



IAR-5000

Internet Activity Recorder

User's Manual





Copyright & Disclaimer

No part of this publication may be reproduced in any form or by any means, whether electronic, mechanical, photocopying, or recording without the written consent of OvisLink Corp.

OvisLink Corp. has made the best effort to ensure the accuracy of the information in this user's guide. However, we are not liable for the inaccuracies or errors in this guide. Please use with caution. All information is subject to change without notice

All Trademarks are properties of their respective holders.

© 2009 OvisLink Corporation, All Rights Reserved

Table of Contents

1. Introduction	1
1.1 Overview	1
1.2 Firmware Upgrade and Tech Support	1
1.3 Features	2
2. Installing the IAR-5000	3
2.1 Before You Start	3
2.2 Package Content	3
2.3 Knowing your IAR-5000	4
2.4 LED Table	5
2.5 Hardware Installation	6
2.6 Restore Settings to Default	8
3. Configuring the IAR-5000	11
3.1 Important Information	11
3.2 Prepare your PC	11
3.3 Management Interface	12
3.4 Introduction to Web Management	13
3.5 Initial Configurations	16
3.6 About IAR-5000's Menu Structure	21
4. System	22
4.1 Admin	22
4.2 Interface	24
4.3 Settings	25
4.4 Date/Time	30
4.5 Permitted IPs	31
4.6 Logout	32
4.7 Software Update	32
5. User List	34
6. Authentication	46

6.1 Settings.....	46
6.2 Auth User	48
6.3 RADIUS	49
6.4 POP3	60
6.5 LDAP	61
7. IM Management	74
7.1 Login Notice	75
7.2 Default Rule	78
7.3 Account Rule.....	79
7.4 Configuration Example.....	80
8. Application Management.....	89
8.1 Default Rule	89
8.2 Custom Rule	91
9. Record: Settings	93
9.1 Settings.....	93
9.2 Settings Example.....	96
10. Record: User and Service	109
10.1 SMTP	109
10.2 HTTP	115
10.3 IM.....	118
10.4 Web SMTP.....	120
10.5 Web POP3.....	123
10.6 FTP	126
10.7 Telnet	129
10.8 Custom Log	131
11. Record: Access Record	135
11.1 Accessing Emails Sent via SMTP Protocol	135
11.2 Accessing Emails Sent via POP3/IMAP Protocol.....	139
11.3 Accessing Visited Webpages via HTTP Protocol	141
11.4 Accessing Details of an IM Conversation.....	143

11.5 Accessing Emails Sent via Web-Based Email Service.....	146
11.6 Accessing Emails Received via Web-Based Email Service	147
11.7 Accessing Files Transferred via FTP Protocol.....	149
11.8 Accessing Details of Sessions Established via TELNET Protocol..	151
12. Content Auditing	153
13. Anomaly Flow IP	168
14. Local Disk	174
14.1 Storage Time.....	174
14.2 Disk Space	175
15. Remote Backup	177
15.1 Backup Settings.....	177
15.2 Browse Settings.....	180
16. Reporting	182
17. Status	188
17.1 System Info	188
17.2 Authentication	190
17.3 Current Session	190
17.4 IM / Application Log	191
17.5 Even Log.....	192
18. Specifications.....	195

1

Introduction

1.1 Overview

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.

1.2 Firmware Upgrade and Tech Support

If you encounter a technical issue that can not be resolved by information on this guide, we recommend that you visit our comprehensive website support at www.airlive.com. The tech support FAQ are frequently updated with latest information.

In addition, you might find new firmwares that either increase software functions or provide bug fixes for IAR-5000. You can reach our on-line support center at the following link: http://www.airlive.com/support/support_2.jsp

Since 2009, AirLive has added the “Newsletter Instant Support System” on our website. AirLive Newsletter subscribers receives instant email notifications when there are new download or tech support FAQ updates for their subscribed airlive models. To become an AirLive newsletter member, please visit: http://www.airlive.com/member/member_3.jsp

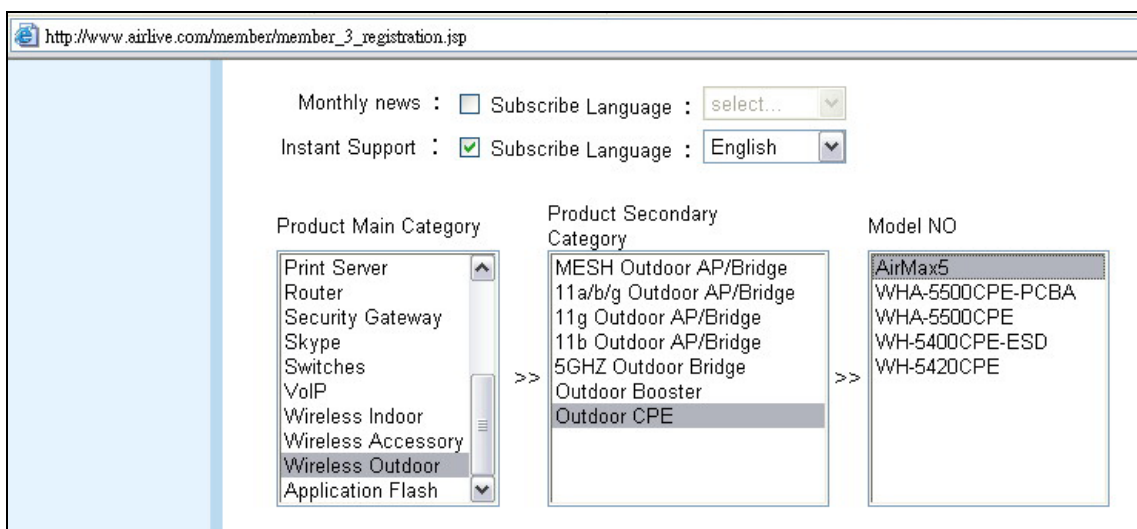


Figure: AirLive Newsletter Support System

1.3 Features

- Sniffer and Bridge mode
- SMTP, POP3/IMAP, HTTP, IM, Web SMTP, Web POP3, FTP, and Telnet Content Record
- IM, P2P, Web mail signature pattern update
- IM Management
- Application Management for Peer-to-Peer Sharing, Multimedia Streaming, Online Gaming, VPN Tunneling, and Remote Controlling program
- User Authentication
- Content Auditing
- Anomaly Flow IP
- Remote Backup

2

Installing the IAR-5000

This section describes the hardware features and the hardware installation procedure for the IAR-5000. For software configuration, please go to chapter 3 for more details.

2.1 Before You Start

It is important to read through this section before you install the IAR-5000

- The IAR-5000 is built-in with hard disk installed, so please install IAR-5000 gently and carefully.
- The default hard disk type and size is IDE 160 GB, you can change higher capacity of hard disk to replace the original one.
- You must power off IAR-5000 before to change hard disk. When new hard disk is installed and power on IAR-5000, system will format hard disk automatically.
- The maximum capacity of IDE hard disk is 750 GB.

2.2 Package Content

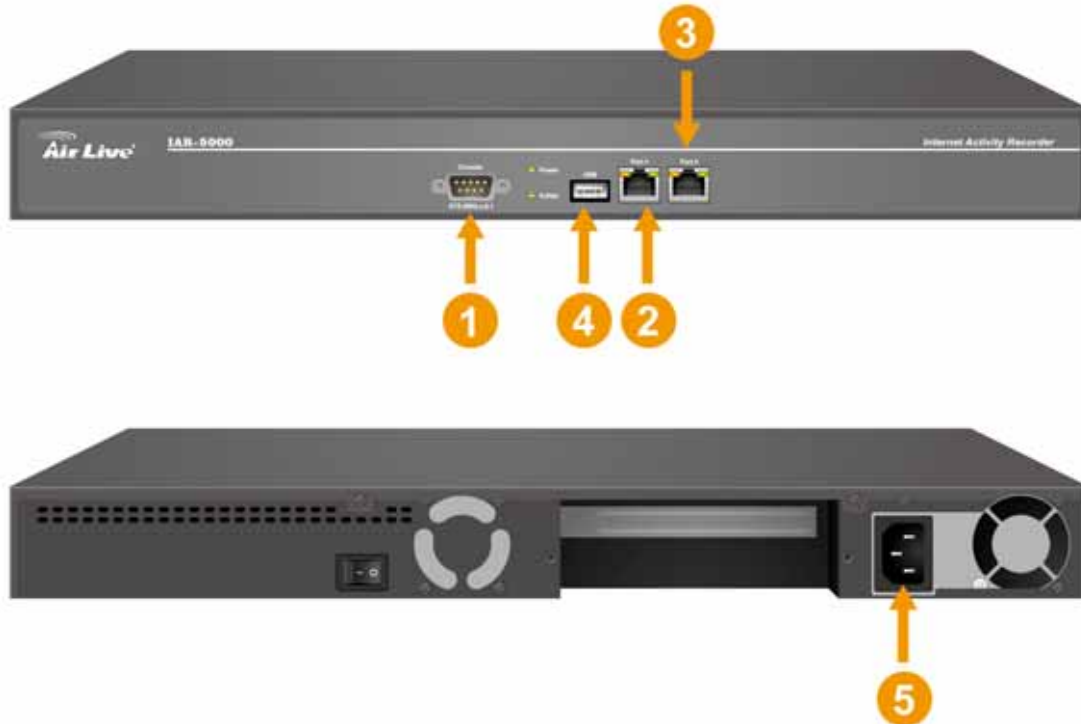
The IAR-5000 package contains the following items:

- One IAR-5000 main unit
- User's Guide CD
- Quick Start Guide
- CAT-5 UTP Fast Ethernet cable
- CAT-5 UTP Fast Ethernet cross-over cable
- RS-232 cable
- Power code
- Rack mount kits and accessories



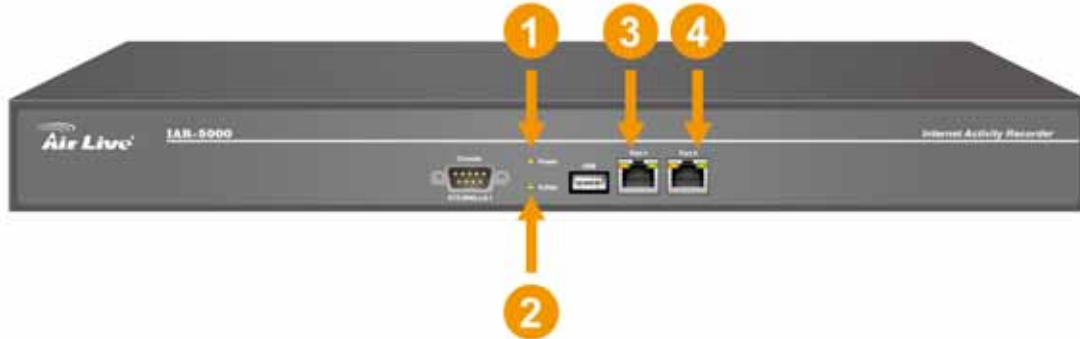
2.3 Knowing your IAR-5000

Below are descriptions and diagrams of the product:



No	Port	Description
1	Console Port	9-pin serial port connector for checking setting and restore to the factory setting
2	Port 1	Use this port to connect to a router, DSL router, or Cable modem router
3	Port 2	Use this port to connect to hub, switch, or switch's mirror port
4	USB	Not Available
5	AC Power	Input voltages ranging from 100 ~ 240 VAC, and with a maximum power output of 85 watts.

2.4 LED Table



IAR-5000:

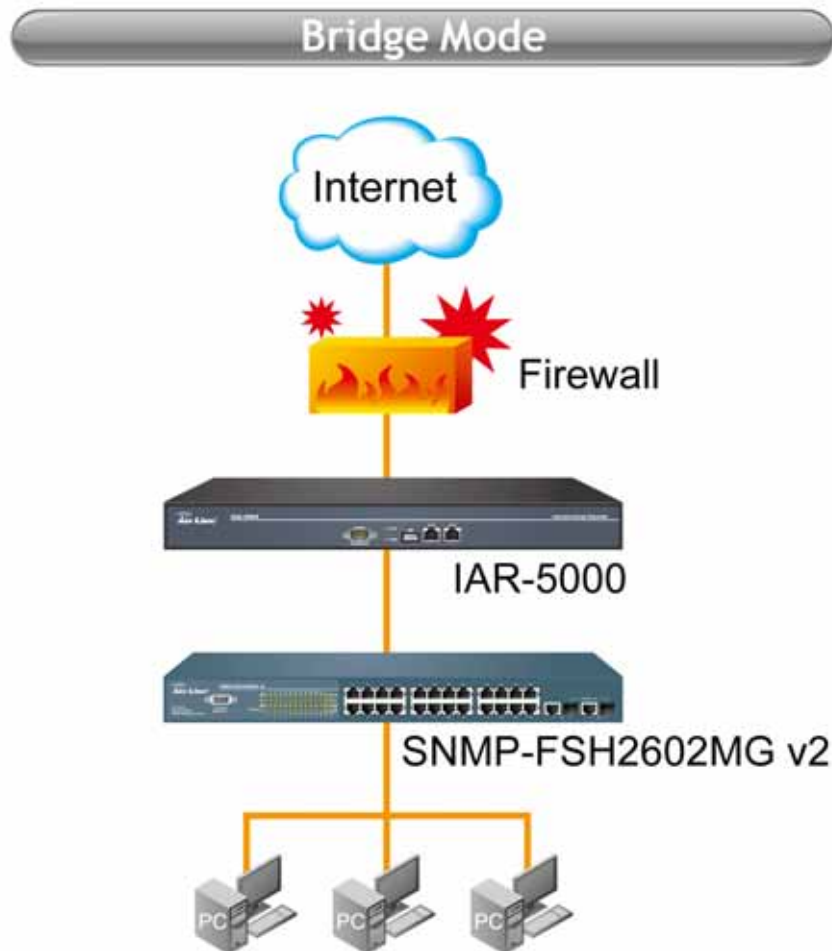
No	LED	Color	Status	Description
1	POWER	Green	On	Power on the device
2	Hard Disk	Green	Blinking	Data reading / accessing
3	Port1 (L)	Orange	Blinking	Sending / Receiving
	Port1 (R)	Green	On	100 Mbps
4	Port2 (L)	Orange	Blinking	Sending / Receiving
	Port2 (R)	Green	On	100 Mbps

IAR-5000 v2:

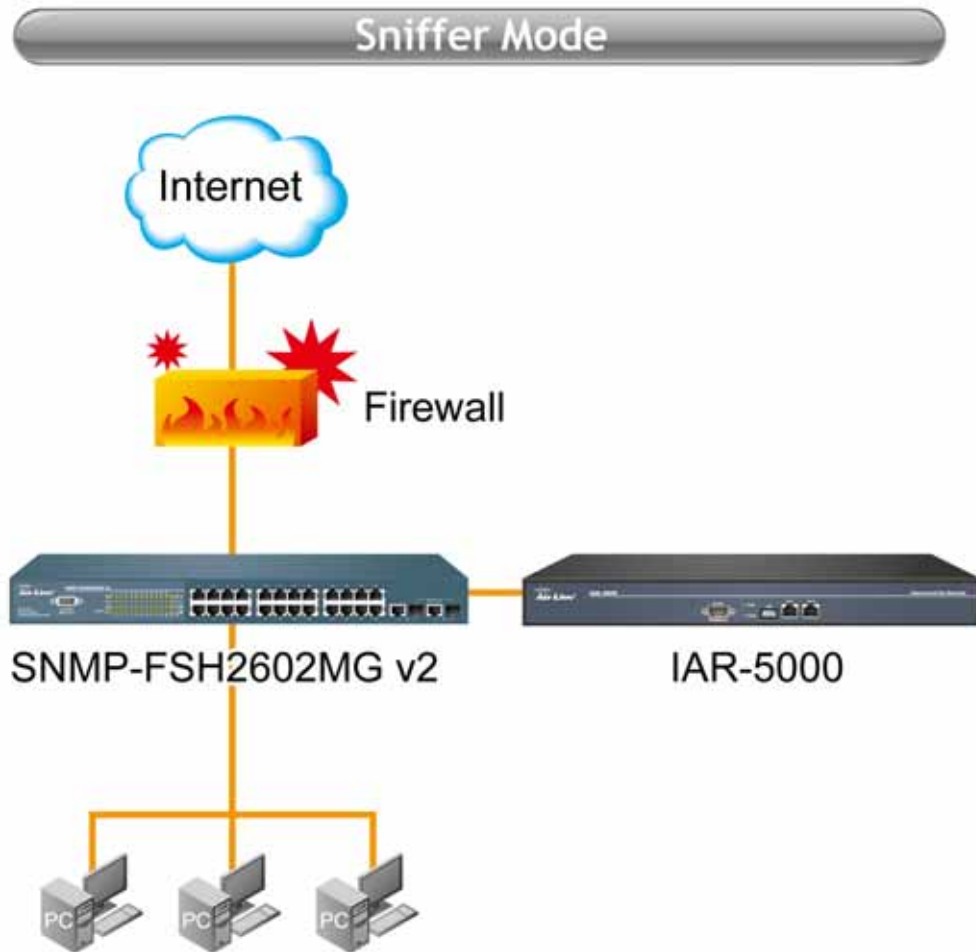
No	LED	Color	Status	Description
1	POWER	Green	On	Power on the device
2	Hard Disk	Green	Blinking	Data reading / accessing
3	Port1 (L)	Orange	Blinking	Sending / Receiving
	Port1 (R)	--	Off	10 Mbps
		Green	On	100 Mbps
	Port1 (R)	Orange	On	1000 Mbps
4	Port2 (L)	Orange	Blinking	Sending / Receiving
	Port2 (R)	--	Off	10 Mbps
		Green	On	100 Mbps
	Port2 (R)	Orange	On	1000 Mbps

2.5 Hardware Installation

- Bridge Mode: Connect the Port 1 to the firewall or gateway and Port 2 to a LAN hub or switch.



- Sniffer Mode: Connect the Port 1 to the mirror port of a core switch or any port available on a LAN hub and Port 2 to the network adaptor of the management PC.



	Sniffer Mode	Bridge Mode
Deployment	Connect Port1 to hub or switch's mirror port	Between LAN and firewall Router
Anomaly Flow IP	Alert only	Alert and Block connection
Application Management	N/A	Yes
IM Management	N/A	Yes
Authentication	N/A	Yes

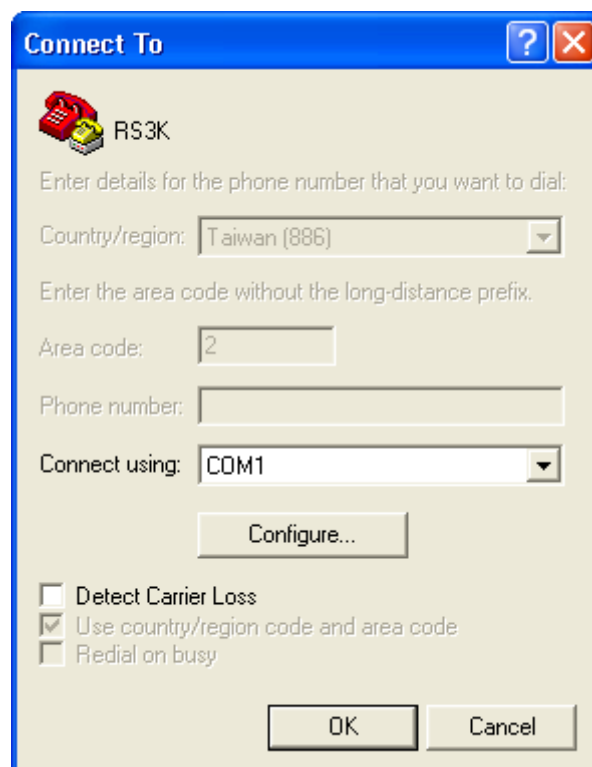
2.6 Restore Settings to Default

If you have forgotten your IAR-5000s IP address, you can restore your IAR-5000 to the default settings by console. Please see diagram below for details.

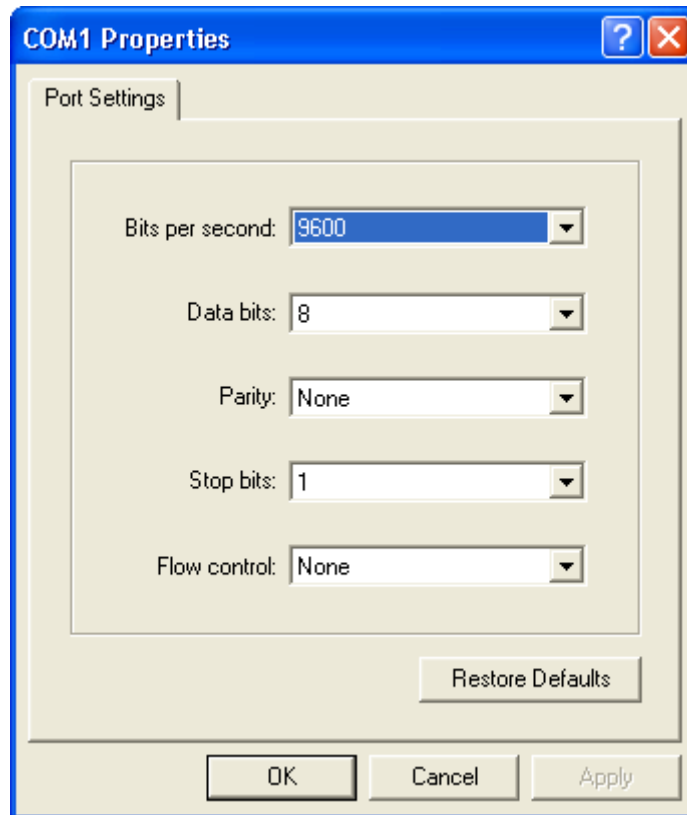
1. Connect 9-pin RS-232 cable to PC and IAR-5000 console port.
2. Open Hyper Terminal program and configure the following settings.
3. Specify a name to the program



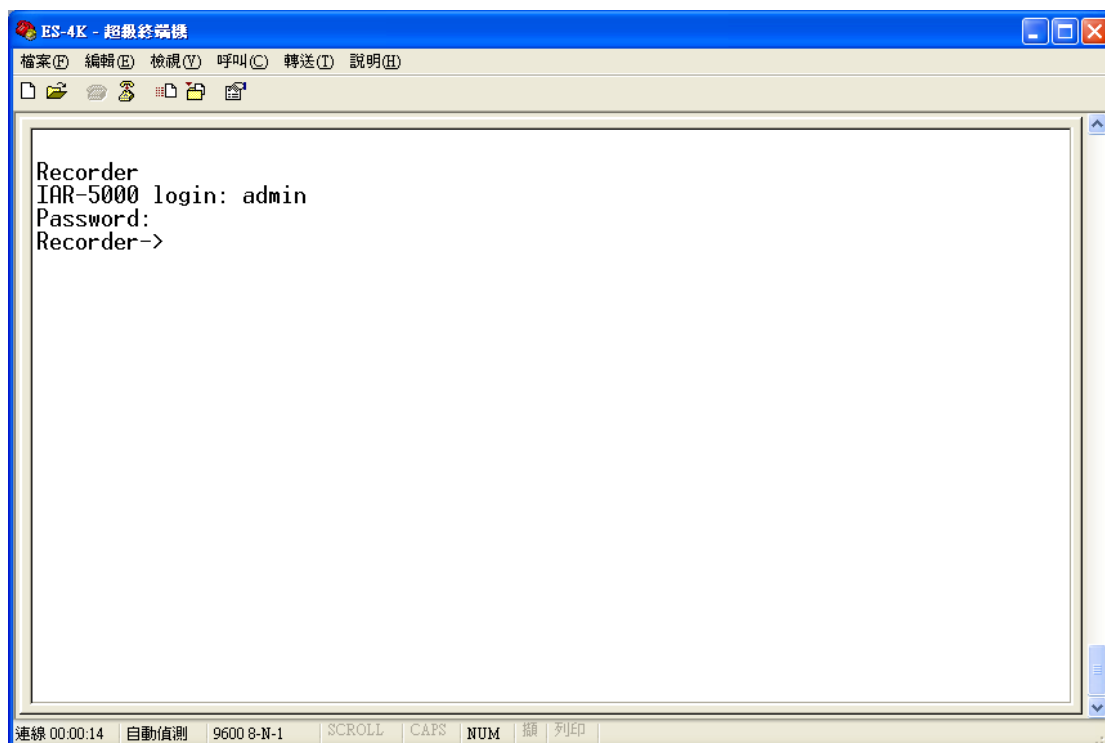
4. Select COM1 as the connecting type



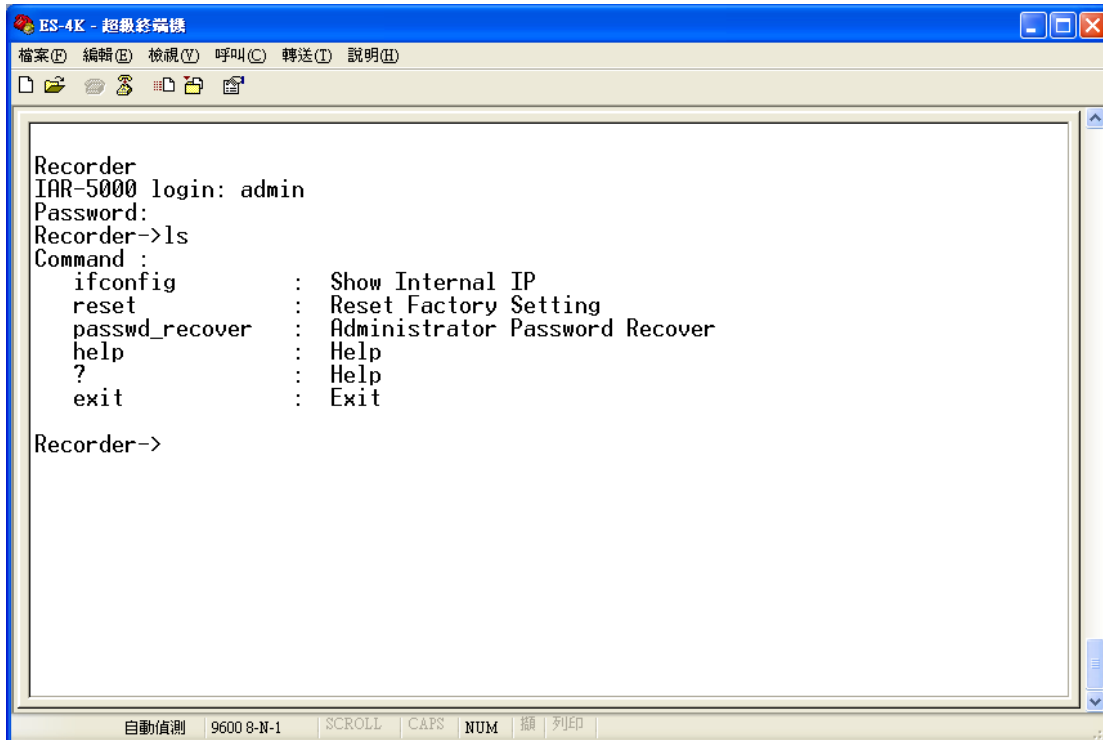
5. Fill in Port Setting as following value and click OK to save the setting



6. Press "Enter" and input Login name "admin" and password "airlive".



7. Type “ls” to display the command list



```
Recorder
IAR-5000 login: admin
Password:
Recorder->ls
Command :
ifconfig      : Show Internal IP
reset         : Reset Factory Setting
passwd_recover : Administrator Password Recover
help         : Help
?            : Help
exit         : Exit

Recorder->
```

8. Type “reset” to reset the device as default.

3

Configuring the IAR-5000

You can configure through standard web browser (http), secured web (https) management. In this chapter, we will explain IAR-5000's available management interfaces and how to get into them. Then, we will provide the introduction on Web Management and recommended initial settings.

3.1 Important Information

The following information will help you to get start quickly. However, we recommend you to read through the entire manual before you start. Please note the password is case sensitive.

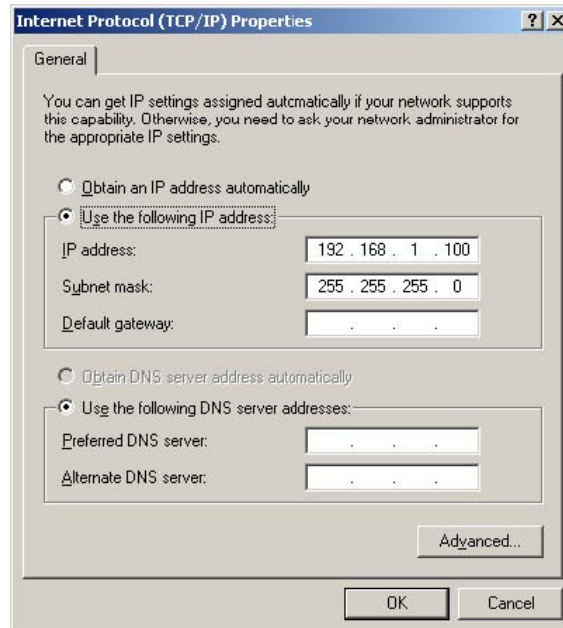
- | |
|--|
| <ul style="list-style-type: none"><input type="checkbox"/> The default IP address is: 192.168.1.1 Subnet Mask: 255.255.255.0<input type="checkbox"/> The default user name: admin<input type="checkbox"/> The default password: airlive |
|--|

3.2 Prepare your PC

The IAR-5000 can be managed by a PC. The default IP address of the IAR-5000 is **192.168.1.1** with a *subnet mask* of 255.255.255.0. This means the IP address of the PC should be in the range of 192.168.1.2 to 192.168.1.254.

To prepare your PC for management with the IAR-5000, please do the following:

1. Connect your PC directly to the Port1 on the of IAR-5000
2. Set your PC's IP address manually to 192.168.1.100 (or other address in the same subnet)

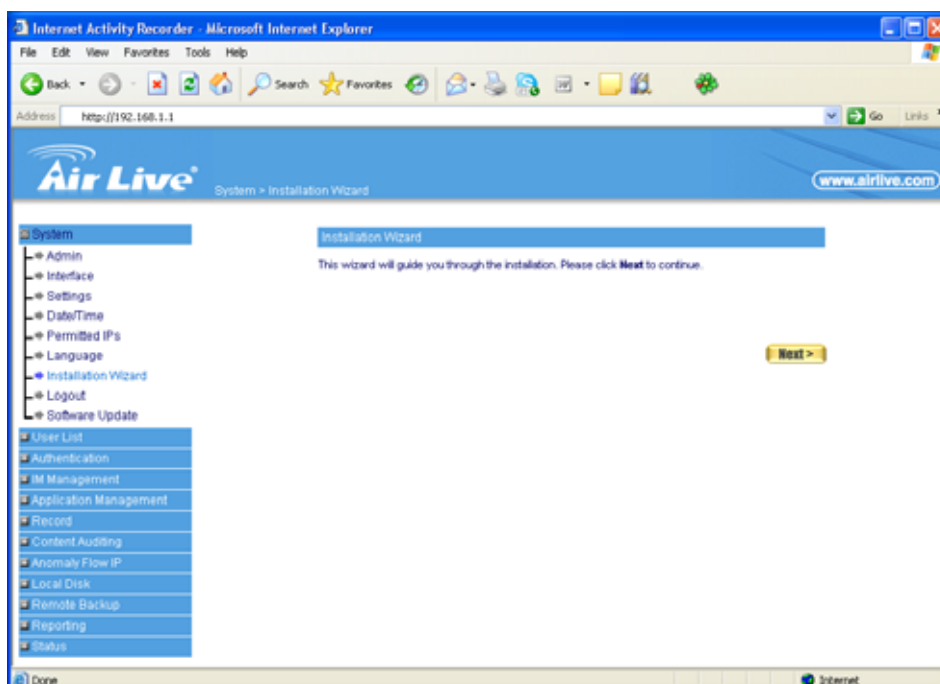


You are ready now to configure the IAR-5000 using your PC.

