figure 7-7 Download the file from FTP

Step19. Click **TELNET**, to know which site has the user login. (Figure 7-8)

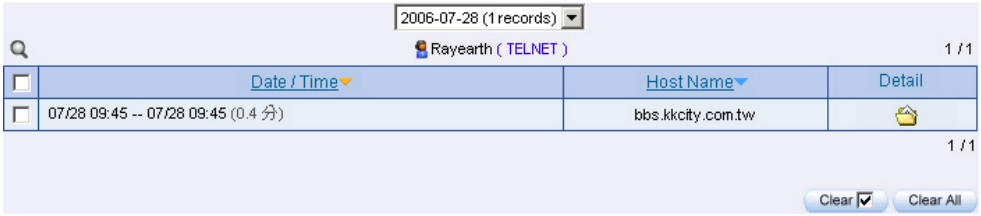


Figure 7-8 The user's record in Telnet service

Step20. Click **view the content**, then it shows the contents. (Figure 7-9)

Figure 7-9 It shows the contents when user's Log in

7.3 Service

IAR-5000 includes eight services, it can let the MIS easy to manage all the information, insecure the security of data transmission, and monitor the employees who use the network resources to access personal activities.

（1） **SMTP**：Record the e-mail sent by the user mail server.

（2） **POP3**： Record the e-mail received by the user through mail server.

（3） **HTTP**： Record the web page browsed by the user.

（4） **IM**：Record the communication record of IM（For example, MSN, Yahoo Messenger, I CQ）.

（5） **Web SMTP**： Record the e-mail sent by the user through the internet mail box.（For example, Yahoo, Gmail, Hotmail）.

（6）**Web POP3**： Record the user's browsed e-mail in internet mail box.（For example, Yahoo, Gmail, Hotmail）

（7） **FTP**： Record the user's files sent by FTP tool.

（8） **TELNET**： Record the user's browsed records of Telnet and BBS.

Search

- According to the characteristic and keywords of mail recipient, sender, subject, name and specific date in the mail attachment, we can offer POP3, SMTP, WebPOP3, Web SMTP services, to search the mail record saved in IAR-5000. The function icon is「 」.

  - In the SMTP, for example：
    1. **Sender** enter the key words about e-mail account
    2. Select **attach**.
    3. Click Search (Figure 7-10)

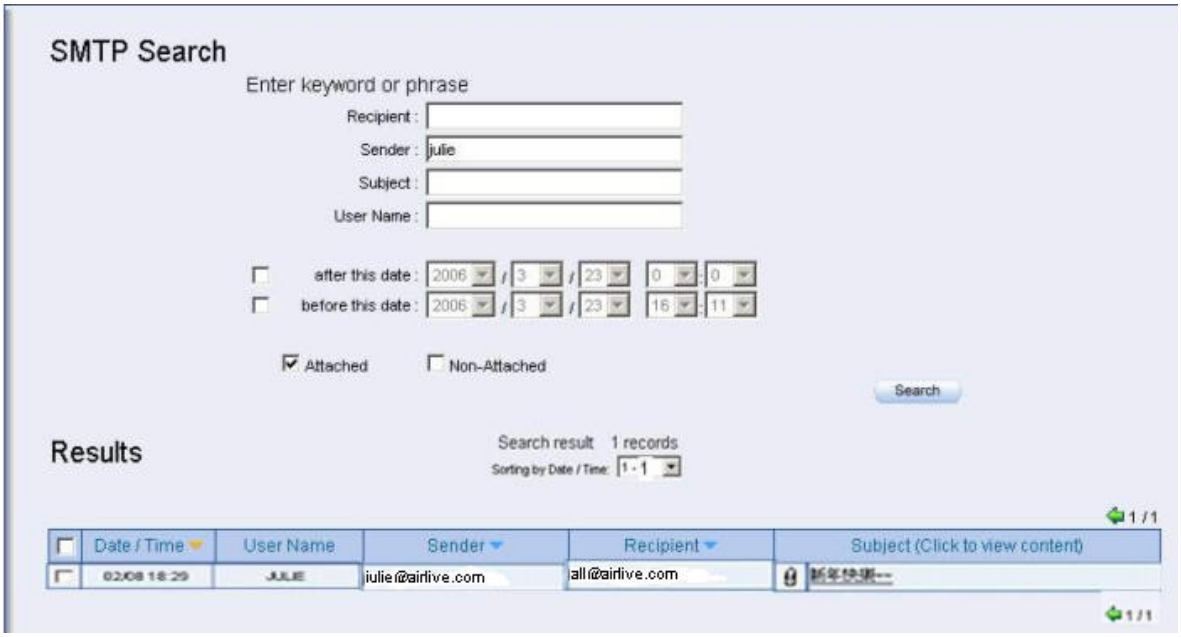


Figure 7-10 Search the specific record in SMTP

- According to the file name, PC name, user name, file size, specific date, some key words and characters, the administrator can use the FTP service to search the files in IAR-5000.
  - We will make some settings in FTP search function.
    1. **User Name** Enter js26.
    2. **Size** Choose over 1KB.
    3. Click Search

Forward：

- The system administrator can choose some records to forward to the specific mail box, according to the search results in POP3 and SMTP. In other words, the records backup function will be more flexible.

  - We will add some settings in this function menu.
    1. Select the record to forward.
    2. Click forward icon「 」.
    3. It shows the forward dialogue box, enter the sender e-mail address, Click **OK**.

SMTP Record

Step1. Click **Record → Service → SMTP**, it shows SMTP window.

Step2. Click Subject to view the e-mail contents.

Step3. It shows the mail contents sent by the user.

It can show the mail contents, forward function, and the MIS engineer can choose to view or save the attachment.

POP3 Record

Step1. Click **Record → Service → POP3**.

Step2. Click **Subject**, to view the mail contents.

Step3. It shows the mail contents sent by the user.

It shows the mail contents, and then forwards it. On the other hands, the attachment also can be viewed or saved.

HTTP Record

Step1. Click **Record → Service → HTTP**.

Step2. Click **Web Site** to view.

Step3. It shows the web site record. (Figure 7-11)

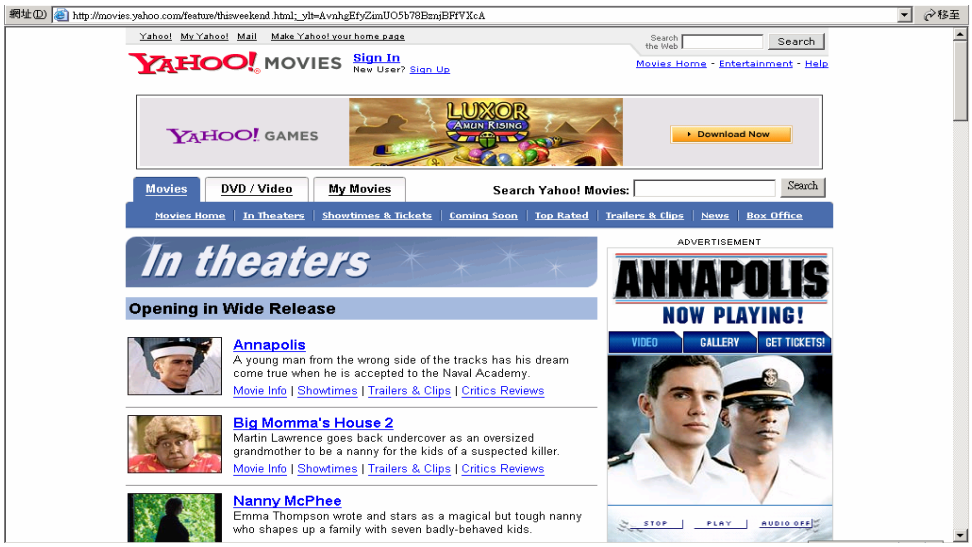


Figure 7-11 The user's web site record

IM Record

Step1. Click **Record → Service → IM**. (Figure 7-12)

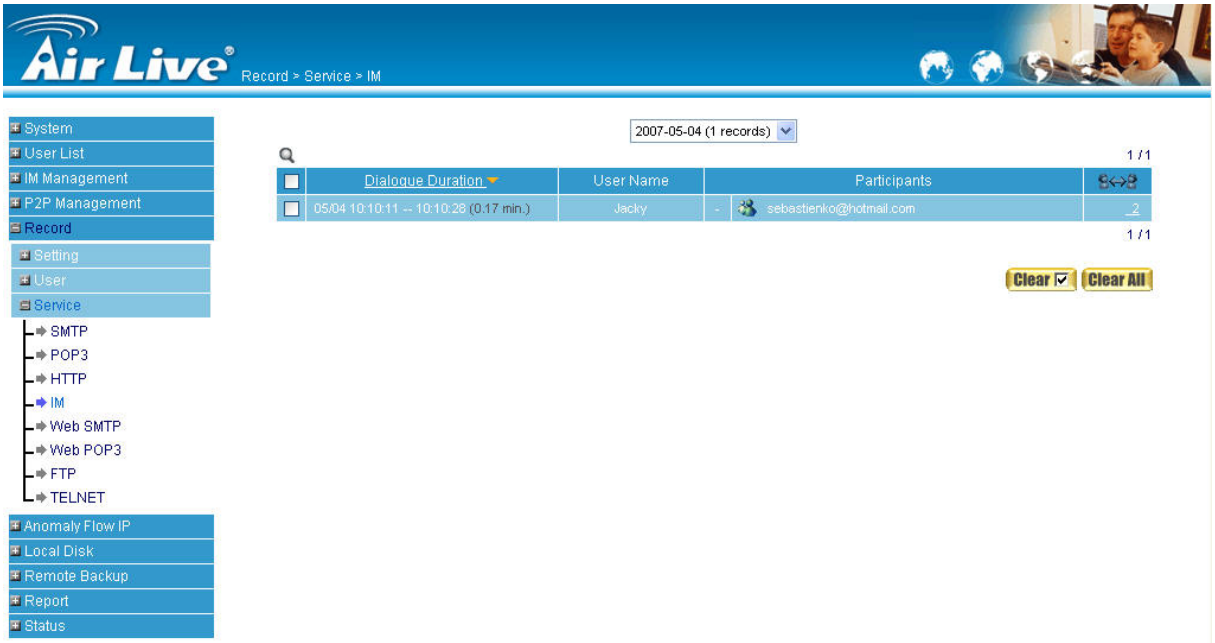


Figure 7-12 IM

Step2. Click the **IM** record to view. (Figure 7-13)

