

# IAR-5000

Internet Activity Recorder

8

# **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

<u>Clause</u>	<b>Description</b>
■ EN 55022:1998/A1	Limits and methods of measurement of radio disturbance
:2000/A2:2003	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/	Disturbances in supply systems caused by household appliances
A1:2001	and similar electrical equipment "Voltage fluctuations"
■ EN 55024:1998/A1	Information Technology equipment-Immunity characteristics-Limits
:2001/A2:2003	And methods of measurement
■ CE marking	CE

■ CE marking

Manufacturer/Importer

Signature : Name : Position/ Title :

Albert Yeh Vice President

Date : 2006/4/20

(Stamp)

## RS-4000 / IAR-5000 CE Declaration Statement

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

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' reputation

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 des.

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 a section 1 above.

#### 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 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 for 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 base the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this Licens

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, 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 The source code for a work means the preferred form of the work for making induitications 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 you do not 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 7. In, as a consequence or a court judgment or allegation to paterin infiningement or nor any outer reason (not infinited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradic the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satify 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 Porgram by all those who receive cocies 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 warranty of MERCHANT 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 Fun	ctions and Features	4
1.2 Dep	loyment	5
1.3 Fror	nt Panel	5
1.4 Pac	king List	6
Chapter 2	Software Installation	7
Chapter 3	System	13
3.1 Adm	nin	16
3.2 Inte	rface IP	18
3.3 Sett	ing	19
3.4 Date	e/Time	23
3.5 Peri	nitted IP	25
3.6 Log	out	26
3.7 Soft	ware Update	27
Chapter 4	User List	28
Chapter 5	IM Management	39
5.1 Con	figure	40
5.2 Auth	nentication	42
5.3 Rule	Э	95
Chapter 6	P2P Management	110
Chapter 7	Record	112
7.1 Sett	ing	112
7.2 Use	r	114
7.3 Serv	<i>v</i> ice	119
Chapter 8	Anomaly Flow IP	131
Chapter 9	Local Disk	135
9.1 Stor	age 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	र Green On		Power on the device
Hard Disk	Green	Blinking	Data reading / accessing
	Green	Blinking	Sending / Receiving
Port1	Orange	On	100 Mbps
5	Green	Blinking	Sending / Receiving
Port2	Orange	On	100 Mbps

#### Ports:

Port	Description
	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 <a href="http://192.168.1.1">http://192.168.1.1</a> •
- 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

Enter Netv	vork Passwor	d	? ×
<b>?</b> >	Please type yo	our user name and password.	
2	Site:	172.19.0.1	
	Realm	Internet Recorder Administration Tools	
	User Name	admin	
	Password	****	
	🔽 Save this p	password in your password list	
		OK Can	cel

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).

V	Vizard Setup
ſŢ	is Wizard will guide you to complete every setting. Please click [ Next ] to start.
	Next >
	Figure 2-2 Enter the setting wizard
Step5.	Select the language (System will change to the selected language automatically) and click <b>Next</b> (Figure 2-3).

Step 1: Language Setting	
Please select the User Language Web UI and click [ Next ].	
Language Setting : English Version	
	Next >
Figure 2-3 Select the language	

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

tep 2 : Synchronize system clock	
Enable synchronize with an Interne	t time Server
Set offset +8 💌 hours from GI	MT Assist
Enable daylight saving time set	ting
From 1 V 1 To	1 💌 / 1 💌
Server IP / Name 0.0.0.0	Assist
Update system clock every 0 system booting )	minutes ( Range: 0 ~ 99999, 0 : refers to update during

< Back | Next >

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).

Step 4 : Network Deployment Mode

Please select a kind of Network Deployment Mode, then click [ Next ].

- Bridge Mode : Link one of this device's ports to firewall or gateway, the other port connects to the internal network via hub or switch.
- · Sniffer Mode : Link one of this device's port to the mirror port of core switch or any port of the hub
- Bridge Mode
- O Sniffer Mode( Port 1 : Mirror Port, Port 2 : Management Port )



Figure 2-6 Select the Network Deployment Mode

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

Step 5 : User Name	e binds to IP / MAC Address
User Name-IP bindi The log can be re will be decide to be the static IP.	ng : cord depends on the user's IP address, when it comes from the same IP address, e same user.The function is especially focus on the Corporation which use the
<ul> <li>User Name-MAC bi The log can be re address, will be decide Company use the DHC</li> </ul>	inding : cord depends on the user's MAC address, when it comes from the same MAC e to be the same user.Normally, the user's IP is the dynamic IP address (The :P).
Please select one of th	ne combinations and click [ Next ].
User Name binds to :	P Address
	C MAC Address
	< Back Next >
	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.

[Next].		
IP Address	; 192.168.1.2	254
Netmask	255.255.25	5.0
Default Gateway	192.168.1.1	
DNS Server 1	: 168.95.1.1	
DNS Server 2	:	
Enable VLAN of Port 1		
VLAN ID	:	(Range: 0 ~ 4095)
Enable VLAN of Port 2		
VLAN ID	:	(Range: 0 ~ 4095)
Max. Downstream Bandwidth	: 102400	Kbps (Range: 1 ~ 102400)
Max. Upstream Bandwidth	: 102400	Kbps (Range: 1 ~ 102400)

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).

Please enter the IP Address, N [Next].	etmask, Defau	It Gateway, DNS Server, VLAN ID and Bandwidth. Click
IP Address	192.168.1.2	254
Netmask	255.255.25	5.0
Default Gateway	192.168.1.1	
DNS Server 1	: 168.95.1.1	
DNS Server 2	:	
Enable VLAN of Port 1		
VLAN ID	8	(Range: 0 ~ 4095)
Enable VLAN of Port 2		
VLAN ID	:	(Range: 0 ~ 4095 )
Max. Downstream Bandwidth	102400	Kbps (Range: 1 ~ 102400)
Max. Upstream Bandwidth	102400	Kbps (Range: 1 ~ 102400)

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)

Subnet Setting :	Add					
User Setting :	Remove 🔽 🚺	Ignore	Change Department / Group			
						17
Subnet: 192.168.1.0	Select All Select No	ne		Q,	Modify Subnet	Remove Subnet
🗖 🖁 Jacky						
and the second	BULLING BULLING	S)		0	Madify Cubmat	Domous Cubnet

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: <u>http://172.20.108.172:8080</u> 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.

## <u>3.1 Admin</u>

#### 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.

Add New Group-Admin				
Group-Admin name	Group_admin	(Max. 16 characters)		
Password	•••••	(Max. 16 characters)		
Confirm Password	•••••	(Max. 16 characters)		
Write Privilege				
Write Access				
View Group Privilege				
Select All C	iroups		Clear All Gr	oups
1 Group_1 2	Group_2	3 Group_3		Group_4
5 Group_5 8	Group_6	7 Group_7		Group_8
9 Group_9 10	Group_10	11 Group_1	1 12	Group_12

OK Cancel

#### 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.

lodify Admin Password					
Admin Name s	admin				
Password	•••••	(Max. 16 characters)			
New Password	•••••	(Max.16 characters)			
Confirm Password	•••••	(Max:16 characters)			
Write Privilege					
Virite Access					
View Group Privilege					
Select All Gr	Select All Groups Clear All Groups				
1 Group_1 2	Group_2		Group_3		Group_4
5 Group_5 6	Group_6	7	Group_7	8	Group_8
9 Group_9 10	Group_10	11	Group_11	12	Group_12

OK Cancel

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)

Interface Address				
IP Address	192.168.1.2	254		
Netmask	255.255.25	5.0		
Default Gateway	192.168.1.1			
DNS Server 1	168.95.1.1			
DNS Server 2				
Enable VLAN of Port 1				
VLAN ID		] ( Range: 0 ~ 409	5)	
Enable VLAN of Port 2				
VLAN ID		] ( Range: 0 ~ 409	5)	
WAN Bandwidth				
Max. Downstream Bandwidth	102400	Kbps (Range: 1	~ 102400 )	
Max. Upstream Bandwidth	102400	Kbps (Range:1	~ 102400 )	
Enable	Ping	НТТР	HTTPS	
				OK Cancel

#### 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)

Internet Activity Re	ecorder Configurat	tion							
Export System Setti	Choose file							2	
Import System Setti	Chioose me						-		-
	Look in:	Firmware			-	0000	•		_
Reset Factory	à	IAR-5000.con	ıf						
Format Hard D	My Recent								
Database Check	Documents								
Database Check / R									
E-mail Setting	Desktop								
Enable E-mail A									
Company Nam	Mu Documents								
Device Name	My Documents								er)
Sender Addre:									)
SMTP Server	My Computer								
E-mail Address	<b>6</b> 7								
E-mail Address									
Enable SMTP S	My Network Places	File name:	IAR-5000			-		Open	
Username		Files of type:	All Files (*.*	")		-		Cancel	
Password									
						y to suver	•		
E-mail Address	\$ 1			(	Max. 60 (	characters, ex	: user1@n	nydomain.c	om)
E-mail Address	\$ 2			(	Max. 60 (	characters, ex	: user2@n	nydomain.c	om)
Enable SMTP S	erver Authentication	i.							
Username									
Password M	icrosoft Internet	t Explorer						×	
Mail Test	Click "OK" I	to confirm system u	Indata						
Network Depl	Please wai	t 60 seconds during	g software up	date and do not	turn off	the power or (	lose the p	age.	
O Bridge Mod		<b>F</b>	OK	Capcel	ř.				
O Sniffer Mod		-		Cancor	6. 				
Web Managemer	nt (Port Number)								
HTTP Port			80	( Range: 1 ~ 65	535)				
HTTPS Port			443	(Range: 443 or	1025 ~ 6	65535)			
Log Storage Time	e.								÷
Storage Time			14 De	ays (Range:1 -	- 999 )				
System Reboot									
Reboot Internet Acti	ivity Recorder Applia	nce <b>( Reboot )</b>	1						
							1	04	Concel
								NU	vallugi

Figure 3-6 Confirm the import setting

## **Reset Factory Default**

- Step1. In System  $\rightarrow$  Setting  $\rightarrow$  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)

Internet Activity Recorder Configuration		
Export System Setting to Client		
Import System Setting from Client		Browse
React Factory Setting	( ex: IA_Rec	corder.cont)
Keset Factory Setting		
Database Check / Repair		
Database Check / Repair		
E-mail Setting		
Enable E-mail Alert Notification		
Company Name		( Max. 32 characters, ex: My Company )
Device Name		(Max. 30 characters, ex: Internet Activity Recorder )
Sender Address (Required by some ISPs)		(Max. 60 characters, ex: sender@mydomain.com)
SMTP Server		(Max. 80 characters, ex: mail.mydomain.com)
E-mail Address 1		(Max. 60 characters, ex: user1@mydomain.com )
E-mail Address 2		(Max. 60 characters, ex: user2@mydomain.com)
Enable SMTP Server Authentication		
Username		
Password		
Mail Test	Mail Tes	R
Network Deployment Mode		
💿 Bridge Mode		
O Sniffer Mode ( Port 1 : Mirror Port, Port 2 : Manag	gement Port )	
Web Management (Port Number)		
HTTP Port	80	(Range: 1 ~ 65535)
HTTPS Port	443	](Range: 443 or 1025 ~ 65535)
Log Storage Time		
Storage Time	14 [	Days (Range: 1 ~ 999)
System Reboot		
Reboot Internet Activity Recorder Appliance	leet 1	
		OK Cancel