3.3 Management Interface

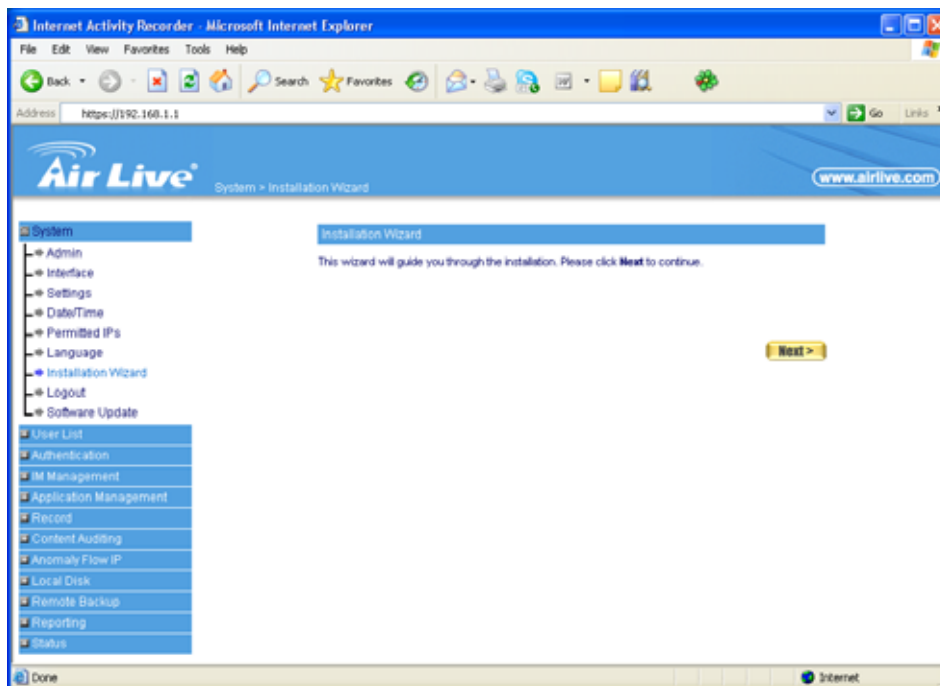
The IAR-5000 can be configured using one the management interfaces below:

- Web Management (HTTP):** You can manage your IAR-5000 by simply typing its IP address in the web browser. Most functions of IAR-5000 can be accessed by web management interface. We recommend using this interface for initial configurations. To begin, simply enter IAR-5000's IP address (default is 192.168.1.1) on the web browser. The default password is "airlive".



- **Secured Web Management (HTTPS):** HTTPS is also using web browser for configuration. But all the data transactions are securely encrypted using SSL encryption. Therefore, it is a safe and easy way to manage your IAR-5000. We highly recommend the Internet service provider to use HTTPS for management.

To begin, simply enter <https://192.168.1.1> on your web browser. A security alert screen from your browser will pop up. Please grant all permission and get certificate to IAR-5000. After you pass the security warning screen, you will enter the IAR-5000's secured web management interface. The default password is "airlive".



3.4 Introduction to Web Management

The IAR-5000 offers both normal (http) and secured (https) Web Management interfaces. They share the same interface and functions, and they can both be accessed through web browsers. The only difference is HTTPS are encrypted for extra security. Therefore, we will discuss them together as "Web Management" on this guide.

If you are placing the IAR-5000 behind router or firewall, you might need to open virtual server ports to IAR-5000 on your firewall/router

- HTTP: TCP Port 80
- HTTPS: TCP/UDP Port 443

This procedure is not necessary in most cases unless there is a router/firewall between your PC and IAR-5000.

Normal Web Management (HTTP)

To get into the Normal Web Management, simply type in the IAR-5000's IP address (default IP is 192.168.1.1) into the web browser's address field.



Secured Web Management (HTTPS)

To get into the Secured Web Management, just type "https://192.168.1.1" into the web browser's address field. The "192.168.1.1" is IAR-5000's default IP address. If the IP address is changed, the address entered in the browser should change also.



A security warning screen from your browser will then pop-up depending on the browser you use. Please follow step below to clear the security screen.

- Internet Explorer: Select "Yes" to proceed



❑ Firefox:

1. Select “or you can add an exception”



2. Click on “Add Exception”



3. Click on “Get Certificate”. Then, please enter IAR-5000’s IP address. Finally, please click on “Confirm Security Exception.”



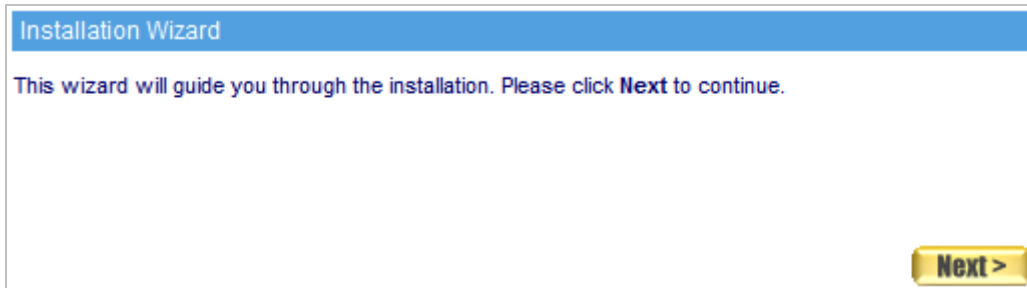
3.5 Initial Configurations

We recommend users to browse through IAR-5000's web management interface to get an overall picture of the functions and interface. Below are the recommended initial configurations for first time login:

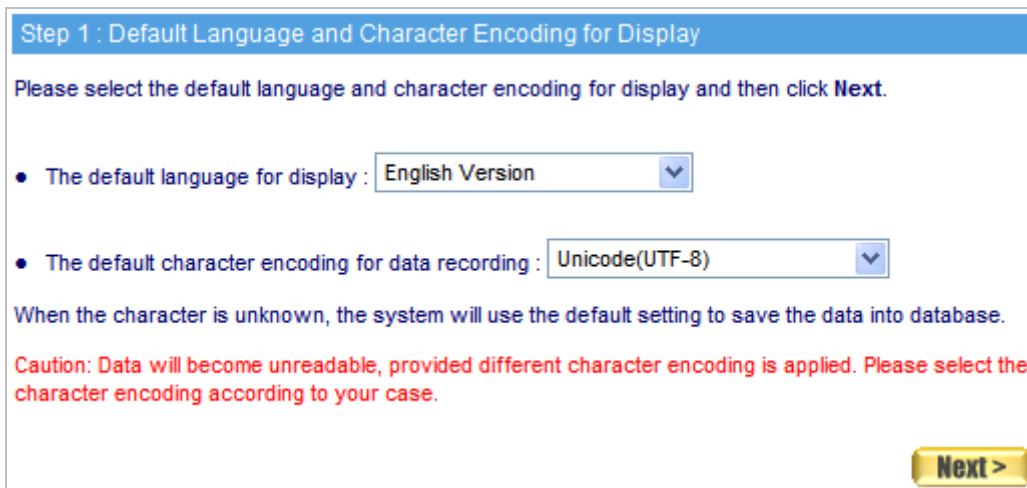
- Step1.** Connecting the administrator's PC and IAR-5000 (port1 or port2) to the same hub or switch, and then use the web browser " IE or Netscape" to connect IAR-5000. The default IP port address in IAR-5000's management interface is <http://192.168.1.1>.
- Step2.** The browser prompts you for the user name and password.
 - **User Name:** admin
 - **Password:** airlive
 - Click on **OK**




Step3. You will be brought to the **Installation Wizard** screen during your first login. It will guide you through the settings.



Step4. Select the language and character encoding for your management interface.





Default character encoding will be used on emails with unspecified character encoding

Step5. Tick **Synchronize with an Internet time server** as well as configure the offset hours from GMT to ensure the time correctness.



Step6. Select an operating mode based on how the device is deployed.

Step 3 : Device Deployment

Select to specify how you will deploy the device and then click **Next**.

- **Bridge Mode :**
Connect one of the two ports to the firewall or gateway and the other to a LAN hub or switch.
- **Sniffer Mode :**
Connect port 1 to the mirror port of a core switch or any port available on a LAN hub and port 2 to the network adaptor of the management PC.

Bridge Mode

Sniffer Mode(Port 1 for traffic mirroring; Port 2 for system management)

< Back **Next >**

Step7. Choose the basis for recording users' online activities.

Step 4 : Username Binding

- **Username-IP Binding :**
Recordings are generated based upon the IP address. Whoever uses the IP address will be treated as the same user. It is recommended if using static IP addresses.
- **Username-MAC Binding :**
Recordings are generated based upon the MAC address. Whoever uses the MAC address will be treated as the same user. It is recommended if using dynamic IP addresses distributed by DHCP server.
- **Username-Loginname Binding :**
Recordings are generated based upon the Active Directory (AD) login name. Whoever uses the user login name to log in to a domain will be treated as the same user. It is recommended if using an AD server.
- **Username-Authname Binding :**
Recordings are generated based upon the authentication name. Users need to be authenticated to access the Internet. Bridge mode deployment is required for username binding.

Please select a binding method that best fits your case and then click **Next**.

Usernames are bound to :

IP addresses

MAC addresses

AD server **Help**

Authentication names **Help**

< Back **Next >**

Step8. Configure the related interface addresses.

- Type a valid IP address from the LAN subnet in the IP Address field and configure its netmask, default gateway and DNS address accordingly.
- To use VLAN, tick Enable VLAN over Port 1 or 2 based on your case and also assign a VLAN ID to the port.
- Specify the maximum downstream and upstream bandwidth respectively.

Step 5 : Interface Addresses

Enter the necessary information for each blank field based on your network topology. When done, click **Next**.

IP Address:	192.168.1.254
Netmask	255.255.255.0
Default Gateway:	192.168.1.1
Primary DNS Server:	168.95.1.1
Secondary DNS Server:	
<input type="checkbox"/> Enable VLAN over Port 1	
VLAN ID:	(0 - 4,095)
<input type="checkbox"/> Enable VLAN over Port 2	
VLAN ID:	(0 - 4,095)
Max. Downstream Bandwidth:	102400 Kbps (1 - 102400)
Max. Upstream Bandwidth:	102400 Kbps (1 - 102400)

< Back
Next >



For your reference, you may configure your management address based on the subnet ranges below:

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

Step9. Configure the device to record the online activities of specific departments or groups by specifying its subnet and mask address.

Step 6 : Recording Target Subnet

Specify the subnet address and its mask for recording as well as decide its department or group by using the drop-down list. When done, click **Finish** . It'll take few seconds or so for settings to take effect and then you'll be brought to the system information page. Note: If the "IP address" field in Step 5 has been changed, then you'll have to manually log on to the new IP address, i.e. the management address.

Subnet	Netmask	Department / Group
<input type="text" value="192.168.1.0"/>	<input type="text" value="255.255.255.0"/>	Group_1 <input type="button" value="v"/>
<input type="text" value="192.168.2.0"/>	<input type="text" value="255.255.255.0"/>	Group_2 <input type="button" value="v"/>
<input type="text" value="192.168.5.0"/>	<input type="text" value="255.255.255.0"/>	Group_3 <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	Group_1 <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	Group_1 <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	Group_1 <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	Group_1 <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	Group_1 <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	Group_1 <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	Group_1 <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	Group_1 <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	Group_1 <input type="button" value="v"/>

Step10. Click on **Finish**.

Installation Wizard

This wizard has already finished all the settings. The page will automatically re-connect in 3 seconds.

Step11. Navigate to **User List** → **Settings**, and then give each department or group a friendly name.

User List Import / Export Settings

Export User List

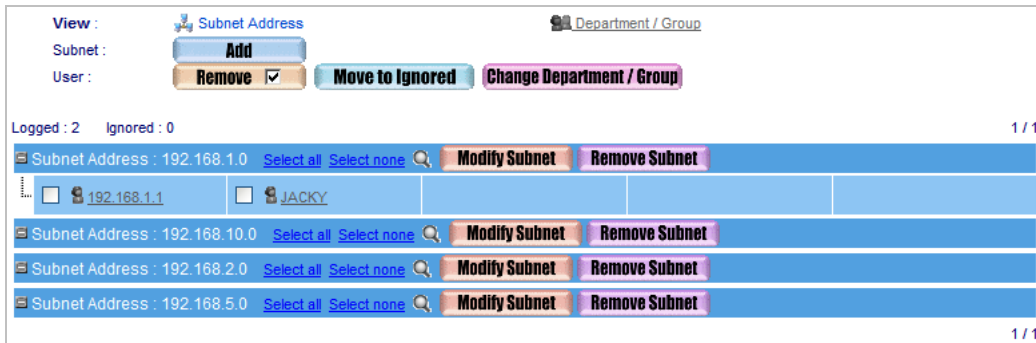
Import User List

(ex: user_set.csv)

Department / Group (Max. 20 characters)

1: <input type="text" value="RD"/>	2: <input type="text" value="Sales"/>	3: <input type="text" value="Warehouse"/>	4: <input type="text" value="Group_4"/>
5: <input type="text" value="Group_5"/>	6: <input type="text" value="Group_6"/>	7: <input type="text" value="Group_7"/>	8: <input type="text" value="Group_8"/>
9: <input type="text" value="Group_9"/>	10: <input type="text" value="Group_10"/>	11: <input type="text" value="Group_11"/>	12: <input type="text" value="Group_12"/>

Step12. Under **User List** → **Logged**, users within the same subnet as the management address will be included in the same subnet category. In another word, IAR-5000 classifies users by the identity of subnet. Also, the device allows system administrator to customize user lists for users resided in other subnets.



3.6 About IAR-5000's Menu Structure

The device's user interface consists of the following two areas:

- The left panel contains all the selectable menu items.
- The configuration panel on the right provides all the available settings for any selected menu item.
- Click on **OK**



Main Menu

Configuration

4

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.

4.1 Admin

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.

Group Monitoring:

- 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.

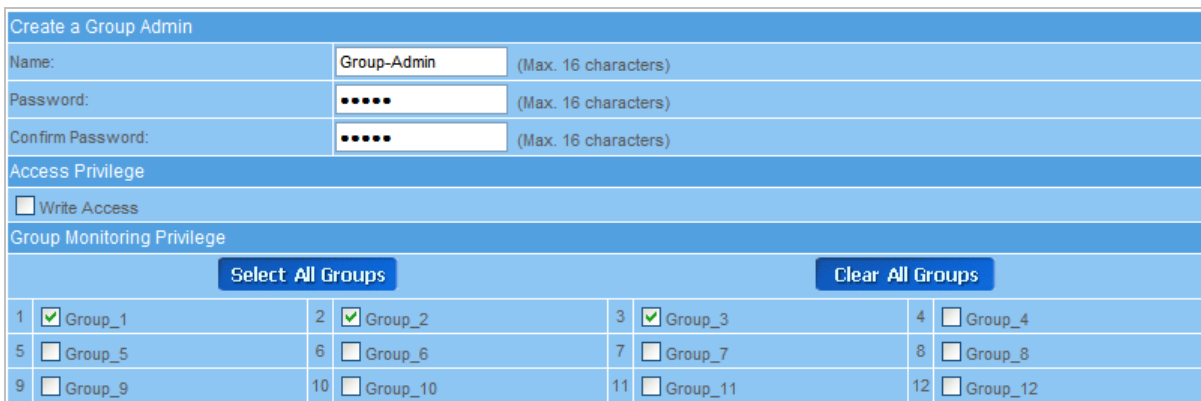
Add New Group-Admin:

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

Step2. In add new group-admin window, enter the following information. (Figure 4-1)

- **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.



Create a Group Admin			
Name:	<input type="text" value="Group-Admin"/>	(Max. 16 characters)	
Password:	<input type="password" value="*****"/>	(Max. 16 characters)	
Confirm Password:	<input type="password" value="*****"/>	(Max. 16 characters)	
Access Privilege			
<input type="checkbox"/> Write Access			
Group Monitoring Privilege			
<input type="button" value="Select All Groups"/>		<input type="button" value="Clear All Groups"/>	
1	<input checked="" type="checkbox"/> Group_1	2	<input checked="" type="checkbox"/> Group_2
3	<input checked="" type="checkbox"/> Group_3	4	<input type="checkbox"/> Group_4
5	<input type="checkbox"/> Group_5	6	<input type="checkbox"/> Group_6
7	<input type="checkbox"/> Group_7	8	<input type="checkbox"/> Group_8
9	<input type="checkbox"/> Group_9	10	<input type="checkbox"/> Group_10
11	<input type="checkbox"/> Group_11	12	<input type="checkbox"/> Group_12

Figure 4-1 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 4-2)

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

Modify Password			
Name	admin		
Password:	<input type="password" value="....."/>	(Max. 16 characters)	
New Password	<input type="password" value="....."/>	(Max. 16 characters)	
Confirm Password:	<input type="password" value="....."/>	(Max. 16 characters)	
Access Privilege			
<input checked="" type="checkbox"/> Write Access			
Group Monitoring Privilege			
<input type="button" value="Select All Groups"/>		<input type="button" value="Clear All Groups"/>	
1	<input checked="" type="checkbox"/> Group_1	2	<input checked="" type="checkbox"/> Group_2
3	<input checked="" type="checkbox"/> Group_3	4	<input checked="" type="checkbox"/> Group_4
5	<input checked="" type="checkbox"/> Group_5	6	<input checked="" type="checkbox"/> Group_6
7	<input checked="" type="checkbox"/> Group_7	8	<input checked="" type="checkbox"/> Group_8
9	<input checked="" type="checkbox"/> Group_9	10	<input checked="" type="checkbox"/> Group_10
11	<input checked="" type="checkbox"/> Group_11	12	<input checked="" type="checkbox"/> Group_12

Figure 4-2 To change the admin password

4.2 Interface

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.

Step1. In **System → Interface**, 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 4-3)

Interface Addresses	
IP Address:	<input type="text" value="172.16.3.254"/>
Netmask:	<input type="text" value="255.255.0.0"/>
Default Gateway:	<input type="text" value="172.16.0.1"/>
Primary DNS Server:	<input type="text" value="168.95.1.1"/>
Secondary DNS Server:	<input type="text"/>
<input type="checkbox"/> Enable VLAN over Port 1	
VLAN ID:	<input type="text"/> (0 - 4,094)
<input type="checkbox"/> Enable VLAN over Port 2	
VLAN ID:	<input type="text"/> (0 - 4,094)
Network Bandwidth	
Max. Downstream Bandwidth:	<input type="text" value="102400"/> Kbps (1 - 102400)
Max. Upstream Bandwidth:	<input type="text" value="102400"/> Kbps (1 - 102400)
Interface allows access by :	<input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS

Figure 4-3 The interface IP setting



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

4.3 Settings

System Settings:

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

Database Check / Repair:

- The records can be inspected and / or fixed if damaged or displayed improperly. To obtain the best performance, please execute it when the network traffic is low in order to avoid system overload.

System E-mail Notification:

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

Device Deployment:

- Bridge mode operates as: Port 1 and port 2 function individually.


- Sniffer mode operates as: Port 1 serves as a packet receiver connected to the mirror port of a core switch whereas port 2 connected to any other port available on that core switch acting as a management use for system administrator.

Management over Web Browser:

- Management port enables the device to be remotely accessed from anywhere via a Web browser. The port number for whether HTTP or HTTPS protocol is alterable.
- If a wrong password has been entered and it exceeds the maximum allowed attempts, the users IP address can be blocked to prevent unauthorized modification.

Log Storage Time

- System administrator can set the log storage time.



When the port number of HTTP and HTTPS had been changed, if the system administrator wants to log in to WebUI, he must change the WebUI port number. (For example: <http://172.16.3.254:8080> and [https:// 172.16.3.254:1025](https://172.16.3.254:1025))

Export the configured file:

- Step1.** In **System → Setting → System Settings**, select **Export System settings**, and click the **Export** 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 4-4)

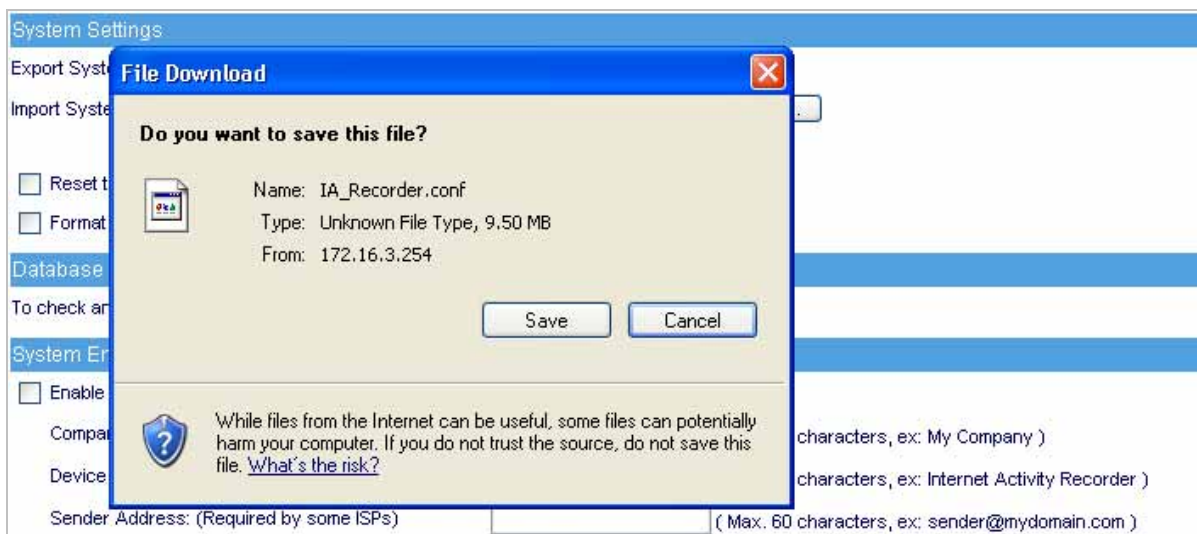


Figure 4-4 Choose where the export file will be saved

Import the configured file

- Step1.** In **System → Setting → System Settings**, select **Import System Settings**, 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 4-5)
- 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 4-6)

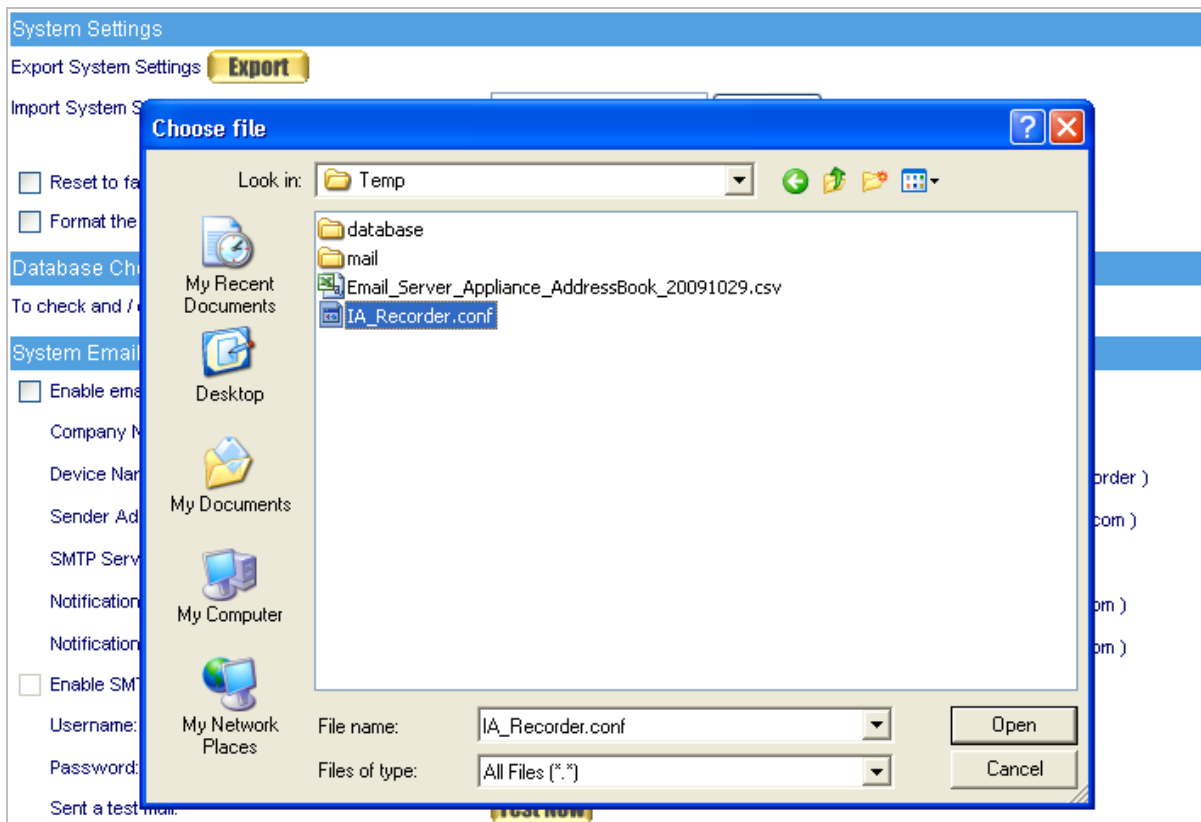


Figure 4-5 Import the file name to the directory to saved

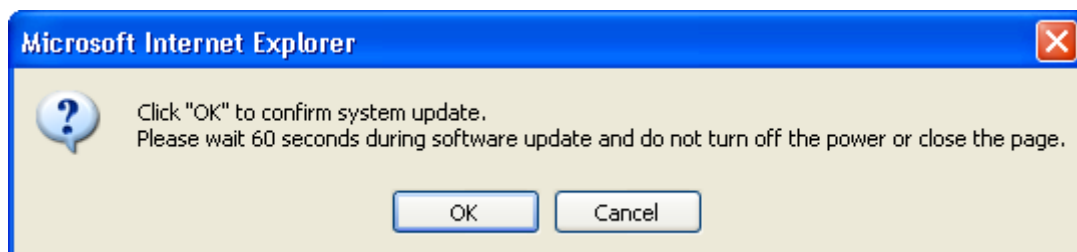


Figure 4-6 Confirm the import setting

Reset Factory Default

- Step1.** In **System** → **Settings** → **System Settings**, 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 4-7)



Figure 4-7 Select Reset Factory Setting

Configure System Email Notification

- Step1.** Select **Enable email notification** under **System Email Notification** section.
- 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.** **Notification Address 1**, enter the e-mail address in the first one position to receive the alarm message.
- Step7.** **Notification 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 4-8)

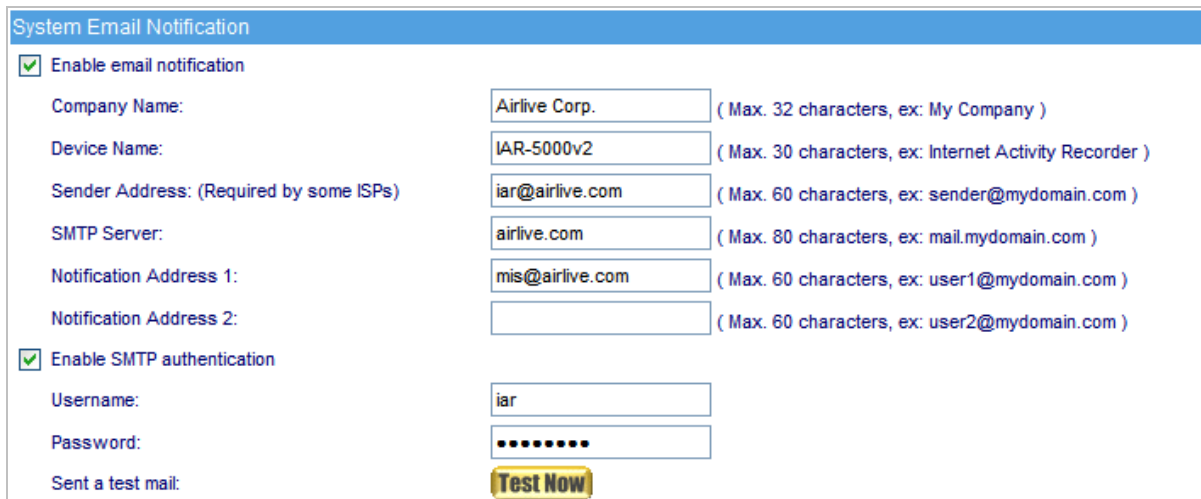



Figure 4-8 Enable the instant mail message alarm of IAR-5000



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

Device Reboot

- Step1.** Click on the **Reboot** button next to **Reboot System**.
- Step2.** A confirmation conversation box appears saying, "Are you sure to reboot ?"
- Step3.** Click OK to reboot IAR-5000, or click Cancel to cancel reboot IAR-5000.
(Figure 4-9)

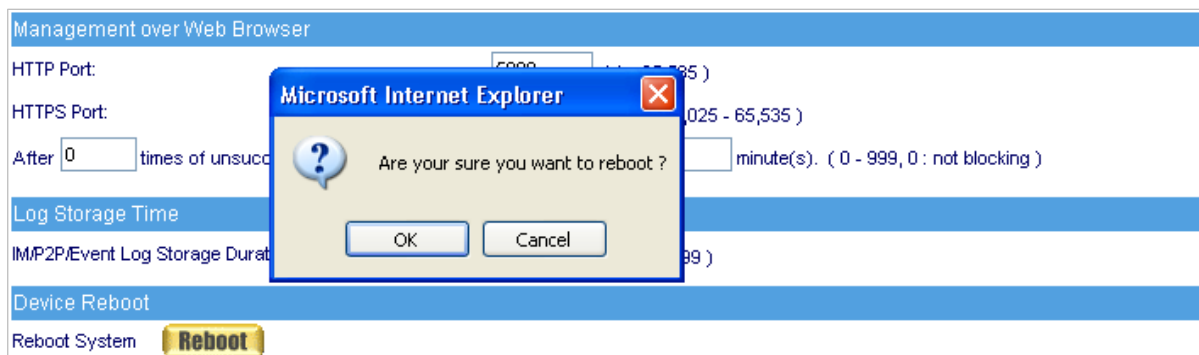


Figure 4-9 Reboot the internet recorder appliance

4.4 Date/Time

System Clock Settings

- The date and time settings can be configured by either syncing to an Internet time server or syncing to the computer's clock.

GMT

- The short form for Greenwich Mean Time. It is the international standard time.

Daylight Saving Time

- Daylight saving time (DST; also summer time) is the portion of a year in which a region's local time is advanced by an hour from its standard official time.

Step1. Select **Enable Synchronize with an Internet Time Server**. (Figure 4-10)

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 interval minute**.