Figure 7-13 Click the IM record

Step3. It shows the communication contents. (Figure 7-14)

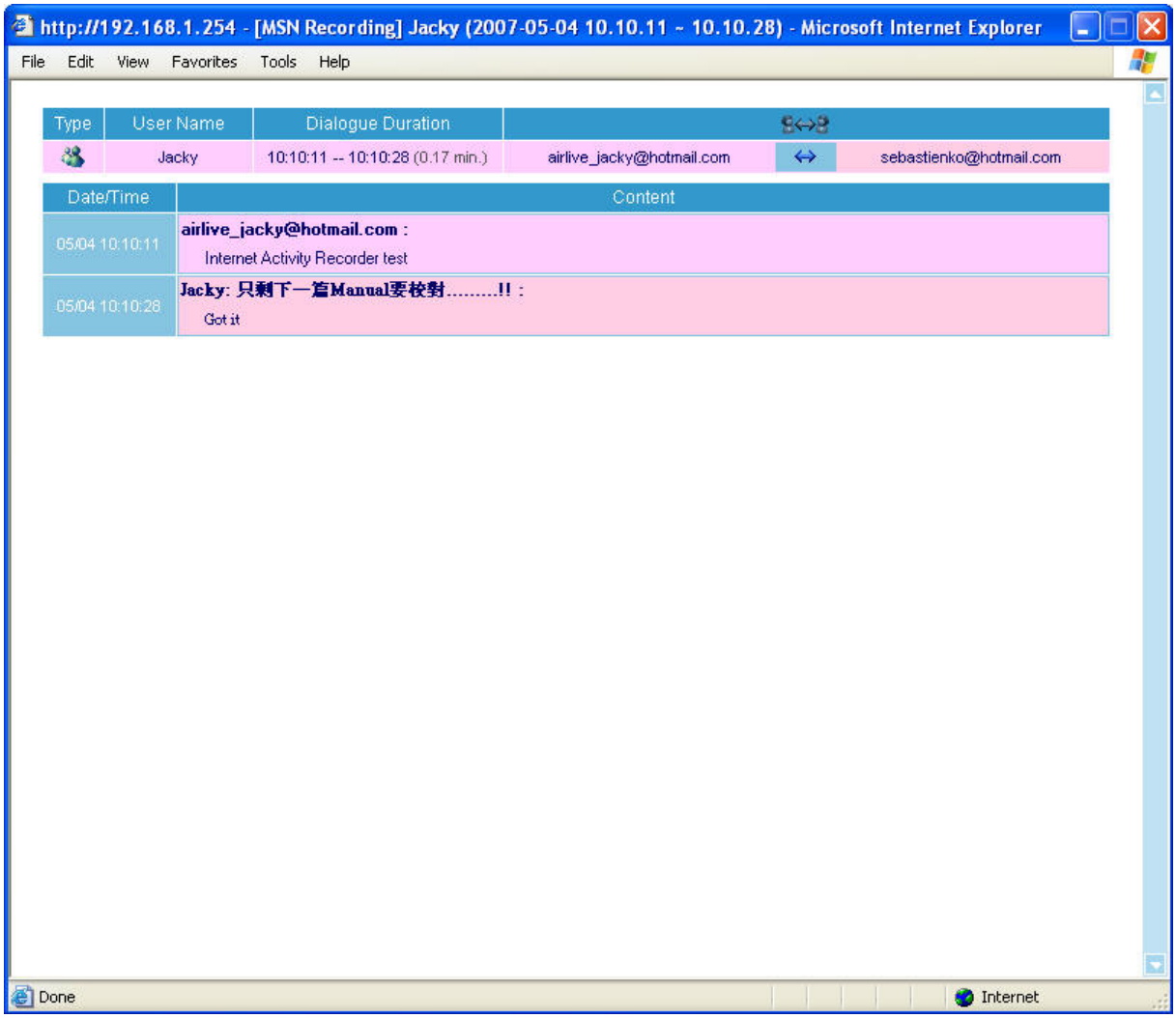


Figure 7-14 The communication contents

Web SMTP Record

Step1. Click **Record → Service → Web SMTP**. (Figure 7-15)

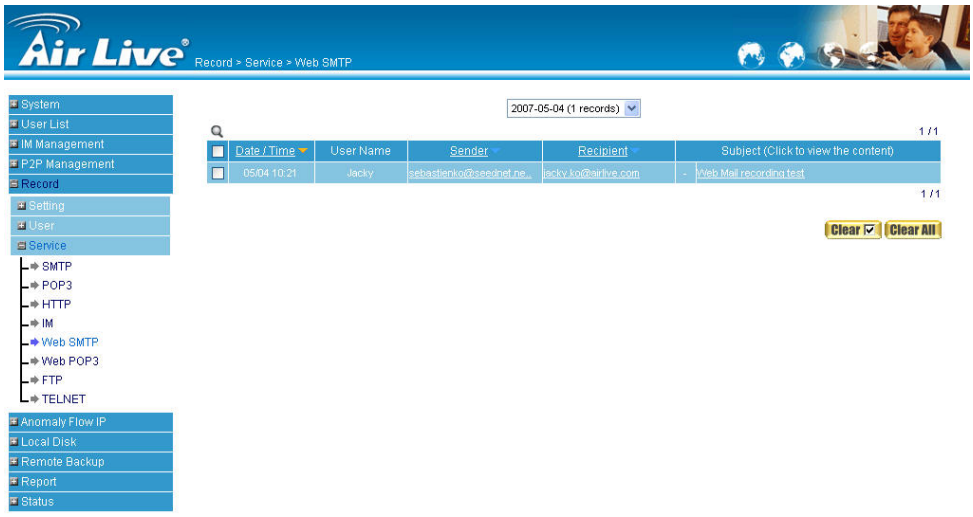


Figure 7-15 Web SMTP

Step2. Click **Subject** to view the e-mail content. (Figure 7-16)

Figure 7-16 Click the subject in Web SMTP

Step3. It shows the Web mail content sent by the user. (Figure 1-37)

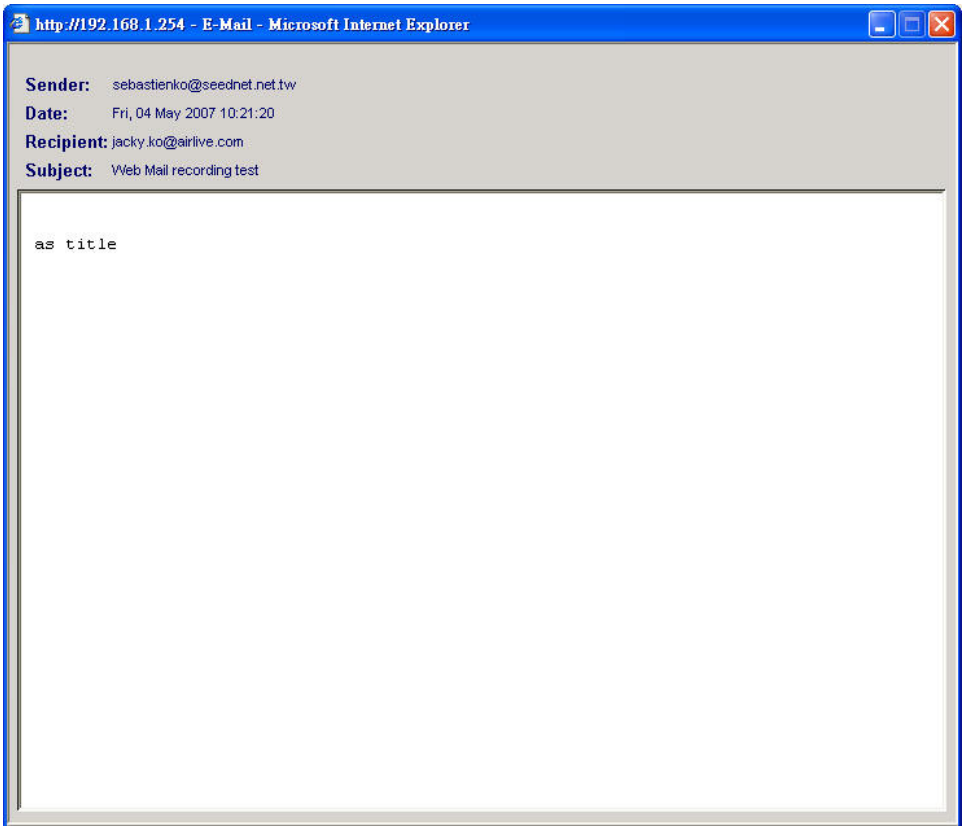


Figure 7-17 The mail content in Web SMTP

This window shows the mail content, and the user can select to view or save the attachment.