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.	<b>E-Mail Address 1</b> , 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)

-mail Setting		
Enable E-mail Alert Notification		
Company Name	AirLive Corp.	(Max. 32 characters, ex: My Company )
Device Name	IAR-5000	(Max. 30 characters, ex: Internet Activity Recorder )
Sender Address (Required by some ISPs)	iar5000@airlive.com	(Max. 60 characters, ex: sender@mydomain.com )
SMTP Server	airlive.com	(Max. 80 characters, ex: mail.mydomain.com )
E-mail Address 1	admin@airlive.com	(Max. 60 characters, ex: user1@mydomain.com )
E-mail Address 2	mis@airlive.com	(Max. 60 characters, ex: user2@mydomain.com )
Enable SMTP Server Authentication		
Username		
Password		
Mail Test	Mail Test	

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)

Network Deployment Mode		
S Bridge Mode		
O Sniffer Mode (Port 1 : Mirror Port, Port 2 : Ma	Microsoft Internet Explorer 🔀	
Web Management (Port Number)	2 Aro you give to Debeet?	
HTTP Port		
HTTPS Port	OK Cancel 5 ~ 65535 )	
Log Storage Time		
Storage Time	14 Days (Range: 1 ~ 999)	
System Reboot		
Reboot Internet Activity Recorder Appliance	Reboot	
		OK Cancel

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**. System time : Sat May 5 23:07:04 2007

Synchronize system clock	
Enable synchronize with an Internet ti	ne Server
Set offset 🕫 💌 hours from GMT	Assist
Enable daylight saving time setting	3
From 1 1 1 To 1	
Server IP / Name 131.188.3.220	Assist
Update system clock every 0	minutes (Range: 0 ~ 99999, 0 : refers to update during system booting )
Synchronize system clock with this client	Sync ) OK Cancel

Figure 3-10 System time setting

Select Synchronize  $\rightarrow$  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)

Add New Permitted IPs						
Name	master	(Max. 20 characters)				
IP Address	192.168.139.30					
Netmask	255.255.255.255					
Service	Ping HTTP	HTTPS				

OK Cancel

#### Figure 3-11 The Permitted IPs setting

Name	IP Address / Netmask	Ping	HTTP	HTTPS	Configure
master	192.168.139.30 / 255.255.255.255	- 🤣 -	- 🂋 -	- Ø	Medify Remove

New Entry



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)

our current o	connection has expired, you have now been logg	ed out
If y	ou want to login, please restart your browser.	
/	· · · · · · · · · · · · · · · · · · ·	

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  $\rightarrow$  Choose file, select the newest version of the software.
- Click the lower right OK, it will process the update. (Figure 3-15)

Software Update	
Version Number :	v3.05.00
Software Update	Ovislink_IAR5000_030500 Browse
	( ex: Ovislink_IAR-5000_030500.img )
	OK Cancel

## 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)

ort User List fro	om Client PC		Browse				
			Diomoc				
		( ex: user_set.c	csv)				
partment / Gro	oup (Max 20)	characters)					
1: Gro	oup_1	2:	Group_2	3:	Group_3	4:	Group_4
5: Gro	up_5	6:	Group_6	7:	Group_7	8:	Group_8
o Gro	oup_9	10:	Group_10	11:	Group_11	12:	Group_12

#### Figure 4-1 Set the user list

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

- Click Q 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)

Select Subnet or	Department/Group :	💑 Subnet	Management / Group		
Subnet Setting :	Add				
User Setting :	Remove 🖂 🕴	Ignore	Change Department / Group		
					1/1
🖬 Subnet : 192.168.1.0	)			Gin Modify Subnet	Remove Subnet
Subnet: 172.16.0.0	Select All Select None			G Search New User	Remove Subnet
🗏 Subnet : 192.168.13	9.0 Select All Select N	lone		Q Modify Subnet	Remove Subnet
🖻 Subnet : 192.168.22	2.208 Select All Select	st None		🔍 📔 Modify Subnet 🜗	🖡 Remove Subnet 👔
					1/1





Figure 4-3 Starting to search new user

🗿 http	://192.168.1.3	254 - Assist Wind	ow List - Microsoft	Internet 🔳 🗖 🔀
Subne Searcł	t / Netmask:: 192.1 h IP Range : <mark>192.1</mark>	68.1.0 / 255.255.255. 68.1.0	192.168.1.255	Search
	IP	MAC	Computer Name	DNS Name
	192,168,1,100	00.0D.88.18.6A.46	OCT1005	1222
		00:16:36:6D:DD:70	JACKY-M9QX1MFQE	
	192.168.1.1	00:17:9A:32:D3:38	1472	
				New User
🙆 Done				🔵 Internet 💦

Figure 4-4 Select the new user to add

Select Subnet or	Department/Group :	💑 Subnet	Department / Group			
Subnet Setting:	Add					
User Setting :	Remove 🖂 🕴	Ignore	🕴 (Change Department / G	roup		
						171
🖻 Subnet : 192.168.1.0	Select All Select Non	<u>e</u>		Q,	Modify Subnet	🖡 Remove Subnet 👔
<b>. 8</b> <u>192.168.1.1</u>	🔲 😫 Jacky	E		<b>8</b> <u>oct1005</u>		
🖻 Subnet : 172.16.0.0	Select All Select None			Q,	Modify Subnet	🖡 Remove Subnet 👔
🖻 Subnet : 192.168.139	0.0 <u>Select All</u> <u>Select N</u>	lone		Q, I	Modify Subnet	Remove Subnet
🖻 Subnet : 192.168.222	2.208 Select All Selec	<u>:t None</u>		Q,	Modify Subnet	Remove Subnet
						171



After finished the setting of System  $\rightarrow$  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  $\rightarrow$  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**  $\rightarrow$  **DNS name**  $\rightarrow$  **IP or MAC** (It depends on the setting of Record  $\rightarrow$  Setting  $\rightarrow$  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)

Select Subnet or	Department/Group :	🚜 Subnet	Separtment / Group
Subnet Setting :	Add 🔰		
User Setting :	Remove 🖂 🚺	Ignore	📄 (Change Department / Group)
			17
🛢 Subnet : 192.168.1.0	Select All Select No	<u>ie</u>	🔍 📔 Modify Subnet 👔 Remove Subnet
	🔲 🖁 Jacky	, I	
Subnet: 172.16.0.0	Select All Select None	2	User Name : JACKY-M9QX1MFQE
■ Subnet : 192.168.13	9.0 <u>Select All</u> <u>Select</u>	None	IP: 192.166.1.101
🗏 Subnet : 192.168.22	2.208 Select All Sele	<u>ct None</u>	Contraction of the second seco
			10

## Figure 4-6 Select the user to modify

Addify User Name								
User Name	Jacky_NB	(Max. 17 characters)						
Department / Group	Product 💌							
Computer Name	JACKY-M9QX1MFQE	JACKY-M9QX1MFQE						
DNS Name								
P	192 168 1 101							
MAC	00:16:36:6D:DD:70							
Move this user to Ignored I	Move this user to Ignored User List							

OK Cancel

Figure 4-7 Enter the user information to modify

Select Subnet or D	epartment/Group :	💑 Subnet	💁 Department /	Group			
Subnet Setting :	Add						
User Setting :	Remove 🖂 🕴	Ignore	Change Departm	ent / Group			
							171
🛢 Subnet : 192.168.1.0	Select All Select Non	<u>e</u>			Q,	Modify Subnet	Remove Subnet
<b>§</b> <u>192.168.1 1</u>	🔲 🖁 Jacky		Sacky_NB		<u>005</u>		
Subnet : 172.16.0.0	Select All Select None				Q,	Modify Subnet	🖡 Remove Subnet 👔
🛢 Subnet : 192.168.139.	0 Select All Select N	lone			Q,	Modify Subnet	🖡 Remove Subnet 👔
🖬 Subnet : 192.168.222.	208 Select All Select	<u>rt None</u>			Q,	Modify Subnet	🖡 Remove Subnet 👔
							1/1

Figure 4-8 Complete to modify the user information
Select Subnet or	Department/Group :	🛃 Subnet	Manager Department / Gr	oup			
Subnet Setting :	Add						
User Setting :	Remove 🔽 🛛	Ignore	📑 (Change Departmen	t / Group			
							171
🛢 Subnet : 192.168.1.0	Select All Select Nor	ie.			Q,	Modify Subnet 💧	🖡 Remove Subnet 🚺
<b>S</b> <u>192.168.1.1</u>	🔲 😫 Jacky	C	Jacky NB				
Subnet: 172.	Name : 192.168.1.1	l.			Q,	Modify Subnet	🖡 Remove Subnet 📗
Subnet : 192.1(     Depart     IP : 19:	tment / Group : Group_' 2.168.1.1	<u>ine</u>			Q	Modify Subnet 🌗	🖡 Remove Subnet 📗
	00:17:9A:32:D3:38	None			Q	Modify Subnet	Remove Subnet
							171

## Figure 4-9 Select the user to modify

Modify User Name		
User Name	Gateway (Max. 17 characters)	
Department / Group	Device_Room 🗸	
Computer Name		
DNS Name		
P	192.468.4.4	
MAC	00 17 9A 32 D3 38	
Move this user to Ignored U		
Ed		
		OK Cancel

Figure 4-10 Enter the user information to modify

Select Subnet or Department/Group : 🚜 Subnet	Management / Group		
User Setting : 🛛 🔽 🔽 🚺 🚺 🚺 🚺 🚺 🚺 🚺	🔋 (Change Department / Group)		
~		1.4	1/1
Subnet : 192.168.1.0 Select All Select None		Modify Subnet	🕴 Remove Subnet 💧
I S Gateway			
Subnet: 172.16.0.0 Select All Select None		Modify Subnet	🖡 Remove Subnet 👔
Subnet: 192.168.139.0 Select All Select None		Modify Subnet	🖡 Remove Subnet 💧
Subnet : 192.168.222.208 Select All Select None		Modify Subnet 🕴	🖡 Remove Subnet 👔
			1/1

Figure 4 -11 Move the user to ignored user list

Select Subnet or	Department/Group :	🚜 Subnet	Separtment / Group			
Subnet Setting :	Add					
User Setting :	Remove 🖂 🛛	Ignore	📄 (Change Department / Group)			
						171
🖻 Subnet : 192.168.1.0	Select All Select Nor	ie.		Q,	Modify Subnet	🖡 Remove Subnet 📗
🛄 🔲 😫 Jacky	🔲 🖁 Jacky M		<b>\$</b> <u>oct1005</u>			
🗏 Subnet : 172.16.0.0	Select All Select None	l.		Q.	Modify Subnet	🖡 Remove Subnet 📗
■ Subnet : 192.168.13	9.0 <u>Select All</u> <u>Select I</u>	lone		Q	Modify Subnet	Remove Subnet
🗏 Subnet : 192.168.22	2.208 Select All Sele	c <u>t None</u>		Q	Modify Subnet	Remove Subnet
						1/1



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)

Add User Subnet / Netmask				
Subnet	192.168.	139.1		
Netmask	255.255.	255.0		
Add a New user to this Department / Group	RD	~		
				OK Cancel



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)

- Step 1. In User List  $\rightarrow$  Setting  $\rightarrow$  User List Configuration  $\rightarrow$  Export User List to Client PC  $\rightarrow$  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)