System time : Mon Nov 30 15:07:02 2009

System Clock Settings

Synchronize with an Internet time server

Set **+8** hours offset from GMT [Assist](#)

Enable daylight saving time from 1 / 1 to 1 / 1

Server IP / Name: 140.109.1.10 [Assist](#)

Update Interval : 60 minutes (0 - 99,999, 0 : update upon a system reboot)

Synchronize system clock with this computer **Sync**

Figure 4-10 System time setting



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



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



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

4.5 Permitted IPs

Creating a Permitted IP Address

- Step1.** In **System → Permitted IPS → New Entry**, add the new setting: (Figure 4-11)
- **Name** enters master.
 - **IP Address** enters 172.16.0.2.
 - **Netmask** enters 255.255.255.255.
 - **Service** selects Ping, HTTP and HTTPS.
 - Click **OK**.
 - **Complete Permitted IPs settings**. (Figure 4-12)

Create a Permitted IP Address	
Name :	<input type="text" value="master"/> (Max. 20 characters)
IP Address :	<input type="text" value="172.16.0.2"/>
Netmask :	<input type="text" value="255.255.255.255"/>
Access by / via:	<input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS

Figure 4-11 The Permitted IPs setting




Name	IP Address / Netmask	Ping	HTTP	HTTPS	Configuration
master	172.16.0.2 / 255.255.255.255				<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure 4-12 Complete the Permitted IPs setting



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

4.6 Logout

Logging out the Management Interface

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 4-13)

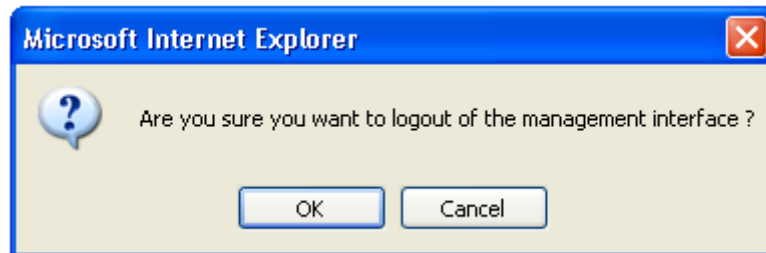


Figure 4-13 Confirm to logout

Step2. Click **OK**, it shows the logout information. (Figure 4-14)

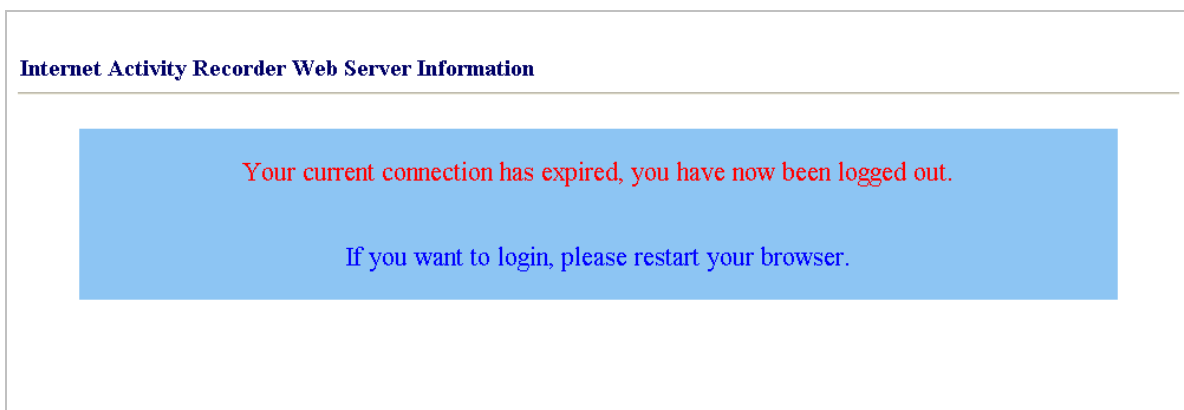


Figure 4-14 The logout WebUI

4.7 Software Update

Updating Firmware

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

- In Version Number, we can know the current version of the software. Go on the internet to gain the newest version of the firmware and download into the storage disk in IAR-5000.
- Click Browse → Choose file, select the newest version of the software.
- Click the lower right OK, it will process the update. (Figure 4-15)

Software Update	
Version Number :	v5.07.00
Software Update :	<input type="text"/> <input type="button" value="Browse..."/>
	(ex: Ovislink_IAR-5000_050700_6.img)

Figure 4-15 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.)

5

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.

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 5-1)

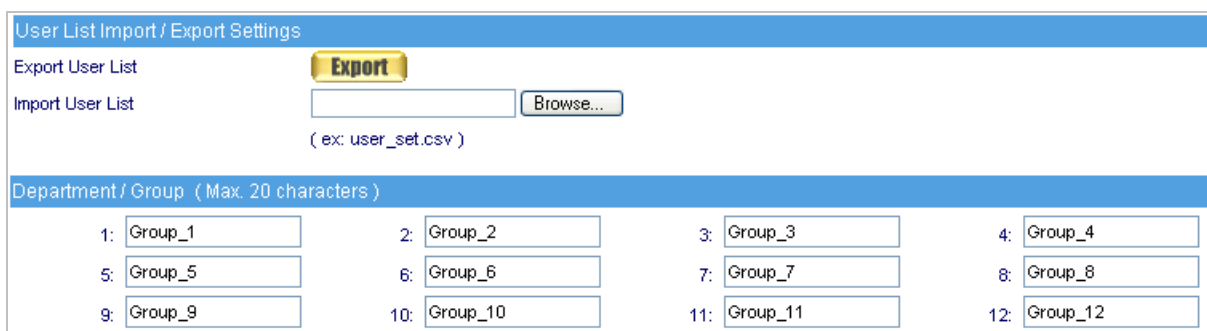



Figure 5-1 Set the user list

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

- Click  of 172.16.0.0 subnet and the IAR-5000 will search the new user in the subnet. (Figure 5-2)
- Wait 1~2 minutes until search complete. (Figure 5-3)
- 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 5-4, 5-5)

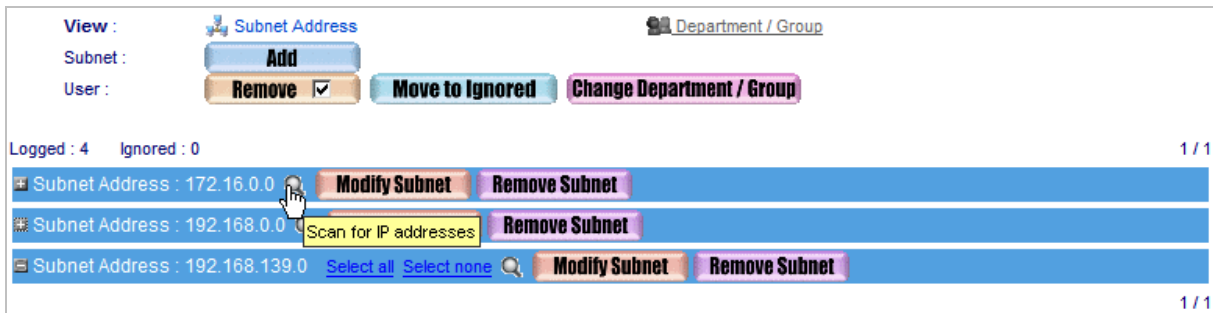


Figure 5-2 Click search new user button

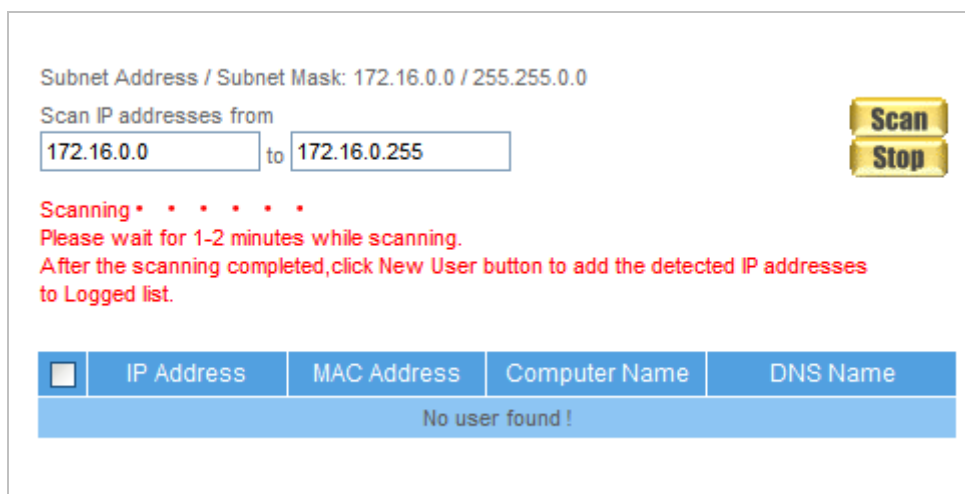


Figure 5-3 Starting to search new user

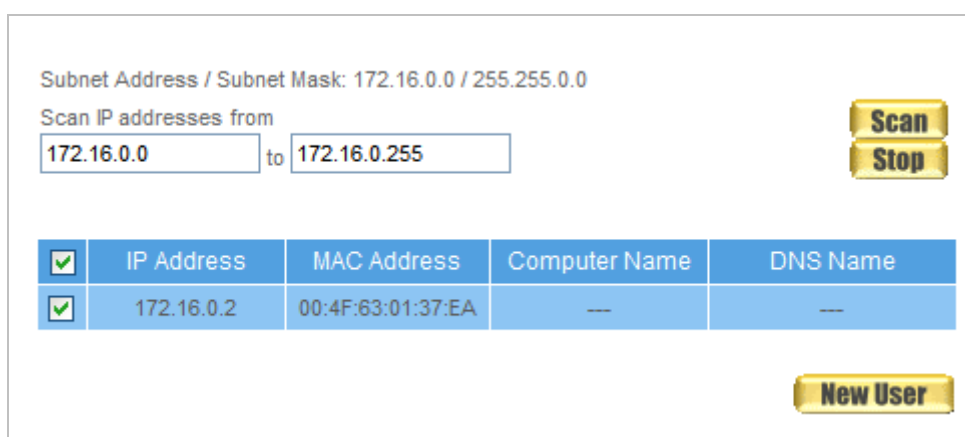


Figure 5-4 Select the new user to add

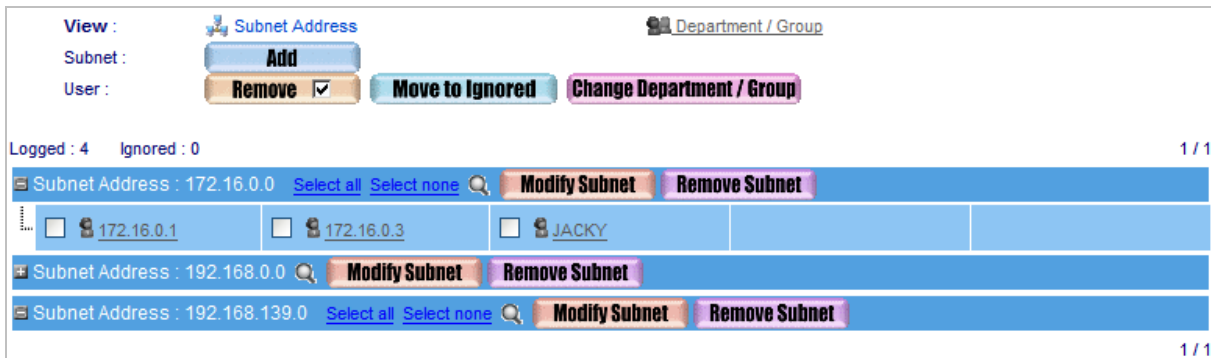


Figure 5-5 Complete to add the new user



The subnet in which management address resided is set to be the first subnet on user list. Users from that subnet will be shown under **User List** → **Logged**.



A user will be automatically added on **Logged** list once the device detects his / her accessing the Internet.



Given that the **Primary DNS Server** (or secondary) is using an internal DNS server, then the device would request that DNS server for users' DNS names while performing user searching.



User names may be displayed in various forms. The display name of a user / client will be chosen from its computer name, its entry from the DNS server, then its IP / MAC address. (If computer name and DNS name are not available, then IP or MAC address will be used. Whether IP or MAC address will be used is determined by the **User names are bound to IP / MAC addresses** setting under **Record** → **Settings** → **Settings**.)

Step3. Modify the user in user list :

- Click User Name of JACKY
- User Name, enter Jacky_PC.
- Department / Group, select Laboratory.
- Click **OK**. (Figure 5-6, 5-7, 5-8)
- 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 5-9, 5-10, 5-11)
- Repeat the steps to complete modifying the user list. (Figure 5-12)

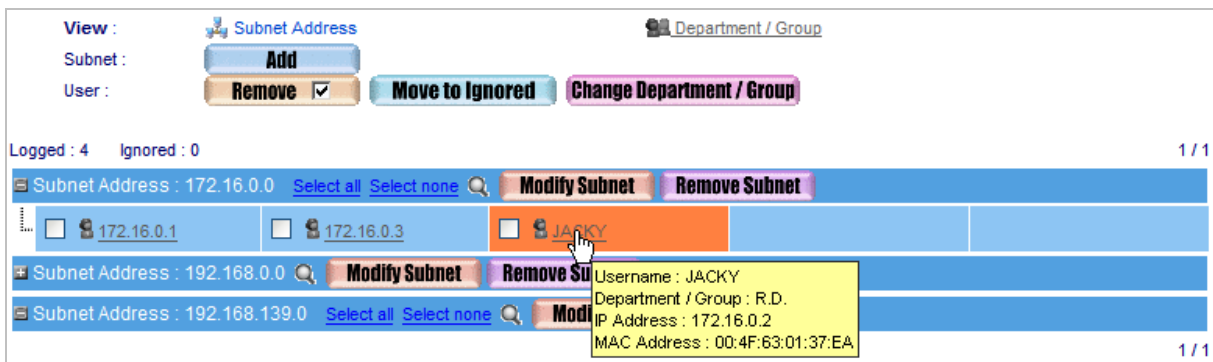


Figure 5-6 Select the user to modify

Modify Username	
Username	JACKY_PC (Max. 17 characters)
Department / Group	R.D. ▼
Computer Name	JACKY
DNS Name	---
IP Address	172.16.0.2
MAC Address	00:4F:63:01:37:EA
<input type="checkbox"/> Move this user to Ignored User List	

Figure 5-7 Enter the user information to modify

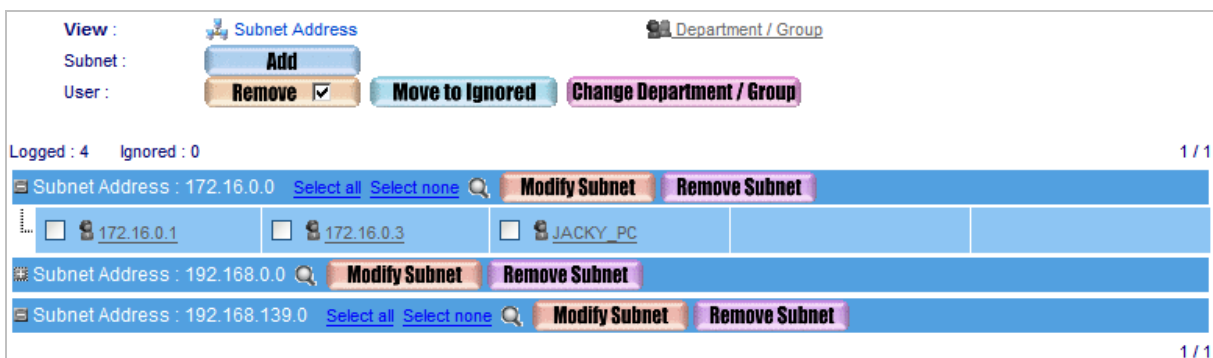


Figure 5-8 Complete to modify the user information

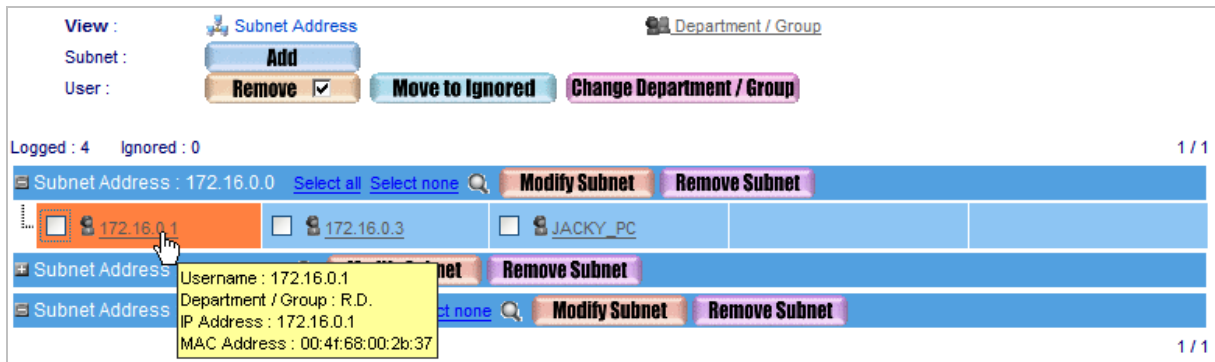


Figure 5-9 Select the user to modify

Modify Username	
Username	RS-3000 (Max. 17 characters)
Department / Group	R.D.
Computer Name	---
DNS Name	---
IP Address	172.16.0.1
MAC Address	00:4f:68:00:2b:37
<input checked="" type="checkbox"/> Move this user to Ignored User List	

Figure 5-10 Enter the user information to modify

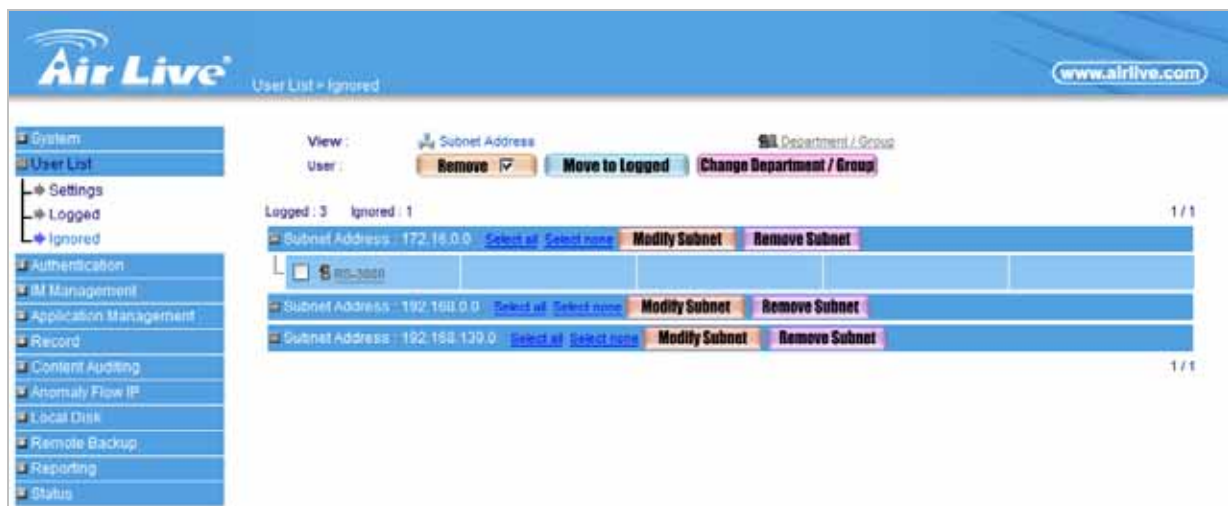


Figure 5-11 Move the user to ignored user list

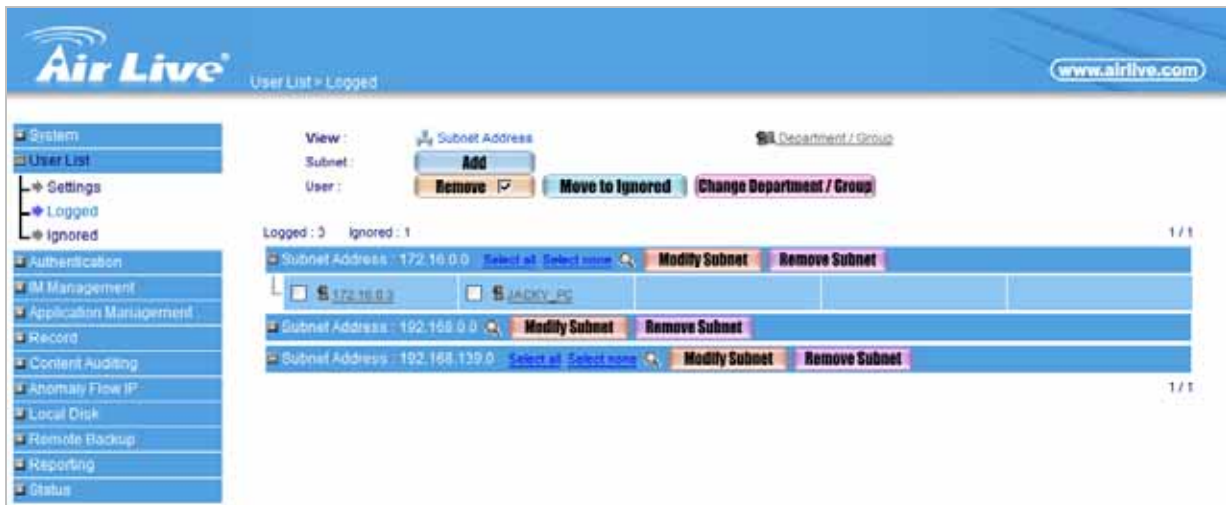




Figure 5-12 Complete to modify the user list

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

- Step4.** In **User List → Logged**, add the new subnet:
- Click **Add**.
 - **Subnet**, enter 192.168.139.1.
 - **Netmask**, enter 255.255.255.0.
 - **Add a New user to this Department / Group**, select RD.
 - Click **OK**. (Figure 5-13)

Add a Subnet	
Subnet Address:	<input type="text" value="192.168.139.1"/>
Netmask:	<input type="text" value="255.255.255.0"/>
Classify new users into:	<input style="border: none; border-bottom: 1px solid #ccc;" type="text" value="R.D."/> ▼

Figure 5-13 Add a new subnet

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

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

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

- Step1.** In **User List** → **Setting** → **User List Configuration** → **Export User List to Client PC** → click **Download**.
- Step2.** When it appears **File Download**, click **Save**, choose the position to save the download file, then click **Save** again. The user list settings will be saved in IAR-5000. (Figure 5-14)

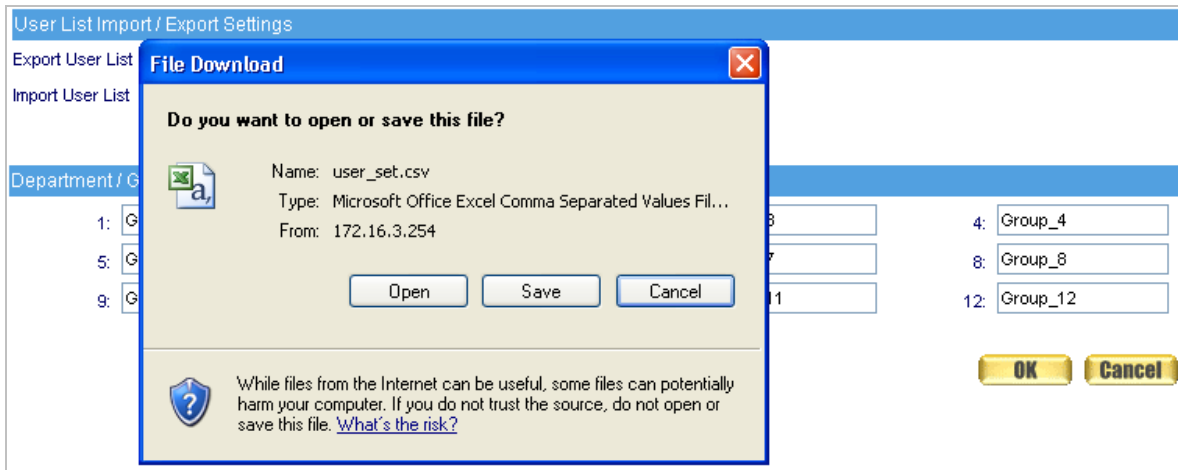


Figure 5-14 Select the position to save the download file

- Step3.** Under **User List** → **Settings**, import the edited user list onto IAR-5000.
- Run Excel to edit the previously downloaded user list. (default file name: user_set.csv) (Figure 5-15)

#####						
#Format:						
#~1	Group_1					
.....						
#####						
Department / Group :						
~1	Intern					
~2	Sales					
.....						
192.168.139.0	255.255.255.0	1				
192.168.139.30	Mail_Server	*	0	00:0C:76:B7:96:3B		11
192.168.139.216	Jacky	Product	3	00:12:0E:2E:CF:DA		10
172.19.0.0	255.255.0.0	9				
172.19.100.10	Hanson	Product	3	08:E0:18:25:F4:BC		9
172.19.100.11	Hans	*	3	00:02:44:8E:B7:C7		9
.....						

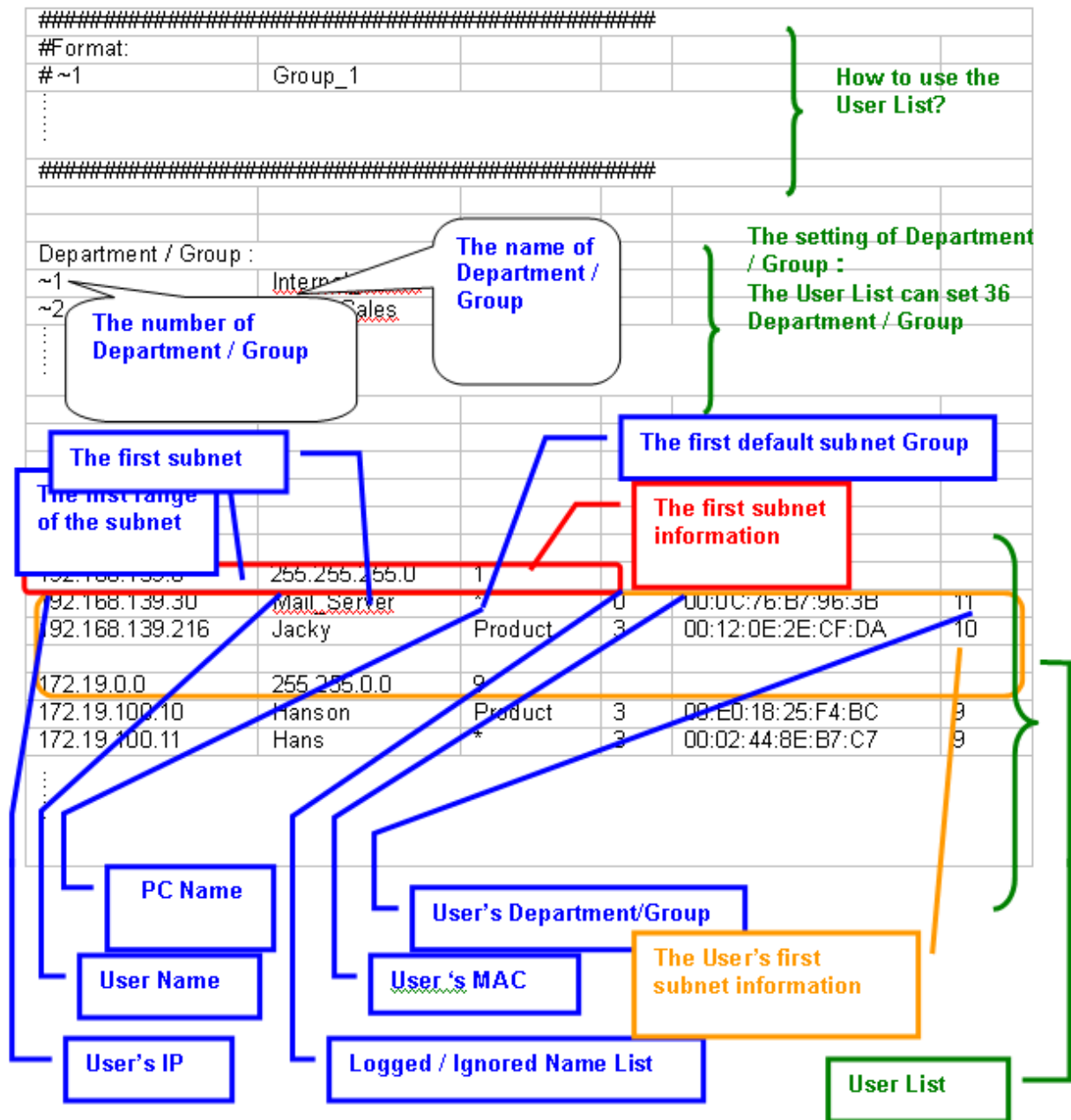


Figure 5-15 Editing the User List in Excel

- Step4.** Change the information of **Department / Group**.
- 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**. (Figure 5-16)


Department / Group :		Department / Group :	
~1	Internal_Sales	~1	Internal_Sales
~2	Asian_Sales	~2	Asian_Sales
~3	European_Sales	~3	European_Sales
~4	American_Sales	~4	American_Sales
~5	Bursary	~5	Bursary
~6	Human_Resouces	~6	Human_Resouces
~7	Marketing	~7	Marketing
~8	Customer_Service	~8	Support
~9	R.D.	~9	R.D.
~10	Laboratory	~10	Laboratory
~11	Device_Room	~11	Device_Room
~12	Group_12	~12	R.D._2
~13	Group_13	~13	Group_13


Figure5 -16 Change the Department / Group information from excel

- Step5.** To add and modify the user information in the first subnet. (Figure 5-17)
- Change **192.168.1.2 (Jacky)**Department / Group information, and change the **1th Department / Group** into **9th Department / Group**.
 - Insert a row under the user list in the first subnet, and enter the new user information in the row. (User IP , User Name, PC Name, Logged / Ignored User List, User MAC, User Department / Group)

User List :					User List :				
192.168.1.0	255.255.255.0	1			192.168.1.0	255.255.255.0	1		
192.168.1.2	Jacky	WRITTER	3	00:D0:59:84:00:01	192.168.1.2	Jacky	WRITTER	3	00:D0:59:84:00:09
192.168.1.100	*	OCT1005	3	00:0D:88:11:11:11	192.168.1.100	*	OCT1005	3	00:0D:88:11:11:11
192.168.1.101	Jacky_NB	JACKY-M	3	00:16:36:66:00:01	192.168.1.101	Jacky_NB	JACKY-M	3	00:16:36:66:00:01
192.168.1.1	Gateway	---	1	00:17:9A:33:00:01	192.168.1.1	Gateway	---	1	00:17:9A:33:00:01
					192.168.1.10	John	PM	6	00:15:5A:33:00:06

Figure 5-17 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 5-18)

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

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

Figure 5-18 Add the user's information in the third subnet by excel

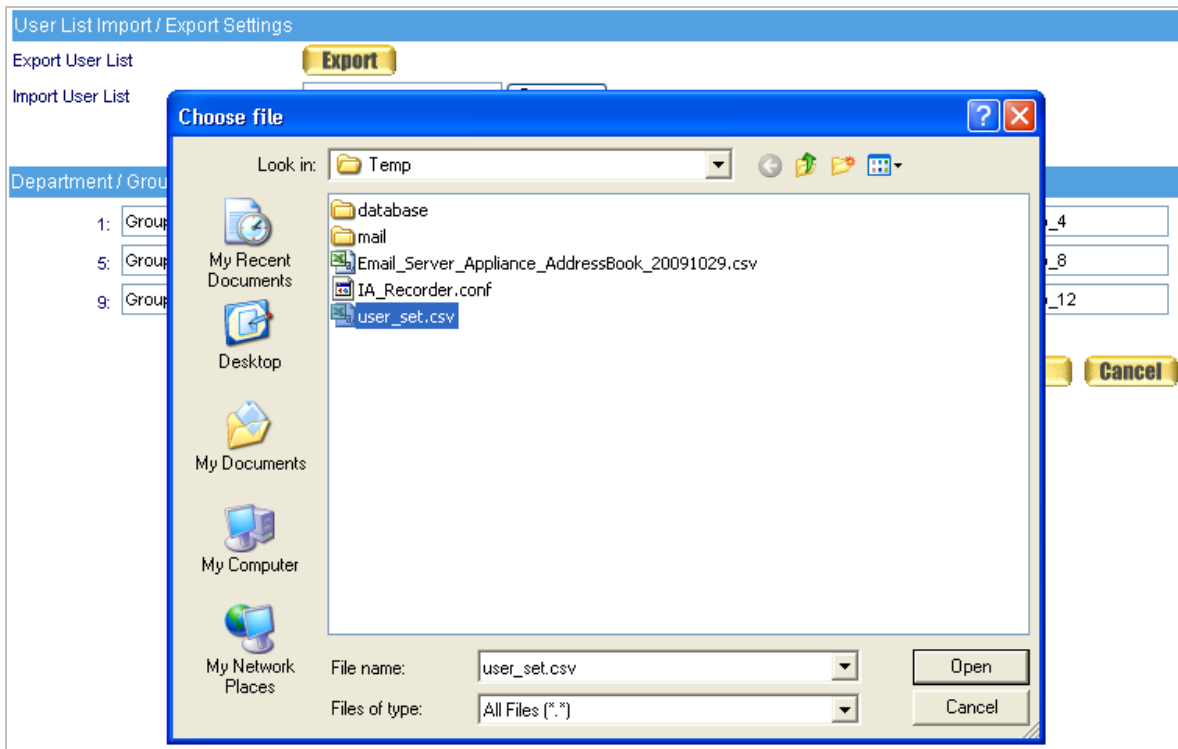


Leaving a blank row as a separator in between any two subnet information is essential while editing user list in Excel.