Web POP3 Record

Step1. Click **Record → Service → Web POP3**. (Figure 7-18)

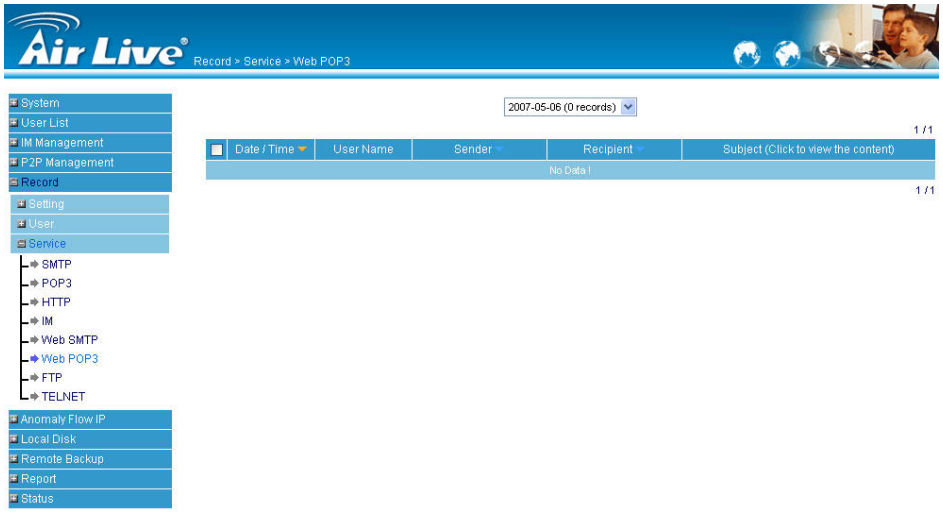


Figure 7-18 Web POP3

Step2. Click the **Subject** to view the mail content. (Figure 7-19)

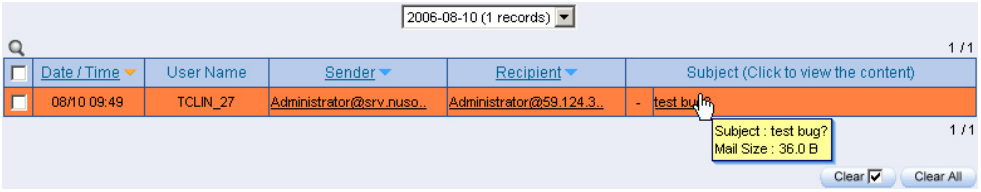


Figure 7-19 Click the subject in Web POP3

Step3. It shows the web mail contents browsed by the user. (Figure 7-20)

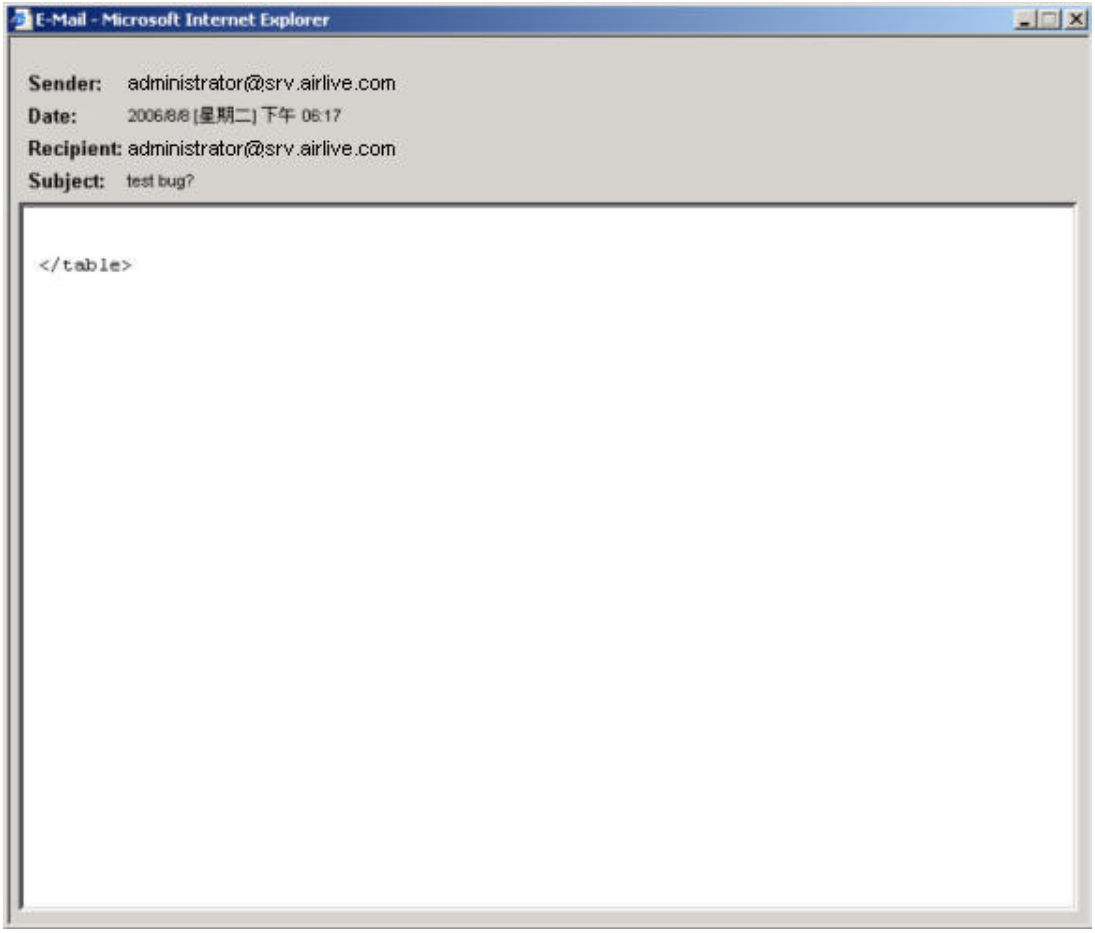


Figure 7-20 The mail content in Web POP3

It shows the mail content, and the user can choose to view or save the attachment.

FTP Record

Step1. Click **Record →Service →FTP**.

Step2. Click the FTP record to view. (Figure 7-21)

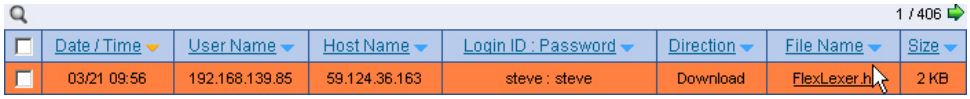


Figure 7-21 Click the FTP record

Step3. The user can select to open or save files via the FTP tools. (Figure 7-23)

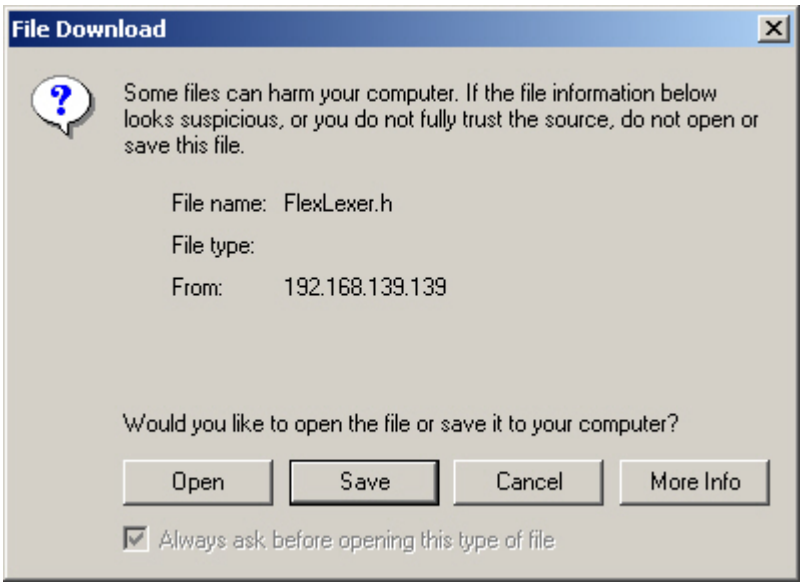


Figure 7-23 To open or save the file

Telnet Record

Step1. Click **Record → Service → TELNET**. (Figure 7-24)

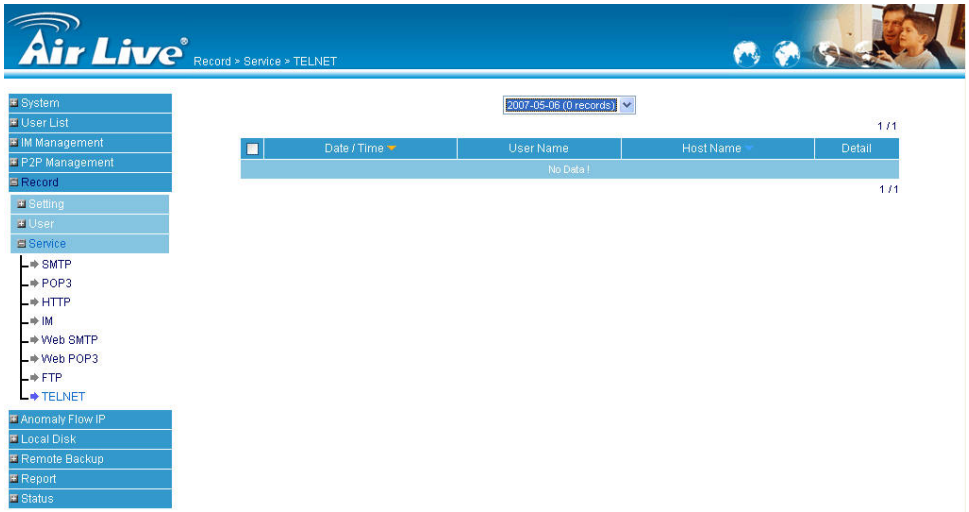


Figure 7-24 TELNET

Step2. Click the **TELNET** content to view.