User List Configuration		
Export User List to Client PC	Download	
Import User List from Client PC	File Download	
Department / Group (Max. 20 ch 1: Group_1 5: Group_5 9: Group_9	Do you want to open or save this file? Name: user_set.csv Type: Microsoft Excel Comma Separated Values File, 950 From: 192.168.1.254 Open Save Cancel	4: Group_4 8: Group_8 12: Product
	While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. <u>What's the risk?</u>	

**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)

#### *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**.

2	Departmen	t / Group :	2	Departmen	t / Group :
5	~1	Internal_Sales	5	~1	Internal_Sales
-	~2	Asian_Sales		~2	Asian_Sales
5	~3	European_Sales	5	~3	European_Sales
5	~4	American_Sales	5	~4	American_Sales
2	~5	Bursary	1	~5	Bursary
8	~6	Human_Resouces	ł	~6	Human_Resouces
)	~7	Marketing		-1	Marketing
)	~8	Customer_Service		~8	Support
	~9	R.D.		~9	R.D.
2	~10	Laboratory	2	~10	Laboratory
5	~11	Device_Room	5	~11	Device Room
	~12	Group_12	ŀ	~12	R.D2
5	~13	Group_13	5	~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 1<sup>th</sup> Department / Group into 9<sup>th</sup> 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 :							User List :						
192.168.1.0	255.255.25	1					192.168.1.0	255.255.25	1				
192.168.1.2	Jacky	WRITTER	3	00:D0:59:	1	*	192.168.1.2	Jacky	WRITTER	3	00:D0:59:	9	*
192.168.1.100	*	OCT1005	3	00:0D:88:	1	*	19 168.1.100	*	OCT1005	3	00:0D:88:	1	*
192.168.1.101	Jacky_NB	JACKY-M	3	00:16:36:6			.1.101	Jacky_NB	JACKY-M	3	00:16:36:6	12	*
192.168.1.1	Gateway	9 <b></b> 28	1	00:17:9A:	11	*	192.168.1.1	Gateway	2 <b></b> 2	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.	Gateway		1	00:17:9A:	11
192.168.1.	IJohn	PM	6	00:15:5A:	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  $\rightarrow$  Setting, Click User List Configuration  $\rightarrow$  Import User List from Client PC  $\rightarrow$  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)

IM A	lert Notification Setting		
<b>V</b>	Enable NetBIOS Alert Notification	Test IP of NetBIOS Alert Notification:	Msg. Test
¥	Enable MSN Alert Notification ( Bridge Mode Only )	8. <del></del>	
	Enable ICQ Alert Notification ( Bridge Mode Only )		
~	Enable Yahoo Alert Notification ( Bridge Mode Only	)	
Send	er: Internet Activity Recorder	(Max. 40 characters, ex: Administer)	
Conte	ent: (Max. 1024 characters )		
) are tha	all instant message will be logg subject to archival monitoring an the recipient.	ed by the Internet Activity Re or disclosure to someone othe	corder and r
			OK Cancel

#### 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 authentication messages while he/she login the authentication 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

Authentication	
Name	(Max. 128 characters)
Password	(Max. 128 characters)

You have to pass the IM authentication then you are allowed to create the IM connection.

MSN	
Account	(Max. 128 characters)
🝚 Yahoo	
Account	(Max. 128 characters)
<b>8</b> aa	
Account	(Max. 128 characters)
Password	(Max. 128 characters)
Confirm Password	(Max. 128 characters)
🔅 ICQ	
Account	(Max. 128 characters)

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)

Configure
Modify Remove
Modify Remove
Modify Remove
modily Remove

**Step1.** Add authentication user in **Authentication**  $\rightarrow$  **User.** (Figure 5-5)

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.



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)

	Authentication					
	Name	eric	(Max. 128 charact	ters)		
	Password	****	(Max. 128 charact	ters)		
You have to	ness the TM en	hentication then w	ou ere ellowed	to greate th	о ти	connection
Iou nave co	pass che in au	chemcicación chem y	ou are arrowed	I CO CIEACE CH	e 111	conneccion.
					_	
	IM Protocol					
	🍊 MSN					
	Account	ericflydog@hotmail.com	(Max. 128 charact	ters)		
	😛 Yahoo					
	Account		(Max. 128 charact	ters)		
	800					
	Account		(Max. 128 charact	tersì		
	Password		(Max 128 charact	iers)		
	Confirm Boooword		(max. 120 charact			
	Commini Password		(Max. 128 charact	(ers)		
	*					
	🗫 ICQ					
	Account		(Max. 128 charact	ters)		
				OK Car	ncel	
			1	Uni Uai	1001	

Figure 5-7 Authentication setting

	Authentication	
	Name	(Max. 128 characters)
	Password	(Max. 128 characters)
<i>l</i> ou have to	pass the IM authentication then	you are allowed to create the IM connection
	IM Protocol	
	MSN .	
	Account	(May 128 obsectors)
		(Max. 120 characters)
	Microsoft Int	ernet Explorer 🛛 🗶
	Vahoo	
	Account Au	ithentication Succeeded s)
	🐣 qq	ОК
	Account	
	Password	(Max, 128 characters)
	Confirm Password	(Mary 428 alternations)
		(Max. 120 Characters)
	<b>4</b>	
	<b>%</b> -lcQ	_
	Account	(Max. 128 characters)
		OK Cancel

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)

indows Components		5
You can add or remove comp	onents of Windows XP.	
To add or remove a compone part of the component will be	nt, click the checkbox, A s	haded box means that only luded in a component, click
Details.	insidiled. To see wildes inc	lubbe in a component, click
Components:		
🗌 🜌 Message Queuing		0.0 MB 🔺
🗆 🏹 MSN Explorer		13.2 MB
🗹 🚉 Networking Services		0.3 MB
🖾 📲 Other Network File an	d Print Services	0.0 MB
Call Outlook Express		0.0 MB 🗾
Description: Contains a varie	ty of specialized, network-re	lated services and protocols.
Table Ball Concerns and South		13 March 19 State 201
Total disk space required:	55.6 MB	Details

Figure 5-9 Windows components wizard

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

ans that only part ant, click Details,
1.6 MB 🔺
0.0 MB
0.0 MB
0.0 MB
0.0 MB
0.9 MB
dial-up and VPN
Dietaiks:
E Contraction
Cancel

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)

254	
	⊻erify
	2
	254

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)

endor of the RADIUS client.	solicies based on the client vehicle autoace, specify the
<u>Client-Vendor:</u>	
RADIUS Standard	
<u>S</u> hared secret:	*****
Confirm shared secret	*****
Request must contain the	Message Authenticator attribute

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)

🤣 Internet Authentication	Service			- 🗆 ×
File Action View Help				
⇔ → 🖻 🖬 🖾	1			
Internet Authentication Server     ADIUS Clients     Remote Access Logging     Demote Access Logging	rice (Local)	Name Connections to Microsoft Routing and Remo Connections to other access servers	Order ote 1 2	
E Connection Request Pr	New Remote	e Access Policy		
	New	•		
	⊻iew	•		
	Refresh Export List.			
	Help			
New Remote Access Policy				

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)

		-
Policy Configu	ration Method	ť
The wizard c	an create a typical policy, or you can create a custom policy.	
How do you w	vant to set up this policy?	
	e wizard to set up a typical policy for a common scenario	
C Set up	a custom policy	
Type a name t	hat describes this policy.	
Type a name t Policy name:	hat describes this policy. Radius	
Type a name t <u>P</u> olicy name:	hat describes this policy. Radius Example: Authenticate all VPN connections.	
Type a name t <u>P</u> olicy name:	hat describes this policy. Radius Example: Authenticate all VPN connections.	
Type a name t Policy name:	hat describes this policy.          Radius         Example: Authenticate all VPN connections.	

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

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

Acces: Pol	s Method icy conditions are based on the method used to gain access to the network.
Selec	t the method of access for which you want to create a policy.
C	VPN
	Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.
C	Dial-up
	Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.
0	<u>Wireless</u>
	Use for wireless LAN connections only.
C	Ethernet
	Use for Ethernet connections, such as connections that use a switch.
	< <u>B</u> ack <u>Next&gt;</u> Cancel

56

Step11. Select User. (Figure 5-18)

You can grant act groups.	ess cess to individual users, or you can grant access to selected
Grant access based	on the following:
<ul> <li>User</li> <li>User access per</li> </ul>	missions are specified in the user account.
C <u>G</u> roup Individual user pe Group name:	ermissions override group permissions.
	A <u>d</u> d
	Elemove
1	
1	

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

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

New Remote Access Policy Wizard	×
Authentication Methods EAP uses different types of security devices to authenticate users.	ŷ
Select the EAP type for this policy.	
MD5-Challenge	Configure
< Back	> Cancel

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

**Step13.** Right click on the **Radius**  $\rightarrow$  **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)

×			
Specify the cond	litions that conne	ection requests must match	<b>b</b>
olicy conditions	10		
NAS-Port-Type	matches "Etherr	iet"	
Add	Edit	Bemove	
			(1997) <b>H</b> E (1997)
t connection rec associated profile	uests match the e will be applied	conditions specified in this to the connection.	s policy, the
8. 1999: 1999: 1999: 1999: 1999: 1999: 1999: 1999: 1999: 1999: 1999: 1999: 1999: 1999: 1999: 1999: 1999: 1999: 19	2.0		
Edit Profile			
Jnless individua	access permiss	ions are specified in the us	er profile, this
olicy controls a	cess to the net	vork.	
	equest matches	the specified conditions:	
f a connection r	access nermissi	on	
f a connection r	access hermiss		
f a connection r Deny remote		52	

Figure 5-21 The RADIUS properties settings

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

Name	Description
Called-Station-Id Calling-Station-Id Client-Friendly-Name Client-IP-Address Client-Vendor Day-And-Time-Restric Framed-Protocol MS-RAS-Vendor NAS-Identifier NAS-Identifier NAS-IP-Address NAS-Port-Type Service-Type Tunnel-Type Windows-Groups	Specifies the phone number dialed by the usi Specifies the phone number from which the c Specifies the friendly name for the RADIUS c Specifies the IP address of the RADIUS clier Specifies the manufacturer of the RADIUS pi Specifies the time periods and days of week Specifies the protocol that is used. Description not yet defined Specifies the string that identifies the NAS the Specifies the IP address of the NAS where the Specifies the type of physical port that is use Specifies the type of service that the user ha Specifies the tunneling protocols used. Specifies the Windows groups that the user the
4	The second s

Figure 5-22 Add new RADIUS properties attribute

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

Available types:		Selected types:
Administrative Call Check Callback Administrative Callback Framed Callback Login Callback Nas Prompt Framed Login NAS Prompt Outbound	Add >>	Authenticate Only
		OK Cancel

Figure 5-23 Add RADIUS properties service-type

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

adius Properties <mark>E</mark>	dit Dial-in Profile		?		
Settings	Dial-in Constraints	) IP	Multilink		
Specify the conc	Authentication	Encryption	Advanced		
Policy <u>c</u> onditions	Select the authentication me	thods you want to allow	for this connection.		
	EAP Methods				
	Microsoft Encrypted A	uthentication version $\underline{2}$	(MS-CHAP v2)		
L	🔲 User can <u>c</u> hang	e password after it has	expired		
Add	Microsoft Encrypted Authentication (MS-CHAP)				
If connection rec	Uger can change password after it has expired				
associated profile	Encrypted authentication (CHAP)				
Edit Profile	I Unencrypted authention	cation (PAP, SPAP)			
Unless individual policy controls ar	Unauthenticated access				
If a connection u	Allow clients to conner	ct without negotiating ar	n authentication		
Deny remote					
C Grant remote					
		or I c	Apple Apple		
			aucer Bbblo		