Step7. Save File (user_set.csv)

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

Step9. In the **Choose File** window, select the modified user list setting, then Click Open. (Figure 5-19)



! Figure 5-19 Selecting the Edited User List to Import

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

Modify the Information of the desirable user:

Step1. Click on the desirable user to change its user information. (Figure 5-20)

Step2. Type a proper user name.

Step3. Select the proper dept. / group. (Figure 5-21)

Step4. Modification is completed.

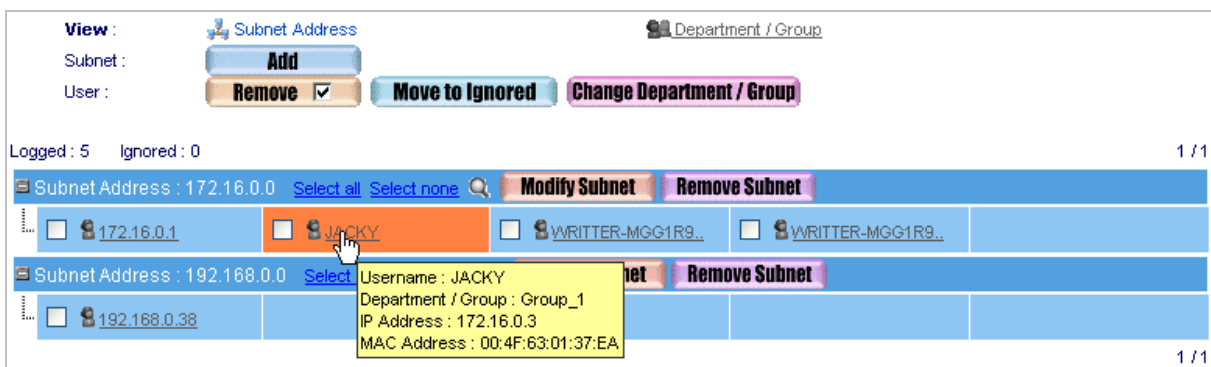



Figure 5-20 Selecting the Desirable User to Change User Information

Modify Username	
Username	JACKY (Max. 17 characters)
Department / Group	Group_1
Computer Name	JACKY
DNS Name	---
IP Address	172.16.0.3
MAC Address	00:4F:63:01:37:EA
<input type="checkbox"/> Move this user to Ignored User List	

Figure 5-21 Modifying the User Information



System administrator can record or ignore the online activities of a specific internal user simply by selecting the user on the user list and then click on **Logged** or **Ignored** button on the top of the first list.

Add a new subnet:

- Step 1.** Navigate to **User List → Logged**, and then add a new subnet.
- Click on **Add** next to **Subnet**.
 - **Subnet Address:** Type 192.168.139.0
 - **Netmask:** Type 255.255.255.0
 - **Classify new users into:** Select R.D. (customize accordingly) (Figure 5-22)
 - Refer to Step 2 in page 34 to add users resided in the subnet. (Figure 5-23)

Add a Subnet	
Subnet Address:	192.168.139.0
Netmask:	255.255.255.0
Classify new users into:	R.D.

Figure 5-22 Adding a Subnet to be Recorded

View : Subnet Address Department / Group

Subnet: **Add**

User: **Remove** **Move to Ignored** **Change Department / Group**

Logged : 5 Ignored : 0 1 / 1

Subnet Address : 172.16.0.0	Select all	Select none	Modify Subnet	Remove Subnet
<input type="checkbox"/> 172.16.0.1	<input type="checkbox"/>	JACKY	<input type="checkbox"/> WRITTER-MGG1R9..	<input type="checkbox"/> WRITTER-MGG1R9..
Subnet Address : 192.168.0.0	Select all	Select none	Modify Subnet	Remove Subnet
<input type="checkbox"/> 192.168.0.38				
Subnet Address : 192.168.139.0	Select all	Select none	Modify Subnet	Remove Subnet

1 / 1

Figure 5-23 New User List Added

6

Authentication

The device supports four types of authentication: RADIUS, POP3, LDAP and the device's inbuilt user authentication. The IT administrator may regulate users' Internet access using these authentication mechanisms.

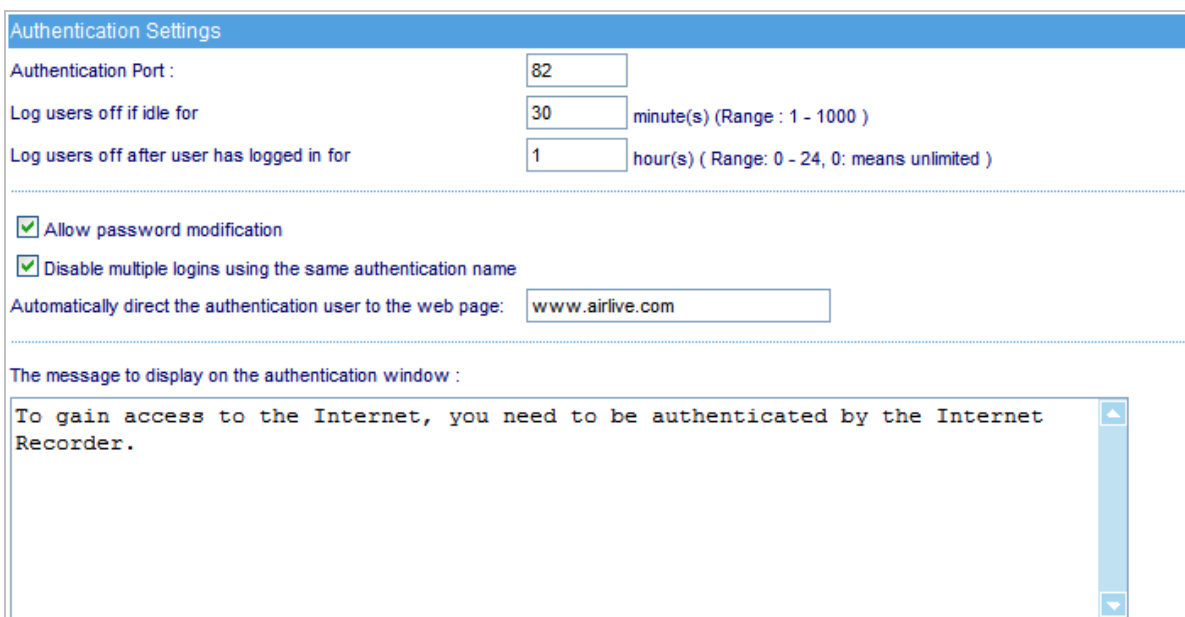
6.1 Settings

Authentication Settings:

- **Authentication Port:** The port number used for authentication mechanism. It is "82" by default.
- **Log users off if idle for:** You can specify a period of time to log off idle users. If the idle time of a user has exceeded the value specified, the authentication of the user will automatically expire. Default value is "30".
- **Disable multiple logins using the same authentication name:** Users will fail to be authenticated if using the same name.
- **Automatically direct the authentication user to the web page:** Users will be taken to the web page specified right after authentication. If leaving the field blank, users will have direct access to their desirable web page.
- **The message to display on the authentication window:** The informative or greeting message (support HTML language) for authenticated users. To discard the setting and leave the field blank.
- **Authentication-Free List:** Users can be exempted from the authentication mechanism by specifying their IP addresses on the list.

Procedure to pass Authentication:

- Define the Authentication settings. (Figure 6-1)



Authentication Settings

Authentication Port :

Log users off if idle for minute(s) (Range : 1 - 1000)

Log users off after user has logged in for hour(s) (Range: 0 - 24, 0: means unlimited)

Allow password modification

Disable multiple logins using the same authentication name

Automatically direct the authentication user to the web page:

The message to display on the authentication window :

Figure 6-1 General Authentication Settings

- Surf any webpage, user will see: (Figure 6-2)

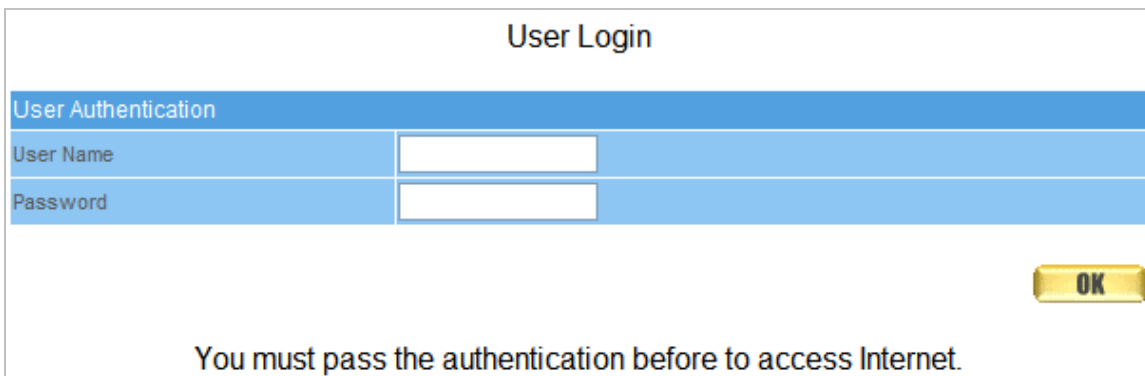


Figure 6-2 The Login Screen for Authentication Mechanism

- The designated web site will show up after passing authentication. (Figure 6-3)

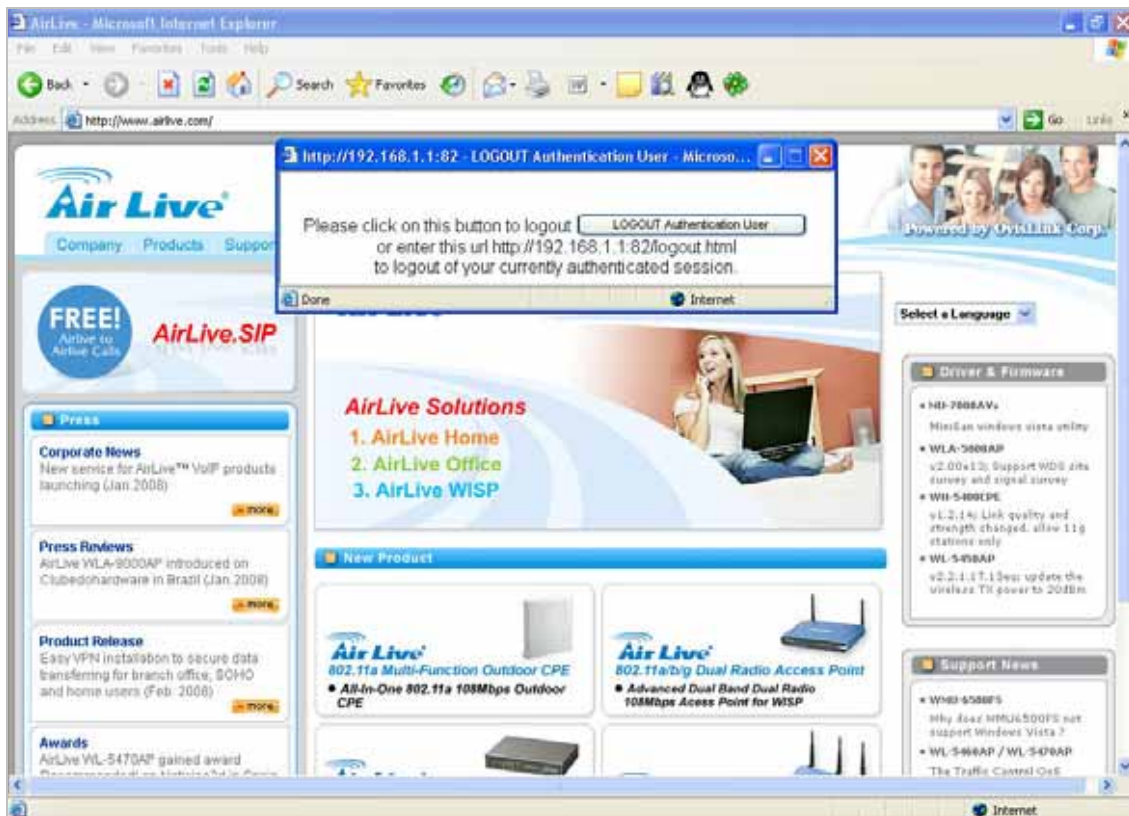


Figure 6-3 The Designated Web Site for Authentication Login



The device's authentication mechanism requires Bridge mode deployment.



The login screen for authentication is available by a manual input of the device's management address appended with the authentication port number in the **Address** field of a web browser.

6.2 Auth User

Auth Name:

- The authentication name for a user.

Password:

- The password for the authentication.

Confirm New Password:

- The confirmation of the password.

Regulate Users' Internet Access:

Step1. Under **Authentication** → **Auth User**, create as many authenticated users as needed. (Figure 6-4)

Auth Name	Expiration Date	Configuration
peter		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
Dina		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
johnson		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
patty		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
angie		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
sandy		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
stan		<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Figure 6-4 Creating Authenticated Users

Step2. The login screen for authentication will show upon users's web browsing attempt. If the login information is correctly applied, the authentication will be successful. (Figure 6-5)

User Login

User Authentication	
User Name	<input style="width: 90%;" type="text" value="peter"/>
Password	<input style="width: 90%;" type="password" value="****"/>

You must pass the authentication before to access Internet.

Figure 6-5 The Login Screen for Authentication Mechanism

Step3. To log out of the authenticated session, click on Logout in the Authentication Logout window. If the window has been closed, please enter <http://device's management address:authentication port/logout.html> (ex. <http://192.168.1.1:82>) in the **Address** field of a web browser to re-open the window.. (Figure 6-6)



Figure 6-6 The Window for Logging Out the Authenticated Session

6.3 RADIUS

RADIUS Server Secret

- The password for the RADIUS authentication.

802.1x RADIUS Server Authentication

- Provides your RADIUS authentication with Port-based Network Access Control

How to setup a Windows-based RADIUS server

Step1. Navigate to **Start → Settings → Control Panel → Add/Remove Programs** and then click on **Add/Remove Windows Components** from the left panel.

Step2. **Networking Services** from the components and then click on **Details**. (Figure 6-7)

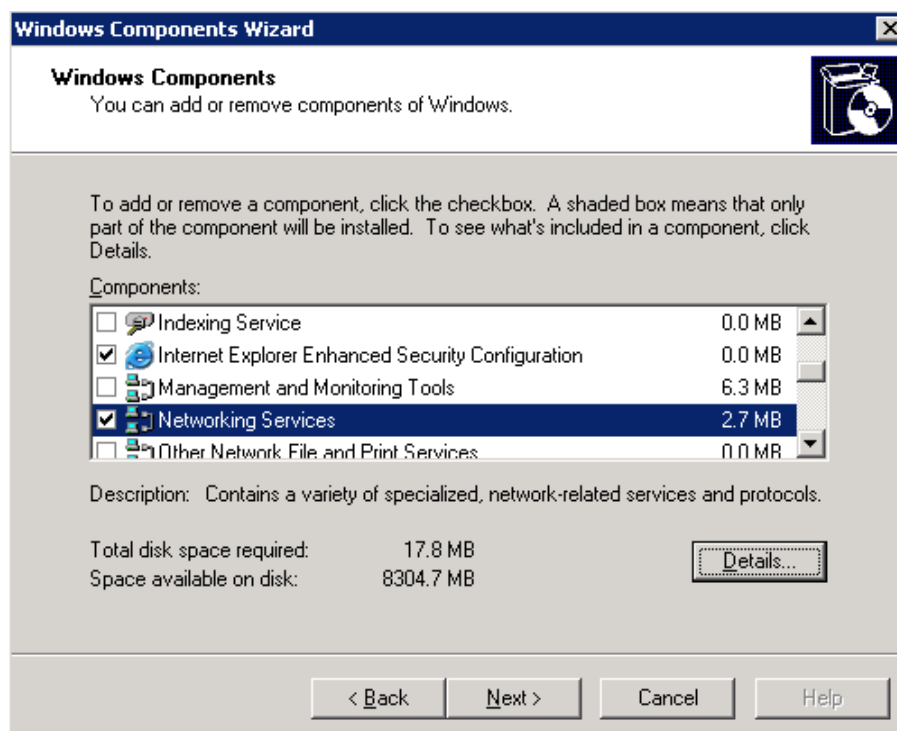


Figure 6-7 Windows Components Wizard

Step3. Select **Internet Authentication Services**. (Figure 6-8)

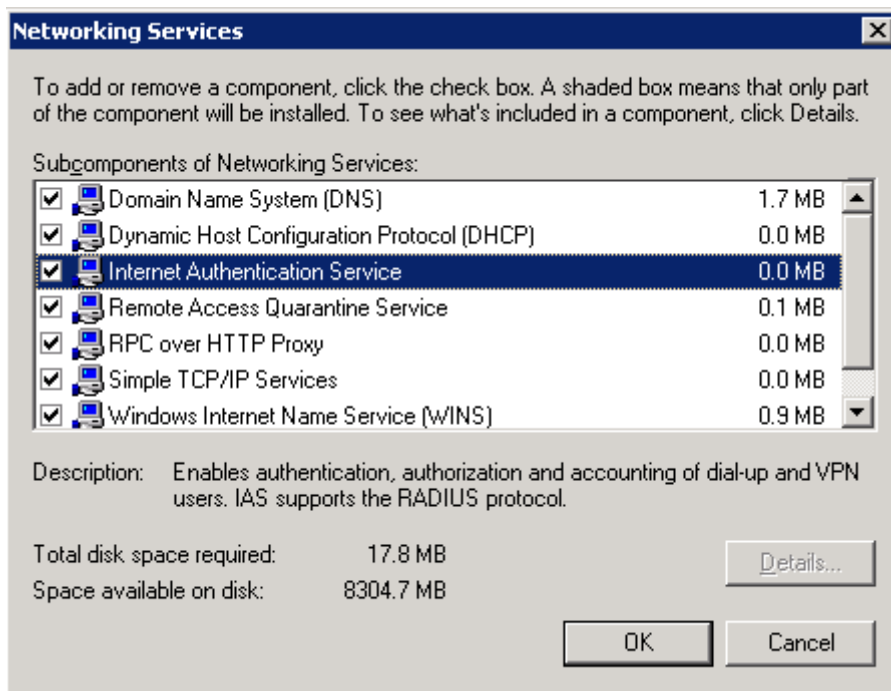


Figure 6-8 Adding Internet Authentication Services from the Subcomponents

Step4. Navigate to **Start → Control Panel → Administrative Tools** and then select **Internet Authentication Service**. (Figure 6-9)

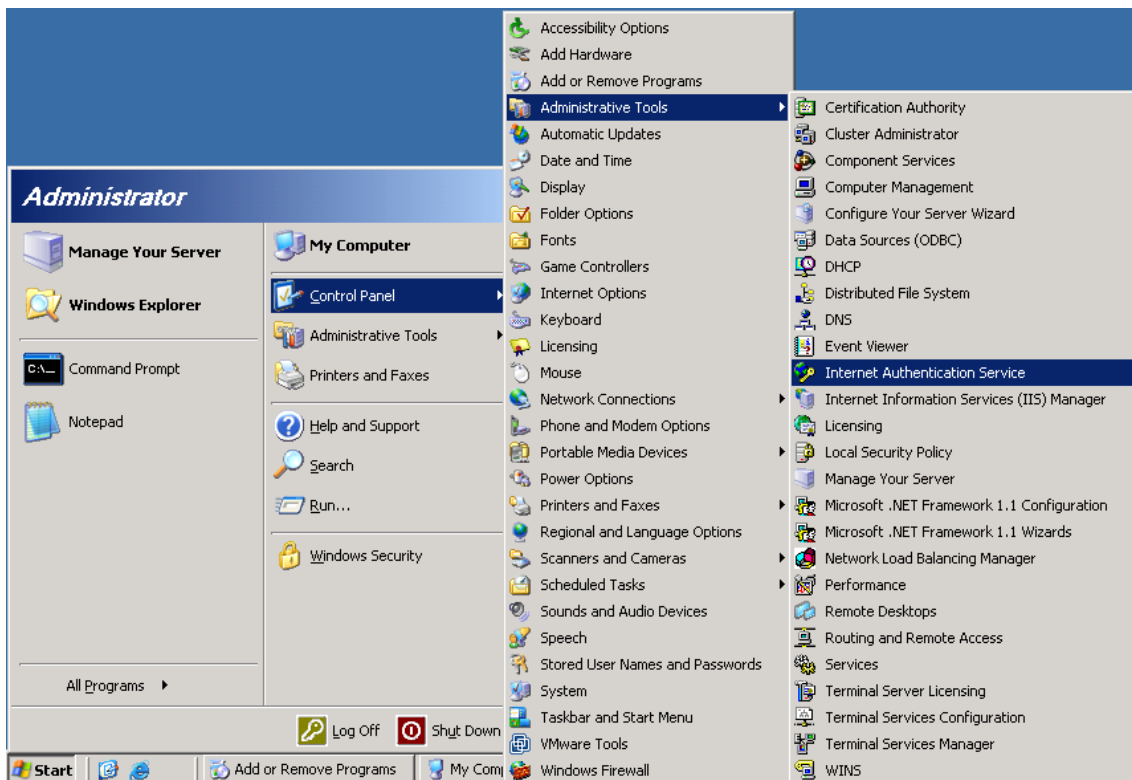


Figure 6-9 Selecting the Internet Authentication Service

Step5. Right-click on **RADIUS Clients** and then select **New RADIUS Client**. (Figure 6-10)

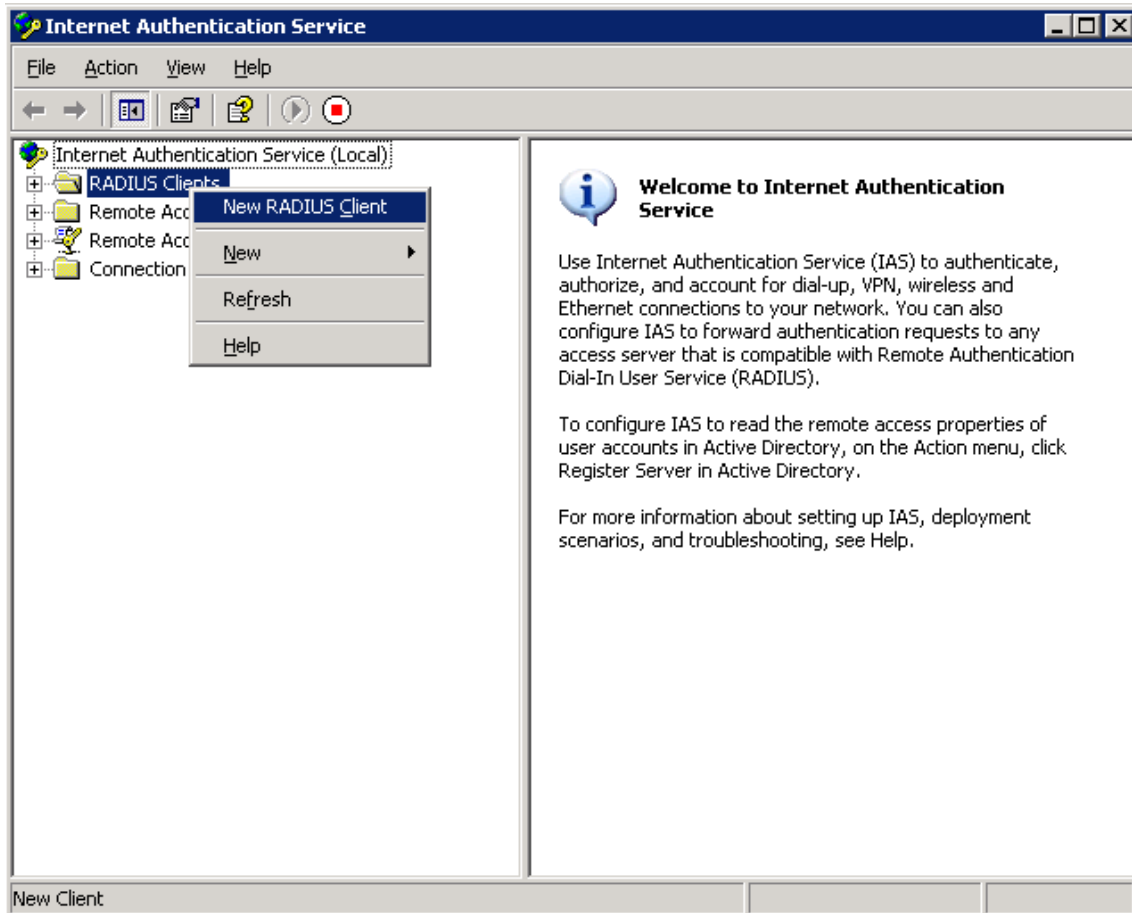
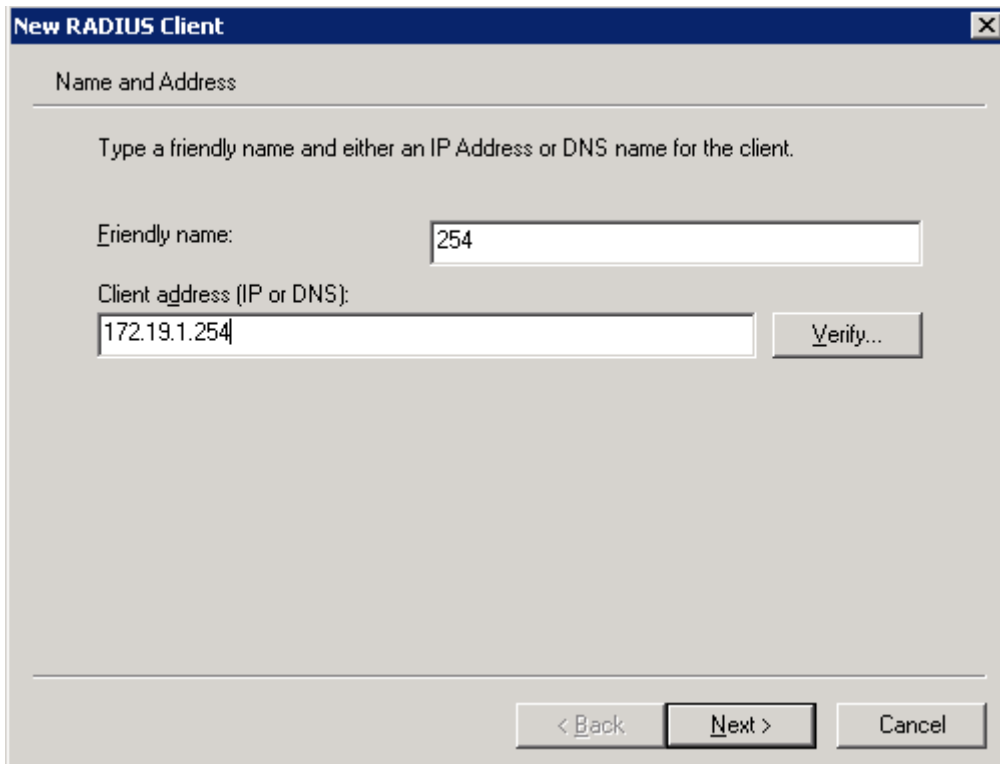


Figure 6-10 Adding a New RADIUS Client

Step6. Type a name and the client address (the device's management address) respectively in the corresponding fields. (Figure 6-11)



New RADIUS Client

Name and Address

Type a friendly name and either an IP Address or DNS name for the client.