Step3. It shows the TELNET content. (Figure 7-25)

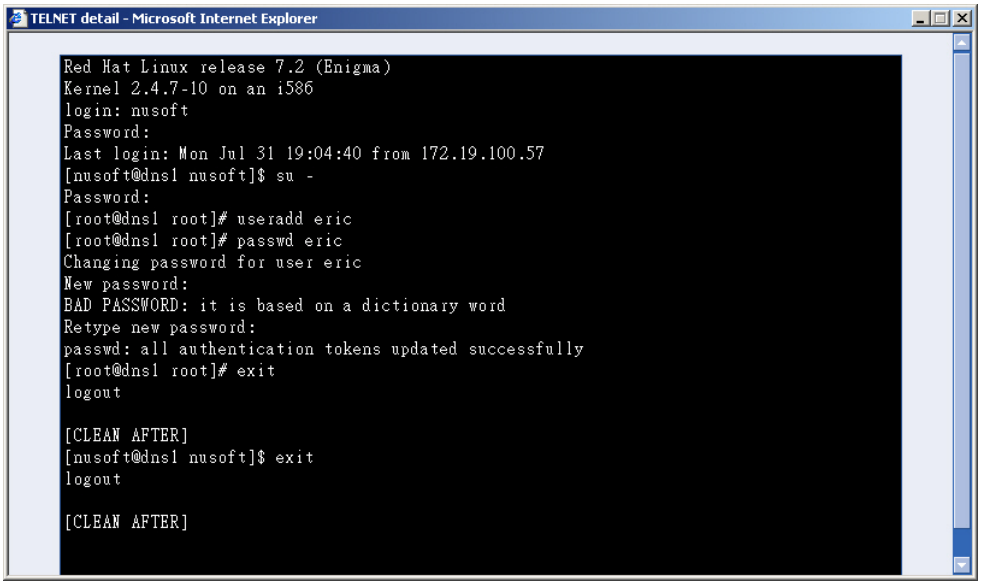


Figure 7-25 The TELNET content

Chapter 8 Anomaly Flow IP

IAR-5000 can block the internal anomaly mount of packets sent from external hackers and also included the mechanism of co-defense system, can enhance the enterprise network security and stability.

In this chapter, we will make the introduction and settings of Anomaly Flow IP.

The threshold sessions of anomaly flow (per source IP)

- When the session number (per source IP) has over the limitation of anomaly flow sessions per source IP, then IAR-5000 will take this kind of IP to be anomaly flow IP and make some actions. For example, block the anomaly flow IP or send the notification)

Anomaly Flow IP Blocking

- IAR-5000 can block the sessions of anomaly flow IP.

Notification

- IAR-5000 can notice the user and system administrator by e-mail or NetBIOS notification as any anomaly flow occurred.

Co-Defense System

- IAR-5000 has the co-defense mechanism which can integrate the switch, so that can enhance the enterprise network security protection.

Non-detected IP

- System administrator can set which IP address to be the non-detected IP, it is because some of these IP provide amount of services, so that will let IAR-5000 define it to be anomaly flow IP. We can use this function to avoid the problem.

Set the anomaly flow setting alarm and block the intrusion packets which sent by internal virus-infected PCs.

Step1. In **Anomaly IP → Setting** :

- Set The threshold sessions of anomaly flow(per source IP)（The default setting is 100 Session / Sec）.
- Select Enable Anomaly Flow IP Blocking , and set the Blocking Time（The default setting is 60 seconds）.
- Select **Enable E-Mail Alarm Notification**.
- Select **Enable NetBIOS Alarm Notification**.
- IP Address of Administrator, enter 172.19.100.254.
- Select enable co-defense system, and enter the IP address of switch, user name and password.
- Click OK.

Step2. Set the **Non-detected IP :**

- Click **New Entry.**
- Enter the **IP Address** and **Netmask**.（Figure 8-1）
- Click **OK**. (Figure 8-2)

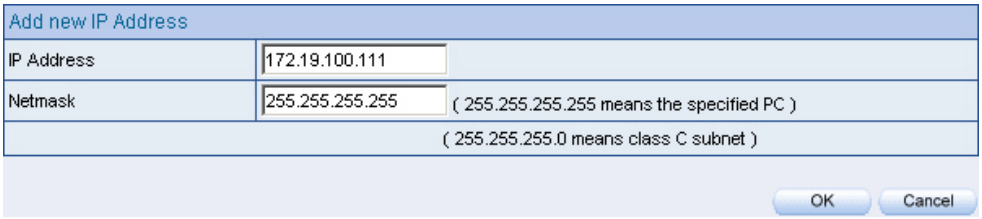


Figure 8-1 Enter the ip and netmask

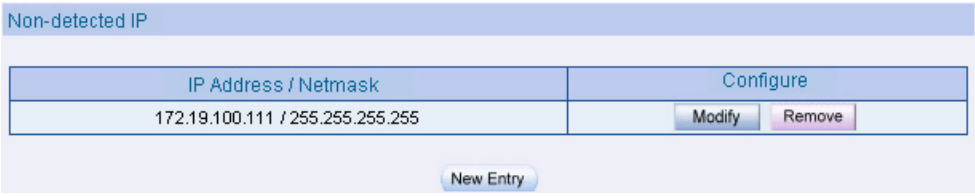


Figure 8-2 Complete the setting

After complete the alarm setting, if the system has detected that there are many intrusion packets, it will show the alert message in Virus – Infected IP, or send NetBIOS alert message to the virus – infected user and MIS engineer's PC. (Figure 8-3)

Threshold Sessions / Sec: 100

User Name	Virus-infected IP	MAC Address	Alarm Time
AIRLIVE_2007	172.19.50.7	00:01:80:5F:B0:6C	2006-02-23 15:49:52

Clear Download

Figure 8-3 The alarm message in internal virus–infected IP

If the system administrator selects **Anomaly Flow IP→ Setting→ Enable E-Mail Alert Notification,** the IAR-5000 will automatic send the mail to alarm the system administrator. (Figure 8-4)

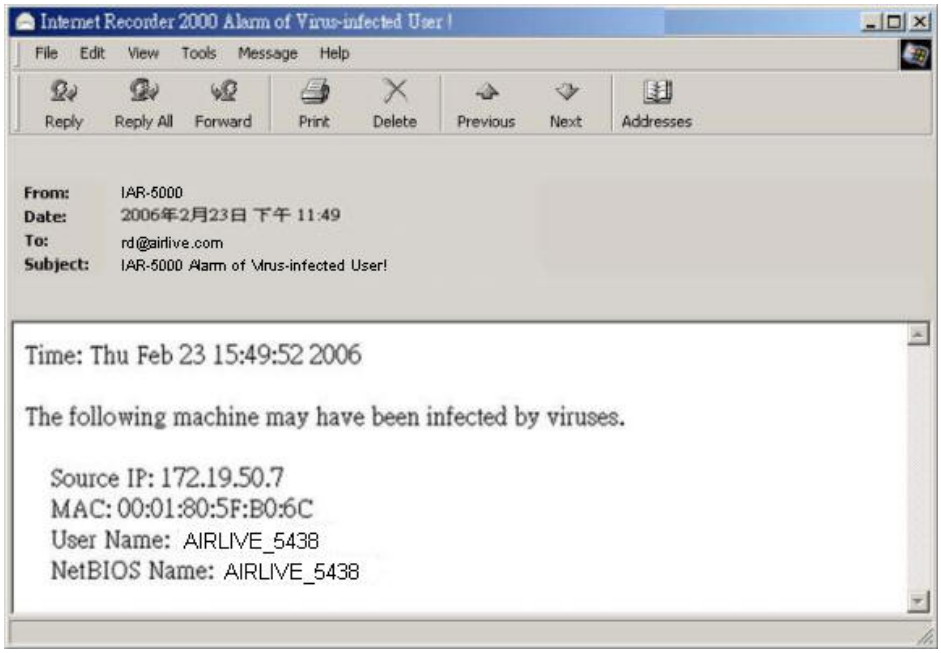


Figure 8-4 The E-Mail notification of virus – infected IP

When we complete the notification setting, the system will instant show the message at intrusion IP or send NetBIOS alarm notification to the invader and administrator 's PC after system has detected there are many intrusion packets from the external computer. (Figure 8-5)

Figure 8-5 The notification of intrusion IP

If the system administrator selects **Anomaly Flow IP → Setting → Enable E-Mail Alert Notification,** the IAR-5000 will automatic send the mail notification to system administration.

Chapter 9 Local Disk

MIS engineer can easily know the current disk utilization included disk space and the estimated disk utilization and percentage of 8 services depends on the storage time that MIS engineer had set.

9.1 Storage Time

Total Hard Disk Space

- The total hard disk space in IAR-5000.

Estimated Storage Utilization and Percentage

- IAR-5000 can estimate how much does the service utilization take part of total storage space and its percentage depends on daily average service flow and storage time. (Figure 9-1)

Average Size / Day ：

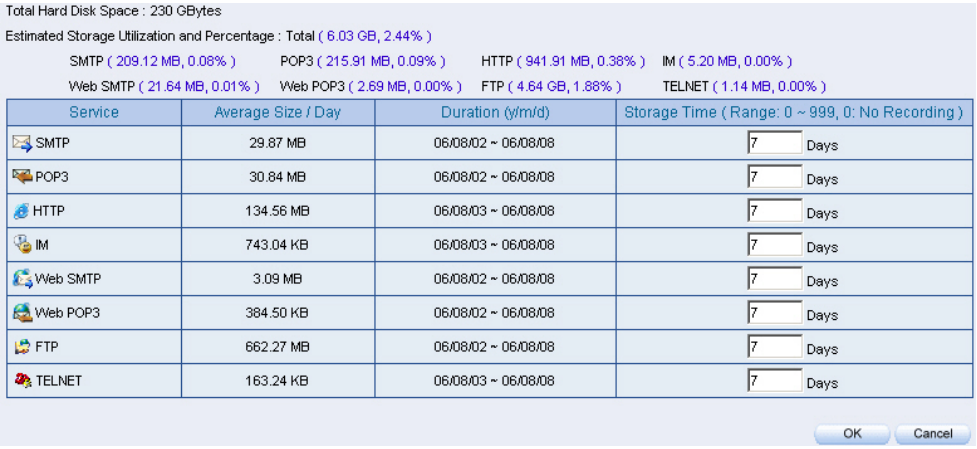
- The average flows in a day.

Duration (y / m / d)：

- It means the duration of storage time. Use A.D. mode to display, include the year, month, and date. For example, 06/01/15~06/02/15.

Storage Time ：

- We can set the storage time depends on the real network usage of the company. (0 day means **No Recording**).