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)

RADIUS Server		
Enable RADIUS Server Authentication	<u>Test</u>	
RADIUS Server ( IP or Domain Name )	172.19.250.10	(Max. 80 characters)
RADIUS Server Port	1812	(Range: 1025 - 65535 )
Shared Secret	master	(Max. 80 characters)
Enable 802.1× RADIUS Server Authentication	i i i i i i i i i i i i i i i i i i i	
		OK Cancel

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)



- 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)

	Authentication			
	Name	eric	(Max. 128 characters)	
	Password	****	(Max. 128 characters)	
V 1 +	ware the TW are			
iou nave to	pass the in au	chentication then y	ou are allowed to create t	ne in connection.
	-			
	IM Protocol			
	🖑 MSN			
	Account		(Max. 128 characters)	
	⊖ Yahoo			
	Account	mcgaver_2002	(Max. 128 characters)	
	🐣 qq			
	Account		(Max. 128 characters)	
	Password		(Max. 128 characters)	
	Confirm Password		(Max. 128 characters)	
		·		
	🐝 ica			
	Account		(May 128 characters)	
			(Max. 120 characters)	
			ОК С	ancel

Figure 5-29 Authentication setting

• Click **OK.** (Figure 5-30)

	Authoritication	
	Autrentication	
	Name	(Max. 128 characters)
	Password	(Max. 128 characters)
	-	
You have to	pass the IM authentication then y	you are allowed to create the IM connection.
	IM Protocol	
	MSN	-
	Account	(Max. 128 characters)
	Microsoft Inter	net Explorer
	😛 Yahoo	
	Account Account	entication Succeeded
	<u> </u>	
	<b>A</b>	or 1
		<u>OK</u>
	Account	(3
	Password	(Max. 128 characters)
	Confirm Password	(Max. 128 characters)
	<b>*</b>	
		-
	Account	(Max. 128 characters)
		OK Cancel
		OK OUND
	Figure 5-30 Authent	icated 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)

Step 1. Select Accept : Authentication passed and QQ Password valid in IM Management  $\rightarrow$ Rule  $\rightarrow$  Default Rule  $\rightarrow$  QQ. (Figure 5-31)

🦰 qq
C Accept: QQ Password valid
Drop : QQ Password invalid
$\odot~\text{Accept}$ : Authentication passed and QQ Password valid
<b>Drop</b> : Authentication failed or QQ Password invalid
O Accept: Authentication passed
Drop : Authentication failed
O Accept: Always
O Drop : Always
Figure 5-31 Set the QQ default rule

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

hable POP3 Server Authentication	Test		
OP3 Server ( IP or Domain Name )	mail.airlive.com	(Max. 15 characters)	
POP3 Server Port	110	(Max. 5 characters)	

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)

	Authentication			
	Name	eric	(Max. 128 characters)	
	Password	****	(Max. 128 characters)	
You herre to	noss the TM ou	thentication then	you are allowed to create the	TM connection
Iou nave co	pass one in au	chencicación chen	you are arrowed to create the	In connección
				_
	IM Protocol			
	🍊 MSN			
	Account		(Max. 128 characters)	
	⊖ Yahoo			
	Account		(Max. 128 characters)	
	800			
	Account	macgyver	(Max. 128 characters)	
	Password	****	(Max. 128 characters)	
	Confirm Password	*****	(Max, 128 characters)	
	<b>se</b> iro			
	lecourt			
	Account	1	(Max. 128 characters)	
			OK Canc	el

Figure 5-33 Enter the QQ account and password
• Click **OK**. (Figure 5-34)

Authentication	
Name	(Max. 128 characters)
Password	(Max. 128 characters)
You have to pass the IM auth	entication then you are allowed to create the IM connection
IM Protocol	
🚳 MSN	
Account	(Max. 128 characters)
🝚 Yahoo Account	
ea Accession of the second sec	
Account	b)
Password	(Max. 128 characters)
Confirm Password	(Max. 128 characters)
🗱 ICQ	
Account	(Max. 128 characters)
	OK Cancel

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)

💐 Manag	e Your Server		×
	Manage Your Server	<u>Search</u> Help and Support C	ienter 🗾 🔁
9	Managing Your Server Roles Use the tools and information found here to add or remove roles and perform your daily administrative tasks. Your server has been configured with the following roles:	<ul> <li>Add or remove a role</li> <li>Read about server roles</li> <li>Read about remote administration</li> </ul>	<u>Tools and Updates</u> Administrative Tools More Tools Windows Update Computer and Domain Name Information Internet Explorer Enhanced Security Configuration
	File Server File servers provide and manage access to files.	<ul> <li>Manage this file server</li> <li>Add shared folders</li> <li>Review the next steps for this role</li> </ul>	Sge Also Help and Support Microsoft TechNet Deployment and Resource Kits List of Common Administrative Tasks Windows Server Communities What's New Strategic Technology Protection Program
	Don't display this page at logon		

Figure 5-35 Click add or remove a role

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

figure	Your Server Wizard	
Prelim Yoi cor	inary Steps u can ensure that you successfully configure your server by completing the following steps before ntinuing.	1
Bef	ore continuing, verify that the following steps have been completed.	
•	Install all modems and network cards.	
	Attach all necessary cables.	
	If you plan to use this server for Internet connectivity, connect to the Internet now.	
	Turn on all peripherals, such as printers and external drives.	
	Have your Windows Server 2003 Setup CD available, or know your network installation path.	
° Wh	ien you click Next, the wizard will search for network connections.	
		Help

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)

nfigure Your Server Wizard	
Summary of Selections View and confirm the options you have selected.	S
Summary:	
Run the Active Directory Installation Wizard to set up this server as a domain	controller
To change your selections, click Back. To continue setting up this role, click Nex	t.

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)

Active	Directory Installation Wizard
Oţ	Derating System Compatibility Improved security settings in Windows Server 2003 affect older versions of Windows.
	Domain controllers running Windows Server 2003 implement security settings that require clients and other servers to communicate with those domain controllers in a more secure way.
	The following older versions of Windows cannot meet the new requirements:
	Windows 95
	<ul> <li>Windows NT 4.0 SP3 or earlier</li> </ul>
	By default, computers running those versions of Windows will not be able to log on with a domain controller running Windows Server 2003 or access domain resources.
	For more information, see Compatibility Help.
	<u> </u>
	₩ ₩

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)

Active Directory Installation Wizard	×
Domain Controller Type Specify the role you want this server to ha	ve.
Do you want this server to become a doma additional domain controller for an existing	in controller for a new domain or an domain?
Domain controller for a new domain	
Select this option to create a new child This server will become the first domain	I domain, new domain tree, or new forest. n controller in the new domain.
C Additional domain controller for an exist	ting domain
🔥 Proceeding with this option will de	lete all local accounts on this server.
All cryptographic keys will be delet continuing.	ted and should be exported before
All encrypted data, such as EFS-e before continuing or it will be perm	ncrypted files or e-mail, should be decrypted anently inaccessible.
	Kack Nervy Cancel

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)

Se	lect which type of domain to create.
Cre	sate a new:
(F	Domain in a new forest
	Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.
С	Child domain in an existing domain tree
	If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters, example, microsoft, com as a child domain of the domain example, microsoft, com.
С	Domain tree in an existing forest
	If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.

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)

N	Directory Installation Wizard w Domain Name
	Specify a name for the new domain.
	Type the full DNS name for the new domain (for example: headquarters.example.microsoft.com),
	Eull DNS name for new domain:
	my.com

Figure 5-43 The new domain name window

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

Active Directory Installation V	Vizard	×
NetBIOS Domain Name Specify a NetBIOS name f	or the new domain.	S.
This is the name that users domain. Click Next to acce	of earlier versions of Windows will use to identify th pt the name shown, or type a new name.	e new
Domain NetBIOS name:		
	< <u>Back</u>	Cancel

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)

For best hard dis	performance and rikes.	ecoverability, st	ore the database an	d the log on separate
Where a	do you want to store	e the Active Dire	ctory database?	
Databas	e folder:			
D:\WIN	IDOWS\NTDS			Biowse
Where c	lo you want to store	e the Active Dire	ctory log?	
Log fold	er:			
D:\WIN	IDOWS\NTDS			Browse

Figure 5-45 The database and log folder window

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

Shared S	System Volume			6
Spec	iry the folder to be share	d as the system volume.	2	R
The 9 of the	YSVOL folder stores the SYSVOL folder are repli	e server's copy of the do icated to all domain con	omain's public file atrollers in the don	s. The contents nain.
The S	SYSVOL folder must be li	ocated on an NTFS vol	ume.	
Enter	a location for the SYSV(	DL folder.		
Eolde	r location:			
D:\W	/INDOWS\SYSVOL			Browse
100				

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)

Activ	ve Directory Installation Wizard
Ţ	DNS Registration Diagnostics Verify DNS support, or install DNS on this computer.
	Diagnostic Results The registration diagnostic has been run 1 time. The wizard encountered an error while trying to determine if the DNS server with
	which this domain controller will register supports dynamic updates.
	The primary DNS server tested was: ns1.hs.aosoft.com (67.18.222.178)
	<ul> <li>I have corrected the problem. Perform the DNS diagnostic test again.</li> <li>Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server.</li> </ul>
	Will correct the problem later by configuring DNS manually. (Advanced)
	< <u>Back</u> <u>Next</u> Cancel

Figure 5-47 The DNS registration diagnostics window

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

ve Dir	ectory Installation Wizard				
P <b>ermi</b> s Se	esions lect default permissions for user and group objects.				
So sto	me server programs, such as Windows NT Remote Access Service, read information red on domain controllers.				
C	Permissions compatible with pre-Windows 2000 server operating systems				
	Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are members of pre-Windows 2000 domains.				
~	Anonymous users can read information on this domain.				
(*	Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems				
	Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain.				
	< <u>B</u> ack <u>N</u> ext > Cancel				
	<u>K</u> Back <u>N</u> ext > Cance				

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)

Active Directory Installation	Wizard	×
Directory Services Resto This password is used wh Mode.	re Mode Administrator Password nen you start the computer in Directory Services Restore	S.
Type and confirm the pas when this server is started	sword you want to assign to the Administrator account use d in Directory Services Restore Mode.	ed
The restore mode Admini account. The passwords both.	strator account is different from the domain Administrator for the accounts might be different, so be sure to remembe	Br
Restore Mode Password:	•••••	
<u>C</u> onfirm password:	•••••	
For more information about	ut Directory Services Restore Mode, see <u>Active Directory I</u>	<u>Help</u> ,
	< <u>B</u> ack <u>N</u> ext >	Cancel

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

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

IUUI	mary
2	review and confirm the options you selected.
Y	(ou chose to:
C	Configure this server as the first domain controller in a new forest of domain trees.
Ţ	The new domain name is my com. This is also the name of the new forest.
T	The NetBIOS name of the domain is MY
0110	)atabase folder: D:\WINDOWS\NTDS .og file folder: D:\WINDOWS\NTDS SYSVOL folder: D:\WINDOWS\SYSVOL
T	The password of the new domain administrator will be the same as the password of he administrator of this computer.
Ţ	o change an option, click Back. To begin the operation, click Next.