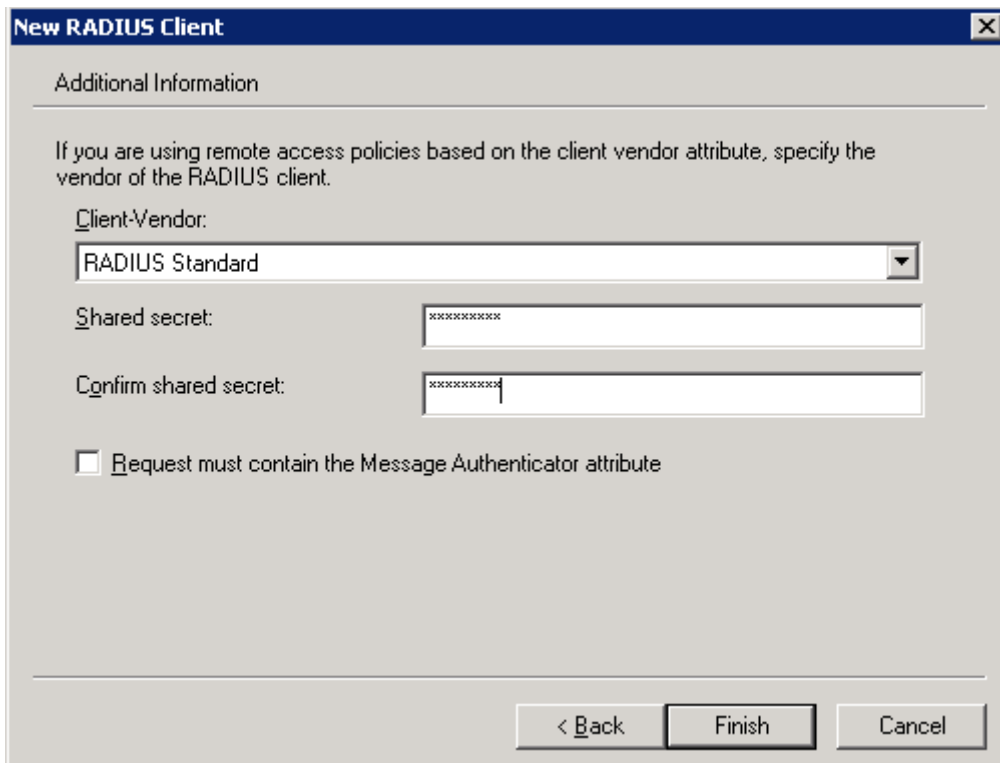
Friendly name:

Client address (IP or DNS):

< Back Next > Cancel

Figure 6-11 Configuring the New RADIUS Client

Step 7. Select **RADIUS Standard** for the **Client-Vendor**, enter the shared secret and then confirm it. (Note: The shared secret must be identical with the one specified for IAR-5000.) (Figure 6-12)



New RADIUS Client

Additional Information

If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

Client-Vendor:

Shared secret:

Confirm shared secret:

Request must contain the Message Authenticator attribute

< Back Finish Cancel

Figure 6-12 Selecting the Client-Vendor and Entering the Shared Secret

Step8. Right-click on **Remote Access Polices** and then select **New Remote Access Policy**. (Figure 6-13)

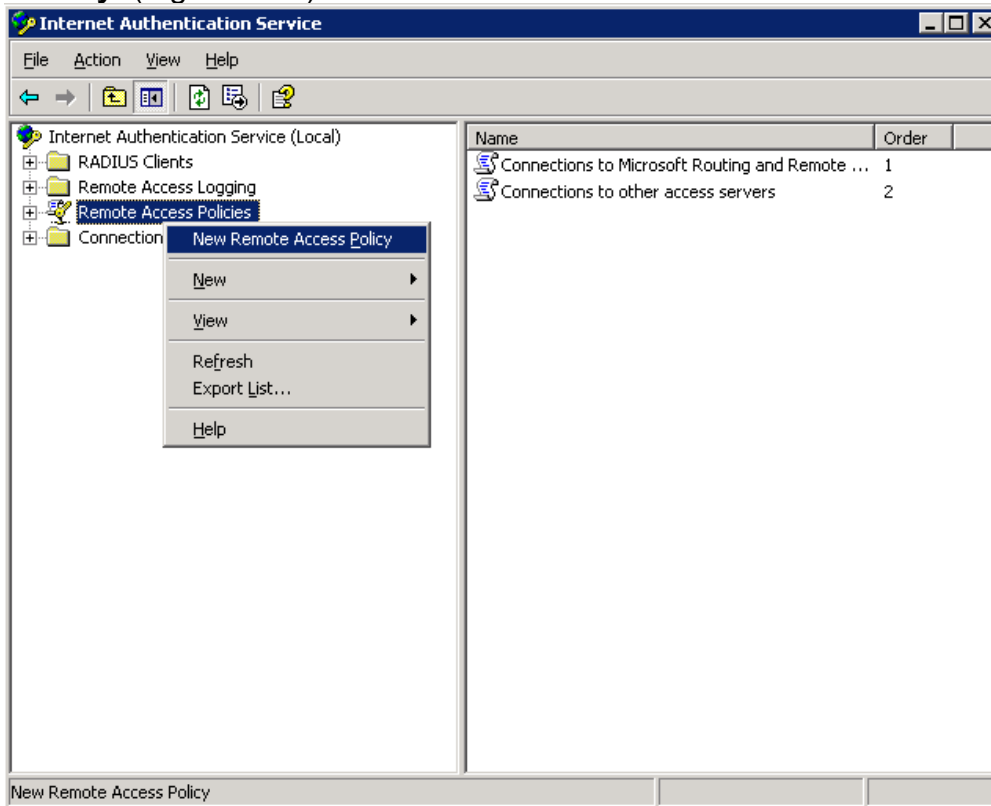


Figure 6-13 Creating a New Remote Access Policy

Step9. Select a policy configuration method and then type a policy name. (Figure 6-14)

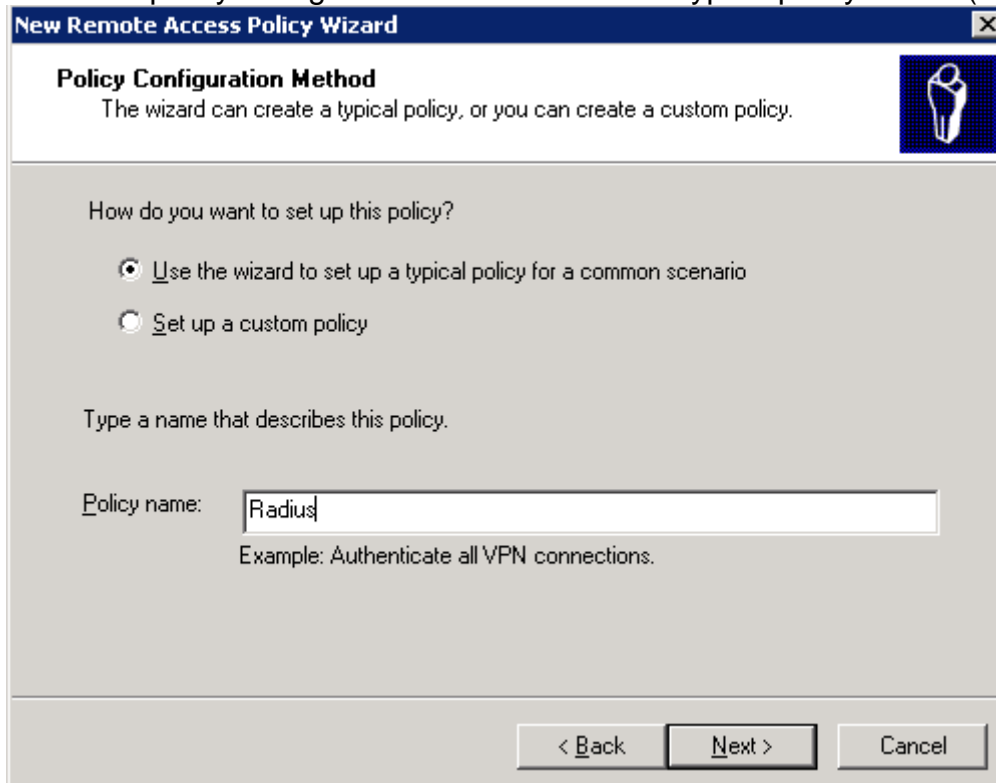


Figure 6-14 Selecting a Policy Configuration Method and Typing a Policy Name

Step10. Select **Ethernet** for the access method. (Figure 6-15)

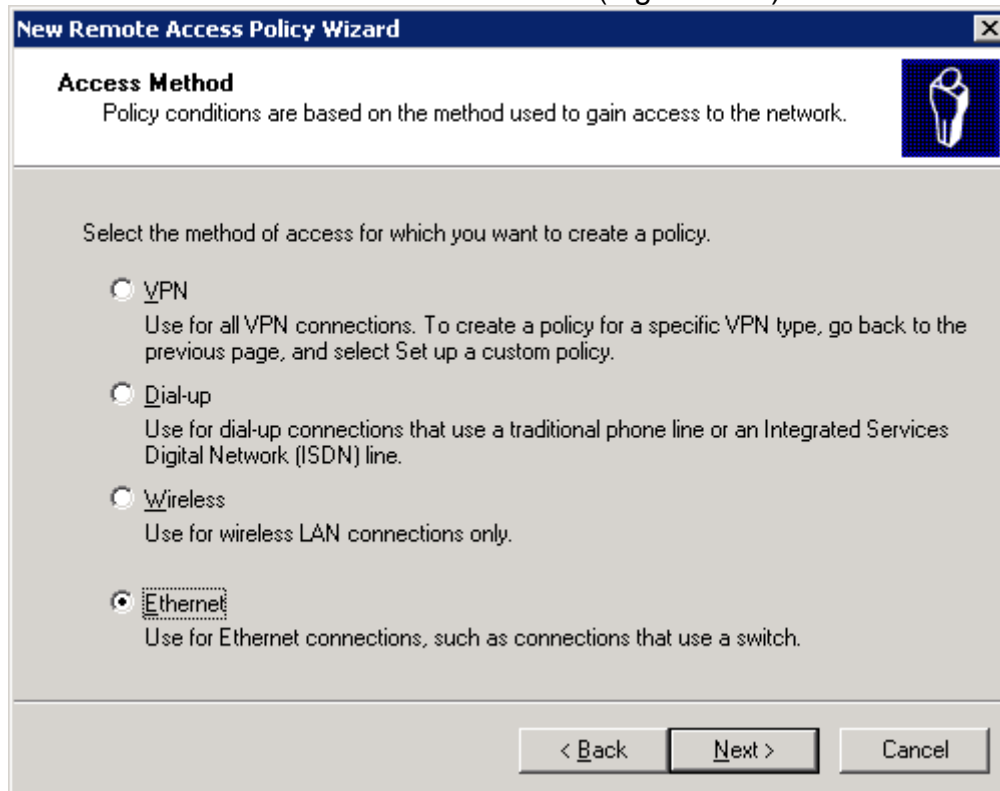


Figure 6-15 Selecting Ethernet for the Access Method

Step11. Grant access based on **User**. (Figure 6-16)

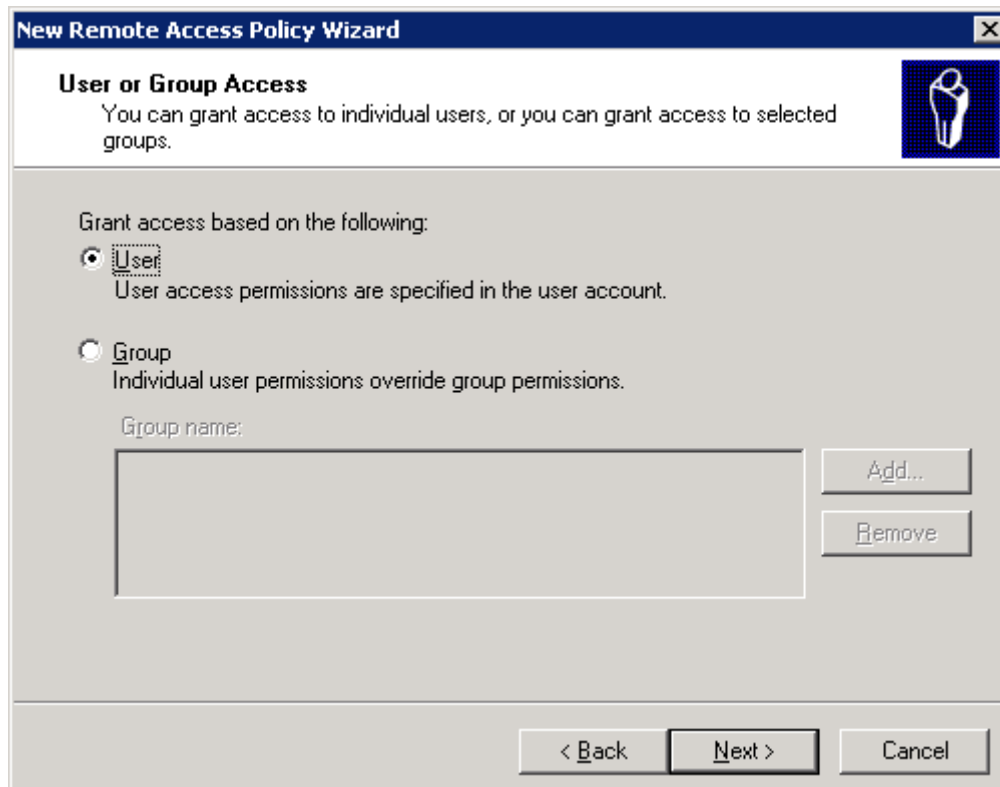


Figure 6-16 Granting Access Based on User

Step12. Select **MD5-Challenge** for **EAP type**. (Figure 6-17)

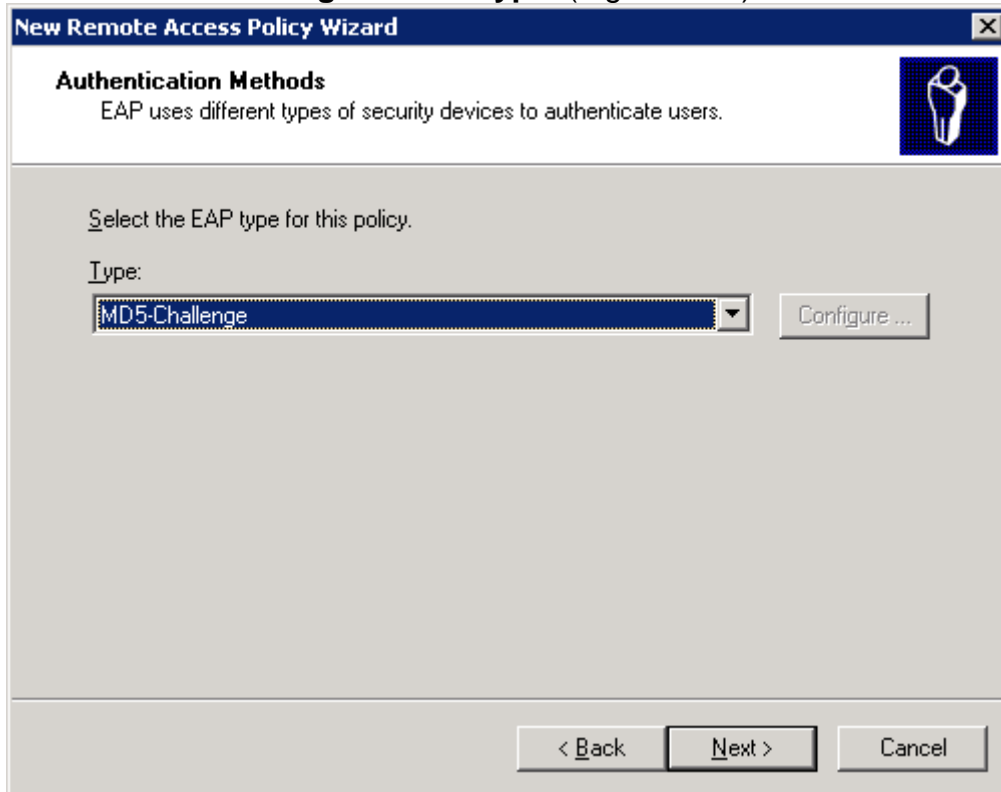


Figure 6-17 Selecting MD5-Challenge for EAP Type

Step13. Right-click on the newly added policy and then select **Properties**. (Figure 6-18)

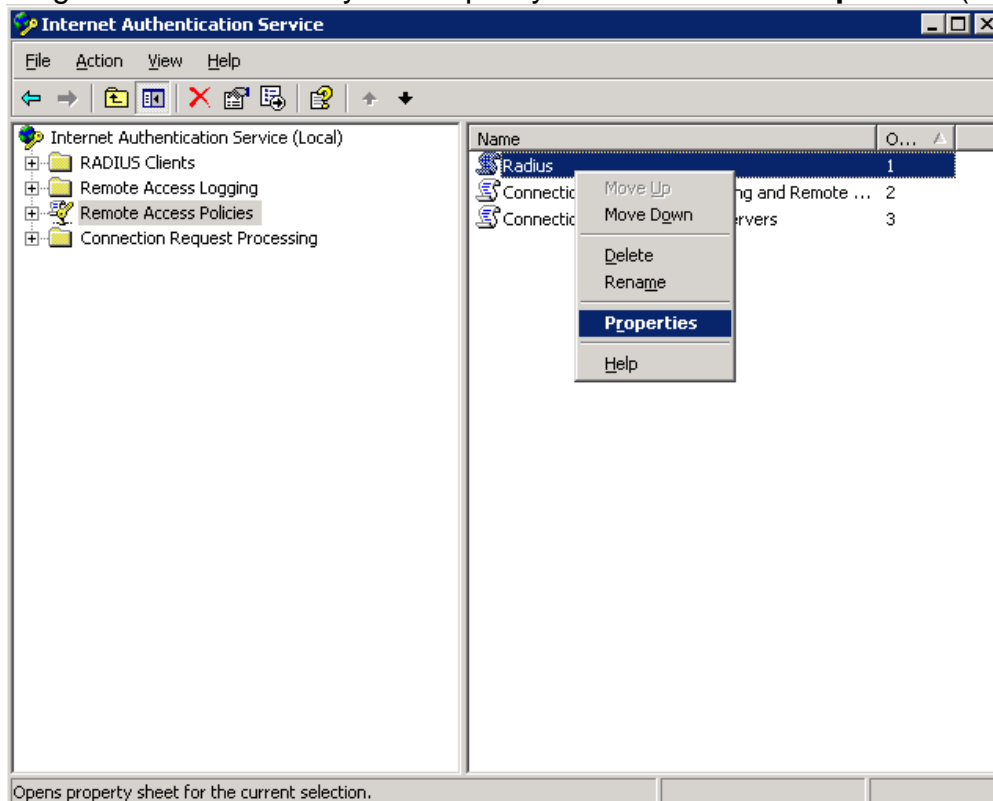


Figure 6-18 Configuring the Properties of the Newly Added Policy

Step14. Choose **Grant remote access permission**, remove the existing policy conditions and then click on **Add**. (Figure 6-19)

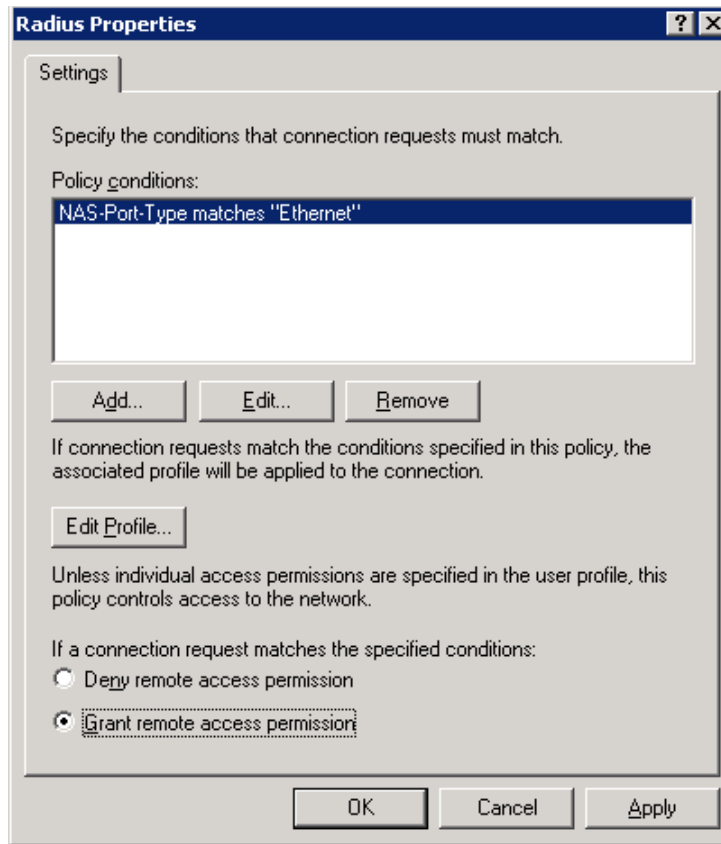


Figure 6-19 Configuring the Properties of the Policy

Step15. Select **Service-Type** from the attribute types. (Figure 6-20)

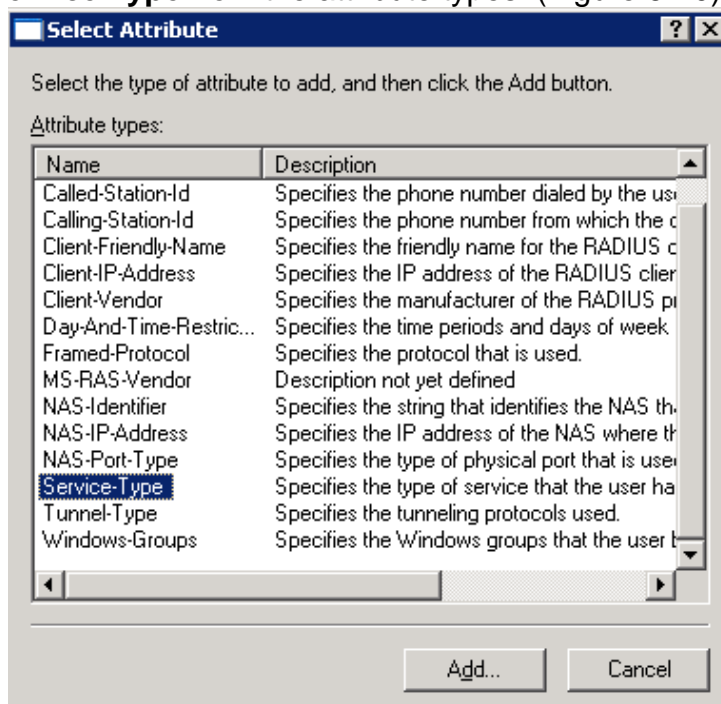


Figure 6-20 Adding a New Attribute Type

Step16. Select **Authenticate Only** from available types and then click on **Add**. (Figure 6-21)

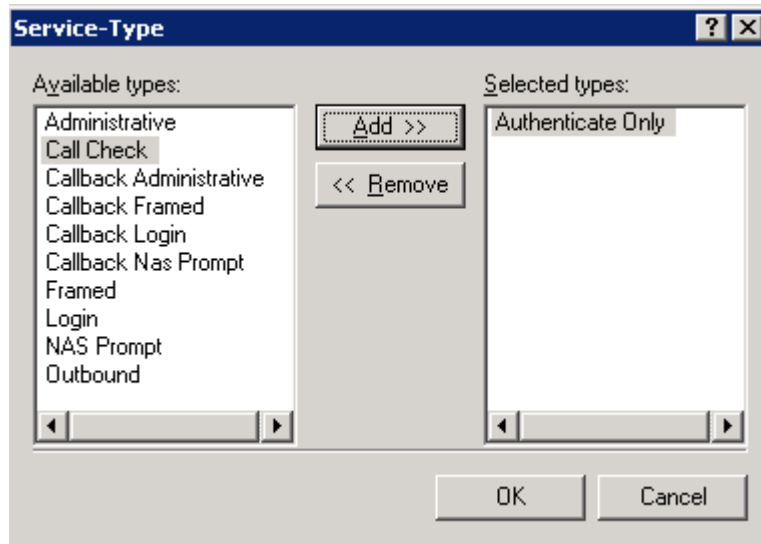


Figure 6-21 Adding a Service Type

Step17. Click on **Edit Profile** button and then **Authentication** tab. Next, select **Unencrypted authentication (PAP, SPAP)** as the method. (Figure 6-22)

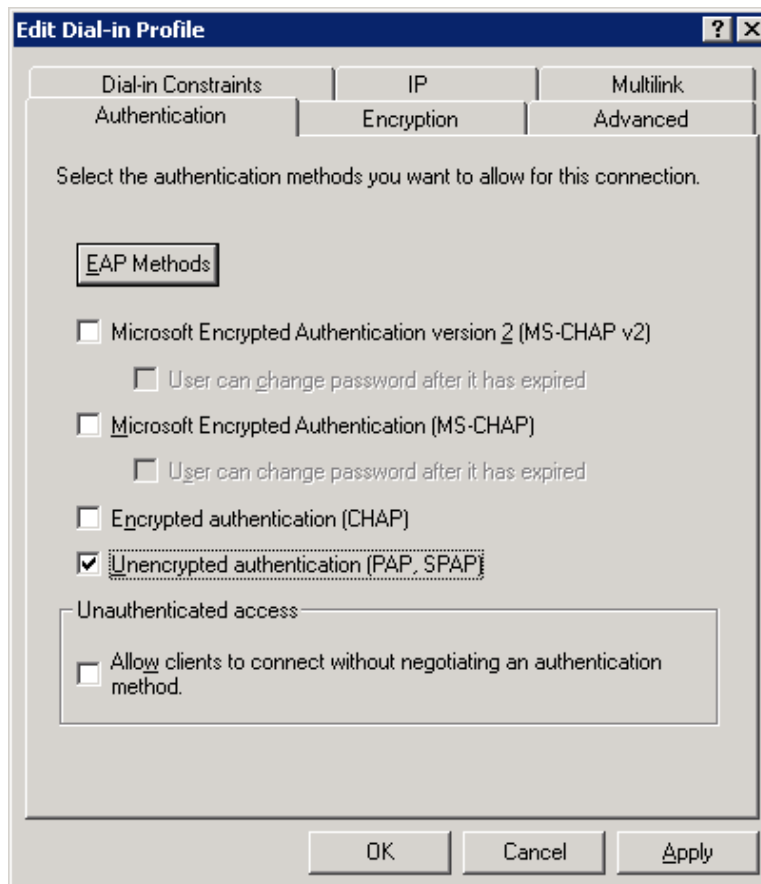


Figure 6-22 Selecting the Authentication Method

Step18. Navigate to **Start → Control Panel → Administrative Tools** and then select **Computer Management**. (Figure 6-23)

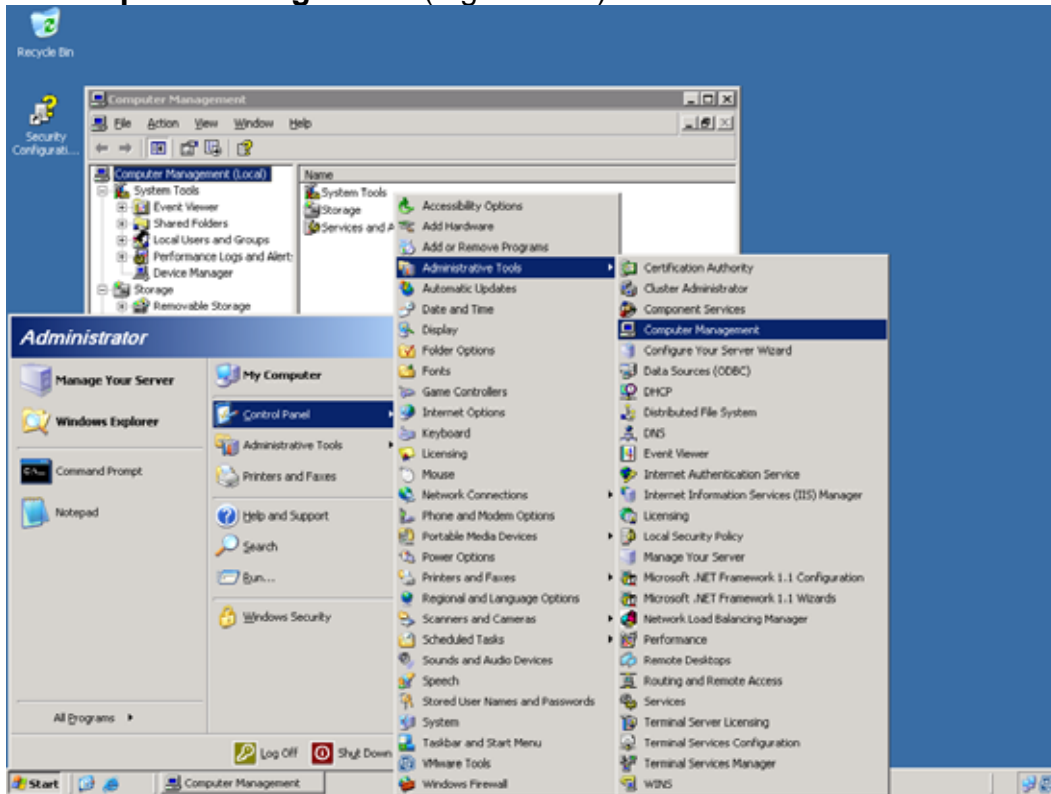


Figure 6-23 The Location of Computer Management on the Start Menu

Step19. On **Local User and Groups**, right-click on **Users** and then select **New User**. (Figure 6-24)

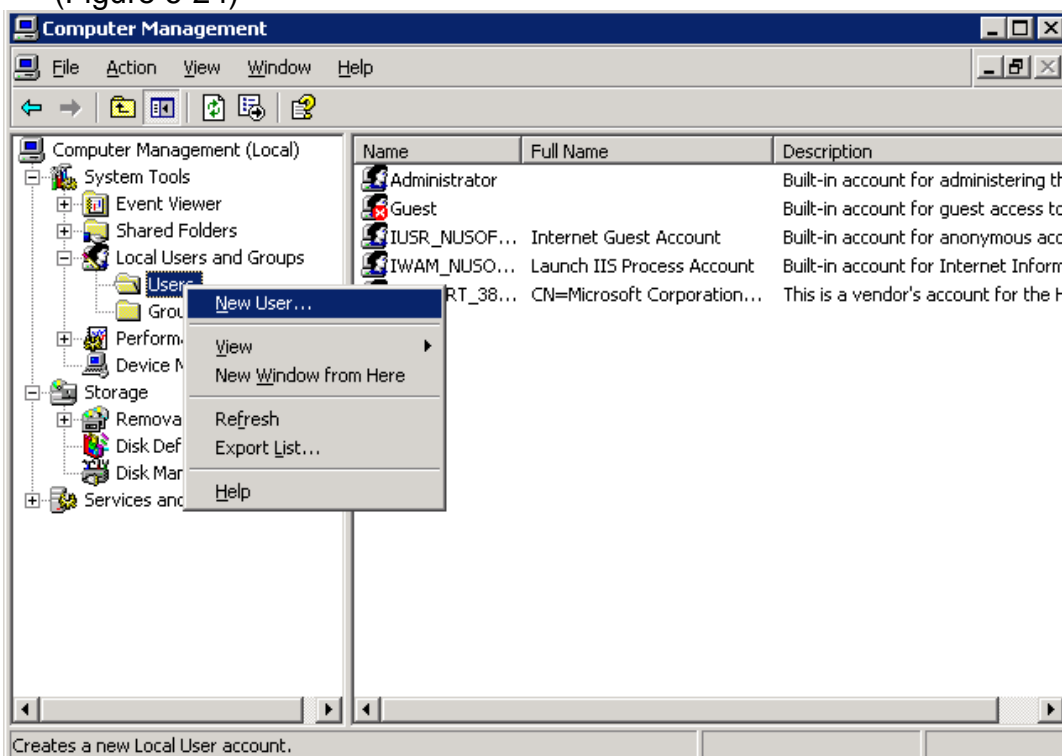
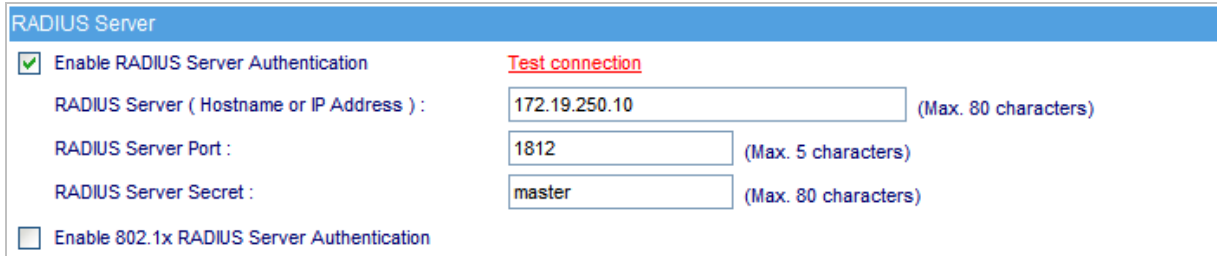


Figure 6-24 Creating a New User

Step20. The RADIUS server setup is completed.