Service	Average Size / Day	Duration (y/m/d)	Storage Time (Range: 0 ~ 999, 0: No Recording)
SMTP	29.87 MB	06/08/02 ~ 06/08/08	7 Days
POP3	30.84 MB	06/08/02 ~ 06/08/08	7 Days
HTTP	134.56 MB	06/08/03 ~ 06/08/08	7 Days
IM	743.04 KB	06/08/03 ~ 06/08/08	7 Days
Web SMTP	3.09 MB	06/08/02 ~ 06/08/08	7 Days
Web POP3	384.50 KB	06/08/02 ~ 06/08/08	7 Days
FTP	662.27 MB	06/08/02 ~ 06/08/08	7 Days
TELNET	163.24 KB	06/08/03 ~ 06/08/08	7 Days

Figure 9-1 The storage duration

9.2 Disk Space

Hard Disk Utilization : (Figure 9-2)

- The 8-recorded services are displayed in different colors, the white color represents the free disk space .Use the mouse point to each color, it shows the service name and the 8-recorded services utilization in the storage disk.

The 8-Recorded Services Utilization:

- It will arrange the TOP 10 user by the service utilization in graphic charts, it depends on the 8-recorded services of SMTP, POP3, HTTP, IM, Web SMTP, Web POP3, FTP, TELNET.

SMTP

NO.	User Name	MBytes	
1	172.19.50.6	96.16	45.99%
2	JOSH12	42.67	20.40%
3	JULIE	21.30	10.19%
4	DXJ	11.85	5.67%
5	COMPUTERCANDY	11.18	5.35%
6	Rayearth	10.44	4.99%
7	172.19.100.89	3.55	1.70%
8	172.19.100.81	2.55	1.22%
9	AIRLIVE-WIN	2.13	1.02%
10	172.19.100.71	1.64	0.78%

Total Used Disk Space: **209.12 MB**

POP3

NO.	User Name	MBytes	
1	172.19.100.82	46.19	20.93%
2	Rayearth	40.50	18.76%
3	JULIE	29.50	13.67%
4	172.19.100.46	19.52	9.04%
5	ADFIND1	18.96	8.78%
6	AIRLIVE-WIN	13.57	6.29%
7	172.19.100.71	7.07	3.28%
8	172.19.100.81	6.95	3.22%
9	COMPUTERCANDY	6.68	3.09%
10	JACKIE-PC	6.19	2.87%

Total Used Disk Space: **215.91 MB**

HTTP

NO.	User Name	MBytes	
1	172.19.50.11	149.02	18.31%
2	172.19.100.82	135.39	16.64%
3	AIRLIVE-WIN	108.67	13.35%
4	Rayearth	57.77	7.10%
5	COMPUTER001	37.11	4.56%
6	172.19.50.6	33.39	4.10%
7	172.19.100.45	28.63	3.52%
8	JU07	27.32	3.36%
9	COMPUTER001	27.31	3.36%
10	JERRY	20.51	2.52%

Total Used Disk Space: **813.72 MB**

IM

NO.	User Name	MBytes	
1	JERRY	2.38	53.38%
2	Rayearth	0.68	15.22%
3	172.19.100.31	0.59	13.29%
4	我是點六	0.59	13.29%
5	JULIE	0.12	2.78%
6	172.19.100.46	0.07	1.55%
7	172.19.50.6	< 0.01	0.19%
8	JACK54	< 0.01	0.10%
9	超級76	< 0.01	0.09%
10	DAVID	< 0.01	0.04%

Total Used Disk Space: **4.46 MB**

Web SMTP

NO.	User Name	MBytes	
1	JERRY	16.72	77.27%
2	172.19.100.45	4.03	18.64%
3	JOY-VMXP	0.77	3.54%
4	172.19.50.6	0.11	0.53%
5	TCLIN_27	< 0.01	0.01%
6	172.19.100.62	< 0.01	0.01%
7	JOSH12	< 0.01	0.01%
8	COMPUTER001	< 0.01	0.00%
9	172.19.50.11	< 0.01	0.00%
10	172.19.50.16	< 0.01	0.00%

Total Used Disk Space: **21.64 MB**

Web POP3

NO.	User Name	MBytes	
1	JERRY	1.28	47.55%
2	172.19.50.16	1.03	38.36%
3	172.19.50.6	0.19	7.04%
4	TCLIN_27	0.15	5.69%
5	COMPUTER001	0.02	0.60%
6	JOSH12	< 0.01	0.33%
7	Rayearth	< 0.01	0.18%
8	我是點六	< 0.01	0.11%
9	172.19.100.82	< 0.01	0.10%
10	JACKIE-PC	< 0.01	0.03%

Total Used Disk Space: **2.69 MB**

FTP

NO.	User Name	GBytes	
1	Rayearth	2.58	55.66%
2	172.19.100.81	1.25	26.89%
3	172.19.100.45	0.44	9.51%
4	172.19.100.82	0.31	6.60%
5	JOSH12	0.05	1.08%
6	SIMSAN	< 0.01	0.19%
7	JERRY	< 0.01	0.04%
8	172.19.50.11	< 0.01	0.03%
9	172.19.100.31	< 0.01	0.00%
10	SIMSAN	< 0.01	0.00%

Total Used Disk Space: **4.64 GB**

TELNET

NO.	User Name	KBytes	
1	172.19.100.82	584.22	59.65%
2	JERRY	90.49	9.24%
3	DAVID	75.09	7.77%
4	SUKENT77	75.94	7.75%
5	172.19.100.31	72.63	7.42%
6	COMPUTERCANDY	22.99	2.35%
7	172.19.100.46	17.69	1.81%
8	DXJ	9.67	0.99%
9	JUSTIN72	9.11	0.93%
10	JERRY	5.47	0.56%

Total Used Disk Space: **979.43 KB**

Figure 9-2 The Storage disk information

Chapter 10 Remote Backup

MIS engineer can backup the IAR-5000 recorded files to remote NAS or file server.

Advantages of remote backup：

1. No storage limitation.

2. To avoid losing recorded files. For example, the records are removed by IAR-5000 when over the storage time or system makes the unpredictable errors.

3. MIS engineer can still browse the remote share directory which contains the backup files. Please refer to **Chapter 6 (Service)** for more information.

Remote Hard Disk

- It is where the remote share directory located.

Connection Status of Remote Hard Disk

- **Connection Status**：To show if IAR-5000 can connect to remote hard disk.
- **Disk Space for Backup**：To show the needed disk space for backup.
- **Hard Disk Utilization**：To show the total remote hard disk space and remained disk space.

E-mail Setting

- IAR-5000 will send the mail notice to recipient after backup completed.

Backup Setting

- **Backup Path**：MIS engineer can set the IP address, Computer Name, Shared Directory Name, Login ID and Password.
- **Service**：Select the Service type to backup.
- **Backup starts at**：MIS engineer can set the specific time to process automatic remote backup.

Backup Immediately

- MIS engineer can set IAR-5000 to backup the record at specific time.

Browse Setting

- If the backup directory is full, then MIS engineer can modify the setting and backup the files to the other directory. If MIS engineer want to check the original backup records then he can make the Browse Setting and see the contents of backup directory in **Remote Backup → Service.** But IAR-5000 still backup the record to the assigned backup directory according to the setting of **Remote Backup → Backup.**

  - Assume the MIS engineer has set a backup directory for each month, for example, **July 2006**, **August 2006**, **September 2006, October 2006** etc. **Now is October 2006**, so that all the backup records will be recorded in this folder of **October 2006**. But if MIS engineer want to look up the record in **July 2006** then he must set the **backup folder to be July 2006** in **Remote Backup → Setting → Browse.** And he can also look up the record in July 2006 in **Remote Backup→ Service**.

To set the backup folder

Step1. Select **The recorder appliance sends mail notice after backup had completed** (Figure 10-1)

Figure 10-1 Set the mail notice setting

Step2. To set the backup path.

- Enter the Computer Name / IP.
- Enter the name of Shared Directory.
- Enter the login ID for IAR-5000 to login.
- Enter the password for IAR-5000 to login (Figure 10-2)

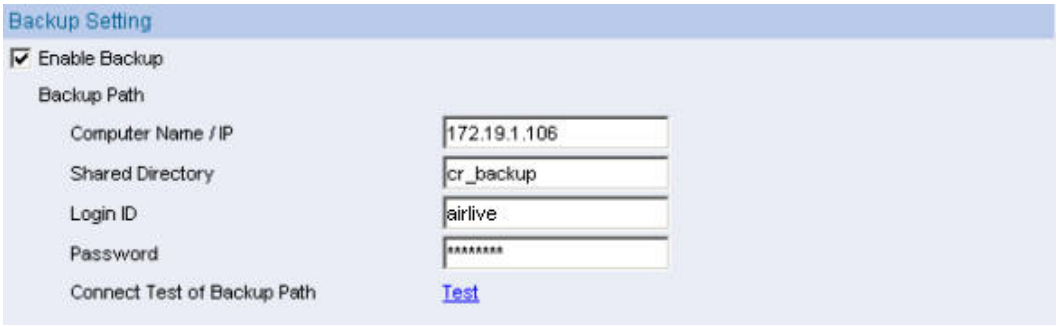


Figure 10-2 Set the backup path

Step3. Click **Test** ,and system shows a pop up window. MIS engineer can click **Connection Test** to see if IAR-5000 can connect to the remote shared directory. (Figure 10-3)

Figure 10-3 To test if IAR-5000 can connect to remote backup folder

Step4. Select the **Service** type to backup and also choose the backup time then click **OK.** (Figure 10-4)