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 Ob	iect–User	window.	enter the settings	. click Next.	(Figure 5-54)
0.0021.		Jeor 0301	window,	ontor the bottings	, опок нели.	$(1 \text{ iguid } 0  0^{+})$

e a constante	<u></u>			
Eirst name:	jacky		Initials:	
Last name:				
Full name:				
∐ser logon name				
jacky		@my.com		*
User logon name	(pre- <u>W</u> indows 20	)00):		
2004/05				

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

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

Password:		
<u>C</u> onfirm password:	<b>•••••</b>	
User <u>m</u> ust change	e password at next logon	
🔲 Uger cannot char	nge password	
Password never e	expires	
C Account is disable	ed	

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

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

ew Objec	t - User					×
g	Create in:	my.com/Use	ns			
When y	ou click Finish, t	he following	object will b	e created:		
Full nar	ne: jacky					~
User lo	gon name: jacky	/@my.domai	n			
The pa	ssword never ex	pires.				
						Ŷ
_						
			< <u>B</u> ack	Finith	Ca	ancel
		~		1		

Figure 5-56 Complete to add the user

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

Default Setting of IM Rule (Bridge Mode Only)	
AN MSN	😛 Yahoo
Accept: MSN Message not encrypted	Accept: Always
Drop : MSN Message encrypted	C Accept: Authentication passed
O Accept: Authentication passed and MSN Message not encrypted	Drop : Authentication failed
Drop : Authentication failed or MSN Message encrypted	O Drop : Always
O Accept: Authentication passed	
Drop : Authentication failed	
O Accept: Always	
O Drop : Always	
<b>A</b> aa	<b>A</b>
🧑 QQ	A CO
C Accept: QQ Password valid	C Accept: Always
Drop : QQ Password invalid	O Accept: Authentication passed
O Accept: Authentication passed and QQ Password valid	Drop : Authentication failed
Drop : Authentication failed or QQ Password invalid	C Drop : Always
O Accept: Authentication passed	
Drop : Authentication failed	
O Accept: Always	
O Drop: Always	

Figure 5-57 The default rule setting of IM

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

Enable LDAP Server Authentication	lest	
LDAP Server ( IP or Domain Name )	192.168.159.223	(Max. 80 characters)
LDAP Server Port	389	( Range: 389 or 1025 - 65535 )
Search Distinguished Name	dc=my,dc=com	(Max. 511 characters, ex. dc=mydomain,dc=com.)
LDAP Filter	objectClass=*	(Max. 255 characters, ex: (objectClass=*))
User Distinguished Name	cn=airlive, cn=users,d	(Max. 1023 characters, ex: cn=users,dc=mydomain,dc=com)
Password	@123456a	(Max. 127 characters)

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 <u>http://IAR-5000</u> interfac/auth in address cloumn of browser. For example, <u>http://192.168.1.1/auth</u>. :
  - Enter the authentication name and password.
  - Enter ICQ account.
  - Click OK. (Figure 5-59)

Authentication	n	
Name	airlive@my.com	(Max. 128 characters)
Password	*****	(Max, 128 characters)

You have to pass the IM authentication then you are allowed to create the IM connection.

- more		
Account		(Max. 128 characters)
😛 Yahoo		
Account	[	(Max. 128 characters)
800		
Account		(Max. 128 characters)
Password		(Max. 128 characters)
Confirm Passw	vord	(Max. 128 characters)
🗱 ICQ		
Account	438891984	(Max. 128 characters)

Figure 5-59 ICQ authentication setting

	Authentication	
	Name	(Max. 128 characters)
	Password	(Max. 128 characters)
You have to	pass the IM authentication then y	ou are allowed to create the IM connection.
	IM Protocol	and the second
	Microsoft Inter	net Explorer 🔀
	Account Authe	entication Succeeded
	😛 Yahoo 📃 👘	
	Account	<u>ок</u> <sub>\$)</sub>
	Account	(Max. 128 characters)
	Password	(Max. 128 characters)
	Confirm Password	(Max. 128 characters)
	<b>Å</b>	
		(May 429 sharestare)
		(Wax. 120 Characters)
		OK Cancel

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

Figure 5-60 Authenticated succeed

## <u>5.3 Rule</u>

#### **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.

- 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.
- 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  $\rightarrow$  Rule  $\rightarrow$  Default Rule  $\rightarrow$  QQ  $\rightarrow$  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)

**************************************	Dialoque Duration	User Name		Participants	8⇔8
	08/08 09:02:34 09:03:00 (0.26 min.)	ERIC13	-	🐣 Unknow Participant	_4
	08/08 09:02:37 09:03:00 (0.23 min.)	AirLive-01	-	🐣 Unknow Participant	_4
	08/08 01:48:15 09:00:42 (432.27 min.)	JACKIE-PC	-	🐣 Unknow Participant	14

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)

Туре	User	Name	Dialogue Duration	ogue Duration Scheller				
8	ERI	C13	C13 09:02:34 09:05:10 (2.36 min.) 372136019 🔶 Unknow Participant					
Date	Date/Time Content							
09/09/	10.02.34	3721360	19:					
00/00 (	J3.UZ.34	The content has already encrypted.						
00/00/	0.00.24	372136019:						
00/00 (	33.02.34	The content has already encrypted.						
00/00/	0.02.00	Unknow Participant :						
00/00 (	33.03.00	The co	ntent has already encrypted.					
00/00/0	0.02.00	Unknow	Participant :					
00/08 (	3.03.00	The co	ntent has already encrypted.					

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)

State	QQ Account	Configure
1	372136019	Remove

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)

	Add New Q	Q Accol	unt		
QQ Account			Microsof	t Internet Euplorer	
ID	372136019		MICroson	t Internet explorer	
Password	*****			Password test succes	sful.
Confirm Password	*****	Test	_		
	÷			OK	

Figure 5-65 Test QQ account

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

Add New QQ Account						
QQ Account			Microsof	t Internet Explorer	×	
ID						
Password				Modify QQ Account succe	essful.	
Confirm Password		Tes		ОК		

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
1	372136019	Remove

Figure 5-67 Password authenticated succeed

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

	Dialogue Duration -	User Name	Partic pants	8⇔8
	08/08 09:02:37 09:53:42 (51.5 min.)	AirLive-02	- 🐣 Unknow Participant	20
Г	08/08 09:52:45 09:53:42 (0.57 min.)	ERIC13	- 🐣 318781555	4
	08/08 09:47:17 09:47:28 (0.11 min.)	Ray	- 🎎 richardwu22@msn.com	_2
	08/08 09:02:34 09:05:10 (2.36 min.)	ERIC13	- 🐣 Unknow Participant	<u>_6</u>
	08/08 01:48:15 09:00:42 (432.27 min.)	JACKIE-PC	- 🐣 Unknow Participant	14

#### Figure 5-68 Can record the QQ contents

Туре	User	Name	Dialogue Duration	열승을			
8	ERI	X13         09:52:45 09:53:42 (0.57 min.)         372136019         +>         318781555					
Date	Date/Time Content						
08/08	08/08 09:52:45 log in successfullM						
08/08	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: ican'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
X	372136019	Remove

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)

🚈 IR2000 - Microsoft Internet Explorer							
File	Edit	View	Favorite	es	Tools	Help	
] 🗇 Ba	ack 🔻	⇒ ~	🛛 🖉	6	Qs	iearch	
Addres	s	http://1	92.168.1	.1/qq			

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				
			ок			

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

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

QQ Account		Microsoft	t Internet Explorer 📃 👂
ID	372136019		
Old Password	*****		Modify QQ Account successful
Password	*****		OK
Confirm Password	*****		

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)

State	QQ Account	Configure
V	372136019	Remove

Figure 5-74 QQ account authenticated succeed

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

		2006-08-0	(10 records) Correct password recor	Correct password records		
Q	vrong password records			1/1		
	Dialogue Duration -	User Name	Participants	8⇔8		
	08/08 09:02:37 11:25:49 (143:12 min.)	AirLive-02	- 🐣 Unknow Participant	<u>34</u>		
	08/08 09:52:45 11:25:49 (93.4 min.)	RIC13	- 🐣 318781555	1		
	08/08 10:20:52 11:22:07 (61.15 min.)	172.19.100.45	🕅 🆓 chenhuiw@citiz.net	<u>60</u>		
	08/08 10:40:34 11:18:34 (38.0 min.)	JACK54	- 🎎 fangji80412@hotmail.com, quan_he@21cn.com,	<u>59</u>		
	08/08 01:48:15 11:17:28 (569.13 min.)	JACKIE-PC	- 🐣 Unknow Participant	18		
	08/08 09:02:34 11:11:26 (128.52 min.)	ERIC13	- 🐣 Unknow Participant	<u>18</u>		

#### Figure 5-75 Record the QQ message contents successfully

Туре	User	Name	Dialogue Duration	\$⇔2				
8	ERI	C13	09:52:45 09:53:42 (0.57 min.)	372136019 🔶 318781555				
Date/Time Content								
00/00/00/50/45		eric :						
00/00 0	55.52.45	log in successfully!						
ດອຸທອດ	0.53.05	318781555 :						
00/00 09.55.05		ya i know i know						
08/08 09:53:06	318781555 :							
	ya i know i know							
00,000	00-52-42	eric :						
08/08 09:53:42		ican's	see you					



# 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)

Account Rule Configuration				
Export Account Rule to Client PC	Download			
Import Account Rule from Client PC		Browse		
	( ex: IM_Rule_List.csv )			



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

Account Rule Cor	File Download	
Export Account Rule Import Account Rule	Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.	
Default Setting of	File name: IM_Rule_List.csv	
20 Line	File type: Microsoft Office Excel Comma Separated Values Fil	
MSN (MSN)	From: 172.19.0.1	
O Accept: MSN		
Drop : MSN		ation passed
• Accept: Auth		ation failed
Drop : Auth	Would you like to open the file or save it to your computer?	
O Accept: Auth	Open Save Cancel More Info	
Drop : Auth	Always ask before opening this type of file	
O Accept: Alwa	M Always ask before opening this gipe of the	
O Drop : Alwa	iys	

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



### Step2. Open the user account list by Excel. (IM\_Rule\_List.csv)

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 MA	AC 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
	<ul> <li>If MIS engineer want to a information.</li> </ul>	add one IM accou	nt, just add one	row and type the rela	ated

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)

Acc	Account Rule Configuration							
Expo	rt Account Rule to C	lient PC	Download					
Impor	nport Account Rule from Client PC Browse							
	Choose file					<u>? ×</u>		
Def	Look in:	🔄 User Accou	nt List Configuration	Ŧ	🔶 🖻 💣 🎟 •			
4 <b>4</b> O	CONTRACTOR History	IM_Rule_List	.csv					
œ	Desktop							
0								
0	My Documents							
<b>8</b> ©	My Computer	File name:	IM Bule Listosy		Ţ	Open		
0	My Network P	Files of type:	All Files (*.*)			Cancel		
	Drop : Authentication failed or QQ Password invalid O Drop : Always							

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.