Step21. Under **Authentication** → **RADIUS**, type the IP address, port number and shared secret respectively in the corresponding fields. (Figure 6-25)



The screenshot shows the 'RADIUS Server' configuration window. It has a blue header with the title 'RADIUS Server'. Below the header, there are several settings:

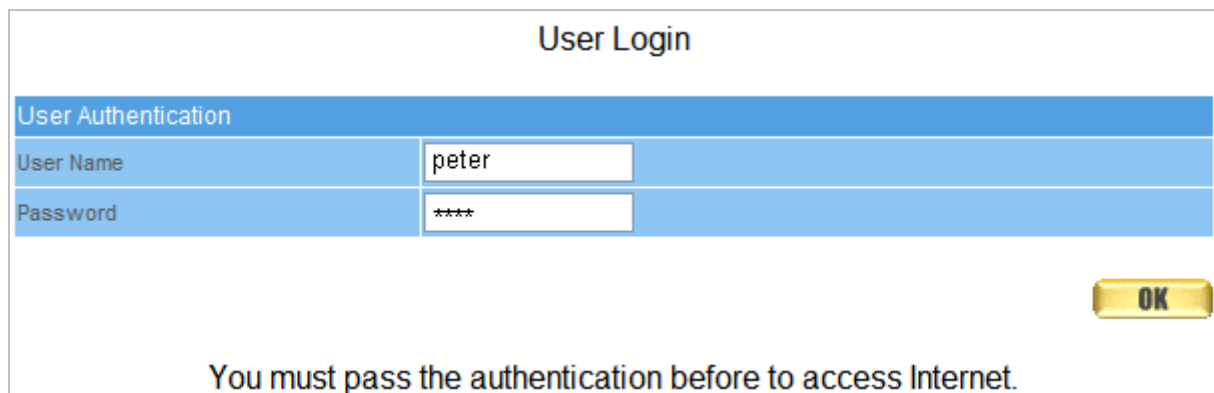
- A checked checkbox labeled 'Enable RADIUS Server Authentication' with a red 'Test connection' link to its right.
- A text input field for 'RADIUS Server (Hostname or IP Address)' containing '172.19.250.10' with '(Max. 80 characters)' to its right.
- A text input field for 'RADIUS Server Port' containing '1812' with '(Max. 5 characters)' to its right.
- A text input field for 'RADIUS Server Secret' containing 'master' with '(Max. 80 characters)' to its right.
- An unchecked checkbox labeled 'Enable 802.1x RADIUS Server Authentication'.

Figure 6-25 Configuring the RADIUS Server Settings



Click on **Test connection** to test the connection to the RADIUS server.

Step22. The login screen for authentication will show upon users's web browsing attempt. If the login information is correctly applied, authentication will be successful. (Figure 6-26)



The screenshot shows a 'User Login' screen with a blue header. Below the header, there is a 'User Authentication' section with two input fields:

- 'User Name' with the value 'peter'.
- 'Password' with the value '****'.

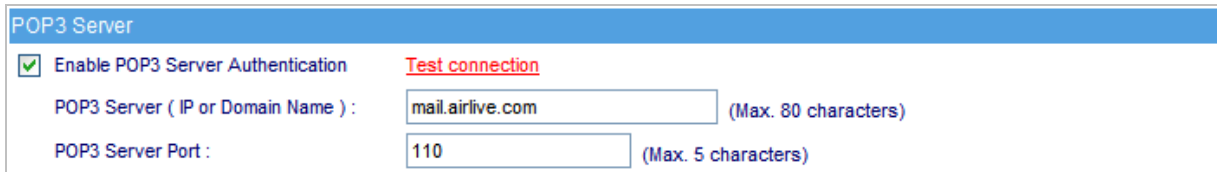
To the right of the password field is a yellow 'OK' button. Below the input fields, the text reads: 'You must pass the authentication before to access Internet.'

Figure 6-26 The Login Screen for Authentication

6.4 POP3

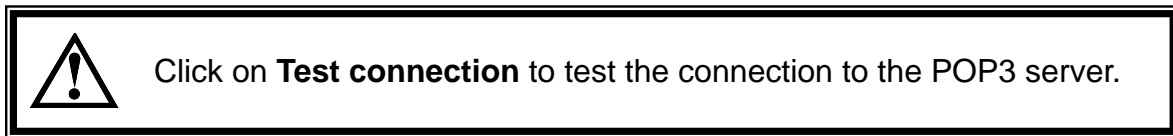
Using a POP3 Server to Regulate Users' Internet Access:

Step1. Under **Authentication** → **POP3**, type the IP address (or domain name) and port number respectively in the corresponding fields. (Figure 6-27)

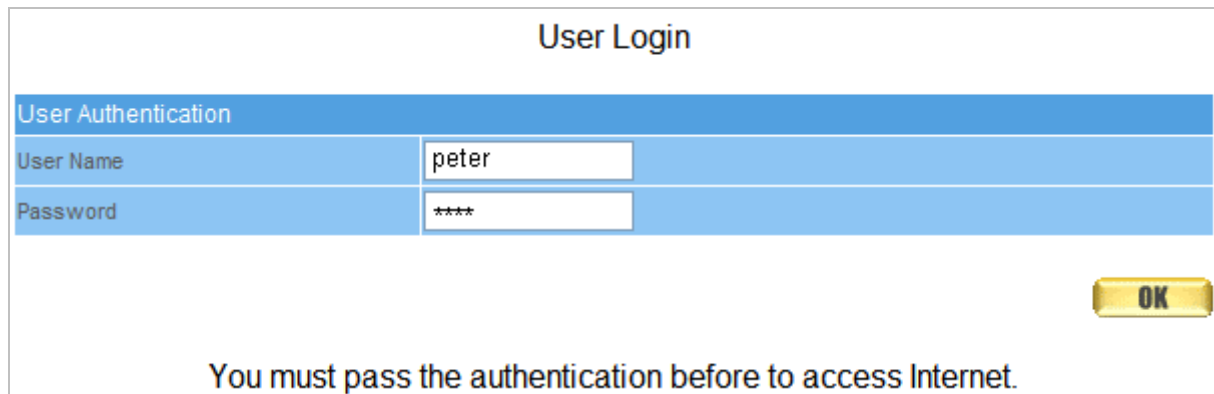


The screenshot shows the 'POP3 Server' configuration window. It includes a checked checkbox for 'Enable POP3 Server Authentication' and a red 'Test connection' link. Below are two input fields: 'POP3 Server (IP or Domain Name)' containing 'mail.airlive.com' (with a '(Max. 80 characters)' note) and 'POP3 Server Port' containing '110' (with a '(Max. 5 characters)' note).

Figure 6-27 Configuring the POP3 Server Settings



Step2. The login screen for authentication will show upon users's web browsing attempt. If the login information is correctly applied, the authentication will be successful. (Figure 6-28)



The screenshot shows the 'User Login' screen. At the top, it says 'User Login'. Below is a blue header bar labeled 'User Authentication'. Underneath are two input fields: 'User Name' with the text 'peter' and 'Password' with '****'. A yellow 'OK' button is located at the bottom right. At the bottom of the screen, a message reads: 'You must pass the authentication before to access Internet.'

Figure 6-28 The Login Screen for Authentication

6.5 LDAP

LDAP Search Distinguished Name:

- The distinguished name for the LDAP authentication.

LDAP Filter:

- The criteria to use in selecting elements within scope.

User's Distinguished Name:

- The distinguished name for the LDAP authentication.

Configuring LDAP Server on Windows Server 2003:

Step1. Go to **Start → Administration Tools → Manage Your Server.**

Step2. Click **Add or remove a role.** (Figure 6-29)

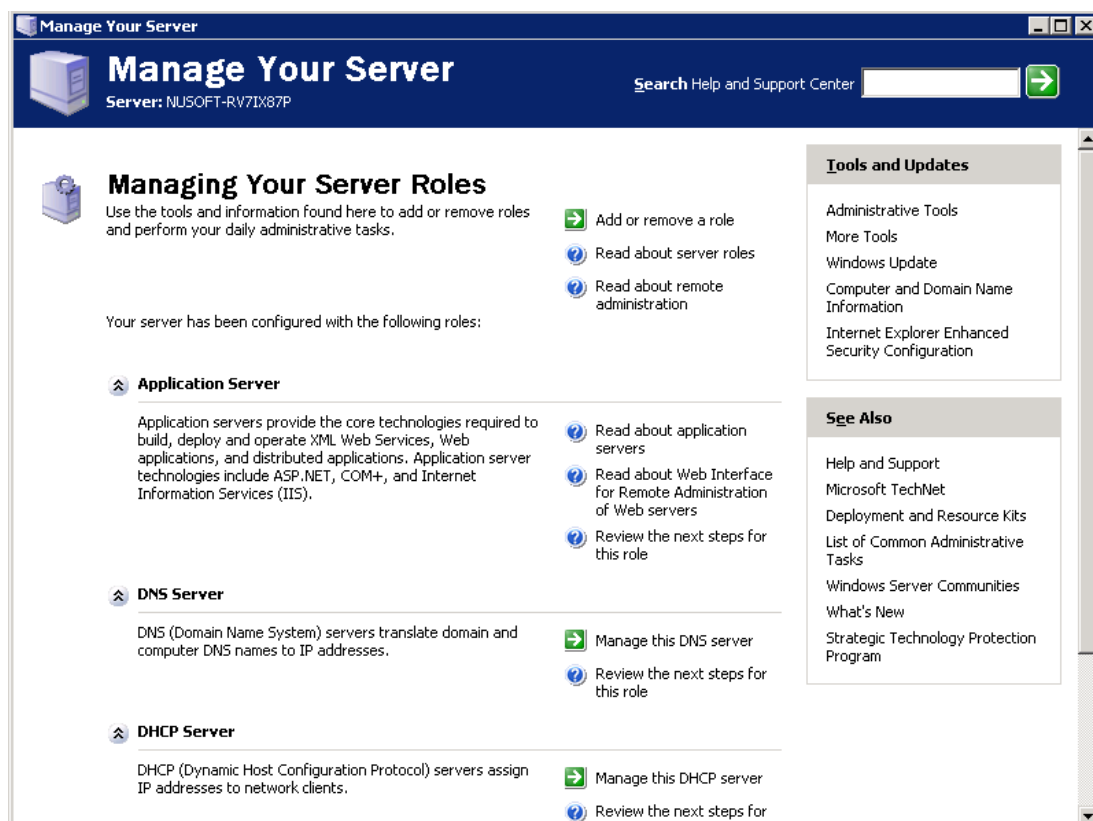


Figure 6-29 The Login Screen for Authentication

Step3. Click Next. (Figure 6-30)

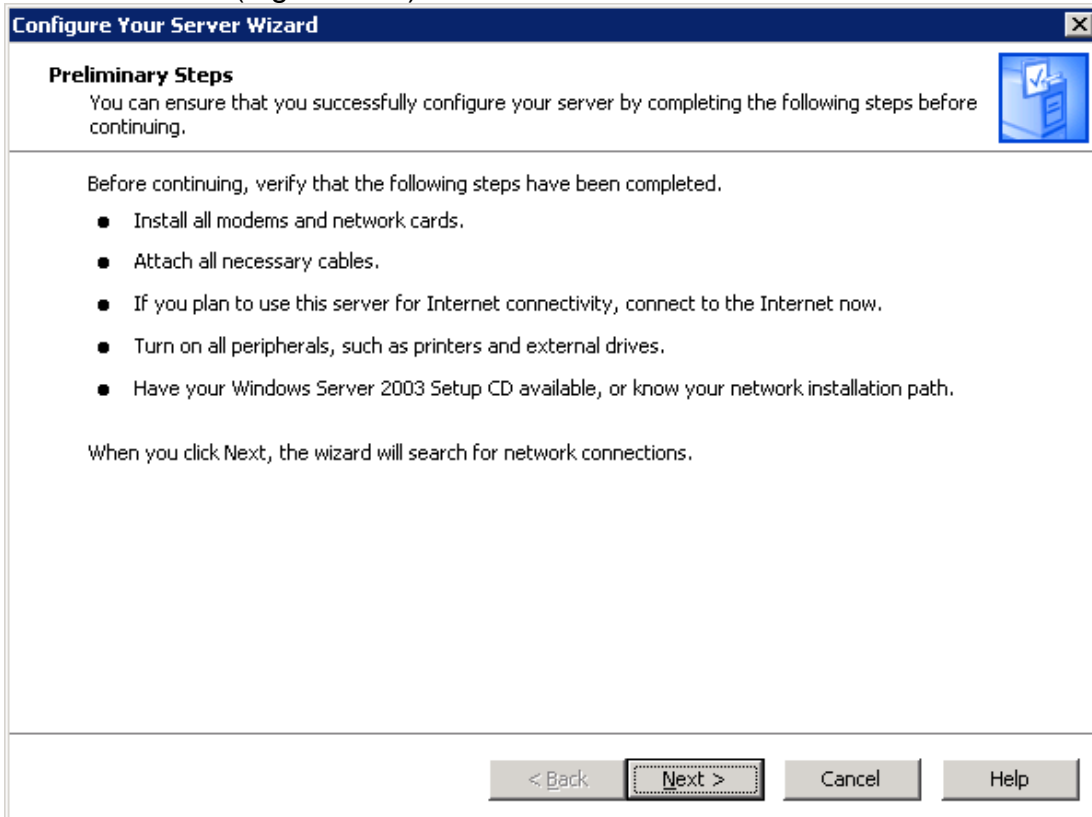


Figure 6-30 Server Configuration Wizard

Step4. Select Active Directory then click Next. (Figure 6-31)

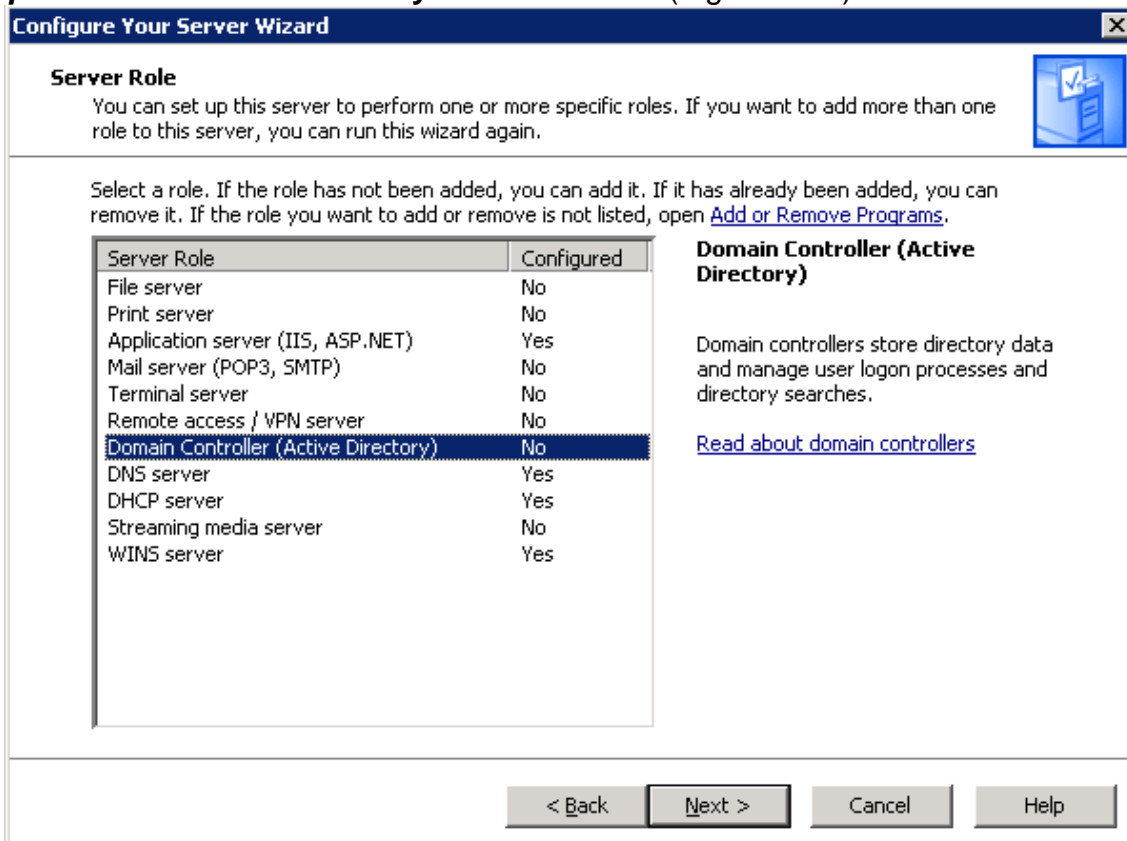


Figure 6-31 Server Role

Step5. Click **Next**. (Figure 6-32)

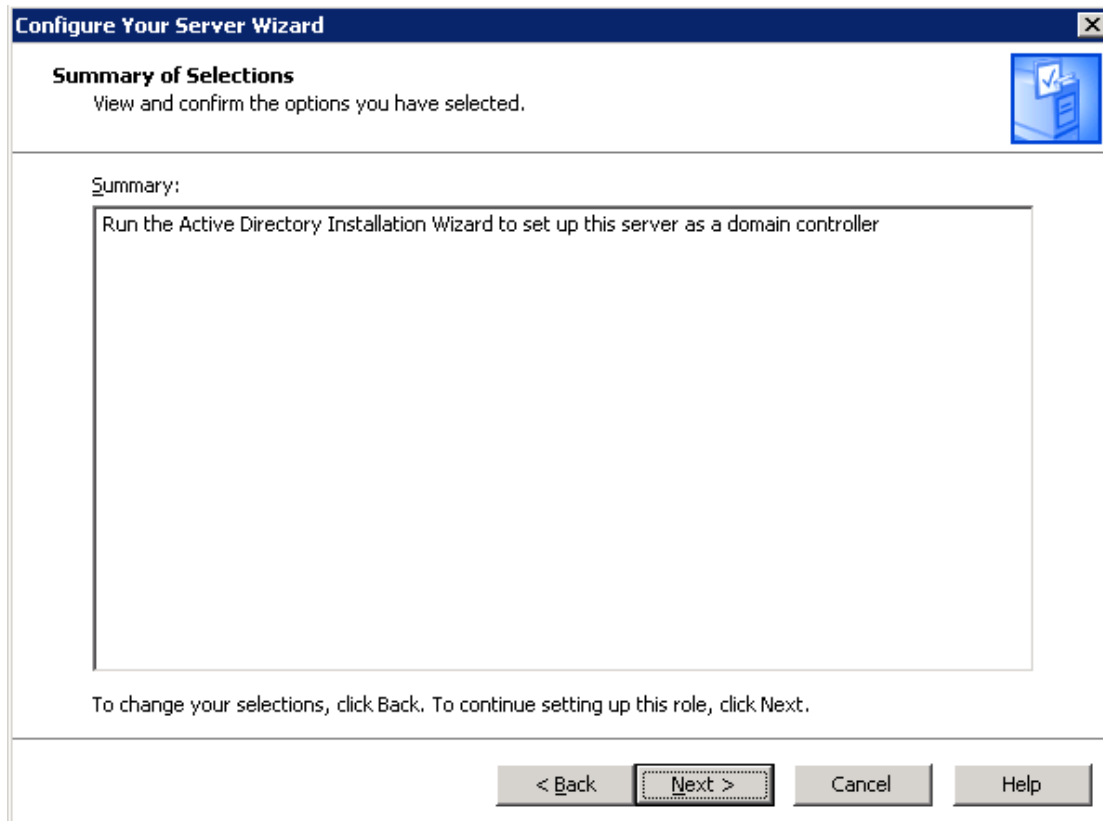


Figure 6-32 Summary of Selections

Step6. Click **Next**. (Figure 6-33)

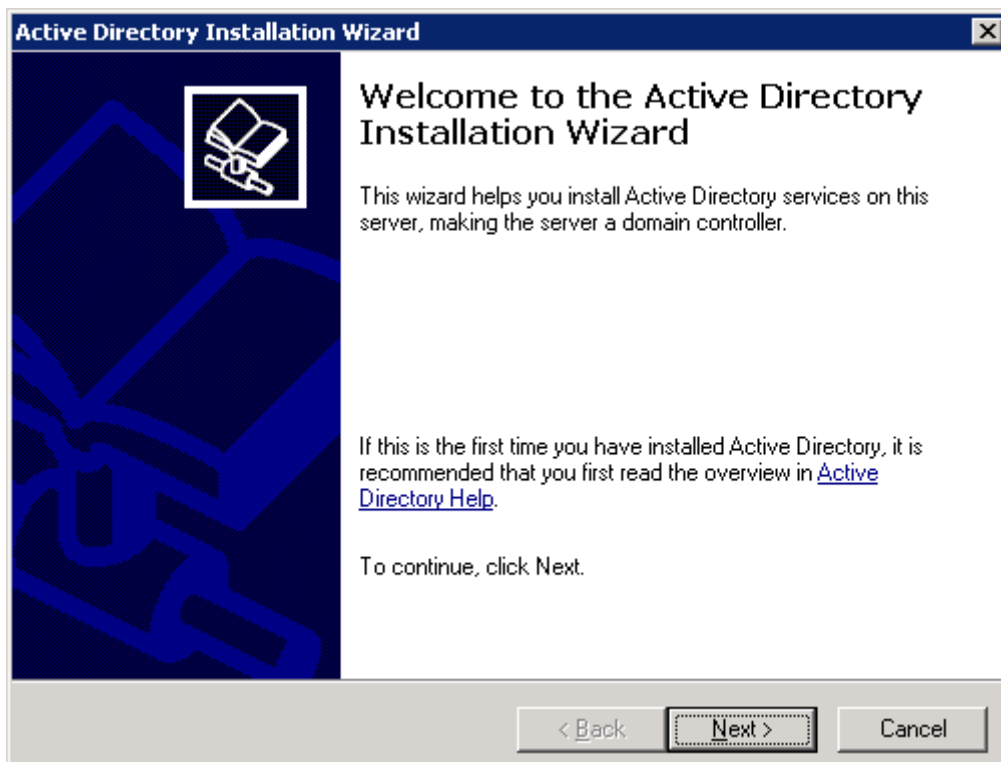


Figure 6-33 Installation Wizard

Step7. Click **Next**. (Figure 6-34)

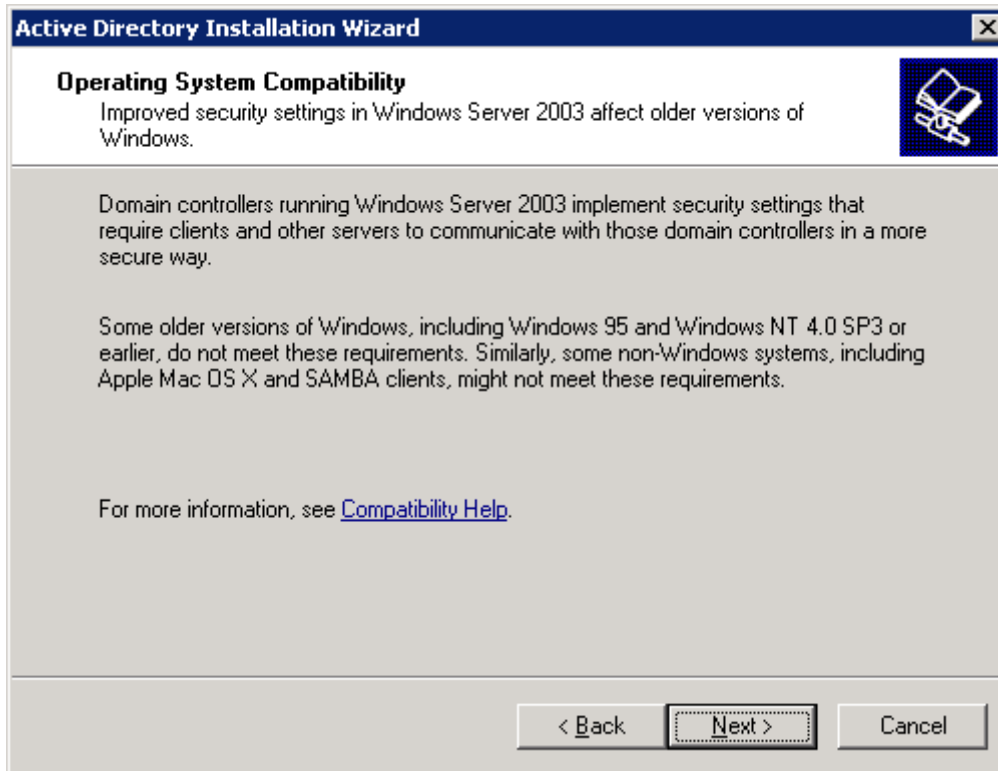


Figure 6-34 Installation Wizard

Step8. Select **Domain Controller for a new Domain** then click **Next**. (Figure 6-35)

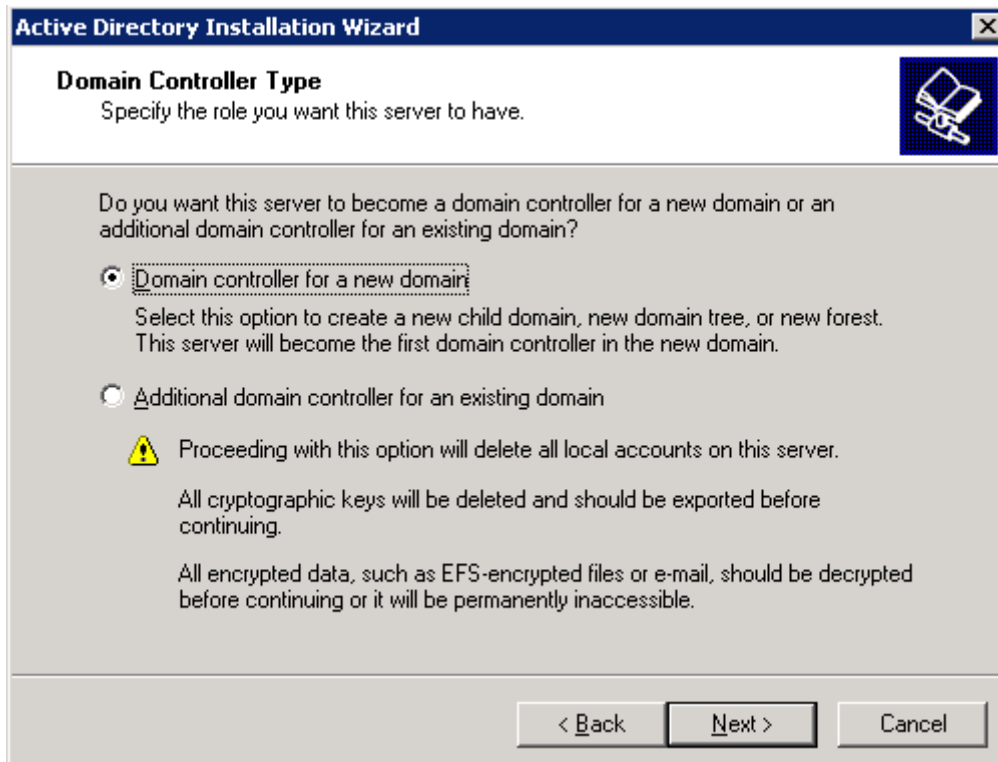


Figure 6-35 Domain Controller Type

Step9. Select **Domain in a new forest** then click **Next**. (Figure 6-36)

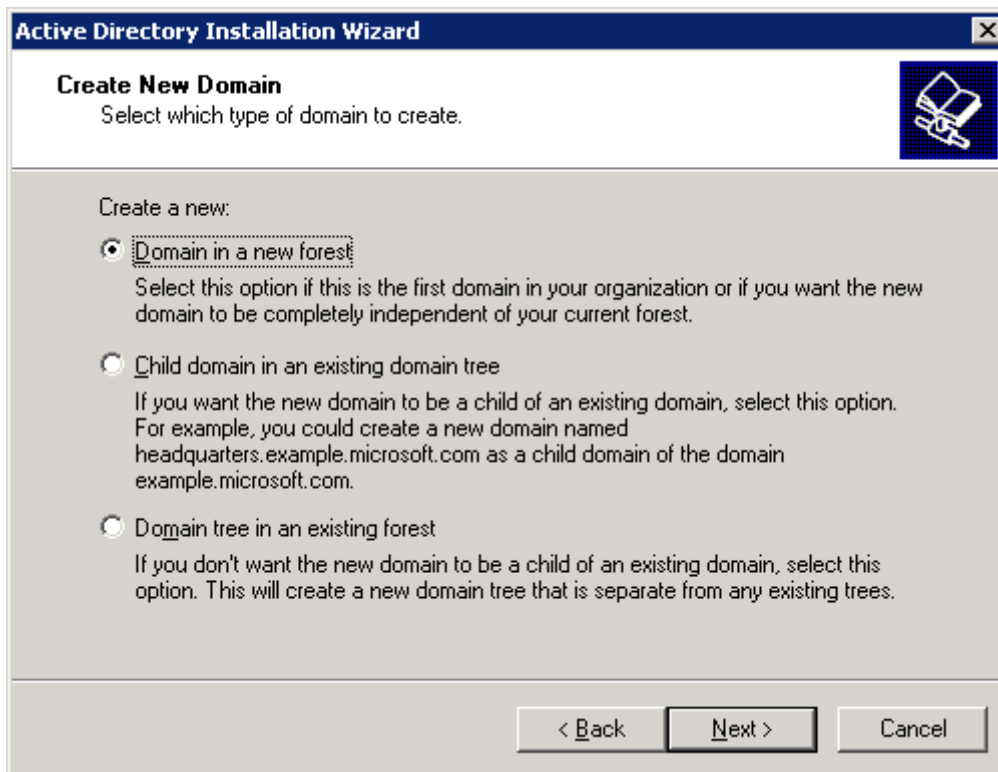


Figure 6-36 Create New Domain

Step10. Type the DNS name for the domain then click **Next**. (Figure 6-37)

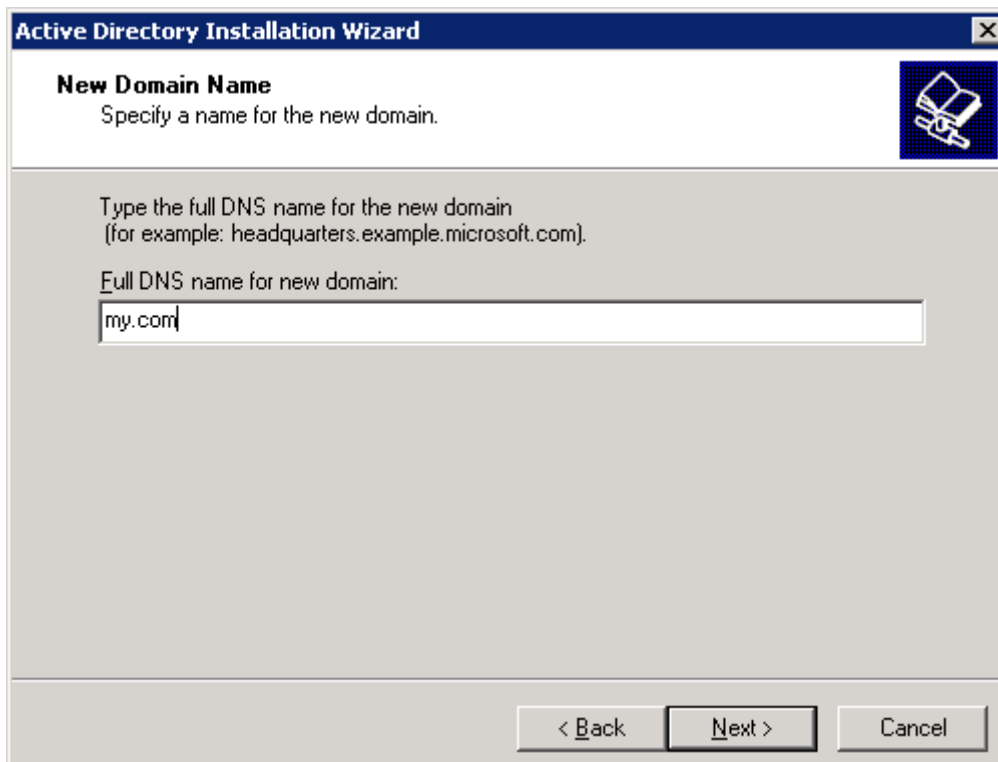


Figure 6-37 New Domain Name

Step11. Enter the NetBIOS domain name then click **Next**. (Figure 6-38)