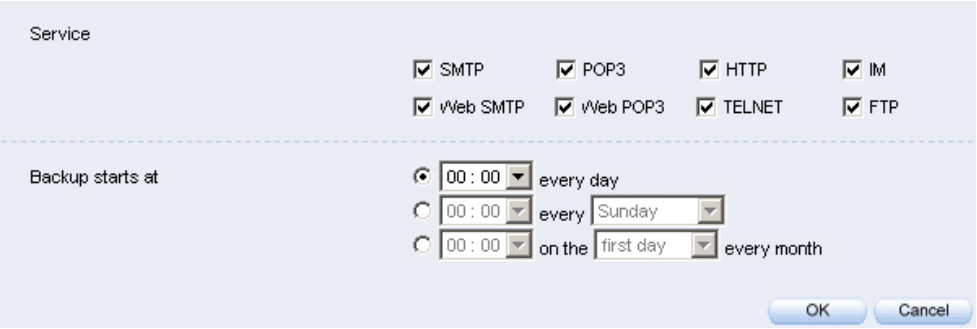


Figure 10-4 Select the service to backup and choose backup time

◆ If IAR-5000 can connect to the remote backup disk then system will show the message in Connection Status of Remote Hard Disk (Figure 10-5)

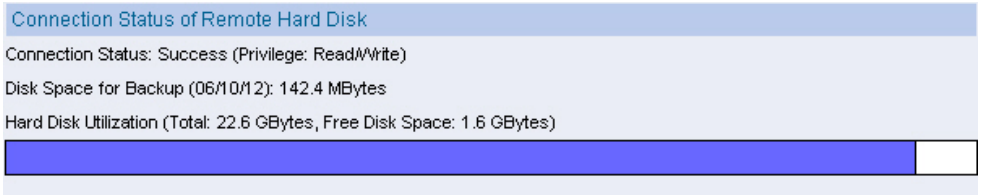


Figure 10-5 Connection Status of Remote Hard Disk

Step5. The IAR-5000 will backup the records to the IP address that MIS engineer had set in **Backup Setting → Computer Name / IP** at **00:00 AM**. (Figure 10-6)

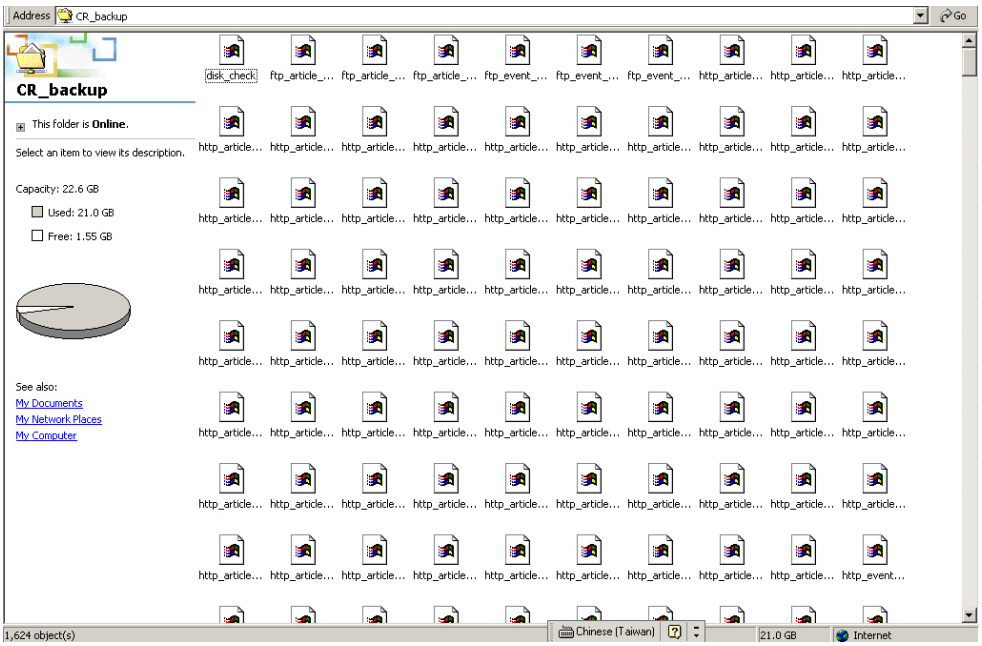


Figure 10-6 Remote shared directory

To set Backup Immediately

Step1. Select the backup time.

Step2. Select the service type to backup.

Step3. Click **OK** (Figure 10-7)

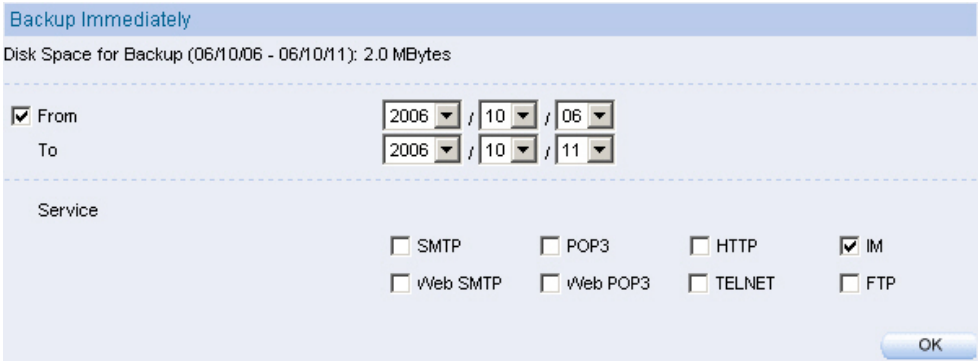


Figure 10-7 Set backup immediately

Step4. IAR-5000 will send mail notice after backup completed. (Figure 10-8)

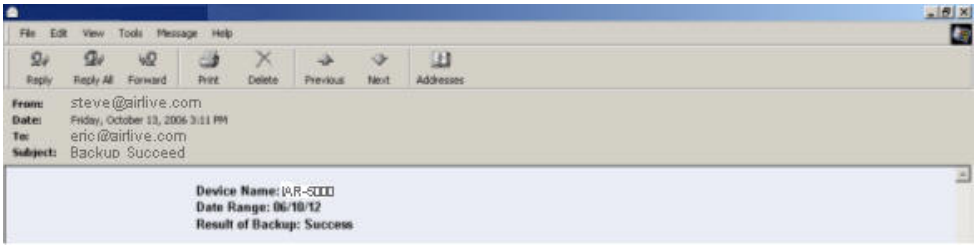


Figure 10-8 Send the mail notice after backup completed

Backup the record of Shared Directory

If MIS engineer want to backup the remote backup record of shared directory to other place, for example, to backup the contents by Compact Disc or backup the records of specific day to other folder, then MIS engineer must prepare the following files.

- The way to name the files in shared directory is **Service name_File type_Date. Extension file name.** The most important thing are the service name and date, that means **MIS engineer need to backup the files which contain the same service name and date.**
  - Not every data type of service name is the same. **For example, HTTP includes 3 types of article, event and icon.**
  - Every data type contains 3 extension file name of **frm, MYD and MYI**.
  - Assume that MIS engineer want to back up the http records on 11th September 2006, then it will at least contain 9 files (**3 data types multiply 3 extension file name**.)

    http_article_20060911.frm
    http_article_20060911.MYD
    http_article_20060911.MYI
    http_event_20060911.frm
    http_event_20060911.MYD
    http_event_20060911.MYI
    http_icon_20060911.frm
    http_icon_20060911.MYD
    http_icon_20060911.MYI

- To backup all the files ignore the elements of which **date, service and service name**.
  - ip_country.frm
  - user.frm
  - user.MDY
  - user.MYI

- The IM record contains 3 plus extension files which not included date. So MIS engineer also need to backup these 3 extension files when processing IM records backup：
  - im_own_alias_.frm
  - im_own_alias_.MYD
  - im_own_alias_.MYI

■ All data types of every service category：

Service Name	Data Type		
HTTP	article	event	icon
FTP	article	event	
IM	article	article_file	event
SMTP	article	event	
POP3	event	event	
Telnet	article	event	
WEB SMTP	Ms_article	Ms_event	Ms_event_att
WEB POP3	Mr_article	Mr_event	Mr_event_att

Set Browse Folder

Step1. Set the backup folder to browse. And the way to set **Browse Setting** is the same as **Backup Setting**. (Figure 10-9)

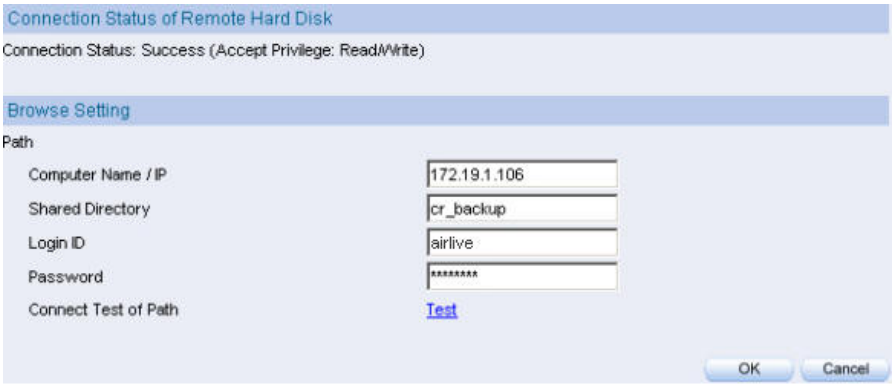


Figure 10-9 Set the browse setting

Step2. MIS engineer can see the record contents saved in remote shared directory in **Remote Backup → Service** after MIS engineer had completed the **browse setting.**

Chapter 11 Report

The report can display the flow status and data in storage disk by the graphic charts. It also can mail the statistics report to specific e-mail address depends on the administrator's demand.

The report included three main parts：**Setting, Flow report and Storage report**. In this chapter, we will make the introduction of these three sections.

Periodic Report:

- Send the report to the recipient periodically, depends on the date of selected report.

History Report:

- Mail the specific report to the recipient
  - In Report → Setting , select Enable E-mail Periodic report, and make the settings：
    1. Select yearly report, monthly report, weekly report and daily report.（Figure 11-1）
    2. Click OK.
    3. The IAR-5000 will send the storage report to the recipient when the time arrived.
    4. In History Report, choose the selected date to mail.（Figure 11-2）
    5. Click **Send Report**.
    6. It will mail the related statistics report to the user. (Figure 11-3)

The way to result the periodic report:

1. Yearly Report: It results the report at 00:00 AM, January yearly.
2. Monthly Report：It results the report at 00:00 AM of the first day monthly.
3. Weekly Report：It results the report at 00:00 AM of the first day weekly.
4. Daily Report ：It results the report at 00:00 AM daily.