WIS 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.

lcon	Name	Description
		Every IM account has a portrait and that means the IM
<b>e</b> 2	Authentication Passed	account is not certificated. But if system added an icon of
	Additional associ	certification near the portrait and that means the IM
		account is certificated.
		It means the applied QQ account and password were
1	Password Correct	passed the authentication and IAR-5000 can record the
		contents of this authenticated QQ account.
		User has not applied the QQ account from IAR-5000 or
	Password Uncertificated	even though he has already add the QQ account but not
		certificated yet. IAR-5000 can not record the contents of
		uncertificated QQ account.
		The user's QQ account and password can not pass the
×	Password Incorrect	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)

IM Service: 44 MS (Bridge Mode Only)	N 🍘 Yahoo 🐣 🔍 🦸	<u>ICQ</u>		
				17
QQ account of default	t rule (Accept) Select All Se	lect None		Add Remove to Accept to Drop
- 🗆 🔒 707756738	Macquyer			
	□ AirLive-03 539208436	□ <mark><sup>9</sup> <u>AirLive-03</u> </mark>	□ <sup>S</sup> <u>AirLive-03</u> <u>↑ 539236964</u>	口 <sup>11</sup> 克洛維 <u>11</u> 539330473
🖬 QQ Accept Account 💲	Select All Select None			Add Remove to Default to Drop
🗖 QQ Drop Account Se	lect All Select None			Add Remove to Default to Accept
				174

Figure 5-80 Select IM account

IM Service:	MSN @	Yahoo 🐣 😡	<u>601</u>					
( bridge mode on	·7.)							17
🗖 QQ account	of default rule (	Accept) <u>Select All</u>	Select				<u>A</u> (	dd Remove to Accept to Drop
<b>S</b>	56738	ERIC13 Inacquiver	- Microsol	Are you sure	you want to accer	Dt ?	<u>R</u> 2	
	E-PC 08604	AirLive-03	- ~ r		Cancel		<u>-04∨9Q</u> <u>4</u>	□ <sup>鲁</sup> 克洛維 <u>♪ 539330473</u>
🗖 QQ Accept A	Account Select	All Select None		- 45			A	dd Remove to Default to Drop
🖬 QQ Drop Ac	count Select Al	Select None					Add	Remove to Default to Accept
								1/

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

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

IM Service: 44 M (Bridge Mode Only)	SN 🍘 Yahoo 🤌 😡 👹	<u>ica</u>		17
QQ account of defau	ilt rule (Accept) Select All Se	lect None		Add Remove to Accept to Drop
<mark>1</mark>				
AirLive-03	□ <mark><sup>¶</sup> <u>AirLive-03</u> <u>√ 539208474</u></mark>	□ <sup>¶</sup> <u>AirLive-03</u> <u>↑</u> 539236964	□ <sup>1</sup> <u>克洛維</u> <u>1</u> <u>539330473</u>	
🗖 QQ Accept Account	Select All Select None			Add Remove to Default to Drop
macqyver				
🗖 QQ Drop Account 🙎	elect All Select None			Add Remove to Default to Accept
÷.				1.71

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)

hanson@airlive	cannyc@hotmail	prankcat0109@m.	CCC_anny@msn.c	erictlydog@hot
	nusoft07@hotma	house0619@hotm	SUKENT77_ sukent@hotmail.	「 <sup>19</sup> 五巻二七 jack@airlive
- <mark>曾</mark> 克洛維 lecyiluna@hotm	C SSEE			
ISN Accept Account Sel	ed All Select None		l.	Add Remove to Default to
julie@airlive	E \$172.19.100.82 steve@airlive	口 <sup>172.19.50.16</sup> airlive2006@hot	Support @airlive	iack54@airlive.
jackie @airlive	irive04@hot	iov airlive@hot	airlive01@hot	airliveD2@hot
SIMSAN		E States States	E 1000000000000000000000000000000000000	

Figure 5-83 Add MSN account of default rule

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

Add Account Policy			
IM Protocol	🔏 MSN		
Account	hello@hotmail.com (Max. 128 characters)		
Policy 🔽 Default 🗖 Accept 🗖 Drop			
	OK Cancel		

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.

Default Setting of P2P Ri	ule (Bridge Mode Only)			
🏠 Edonkey	Accept O Drop	R Bit Torrent	Accept O Drop	
🛞 WinMX	Accept O Drop	🥝 Foxy	Accept O Drop	
KuGoo	Accept O Drop	i 🍎 AppleJuice	Accept O Drop	
🦈 AudioGalaxy	Accept O Drop	😕 DirectConnect	Accept O Drop	
🚳 iMesh	Accept O Drop	MUTE		
K Thunder5	Accept O Drop			

## Figure 6-1 P2P Management Default Rule

OK Cancel

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.

P2P Service: (Bridge Mode Only)	Conkey	<mark></mark>	WinMX <u>DirectConnect</u>	Foxy Mesh	
	<u> </u>				171
🖻 Edonkey accol	unt of default rule ( <u>C</u>	omment) Select All Selec	t None		to Accept to Drop
📙 🗾 🔮 Gateway	🗖 😫 Ja	cky_NB	DCT1005		
🗐 Edonkey Accep	ot Account Select All	Select None			to Default to Drop
📙 🛄 🔮 Jacky					
🗏 Edonkey Drop	Account Select All S	elect None			to Default to Accept
					171



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)

	Select Subnet or Department/Group : 🚜 Subnet 🛛 🏨 Department / Group					
					1/1	
	Subnet: 172.19.0.0		2			
-	<b>172.19.0.2</b>	<b>1</b> 72.19.1.254	<b>§</b> <u>172.19.100.112</u>	<b>§</b> <u>172.19.100.14</u>	§ <u>172.19.100.16</u>	
-	<b>172.19.100.35</b>	<b>1</b> 72.19.100.36	<b>§</b> <u>172.19.100.37</u>	<b>§</b> <u>172.19.100.41</u>	<b>§</b> <u>172.19.100.45</u>	
-	<b>172.19.100.56</b>	<b>172.19.100.57</b>	<b>§</b> <u>172.19.100.62</u>	<b>§</b> <u>172.19.100.64</u>	<b>§</b> <u>172.19.100.65</u>	
-	<b>172.19.100.66</b>	<b>172.19.100.68</b>	<b>§</b> <u>172.19.100.69</u>	<b>§</b> <u>172.19.100.71</u>	<b>§</b> <u>172.19.100.74</u>	
	<b>\$</b> <u>172.19.100.78</u>	<b>1</b> 72.19.100.79	<b>§</b> <u>172.19.100.80</u>	<b>§</b> <u>172.19.100.82</u>	<b>§</b> <u>172.19.100.85</u>	

Figure 7-1 Select subnet classification

	Select Subnet or Depar	tment/Group : 🚜 Subnet	😫 Department / Group		
_					1/1
	Department / Group : Grou	p_1			
ŀ	<b>1</b> 72.19.0.2	<b>172.19.100.112</b>	<b>1</b> 72.19.100.14	<b>§</b> <u>172.19.100.16</u>	<b>172.19.100.35</b>
-	<b>1</b> 72.19.100.36	<b>172.19.100.37</b>	<b>§</b> <u>172.19.100.41</u>	<b>§</b> <u>172.19.100.45</u>	<b>§</b> <u>172.19.100.56</u>
ŀ	<b>1</b> 72.19.100.57	<b>172.19.100.62</b>	<b>§</b> <u>172.19.100.64</u>	<b>§</b> <u>172.19.100.65</u>	<b>§</b> <u>172.19.100.66</u>
ŀ	<b>1</b> 72.19.100.68	<b>172.19.100.69</b>	<b>§</b> <u>172.19.100.71</u>	<b>§</b> <u>172.19.100.74</u>	<b>§</b> <u>172.19.100.78</u>
-	<b>1</b> 72.19.100.79	<b>172.19.100.80</b>	<b>§</b> <u>172.19.100.82</u>	<b>§</b> <u>172.19.100.85</u>	<b>§</b> <u>172.19.100.89</u>
-	<b>1</b> 72.19.101.5	<b>172.19.101.6</b>	<b>§</b> <u>172.19.11.44</u>	<b>§</b> <u>172.19.138.109</u>	<b>§</b> <u>172.19.19.0</u>

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)

Select Subnet or De	epartment/Group : 斗 S	Subnet Subnet / Group
🖬 Subnet : 192.168.1.0	10	
	S Jacky NB	<b>S</b> <u>OCT1885</u>
🔊 Today Log		
SMTP		
🌤 РОРЗ		
🧶 НТТР		
N 🏀		
🖄 Web SMTP		
🚵 Web POP3		
😫 FTP		
A TELNET		
🐻 Custom View		

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)

E-Mail	- Macroo	oft indenset B	states			X Dia
File	Edit	View	Favorites	Tools	Help	16
Gran	ward)					
From:	Ken	re @aidive	e.com>			
Date:	Pri.	27 Jan 2006	14 31 56 +0800			
To:	kia	ne @aidioo	e.com>			
Ce	<hr< th=""><th>ss@aidiu</th><th>(e.com)</th><th></th><th></th><th></th></hr<>	ss@aidiu	(e.com)			
Subier	t BRO	MANA MPC	ORT AND EXPORT O	COMPANY PL	c	
Attach	ed All	ach tie list				
Atta I I repr Polya	sent B eric Po	ROWNMI	J IMPORT AND	EXPORT	COMPANY PLC	; hased in UK. My company market and export
We an Ameri assist	e searc ica as v ince to	hing for re rell as mail stand as o	presentatives wh ting payments th ar representative	io can help rough you in your co	us establish a m as our payment o ountry.	sdium of getting to our customens in Europe and fficer. It is upon this note that seek your
Note will b	hat, as t paid i	our repres	entative, you will cont we will ava	Il receive l'	0% of whatever a	mount you clear for the company and the balance

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)

	19,100011 109 109	t Exberiet			
File E	dit View	Favorites	Tools	Help	<b>1</b> -
	(0)				
From:	<eve@airli< td=""><td>ve.com&gt;</td><td></td><td></td><td></td></eve@airli<>	ve.com>			
Date:	Fri, 27 Jan 20	06 14:31:56 +0000			
To:	<jane @airl<="" td=""><td>ve.com&gt;</td><td></td><td></td><td></td></jane>	ve.com>			
Cc	<boss@air< td=""><td>live.com&gt;</td><td></td><td></td><td></td></boss@air<>	live.com>			
Subject:	BROWNMUN	PORT AND EXPORT O	COMPANY PU	c	
Attached	Altach tile its	L			
21/22 B London REPLY	uckingham Pi L14 2AA TO : robin_o	alace Road astro@walla.com			
21/22 B Loadon REPLY Atta Fri I represe	uchingham Pi L14 2AA TO : robin_r rad, rad, rad BROWNB	astro@walls.com	EXPORT	COMPANY PLC based in UK. My company market and export	
21/22 B London REPLY Atta Fri I repres Polymer We are : America	uckingham P: L14 2AA TO: robin_r end, ent BROWNN ic Polyol and searching for a s well as m cc to stand as	astro@walla.com AU IMPORT AND other products for representatives wi aking payments th aking payments th	) EXPORT e world trac to can help trough you t in your co	COMPANY PLC based in UK. My company market and export de. us establish a medium of getting to our customers in Europe and as our payment officer. It is upon this note that seek your varty.	