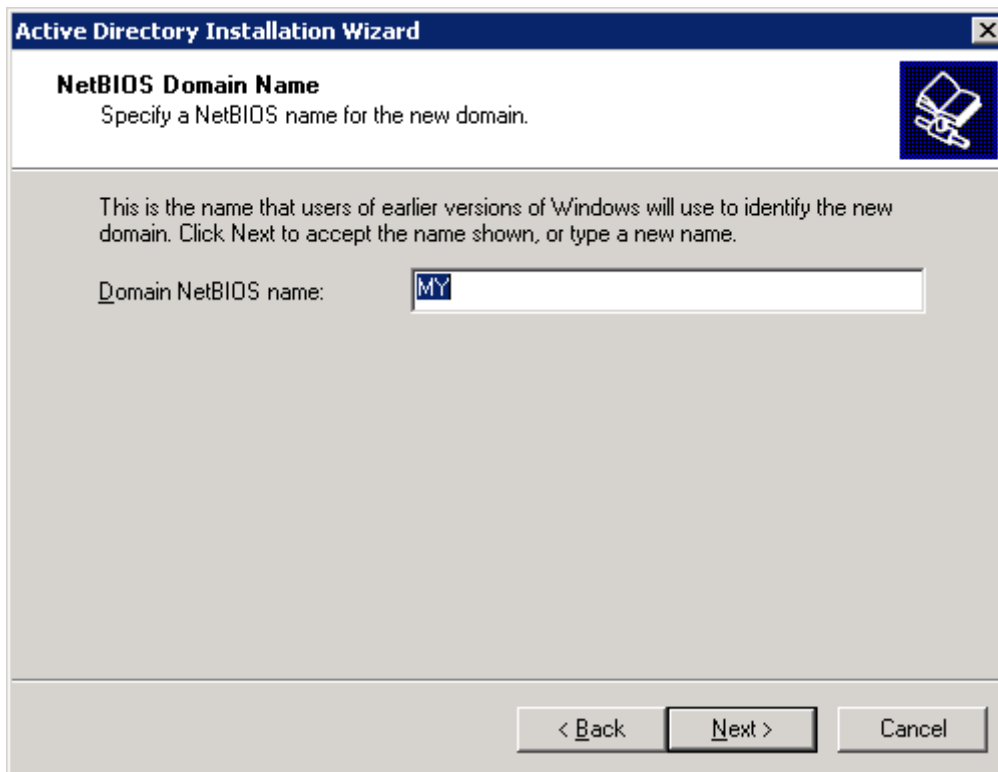


Figure 6-38 NetBIOS Domain Name

Step12. Enter the Domain NetBIOS name then click **Next**. (Figure 6-39)

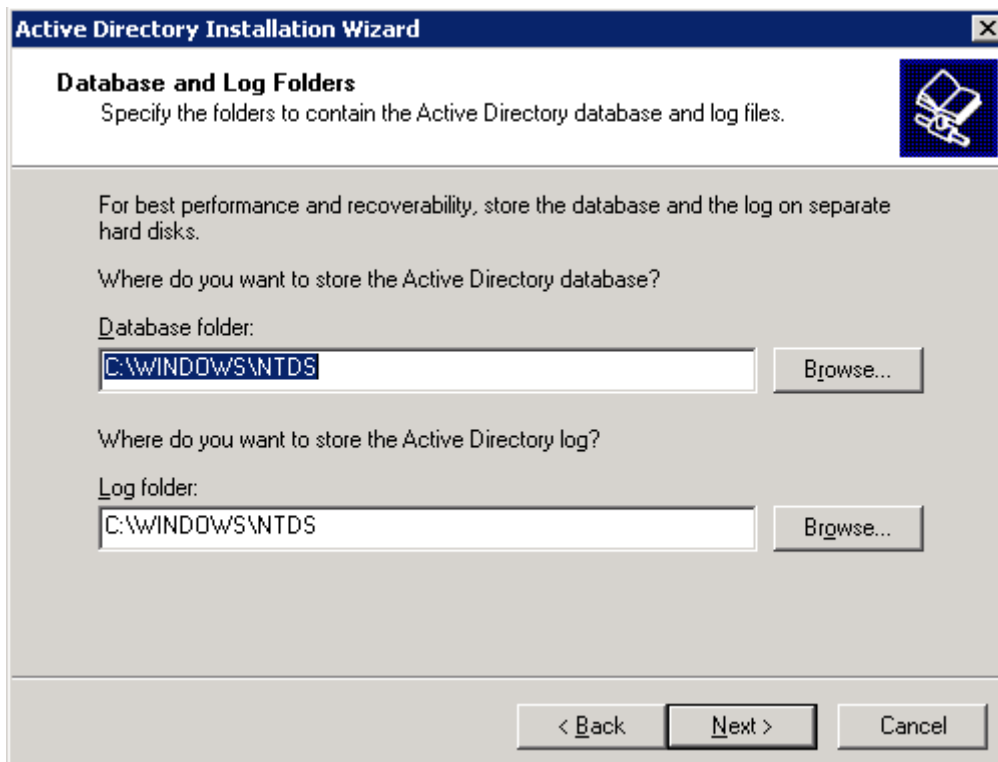


Figure 6-39 Database and Log Folders

Step13. Enter the folder location then click **Next**. (Figure 6-40)

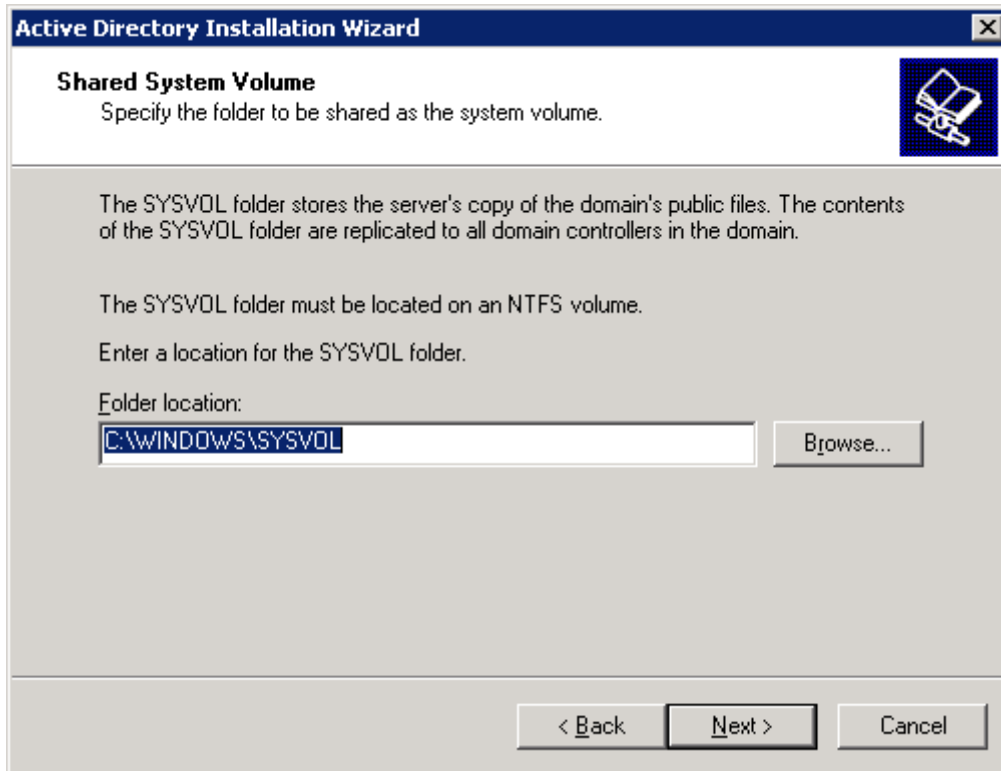


Figure 6-40 Shared System Volume

Step14. Select **I will correct the problem later by configuring DNS manually**. (Figure 6-41)

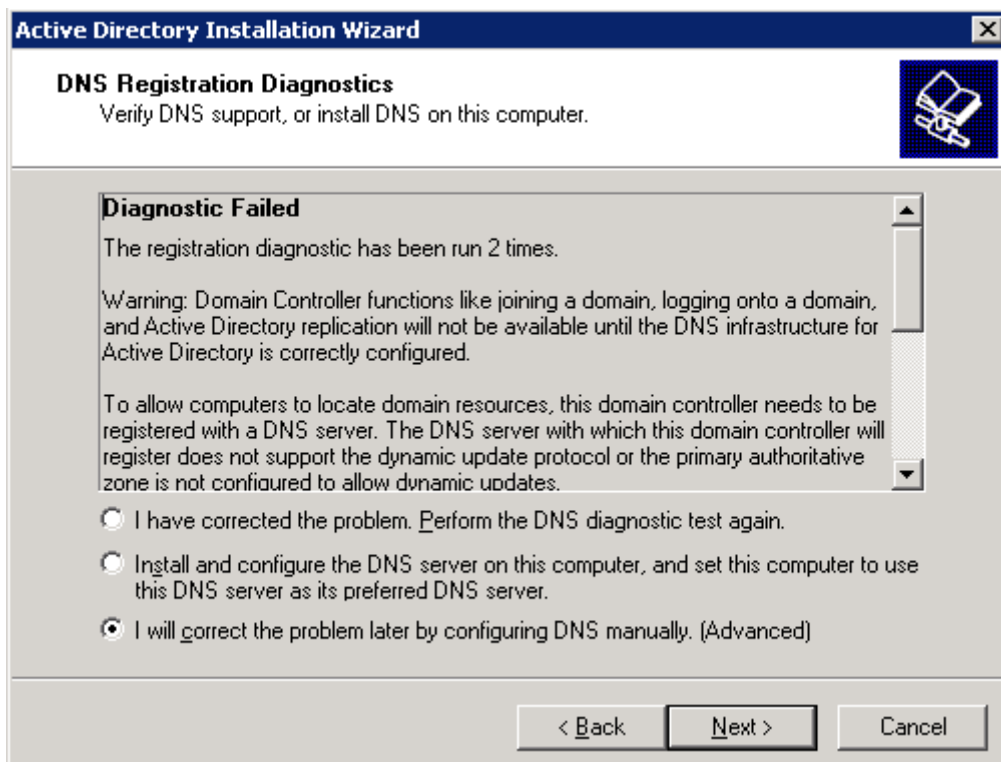


Figure 6-41 DNS Registration Diagnostics

Step15. Select **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems.** (Figure 6-42)

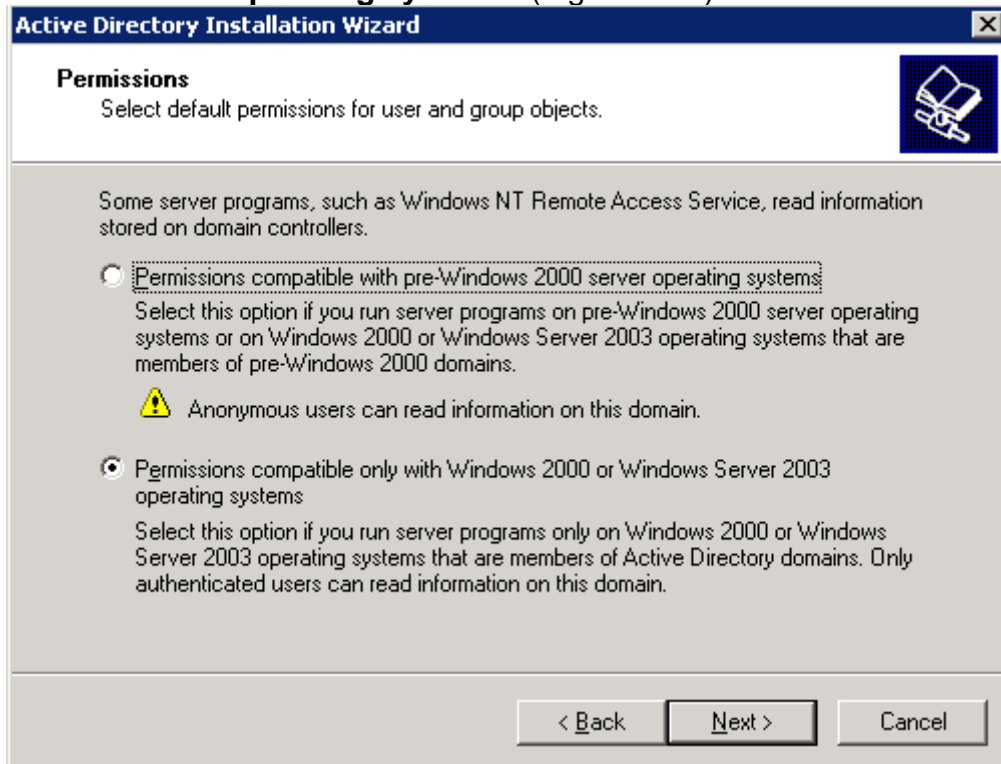


Figure 6-42 Permissions

Step16. Enter a restore mode password and retype it in the **Confirm password** field. (Figure 6-43)

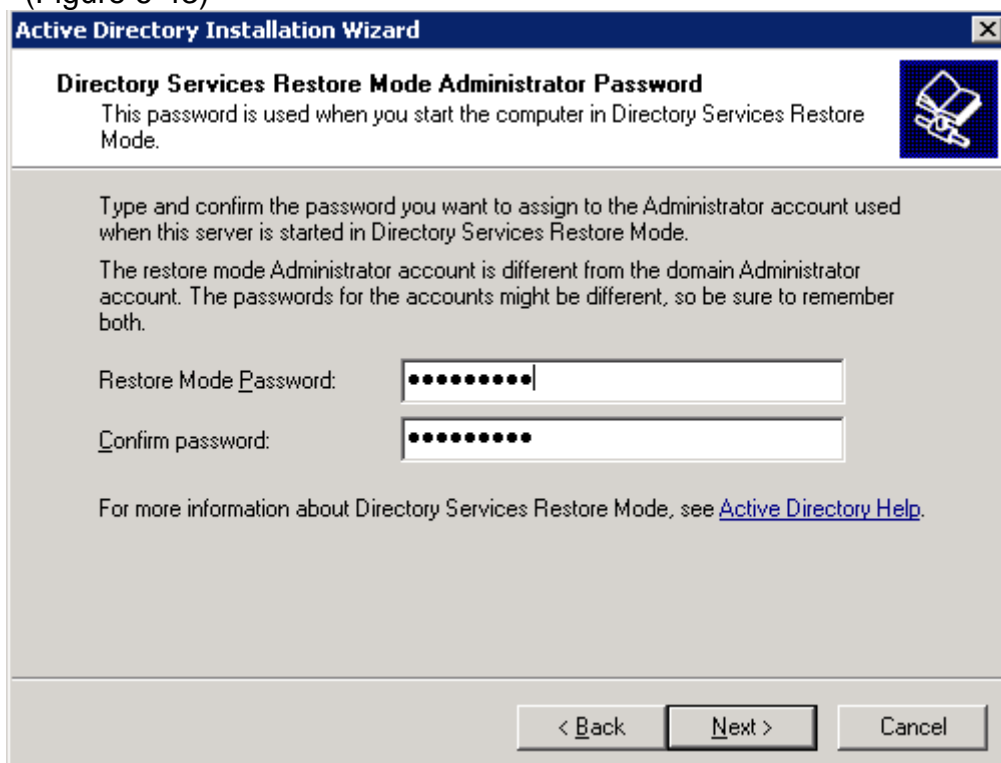


Figure 6-43 Directory Services Restore Mode Administrator Password

Step17. Click **Next**. (Figure 6-44)

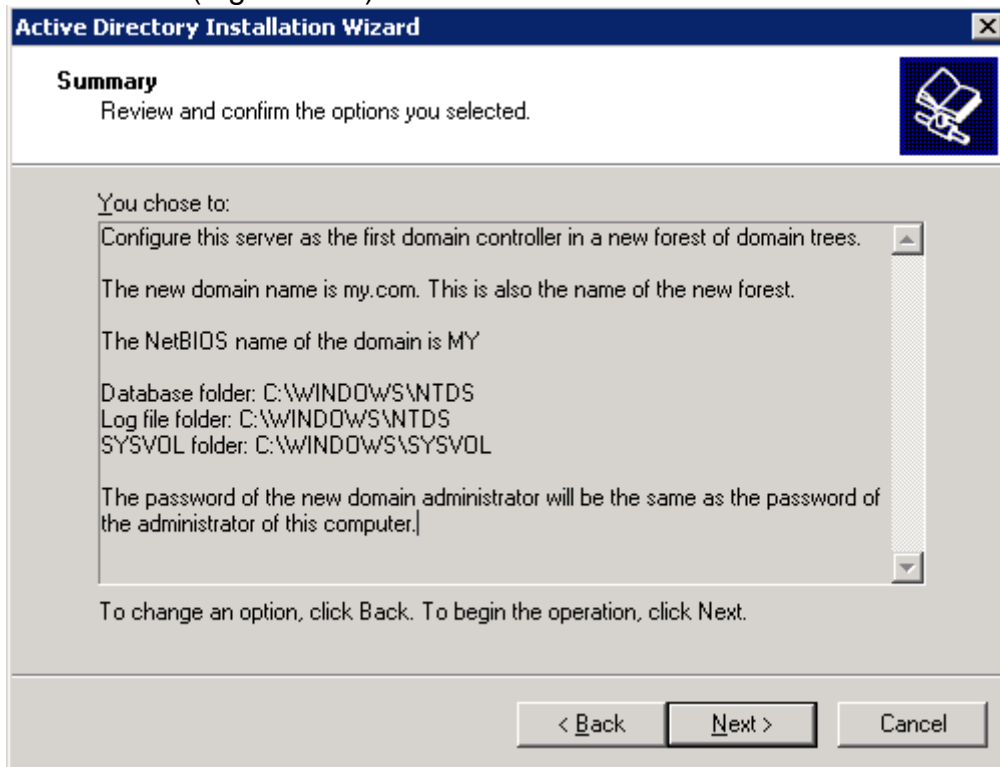


Figure 6-44 Summary

Step18. Settings complete (Figure 6-45).

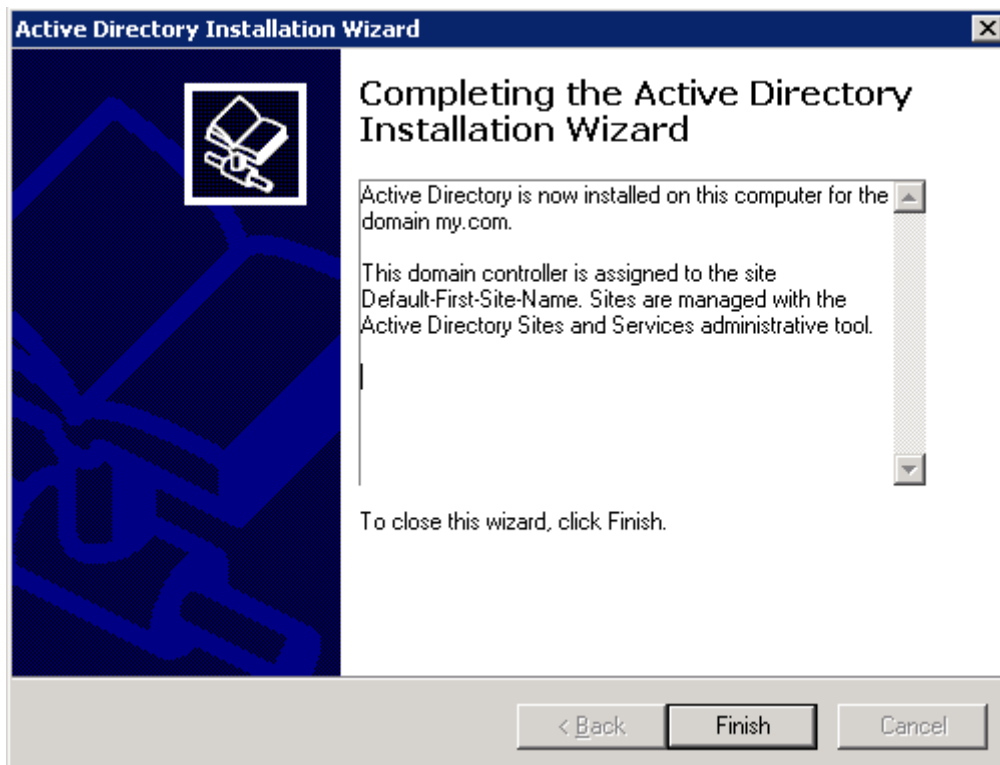


Figure 6-45 Active Directory Settings Complete

Step19. Go to **Start** → **Administrative Tools** → **Active Directory Users and Computers**. (Figure 6-46)

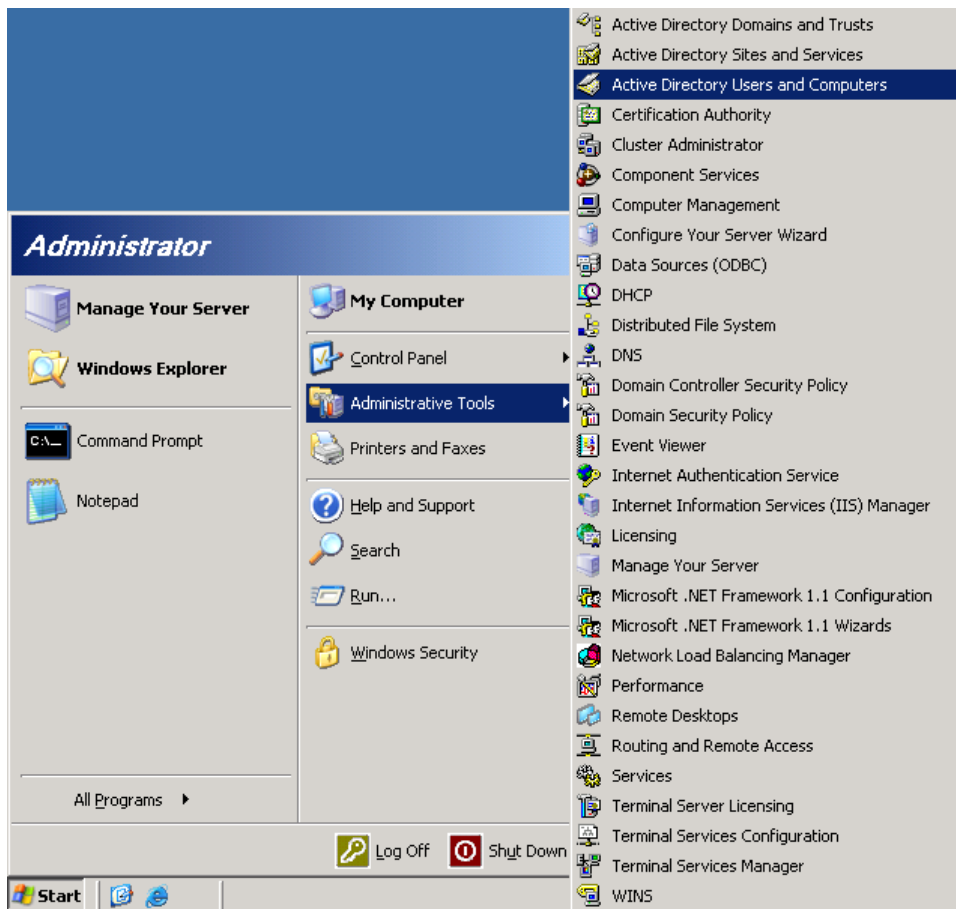


Figure 6-46 Active Directory Settings Complete

Step20. In the **Active Directory Users and Computers** window, right click on **Users** and create a new user. (Figure 6-47)

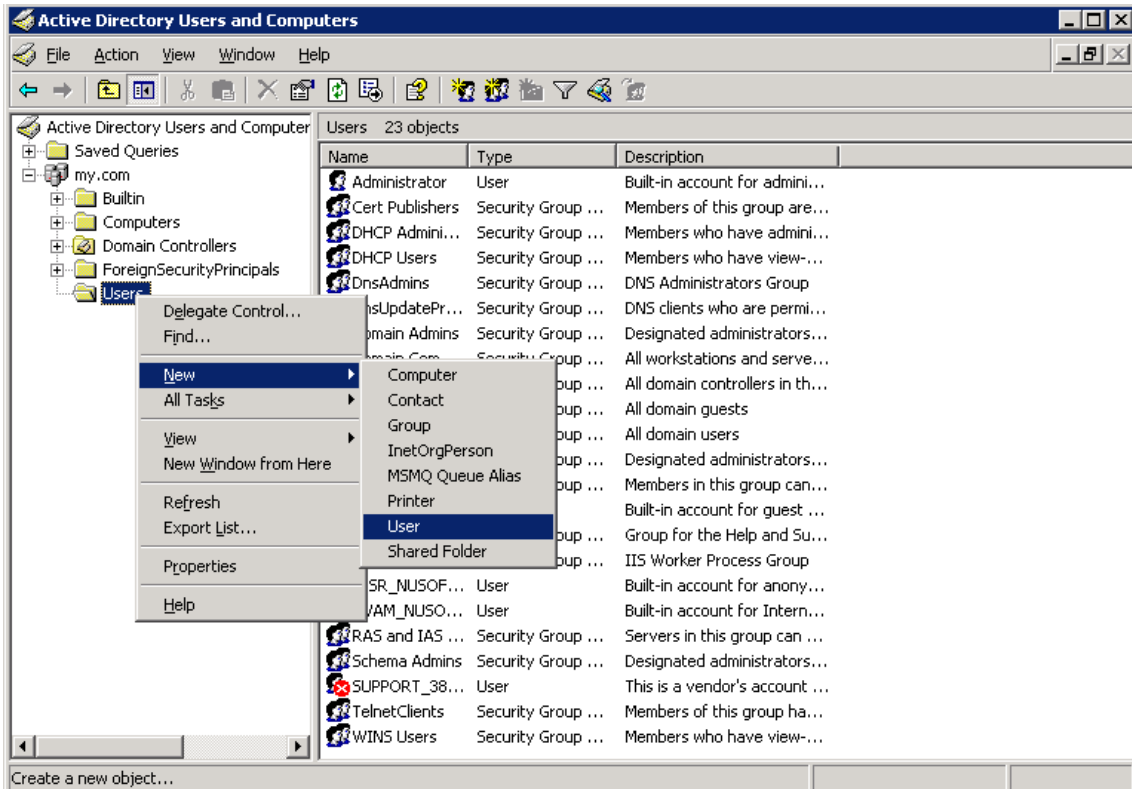


Figure 6-47 Creating a New User

Step21. Enter in the user's data, then click **Next**. (Figure 6-48)

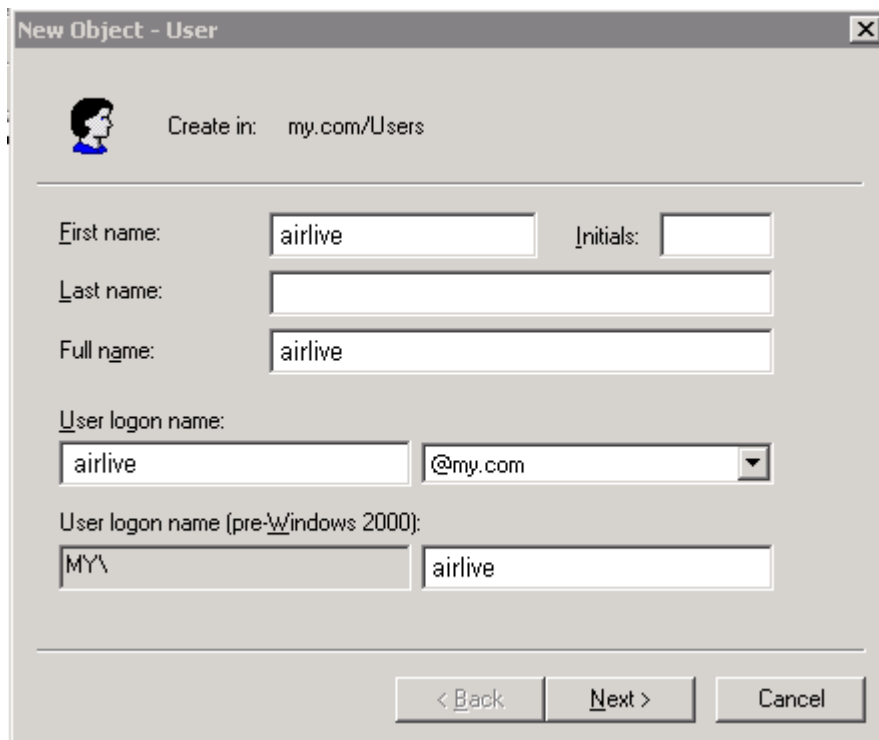


Figure 6-48 Creating a New User

Step22. Enter in a password and click **Next**. (Figure 6-49)

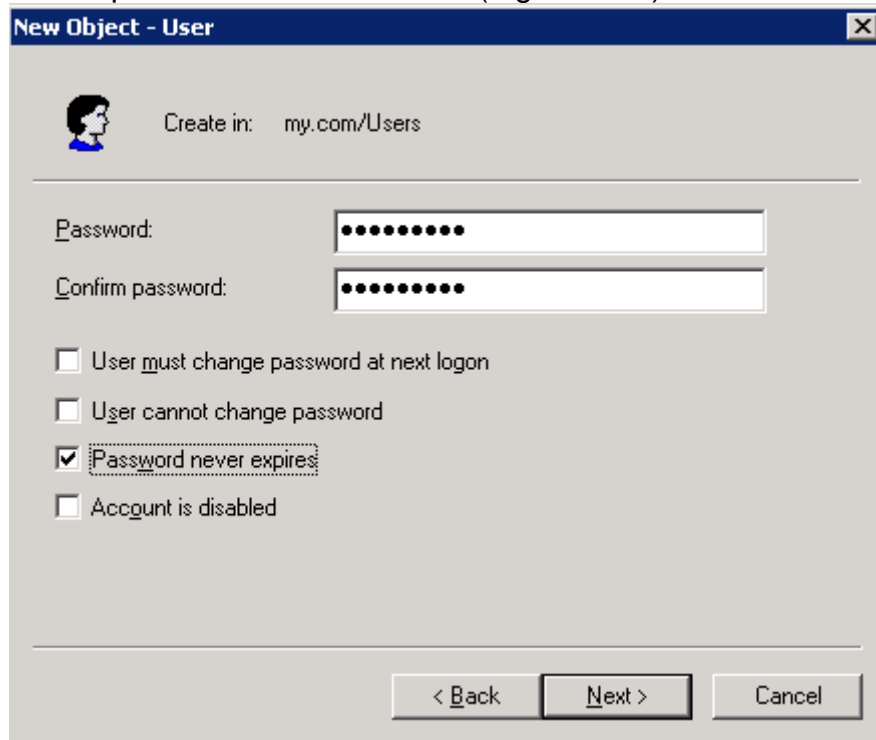


Figure 6-49 Creating a New User

Step23. Settings Complete. (Figure 6-50)

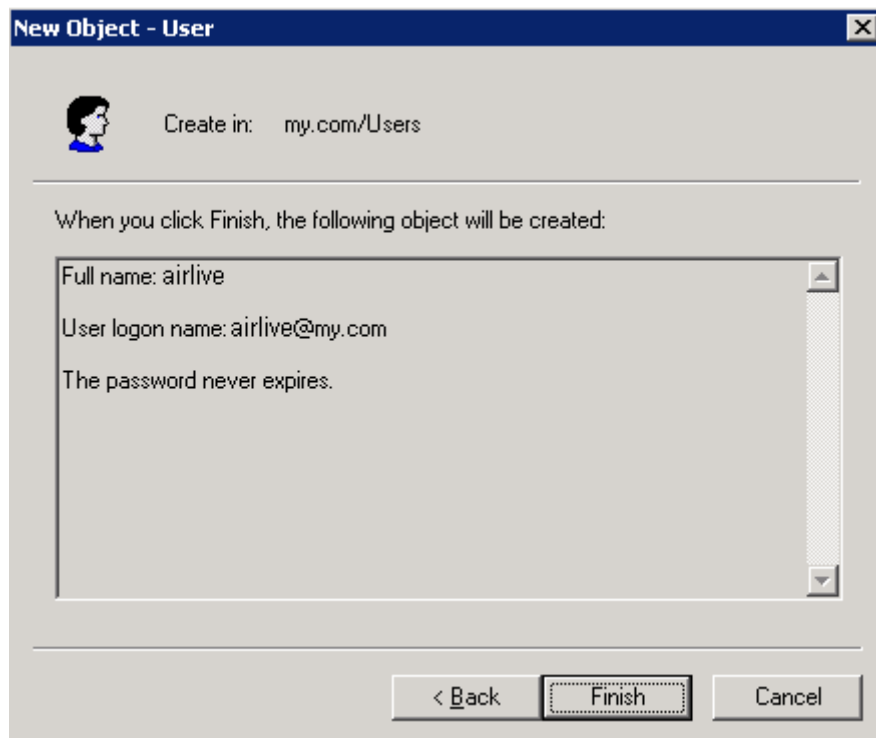


Figure 6-50 Settings Complete

Step24. Go to **Authentication → LDAP** and enter the settings. (Figure 6-51)

LDAP Server	
<input checked="" type="checkbox"/> Enable LDAP Server Authentication	Test connection
LDAP Server (IP or Domain Name) :	<input type="text" value="192.168.139.19"/> (Max. 80 characters)
LDAP Server Port :	<input type="text" value="389"/> (Max. 5 characters)
LDAP Search Distinguished Name :	<input type="text" value="dc=my,dc=com"/> (Max. 512 characters, ex: dc=mydomain,dc=com)
LDAP Filter :	<input type="text" value="(objectClass=*)"/> (Max. 256 characters, ex: (objectClass=*))
User's Distinguished Name :	<input type="text" value="cn=airlive,cn=Users,dc=m"/> (Max. 1,024 characters, ex: cn=users,dc=mydomain,dc=com)
Password :	<input type="password" value="*****"/> (Max. 128 characters)

Figure 6-51 LDAP Server Settings



Clicking on **Test connection** provides a connectivity test to the LDAP server.