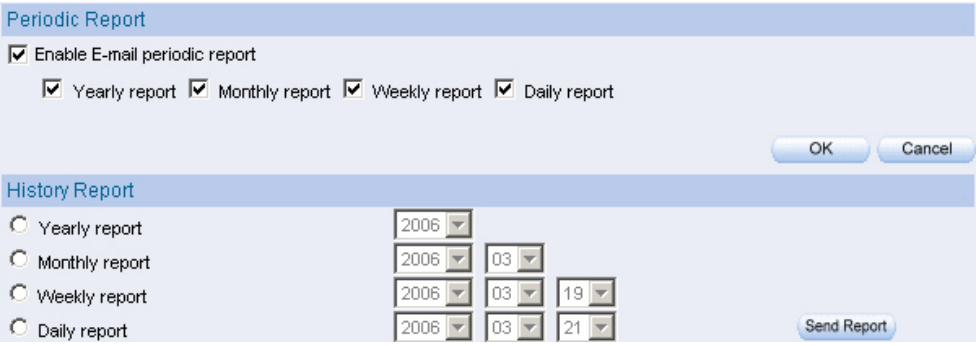


Figure 11-1 The periodic report setting

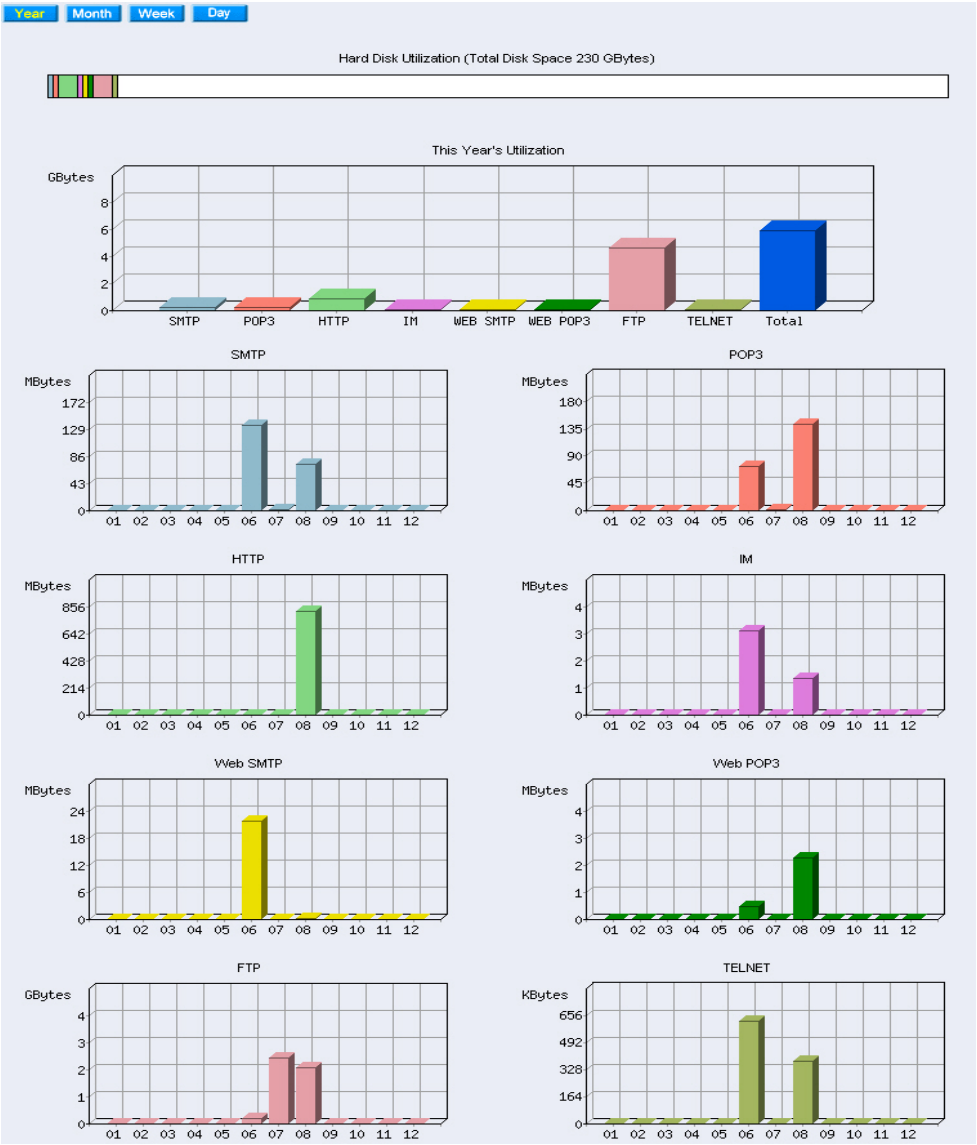


Figure 11-2 The storage report

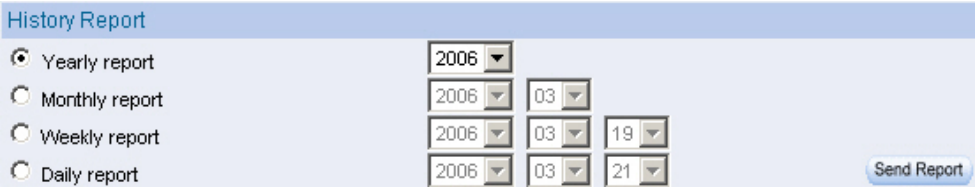


Figure 11-3 The history report mail setting

Figure 11-6 The storage report

The IAR-5000 will mail the statistics report to recipients by PDF attachment.

In Record → Service, it contains the 8 different services as the same as the record in Storage Report. It shows the status of storage space and flow report. The Storage Report is displayed in , , , .

Step1. **Hard Disk Utilization**：The 8 services are record in different colors. When the mouse point to the colors, it will show the service name and the usage space. (Figure 11-7)

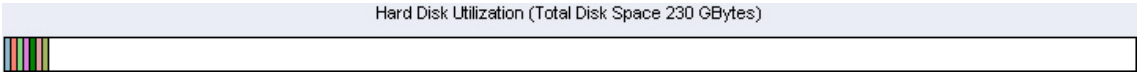


Figure 11-7 The hard disk utilization

Step2. **Today's Utilization**, it is displayed in Day . (Figure 11-8)

- **Ordinate**：The service flow, its unit is Mbytes.
- **Horizontal ordinate**：The service name.

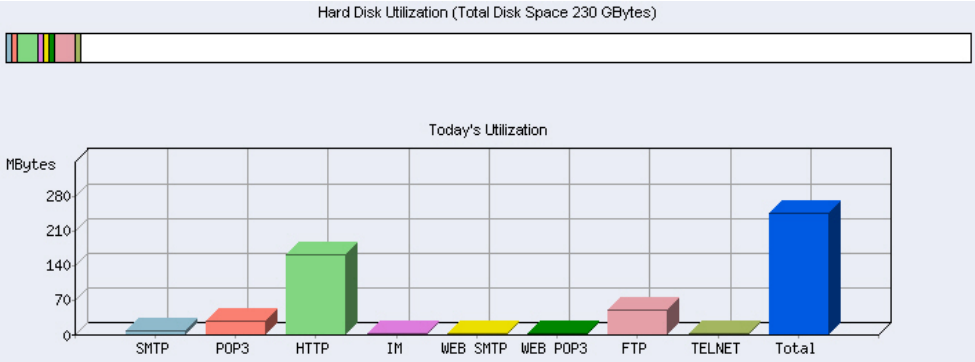


Figure 11-8 The percentage of the service record in hard disk utilization

Step3. According to the time unit in every service. It is displayed in Day. (Figure 11-9)

- **Ordinate**：The service usage. Its unit is Mbytes.
- **Horizontal ordinate**：It represents the Time.

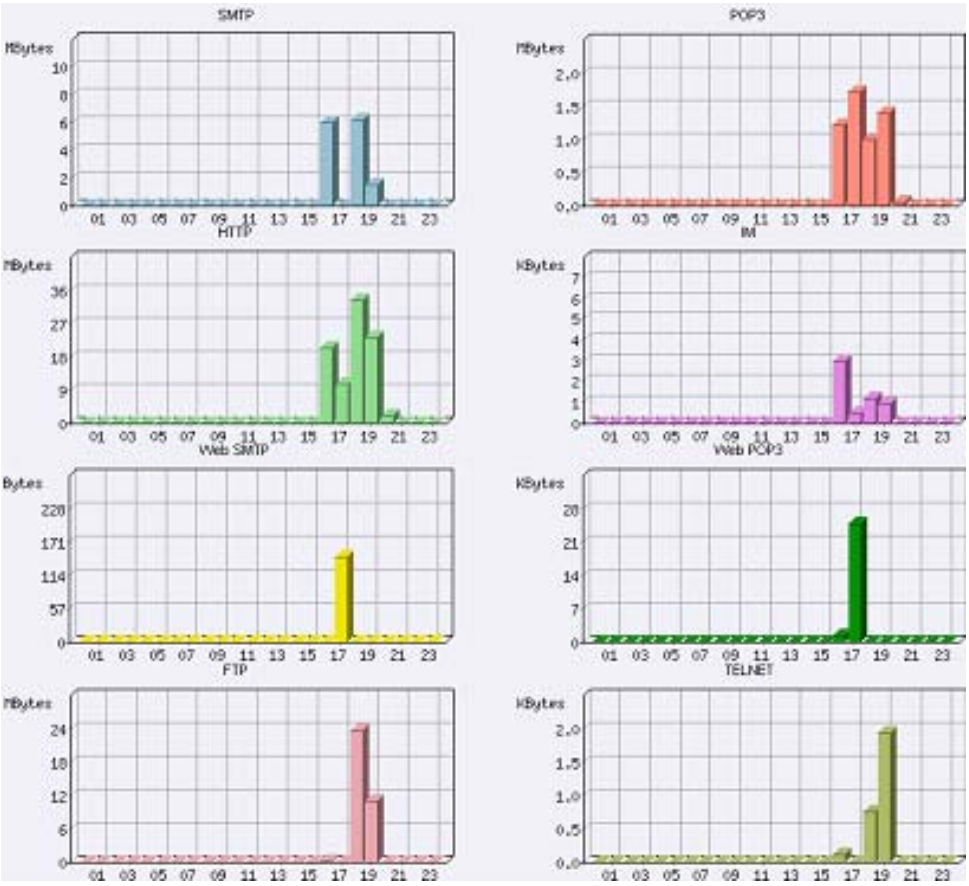


Figure 11-9 The storage report of every service

Chapter 12 Status

To know about the system information, ARP table, 8 services records and event log of IAR-5000.