- 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)

2006-08-08 (1 records)									
Q		🔮 Rayearth (IM)	171						
	Dialogue Duration 🔻	Participants	8⇔2						
	08/08 09:47:17 10:08:38 (21.21 min.)	- 🚳 richardwu22@msn.com	<u>15</u>						
			1/1						
		Clear 🔽	Clear All						
			(						

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)

ile Dow	nload			2
?	Some files can looks suspiciou save this file.	harm your comput is, or you do not fu	er. If the file inform illy trust the source	ation below e, do not open or
	File name:	name.jpg		
	File type:	ЛРG		
	From:	172.19.0.1		
	Would vou like	to open the file or	save it to your co	mputer?
	Open	Save	Cancel	More Info
	Always ask	before opening th	is type of file	

Figure 7-7 Download the file from FTP

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

	2006-07-28 (1 records)	•	
Q	😫 Rayearth ( TELNET	)	1/1
	Date / Time	Host Name	Detail
	07/28 09:45 07/28 09:45 (0.4 分)	bbs.kkcity.com.tw	<u></u>
			1/1
		C	lear 🔽 Clear All

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

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

🚰 TELNET detail - Microsoft Internet Explorer	
	-
[CLEAN]	
C I T Y ?span style="Color:#66FFFF">?span style="Color:#66FFFF"??span style="Color:#66FFFF"??span style="Color:#66FFFF"?"?span style="Color:#66FFFF"?"?span style="Color:#66FFFF"?"?span style="Color:#66FFFF"?"?span style="Color:#66FFFF"?"?span style="Color:#66FFFF"?"?"?"?"?"?"?"?"?"?"?"?"?"?"?"?"?	tyle 1-co
【KKCITY】有人客來驗~(目前共有 S110 個居民在遊蕩中)	
<pre>?span style="background-color:red"&gt;活動時間 ?span style="background-color:black"&gt;2006年2月11日 21:00 於 XKeity/Activitiesf ?span style="background-color:red"&gt;活動時間 ?span style="background-color:black"&gt;2最快答對元官還謎題目者,好種送到家!紛多</pre>	<mark>反(</mark> 與日
請輸入代號: ★ 輸入 [guest] 參觀,以 [new] 註冊 11. 班時回相 http://www.kkk/ty.uww.lt////www.guest	

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

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

User Name	Sender 🕶	Recipient -	Subject (Click to view content)	
			1	41
	Search Sorting t	ch result 1 records by Date / Time: 1 - 1		
			and the	
Attache	d 🔽 Non-Attache	d	Rearch	
	1		a	
before t	his date : 2006 7 / 3	¥ 123 ¥ 16 ¥ 11 ¥	1	
C attert	nie data : 2006 💌 / 3		1	
Use	er Name :			
	Subject :			
	Sender : julie			
R	ecipient :			
Enter keywo	rd or phrase			
	Enter keywo R Use T atter ti Defore ti Attache	Enter keyword or phrase Recipient : Julie Subject : Julie User Name : Attached	Enter keyword or phrase Recipient : Sender : julie Subject : User Name :  Atteched  Control of this date : 2006 (3) (23) (0) (0) Control of this date : 2006 (3) (23) (16) (11) Control of this date : 2006 (13) (23) (16) (11) Control of this date : 2006 (13) (23) (16) (11) Control of this date : 2006 (13) (23) (16) (11) Control of this date : 2006 (13) (13) (23) (16) (11) Control of this date : 2006 (13) (13) (12) (16) (11) Control of this date : 2006 (13) (13) (12) (16) (11) Control of this date : 2006 (13) (13) (12) (16) (11) Control of this date : 2006 (13) (13) (12) (16) (11) Control of this date : 2006 (13) (13) (12) (16) (11) Control of this date : 2006 (13) (13) (12) (16) (11) Control of this date : 2006 (13) (13) (12) (16) (11) Control of this date : 2006 (13) (13) (12) (16) (11) Control of this date : 2006 (13) (13) (12) (16) (11) Control of this date : 2006 (13) (13) (12) (16) (11) Control of this date : 2006 (13) (13) (12) (16) (16) (11) Control of this date : 2006 (13) (13) (12) (16) (16) (16) (11) Control of this date : 2006 (13) (13) (12) (16) (16) (16) (16) (16) (16) (16) (16	Enter keyword or phrase  Recipient : Sender : julie Subject : User Name :  Attached  Search  S

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 <sup>[</sup>
    - 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.

Verify 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.

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 $\rightarrow$ Service $\rightarrow$ IM. (Figure 7-12)

<b>Air Live</b>	Record > Service > IM		0	
■ System ■ User List	q	2007-05-04	I (1 records) 💌	171
🗉 IM Management	Dialogue Duration 🔻	User Name	Participants	8⇔8
P2P Management	05/04 10:10:11 10:10:28 (0.17 min.)	Jacky	- 🚳 sebastienko@hotmail.com	_2
E Record				171
∎ User				Clear 🔽 🛛 Clear All
Service				Contraction of Contra
–⇒ SMTP				
<b>_</b> ⇒ POP3				
–⇒ HTTP				
— <b>→</b> IM				
→ Web SMTP				
Anomaly Flow IP				
🗉 Local Disk				
🖪 Remote Backup				
E Report				
🗉 Status				

Figure 7-12 IM

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

		2007-05-0	)4 (1 records) 💙	
Q				1/1
	Dialogue Duration 🔻	User Name	Participants	8⇔8
	05/04 10:10:11 10:10:28 (0.17 min.)		- 🚜 sebastienko@hotmail.com	_2
				171
			Cle	ar 🔽 🚺 Clear All



<b>)</b> h	ttp://1	92.16	8.1.254	- [MSN	Recording	Jacky (20	07-05-04	10.10.11	- 10.10.28	) - Micro	osoft Int	ernet Exp	lorer (	
ile	Edit	View	Favorites	Tools	Help									
	Type	Hee	er Name		Dialoque Di	uration				6439				
	88		Jacky	10:10	0:11 10:10:2	8 (0.17 min.)	airlive	_jacky@hotn	nail.com	↔	seba	stienko@hot	mail.com	
f	Date/	Time						Content						
	05/04 1	0.10.11	airlive_j	jacky@l net Activit	<b>hotmail.com</b> ty Recorder te:	: st								
			Jacky: J Gotit	只剩下-	-篁Manual3	長校對	II :							
	nne											🥑 Int	ernet	

# 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)



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

	2007-05-04 (1 records) 💌										
Q					4.0		171				
	Date / Time 🔻	User Name	<u>Sender</u>	Recipient		Subject (Click to view the con	tent)				
		Jacky	sebastienko@seednet.ne.	jacky ko@airlive.com		Web Mail recording test					
							171				
						Clear 🗸	Clear All				

Figure 7-16 Click the subject in Web SMTP

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





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)

	2006-08-10 (1 records)									
Q					171					
	Date / Time 🔻	User Name	Sender 🔻	Recipient 🕶	Subject (Click to view the content)					
	08/10 09:49	TCLIN_27	Administrator@srv.nuso	Administrator@59.124.3	- test bu(h)					
					Subject : test bug? 1 / 1					
					Clear Clear All					

Figure 7-19 Click the subject in Web POP3

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

E-Mail - Microsoft Internet Explorer	
Sender: administrator@srv.airlive.com	
Date: 2006/8/8 [星期二] 下午 06:17	
Recipient: administrator@srv.airlive.com	
Subject: test bug?	

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)

Q						1	1 / 406 幹
	Date / Time 🔶	<u>User Name</u> 🗸	<u>Host Name</u> 🗸	Login ID : Password 🗸	Direction 🗸	<u>File Name</u> 🔫	<u>Size</u> 🗸
	03/21 09:56	192.168.139.85	59.124.36.163	steve : steve	Download	FlexLexer.h	2 KB

Figure 7-21 Click the FTP record

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

File Dowr	nload			×
?	Some files can h looks suspicious save this file.	arm your compute , or you do not fully	r. If the file informa v trust the source,	ation below , do not open or
	File name:	FlexLexer.h		
	File type:			
	From:	192.168.139.139		
	Would you like t	o open the file or s	ave it to your con	nputer?
	Open	Save	Cancel	More Info
	Always ask I	pefore opening this	type of file	

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)

🚰 TELNET detail - Microsoft Internet Explorer	
Red Hat Linux release 7.2 (Enigma)	
Kernel 2.4.7–10 on an i586	
login: nusoft	
Password:	
Last login: Mon Jul 31 19:04:40 from 172.19.100.57	
[nusoft@dnsl nusoft]\$ su -	
Password:	
[root@dns] root]# useradd eric	
[root@dnsl root]# passwd eric	
Changing password for user eric	
New password:	
BAD PASSWORD: It is based on a dictionary word	
recype new password:	
passwo. all authentication tokens updated successfully	
Togott	
[CLEAN AFTER]	
[nusoff@dns] nusoftl\$ exit	
logout	
[CLEAN AFTER]	

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)

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 )
	OK Cancel

## Figure 8-1 Enter the ip and netmask

Non-detected IP	
IP Address / Netmask	Configure
172.19.100.111 / 255.255.255.255	Modify Remove

New Entry

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)

er Name	Virus-infected IP	MAC Address	Alarm Time
.IVE_2007	172.19.50.7	00:01:80:5F:B0:6C	2006-02-23 15:49:52

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)

File Edit	t View	Tools Mess	age Help					
Ø₽ Reply	Gev Reply All	92 Forward	Print	) Delete	A Previous	< ≫ Next	Addresses	
From: Date: To: Subject:	IAR-5000 2006年 rd@airliv IAR-5000	) 2月23日で e.com ) Alarm of Mru	午 11:49 is-infected	User!				
Time: T	hu Feb	23 15:49: nachine r	:52 200	б re heen i	nfected b	v virus	40	-
Sourc	ce IP: 17	72.19.50. :80:5F:B0	7 9:6C	000001	moored b,	y 1140		
User	Name:	AIRLIVE_	5438 VE 543	8				
NetB	100 1401	and a state		5765 c				

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)

Alarm Time	Intrusion IP	
2006-02-23 16:27:57	172.29.50.12	
Clear Downlos		

Figure 8-5 The notification of intrusion IP

If the system administrator selects Anomaly Flow IP  $\rightarrow$  Setting  $\rightarrow$  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).

Total Hard Disk Space : 230 C	∋Bytes		
Estimated Storage Utilization a	and Percentage : Total ( 6.03 GE	1, 2.44% )	
SMTP ( 209.12 MB	0.08%) POP3 ( 215.91 f	MB, 0.09% ) HTTP ( 941.91 MB, 0.3	8%) IM (5.20 MB, 0.00%)
Web SMTP ( 21.64	MB, 0.01%) Web POP3 ( 2.6	9 MB, 0.00% ) FTP ( 4.64 GB, 1.88%	) TELNET (1.14 MB, 0.00%)
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
🏁 РОРЗ	30.84 MB	06/08/02 ~ 06/08/08	7 Days
<i>ð</i> € HTTP	134.56 MB	06/08/03 ~ 06/08/08	7 Days
🍓 M	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
			OK Cancel

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.