1. **System Info:** It shows the IAR-5000 CPU utilization, hard disk utilization, memory utilization and ram disk utilization.

2. **ARP Table:** To record all the host ARP connected to IAR-5000.

3. **Session Record:** It shows the current 8 services connection information.（HTTP, FTP, POP3, SMTP, IM, TELNET, Web Mail）

4. **Event Log:** It records every events occurred in IAR-5000, such as modify settings, anomaly flow alert, forward mails, delete files and etc.

System Info

Step1. In **Status → System Info**, it shows the current system information of IAR-5000. (Figure 12-1)

- **System Uptime**：The cumulate time in the IAR-5000 until the current time.
- **CPU Utilization**：The CPU utilization in IAR-5000.
- **HardDisk Utilization**：The hard disk utilization in IAR-5000.
- **Memory Utilization**： The memory utilization in IAR-5000.
- **RamDisk Utilization**：The ramdisk utilization in IAR-5000.

Figure 12-1 The system info

ARP Table

Step1. In **Status → ARP Table**, it shows the information of user name, computer name, IP address and MAC address connected to the IAR-5000. (Figure12-2)

- **User Name**：The identified name of record in the computer.
- **Computer Name**：The identified name on the internet in this computer.
- **IP Address**：The IP address on the internet in the computer.
- **MAC Address**：The identified address in the network adapters in the computer.

User Name	Computer Name	IP Address	MAC Address
192.168.139.33	----	192.168.139.33	00:E0:18:25:F4:BC
AIRLIVE_5438	AIRLIVE_5438	192.168.139.193	00:01:80:5F:B0:6C

Figure 12-2 The ARP table in Web UI

Session Record

Step1. In **Status → Session Record** Info, it shows the current 8 services connection information （HTTP, FTP, POP3, SMTP, IM, TELNET, Web Mail）(Figure 12-3)

- Select the refresh time period in **Manually drop down menu**. Or click **Refresh**, and system will instantly refresh the connection record information.
- Click the service item to view, then system shows all connections of the chosen items. (Figure 12-4)
- Click , to search the related connection information. (Figure 12-5)

Refresh | Manually | 1 / 1

Service	Total Traffic	Established / Unreplied Number	Session Number
ALL	30.5 MB	2536 / 1	2537
FTP	22.1 MB	1991 / 0	1991
HTTP	7.8 MB	421 / 1	422
POP3	204.7 KB	70 / 0	70
SMTP	360.8 KB	45 / 0	45
IM	59.9 KB	7 / 0	7
WebMail	37.0 KB	2 / 0	2

1 / 1

Figure 12-3 Connection record

IM Service

Refresh | Manually | 1 / 1

User Account	Source IP	Destination IP	Port	Start Time	Traffic	Status
support@airlive.com	JOSH12	207.46.2.86	TCP 1056 => 1863	09:21:01	11.7 KB	Established
AIRLIVE_LAB_1	JERRY	scs.msg.yahoo.com	TCP 1035 => 5050	09:17:23	3.6 KB	Established
airlive01@hotmail.com	Rayearth	207.46.4.81	TCP 1046 => 1863	07:31:43	62.9 KB	Established
239408604	JACKIE-PC	219.133.63.15	UDP 4000 => 8000	22:34:10	202.1 KB	Established
	超級76	64.12.24.86	TCP 2009 => 5190	21:45:09	686.0 B	Established
airlive01@hotmail.com	Rayearth	207.46.7.13	TCP 1529 => 80	18:17:15	40.6 KB	Established
	172.19.100.45	207.46.0.64	TCP 57105 => 1863	18:16:27	248.0 B	Established
airlive01@hotmail.com	Rayearth	207.46.0.82	TCP 1439 => 1863	17:53:26	42.4 KB	Established
iack@airlive.com	JACK54	207.46.27.91	TCP 33946 => 1863	17:35:51	5.4 KB	Established
julie@airlive.com	JULIE	207.46.26.36	TCP 1558 => 1863	16:50:41	1.0 KB	Established
	172.19.100.82	LL-220-229-124-252.L...	TCP 35630 => 443	16:13:39	105.9 KB	Established
joy_airlive@hotmail.c...	172.19.100.45	207.46.27.15	TCP 59750 => 1863	14:58:57	2.5 KB	Established
iack@airlive.com	JACK54	207.46.24.23	TCP 33564 => 1863	14:16:52	57.8 KB	Established
372136019	AIRLIVE-20-9	219.133.38.232	TCP 1120 => 80	11:24:59	12.0 KB	Established
airlive01@hotmail.com	Rayearth	207.46.4.52	TCP 1315 => 1863	09:50:20	261.6 KB	Established

1 / 1

Figure 12-4 System shows all connection information

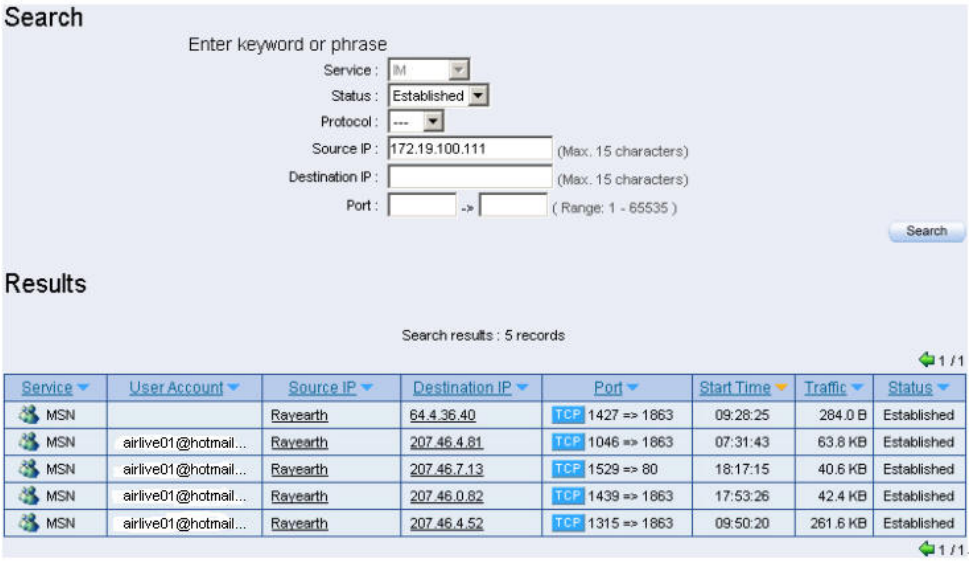


Figure 12-5 Search the related connection information

Event Log

Step1. In **Status → Event Log**, it records events occurred in IAR-5000, such as modify settings, anomaly flow alert, forwarding mails, file delete action and etc. (Figure 12-6)

- Click , and search the event. (Figure 12-7)
- Click , IAR-5000 shows the event information in detail. (Figure 12-8)

1 / 9

Date / Time	Admin Name	IP Address	Event	Detail
Aug 9 08:54:25	admin	172.19.20.13	[Login] Success	-
Aug 9 00:00:01	---	LOCALHOST	[FGuard] Delete outdated records according to Storage Time setting (service(d..	-
Aug 8 21:26:22	admin	172.19.100.31	[IM Policy] Remove 3 Account	
Aug 8 21:25:02	admin	172.19.100.31	[IM Policy] Drop 4 Account	
Aug 8 21:24:19	admin	172.19.100.31	[IM Policy] Acceop 28 Account	
Aug 8 21:24:00	admin	172.19.100.31	[IM Policy] Acceop 1 Account	
Aug 8 21:21:50	admin	172.19.100.31	[IM Policy] Acceop 1 Account	
Aug 8 21:20:14	admin	172.19.100.31	[IM Policy] Drop 28 Account	

Figure 12-6 Event log

Search

Enter keyword or phrase

Event : Non-detected IP

From : 2006 / 7 / 19 9 : 29

To : 2006 / 8 / 9 9 : 32

Search

Results

Search result: 3 records

Download View: 1 - 3 1 / 1

Date / Time	Admin Name	IP Address	Event	Detail
Aug 8 16:54:52	admin	172.19.20.13	[Anomaly Flow IP] Add Anomaly Flow Non-detected IP 172.19.100.111	
Jul 25 14:45:39	admin	172.19.100.57	[Anomaly Flow IP] Add Anomaly Flow Non-detected IP 172.19.100.57	
Jul 25 14:45:30	admin	172.19.100.57	[Anomaly Flow IP] Remove Anomaly Flow Non-detected IP 172.19.100.57	

1 / 1

Figure 12-7 Search the events

Event Log Detail - Microsoft Internet Explorer

Date / Time	Admin Name	IP Address	Event
Aug 8 16:54:52	admin	172.19.20.13	[Anomaly Flow IP] Add Anomaly Flow Non-detected IP 172.19.100.111

Detail

Add new IP Address	
IP Address	172.19.100.111
Netmask	255.255.255.255 (255.255.255.255 means the specified PC)
(255.255.255.0 means class C subnet)	

Figure 12-8 System shows event log in detail