NO.	User Name	MBytes	
4	172.19.50.6	96.16	45.99%
2	JOSH12	42.07	20,40%
з	JULIE	21.30	10.19%
4	DXJ	11.85	6.67%
5	COMPUTERCANDY		5,25%
8	Rayearth	10.44	4.99%
7	172.19.100.89	3.65	1.70%
8	172.19.100.81	2.65	1,22%
9	AIRLIVE-WIN	2.13	1.02%
10	172.19.100.71	1.64	0.78%

NO.	User Name	MBytes	
1	172.19.100.82	45.19	20.93%
2	Rayearth	40.50	18,78%
3	JULIE	29.50	13.07%
4	172.19.100.46	19.52	9.04%
5	ADFIN01	10.95	0.78%
0	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	6.60	3.09%
10	JACKIE-PC	6.19	2.87%

9	AIRLIVE-WIN	2.13	1.02%
10	172.19.100.71	1.64	0.78%
		Total Used Disk Space: 2	09.12 ME
d H	TTP		
NO.	User Name	MBytes	
4	172.19.50.11	149.02	18.31%
2	172.19.100.82	135.39	18.84%
з	AIRLIVE-WIN	108.67	13.35%
4	Rayearth	67.77	7.10%
5	COMPUTER001	37.11	4.58%
0	172.19.50.8	33.39	4.10%
1.4			Contraction in the

NO.	User Name	MBytes	
1	JERRY	2.30	53.38%
2	Rayearth	0.68	15.22%
3	172.10.100.31	0.59	13.29%
4	我是粘六	0.59	13.29%
5	JULIE	<b>0.12</b>	2.78%
0	172.19.100.46	0.07	1.55%
7	172.19.60.6	< 0.01	0.19%
8	JACK54	< 0.01	0.10%
9	北部投76	< 0.01	0.09%
10	DAVID	< 0.01	0.04%

7 172.19.100.45 28.63	3.534
	3704.16
8 JU07 4111 27.32	3.36%
9 COMPUTER001 27.31	3.36%
10 JERRY 20.51	2.52%
Total Used Di	tk Space: 813.72 MB
Web SMTP	
NO. User Name M	Bytes
NO. UserName M 1 JERRY	Byles 18,72 77,27%
NO.         User Name         M           1         JERRY	Byles 16.72 77.27% 18.64%

0.11

< 0.01 < 0.01

< 0.01

< 0.01

< 0.01

< 0.01

4

5

0

7

8

.

10

172.19.50.6

TCUN\_27

172.19.100.62

JOSH12

COMPUTER001

172.19.50.11

172.19.50.16

NO:	User Name	MBytes	
1	JERRY	1.28	47.65%
2	172.19.50.16	1.03	38.30%
з	172.10.60.6	0.19	7.04%
4	TCLIN_27	0.15	5.69%
5	COMPUTER001	0.02	0.60%
0	JOSH12	< 0.01	0.33%
7	Rayearth	€ 0.01	0.18%
0	我是點六	< 0.01	0.11%
9	172.19.100.02	< 0.01	0.10%
10	JACKIE-PC	< 0.01	0.03%

2 F1	P	33	
NQ.	User Name	OBytes	
1	Rayearth	2.58	55.00%
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%
0	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 GI

20	TE	LN	ET
1	-	-	

0.53%

0.01%

0.01%

0.01%

0.00%

0.00%

0.00%

NO.	User Name	KBytes	
1	172.19.100.82	584.22	59.05%
2	JERRY	90.40	9.24%
3	DAVID	76.09	7.77%
4	SUKENT77	75.94	7.75%
5	172.19.100.31	72.03	7.42%
6	COMPUTERCANDY	22.99	2.35%
7	172.19.100.45	# 17.69	1.81%
8	DXJ	9.87	0.99%
0	JUSTIN72	9.11	0.93%
10	JERRY	6.47	0.66%

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 → Setting.

## To set the backup folder

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

E-mail Setting		
The recorder appliance sends ma	all notice after backup had completed	
From SMTP Server	airlive.com	
To E-mail Address 1	jerry@airlive.com	

#### 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)

Backup Setting		
Enable Backup		
Backup Path		
Computer Name / IP	172.19.1.106	_
Shared Directory	cr_backup	
Login ID	airlive	
Password	*****	
Connect Test of Backup Path	Test	

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)

Service	SMTP	♥ POP3 ♥ Web POP3		IM I▼ FTP
Backup starts at		every day every Sunday on the first day	vevery month	
			OF	Cancel

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)

Connection Status of Remote Hard Disk	
Connection Status: Success (Privilege: Read/Write)	
Disk Space for Backup (06/10/12): 142.4 MBytes	
Hard Disk Utilization (Total: 22.6 GBytes, Free Disk Space: 1.6 GBytes)	

#### 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)

Address 🙀 CR_backup											
	disk_check	ftp_article	ftp_article	ftp_article	ftp_event	ftp_event	ftp_event	http_article.	http_article	. http_article	-
CR_backup	_										
■ This folder is <b>Online</b> . Select an item to view its description.	http_article	. http_article	http_article	http_article	. http_article	http_article	. http_article	http_article.	http_article	. http_article	
Capacity: 22.6 GB	nttp_article	. http_article	http_article	nttp_article	http_article	http_article	. http_article	http_article.	http_article	. http_article	
Free: 1.55 GB											
	nttp_article	. http_article	nttp_article	http_article	http_article	http_article	. http_article	http_article.	http_article	. http_article	
	http_article	. http_article	http_article	http_article	http_article	http_article	. http_article	http_article.	http_article	. http_article	
See also: <u>My Documents</u> <u>My Network Places</u> <u>My Computer</u>	nttp_article	. http_article	http_article	nttp_article	nttp_article	http_article	. http_article	http_article.	http_article	. http_article	
	nttp_article	. http_article	http_article	http_article	http_article	http_article	. http_article	http_article.	http_article	. http_article	
	kttp_article	. http_article	internation in the second seco	nttp_article	http_article	http_article	. http_article	http_article.	http_article	. http_event	
1 624 object/s)		<b>_</b>		<b>_</b>	<b>_</b>	Chinese I	Taiwan) 🕐	;	21.0 GB	Internet	•

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)

Backup Immediately				
Disk Space for Backup (06/10/	06 - 06/10/11): 2.0 MBytes			
✓ From To	2006 V / 10 2006 V / 10	• / 06 • • / 11 •		
Service	SMTP Veb SMTP	POP3 VVeb POP3	HTTP TELNET	FTP OK

Figure 10-7 Set backup immediately

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

2								X
File Edit View Tools Message Help								
Q# Reply	DV Reply Al	WQ Forward	Pret	X	Previous	-⊘⊁ Next	Addresses	
From: Date: Te: Subject:	steve( Filday, Ok eric @a Backut	Bairlive.c tober 11, 20 iirlive.com Succee	iom # 3131 PM Th d					
Sudgent: Backup Succeed Device Name:IAR-SUCE Date Range: 06/10/12 Result of Backup: Success					2			

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 11<sup>th</sup> 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\_icon\_20060911.MYD 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)

Connection Status: Success (Accept Privi	lege: Read/Write)	
	- <u></u>	
Browse Setting		
Path		
Computer Name / IP	172.19.1.106	
Shared Directory	cr_backup	
Login ID	airlive	
Password	******	
Connect Test of Path	Test	
		OK Cancel

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  $\rightarrow$  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.

Periodic Report		
🔽 Enable E-mail periodic report		
🔽 Yearly report 🔽 Monthly repo	ort 🔽 Weekly report 🔽 Daily report	
		OK Cancel
History Report		
C Yearly report	2006 🔽	
C Monthly report	2006 🔽 03 🔽	
C Weekly report	2006 🔽 03 🔽 19 🔽	
C Daily report	2006 🔽 03 🔽 21 🔽	Send Report





Figure 11-2 The storage report

History Report		
Yearly report	2006 💌	
C Monthly report	2006 🔽 03 🔽	
C Weekly report	2006 🔽 03 🔽 19 🔽	
O Daily report	2006 🔽 03 🔽 21 🔽	Send 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  $\rightarrow$  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)

	Hard Disk Utilization (Total Disk Space 230 GBytes)
	Figure 11-7 The hard disk utilization
Step2.	Today's Utilization, it is displayed in

- 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 \_\_\_\_\_. (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. (Figure 12-2)

- 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 Q, to search the related connection information. (Figure 12-5)

Q Refresh Manually	•		1/1
Service	<u>Total Traffic</u> 🔻	Established / Unreplied Number	Session Number 🔻
S ALL	30.5 MB	2536 / 1	2537
😂 <u>FTP</u>	22.1 MB	1991 / 0	1991
<u>ð http</u>	7.8 MB	421 / 1	422
Market POP3	204.7 KB	70/0	70
SMTP	360.8 KB	45/0	45
<u>∿∎ M</u>	59.9 KB	7/0	7
🔀 WebMail	37.0 KB	2/0	2
			1/1

#### Figure 12-3 Connection record

Refresh Manually	•	IM Service	•			<b>4</b> 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.msq.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
8 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
3	172.19.100.45	207.46.0.64	TCP 57105 => 1863	18:16:27	248.0 B	Established
<table-of-contents> airlive01@hotmail.com</table-of-contents>	Ravearth	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
8	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	TOP 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
8 372136019	AIRLIVE-20-9	219.133.38.232	TCP 1120 => 80	11:24:59	12.0 KB	Established
🔏 airlive01@hotmail.com	Ravearth	207.46.4.52	TCP 1315 => 1863	09:50:20	261.6 KB	Established

Figure 12-4 System shows all connection information

Search							
	Enter ke	word or phrase					
		Service :	M				
		Status :	Established				
		Distancel :					
		Protocol.		-			
		Source IP :	172.19.100.111	(Max. 15 characters)			
		Destination IP :		(Max. 15 characters)			
		Port :	->	(Range: 1 - 65535)			
							Search
			Search results : 5 rec	ords			4111
Service 🔻	User Account 💌	Source IP 🔻	Destination IP -	Port -	Start Time 🔻	Traffic 💌	Status -
🚳 MSN	1	Rayearth	64.4.36.40	TCP 1427 => 1863	09:28:25	284.0 B	Established
🚳 MSN	airlive01@hotmail	Rayearth	207.46.4.81	1046 => 1863	07:31:43	63.8 KB	Established
🚳 MSN	airlive01@hotmail	Rayearth	207.46.7.13	TCP 1529 => 80	18:17:15	40.6 KB	Established
🚳 MSN	airlive01@hotmail	Rayearth	207.46.0.82	TCP 1439 => 1863	17:53:26	42.4 KB	Established
					1		
🚳 MSN	airlive01@hotmail	Rayearth	207.46.4.52	TCP 1315 => 1863	09:50:20	261.6 KB	Established

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 Q, and search the event. (Figure 12-7)
  - Click<sup>2</sup> , IAR-5000 shows the event information in detail. (Figure 12-8)

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

#### Figure 12-6 Event log

#### Search

Jul 25 14:45:30

admin

	Enter	keyword or phi	rase	
		Ev	vent : Non-detected IP	
		🔽 Fr	rom : 2006 💌 / 7 💌 / 19 💌 9 💌 : 29 💌	
			To: 2006 ▼ / 8 ▼ / 9 ▼ 9 ▼ : 32 ▼	
				Search
Results				
			Search result: 3 records	
Download			View: 1 - 3 💌	<b>4</b> 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	<u> </u>
Jul 25 14:45:39	admin	172.19.100.57	[Anomaly Flow IP] Add Anomaly Flow Non-detected IP 172.19.100.57	<u></u>



172.19.100.57 [Anomaly Flow IP] Remove Anomaly Flow Non-detected IP 172.19.100.57

Date / Time	Admin Name	IP Address	Event	
ug 8 16:54:52	admin	172.19.20.13	[Anomaly Flow IP] Add Anomaly Flow Non-detected IP 172.19.100.111	
			Detail	
0 del marco	ID Address			
Add new	IP Address			
Add new	IP Address s	172.19.100.111		
Add new IP Address Netmask	IP Address s	172.19.100.111	5 ( 255.255.255.255 means the specified PC )	

Figure 12-8 System shows event log in detail