Step25. When the user attempts to access the Internet though a browser, the following screen will appear requesting authentication via the IAR-5000. (Figure 6-52)

User Login

User Authentication	
User Name	<input type="text" value="peter"/>
Password	<input type="password" value="****"/>

You must pass the authentication before to access Internet.

Figure 6-52 The Login Screen for Authentication

7

IM Management

IM management provides system administrator with the flexibility and the facility to manage IM access. IAR-5000 can be configured to grant or deny IM access based on account or IM application.

IM Management comprises three major settings:

1. **Login Notice:** System administrator may compose a message to advise users not to abuse the IM access for private use or to announce company policy. The message is issued automatically to users who logs on to his / her IM account.
2. **Default Rule:** IM access can be regulated according to what specific IM application or Web-based messenger is used. For newly detected IM users, IAR-5000 will use the default rule on them.
3. **Account Rule:** Accounts are classified into four categories, namely default account, accept account, accept account (no file transfer) and drop account. System administrator may regulate the IM access by arranging users in different categories.



IM Management “**ONLY**” functions when IAR-5000 is deployed as **Bridge** mode.

7.1 Login Notice

When a user successfully logs on to his / her IM account, he /she shall receive the login notice via a NetBIOS broadcast, or receive the alert notification from IAR-5000 presented in a conversation window of the IM application.

Following are the configuration example:

- Step1.** Select **IM Management** → **Configure** → **Login Notice**
- Step2.** Tick **Enable NetBIOS Login Notice**
- Step3.** Tick **Enable MSN Login Notice (Bridge Mode Only)**
- Step4.** Tick **Enable ICQ / AIM Login Notice (Bridge Mode Only)**
- Step5.** Tick **Enable Yahoo Login Notice (Bridge Mode Only)**
- Step6.** Type a name as the **Notice Sender** name
- Step7.** Compose the content of the login notice
- Step8.** Click on **OK** (Figure 7-1)
- Step9.** Users receive alert notification right after login (Figure 7-2, 7-3, 7-4, 7-5)

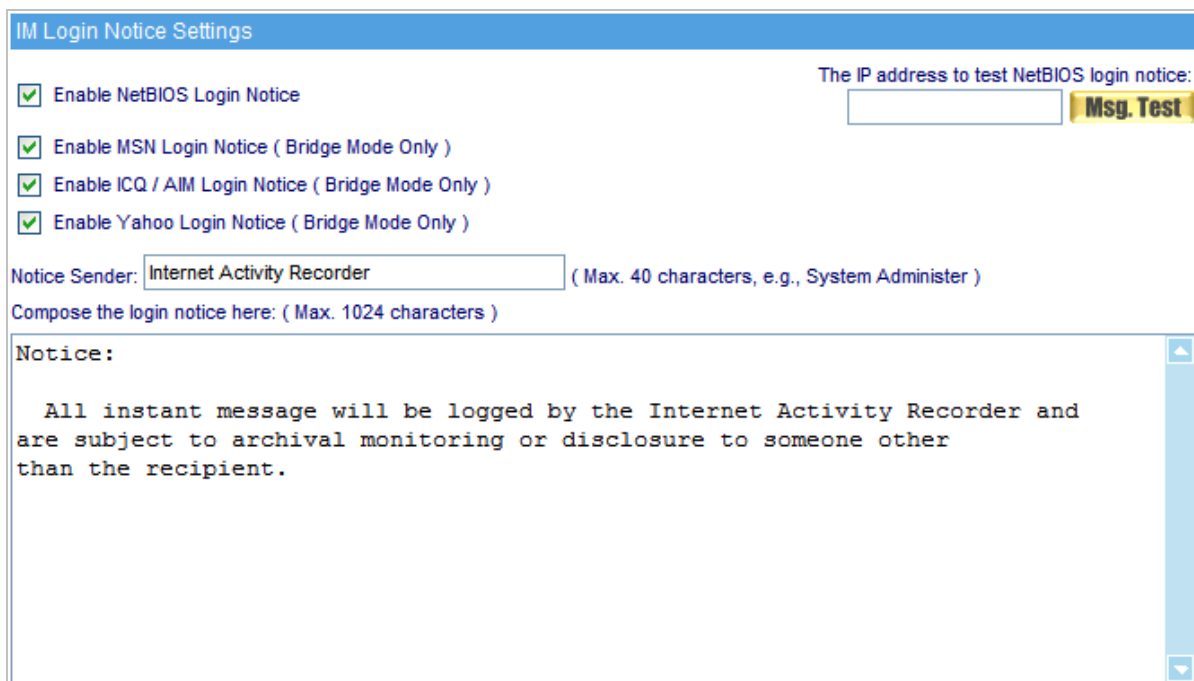


Figure 7-1 IM Login Notice Settings

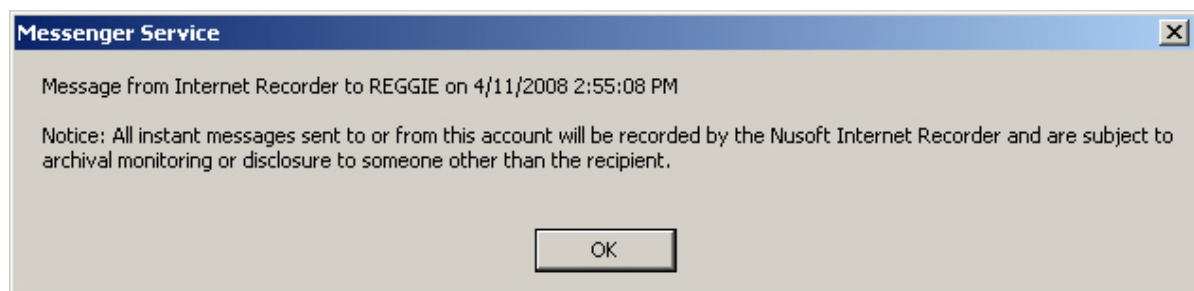


Figure 7-2 Login Notice Sent through a NetBIOS Broadcast

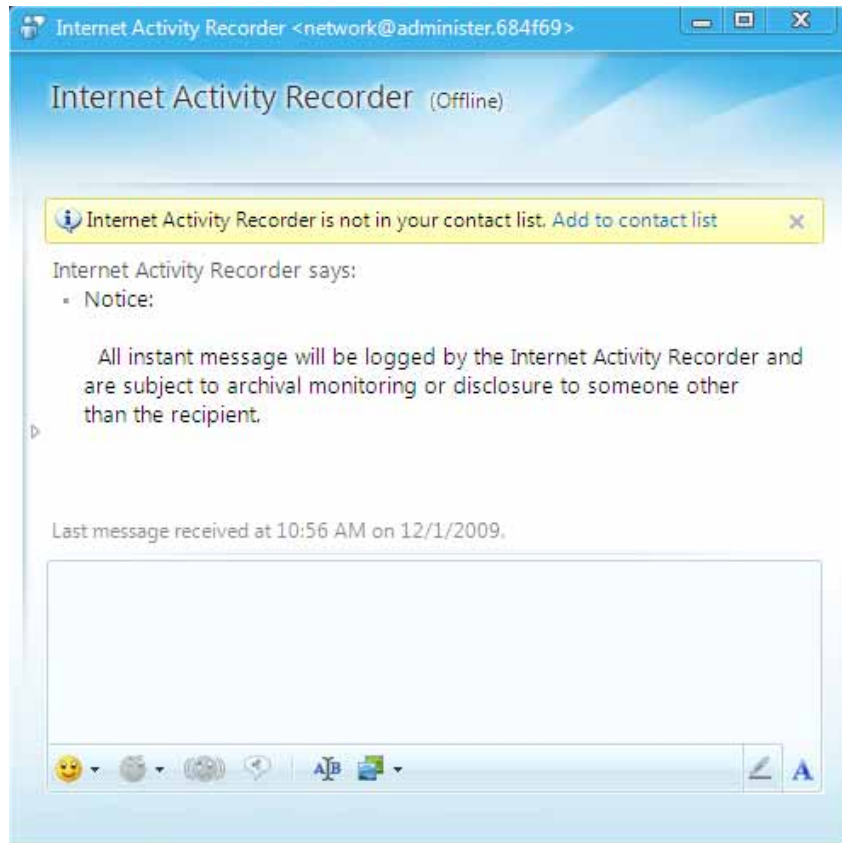


Figure 7-3 Login Notice Shown in a MSN Conversation Window

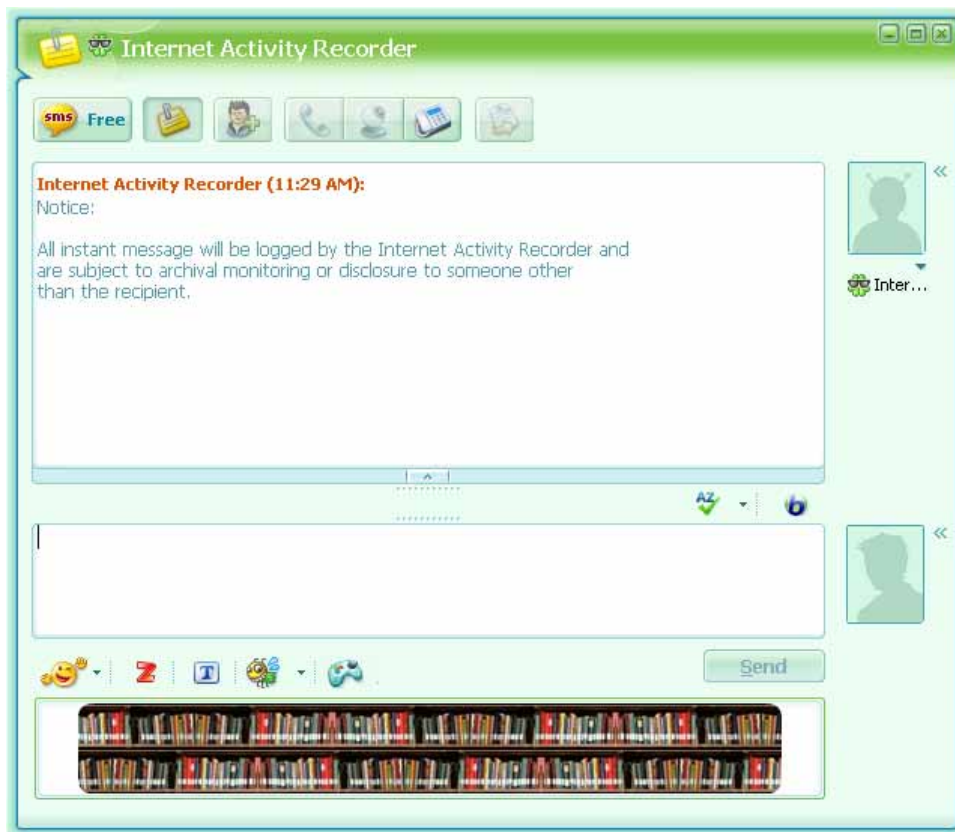


Figure 7-4 Login Notice Shown in an ICQ Conversation Window

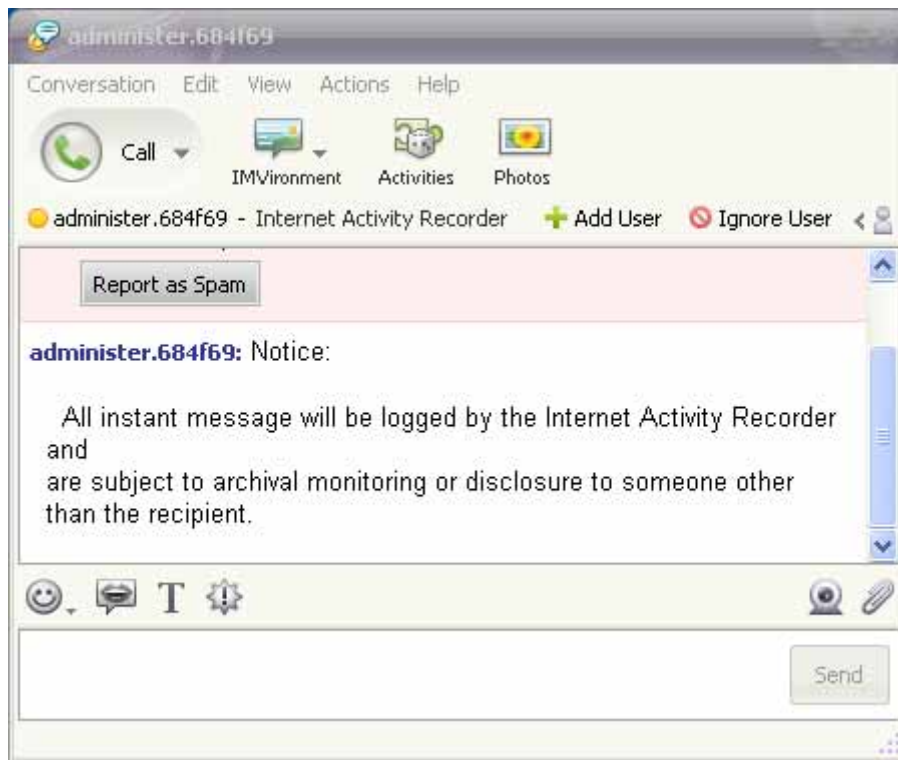


Figure 7-5 Login Notice Shown in a Yahoo Conversation Window

7.2 Default Rule

MIS engineer can make the default IM rule for MSN, Yahoo, ICQ, QQ and else IM software. IAR-5000 will follow the Default Rule setting to assign the access right for new account.

Import / Export Settings of IM Account Rule

- The account rule can be exported as a file for archive purposes and later imported onto IAR-5000 device to restore the settings.

Default Login Rule Settings (Bridge Mode Only)

- You may customize the default access rule for MSN, Yahoo, QQ, ICQ, AIM, Skype, Gadu-Gadu, Google Talk and other Web-based messengers.
- **[Accept: Everyone / Drop: None]:** Everyone is granted with IM access.
- **[Accept: None / Drop: Everyone]:** IM access is denied to everyone.
- **[Accept: Unencrypted message / Drop: Encrypted message]:** Only users sending unencrypted messages are granted with IM access.
- **[Accept: Valid password / Drop: Invalid password]:** To have QQ messenger access, users must verify their account by logging on to the management address appended with “/qq” (use lower case only), such as <http://192.168.1.1/qq>.
- **[Accept: User running IR_Plugin.exe / Drop: Others]:** To have Skype messenger access, users must have the “IR_Plugin.exe” running in the background.
- **[Accept: Official MSN Web Messenger / Drop: Others]:** Only Web-based MSN messenger users are granted with IM access.



QQ uses encryption to transmit its messages, therefore the IAR-5000 must obtain the associated account name and password to decrypt and record the messages. If the **Default Rule** for QQ is set to **Accept: Everyone; Drop: None** or **Accept: Authenticated User; Drop: Unauthenticated User**, the IAR-5000 will not only be able to record messages.



The encrypted messages over MSN or Gadu-Gadu messenger are not recordable.



So far, MSN Web Messenger is the only recordable Web-based messenger.

Default File Transfer Settings (Bridge Mode Only)

- Decides whether to permit or block file transfer over MSN, Yahoo, QQ, ICQ, AIM, Gadu-Gadu, and Google Talk.

7.3 Account Rule

Default ... Accounts (Rule Status)

- Accounts resided in this category are subject to default rule.

Accepted ... Accounts

- Accounts resided in this category are granted with IM access.




Accepted ... Accounts (No File Transfer)

- Accounts resided in this category are granted with IM access, yet without the support of file transfer.

Dropped ... Accounts

- Accounts resided in this category are denied with IM access.

The symbols used in **Account Rule**:

Symbol	Meaning	Description
	Password Valid	The tick mark signifies the input QQ account and password are valid. This means the device can decrypt the encrypted messages over QQ messenger.
	Unauthenticated	The exclamation mark indicates QQ account and password have not been given to IAR-5000, or the authentication has failed. This means the encrypted messages over QQ messenger will not be recordable.
	Password Invalid	The cross mark denotes the input QQ account and password are invalid. This means the encrypted messages over QQ messenger will not be recordable.



IAR-5000 can verify the correctness of QQ login information once a QQ user has logged in.

7.4 Configuration Example

Configuring the Default Rule for IM Access

Navigate to **IM Management** → **Rule** → **Default Rule**, and then set as below: (Figure 7-6)

- Select **Accept: Everyone** for MSN, Yahoo, ICQ / AIM, Skype, Gadu-Gadu and Google Talk as the default rule.
- Select **Accept: Authenticated user with valid password Drop / Unauthenticated user or invalid password** for QQ as the default rule.
- Select **Accept: User running IR_Plugin.exe / Drop: Others** for Skype as the default rule.
- Select **Accept: Official MSN Web Messenger** for Web IM as the default rule.
- Select **Accept** to permit file transfer over MSN, Yahoo, ICQ / AIM, Gadu-Gadu and Google Talk.

Import / Export Settings of IM Account Rule

Export IM Account Rule Settings **Export**

Import IM Account Rule Settings

(ex: M_Rule_List.csv)

Default Login Rule Settings (Bridge Mode Only)

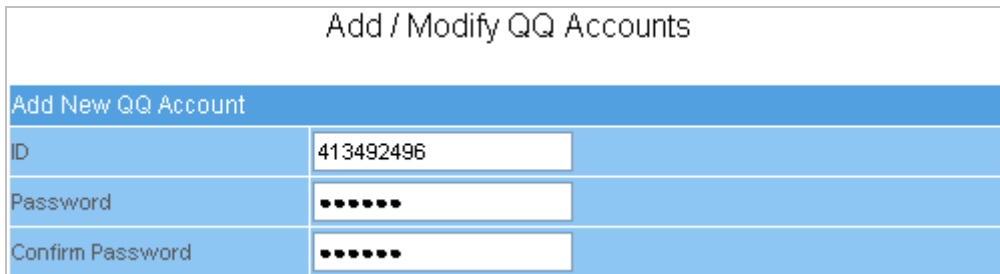
<p>MSN</p> <p><input type="radio"/> Accept: Unencrypted message Drop: Encrypted message</p> <p><input checked="" type="radio"/> Accept: Authenticated user sending unencrypted message Drop: Unauthenticated user or encrypted message</p> <p><input type="radio"/> Accept: Authenticated user Drop: Unauthenticated user</p> <p><input type="radio"/> Accept: Everyone Drop: None</p> <p><input type="radio"/> Accept: None Drop: Everyone</p> <p>Yahoo</p> <p><input checked="" type="radio"/> Accept: Everyone Drop: None</p> <p><input type="radio"/> Accept: Authenticated user Drop: Unauthenticated user</p> <p><input type="radio"/> Accept: None Drop: Everyone</p> <p>QQ</p> <p><input type="radio"/> Accept: Valid password Drop: Invalid password</p> <p><input checked="" type="radio"/> Accept: Authenticated user with valid password Drop: Unauthenticated user or invalid password</p> <p><input type="radio"/> Accept: Authenticated user Drop: Unauthenticated user</p> <p><input type="radio"/> Accept: Everyone Drop: None</p> <p><input type="radio"/> Accept: None Drop: Everyone</p> <p>Gadu-Gadu</p> <p><input checked="" type="radio"/> Accept: Unencrypted message Drop: Encrypted message</p> <p><input type="radio"/> Accept: Authenticated user sending unencrypted message Drop: Unauthenticated user or encrypted message</p> <p><input type="radio"/> Accept: Authenticated user Drop: Unauthenticated user</p> <p><input type="radio"/> Accept: Everyone Drop: None</p> <p><input type="radio"/> Accept: None Drop: Everyone</p>	<p>Skype</p> <p><input checked="" type="radio"/> Accept: Everyone Drop: None</p> <p><input type="radio"/> Accept: User running IR_Plugin.exe Drop: Others</p> <p><input type="radio"/> Accept: None Drop: Everyone</p> <p>ICQ / AIM</p> <p><input checked="" type="radio"/> Accept: Everyone Drop: None</p> <p><input type="radio"/> Accept: Authenticated user Drop: Unauthenticated user</p> <p><input type="radio"/> Accept: None Drop: Everyone</p> <p>Google Talk</p> <p><input checked="" type="radio"/> Accept: Everyone Drop: None</p> <p><input type="radio"/> Accept: None Drop: Everyone</p> <p>Web IM</p> <p><input type="radio"/> Accept: Everyone Drop: None</p> <p><input checked="" type="radio"/> Accept: Official MSN Web Messenger Drop: Others</p> <p><input type="radio"/> Accept: None Drop: Everyone</p>
--	---

Default File Transfer Settings (Bridge Mode Only)

<p>MSN</p> <p><input checked="" type="radio"/> Accept</p> <p><input type="radio"/> Drop</p> <p>ICQ / AIM</p> <p><input checked="" type="radio"/> Accept</p> <p><input type="radio"/> Drop</p> <p>Google Talk</p> <p><input checked="" type="radio"/> Accept</p> <p><input type="radio"/> Drop</p>	<p>Yahoo</p> <p><input checked="" type="radio"/> Accept</p> <p><input type="radio"/> Drop</p> <p>QQ</p> <p><input checked="" type="radio"/> Accept</p> <p><input type="radio"/> Drop</p> <p>Gadu-Gadu</p> <p><input checked="" type="radio"/> Accept</p> <p><input type="radio"/> Drop</p>
--	---

Figure 7-6 Configuring the Default Rule for IM Access

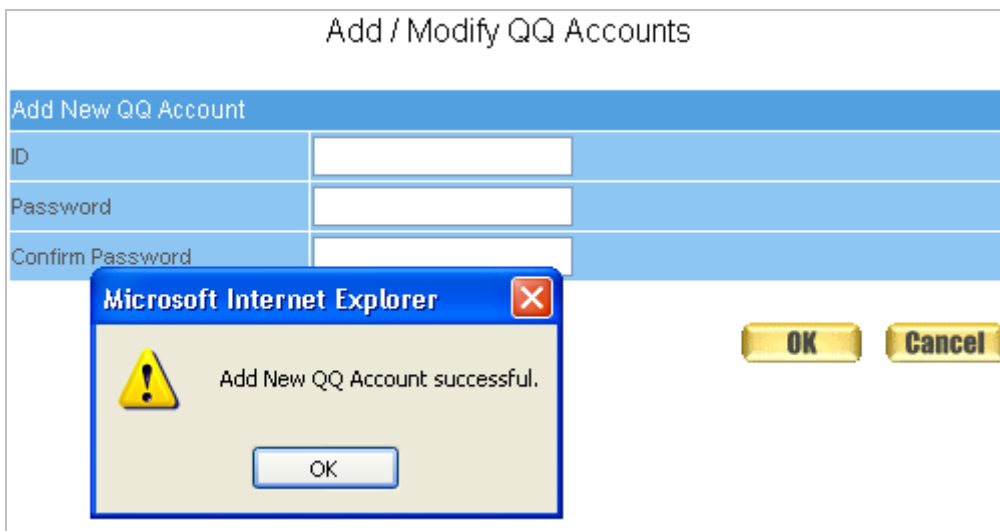
- Step1.** To record Skype conversations, it requires installing the plug-in (IR_Plugin.exe) onto clients' PCs. (Please refer to chapter 9 for advanced configuration)
- Step2.** To access QQ messenger, users must verify their account by logging on to the management address appended with "/qq", such as <http://192.168.1.1/qq>. (Figure 7-7, 7-8)



Add / Modify QQ Accounts

Add New QQ Account	
ID	413492496
Password	*****
Confirm Password	*****

Figure 7-7 Creating an Account on the Device for Account Verification



Add / Modify QQ Accounts

Add New QQ Account	
ID	
Password	
Confirm Password	

Microsoft Internet Explorer


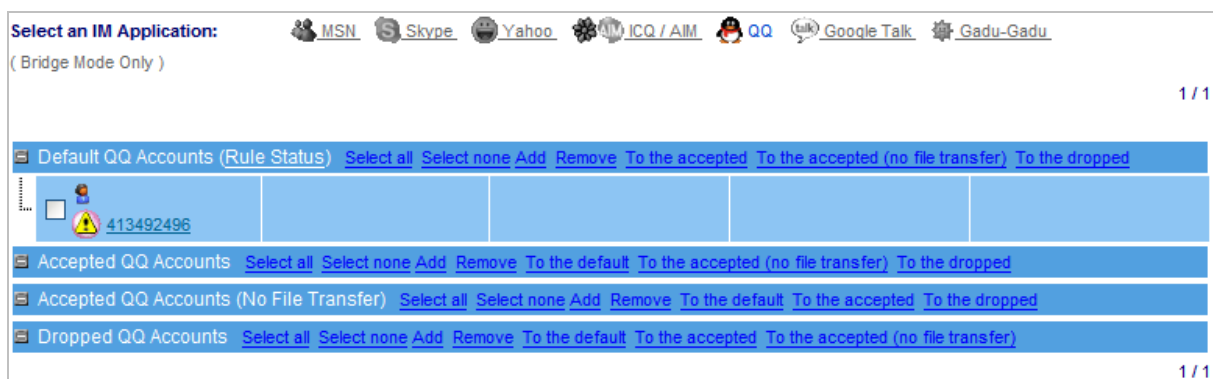







 Add New QQ Account successful.


Figure 7-8 New QQ Account Added

- Step3.** Under **IM Management** → **Rule** → **Account Rule**, there it shows:
- The newly added QQ account without being authenticated. (Figure 7-9)
 - The new QQ account user will be authenticated once he / she logs on to QQ messenger.



Select an IM Application:       

(Bridge Mode Only) 1 / 1

Default QQ Accounts (Rule Status) Select all Select none Add Remove To the accepted To the accepted (no file transfer) To the dropped				
	413492496			
Accepted QQ Accounts Select all Select none Add Remove To the default To the accepted (no file transfer) To the dropped				
Accepted QQ Accounts (No File Transfer) Select all Select none Add Remove To the default To the accepted To the dropped				
Dropped QQ Accounts Select all Select none Add Remove To the default To the accepted To the accepted (no file transfer)				

1 / 1

Figure 7-9 Unauthenticated QQ Account



When the QQ password has been changed, please go to the management address appended with “/qq”, such as <http://192.168.1.1/qq>, to modify the original password.

Step4. Users merely have the access to MSN Web Messenger. Access to other Web-based messengers will be denied.



The IAR-5000 is capable of denying access to Web-based messengers. The system will automatically update itself with new Web-based messenger signatures when they become available.

Step5. To export the account rule for archive and editing, navigate to **IM Management** → **Rule** → **Default Rule** and then follow the steps below:

- Click on **Export** button on the right of **Export IM Account Rule Settings**.
- In the **File Download** conversation box, select **Save this file to disk** and then click on **OK**. Next, specify the storage location and then click on **Save**. (Figure 7-10)

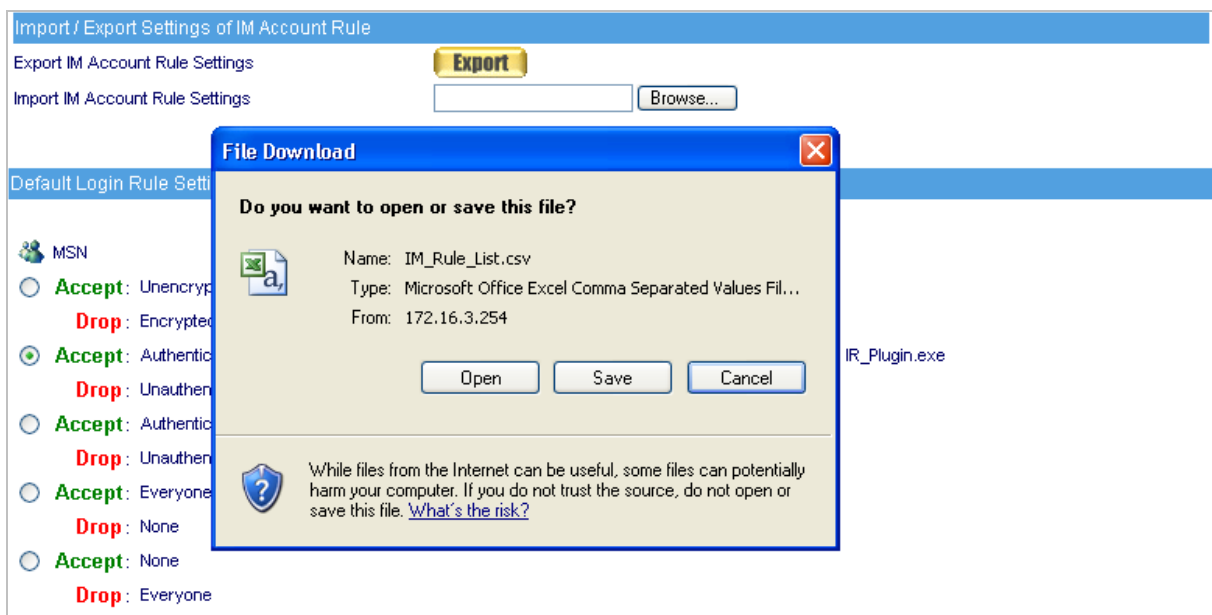


Figure 7-10 Export the Account Rule as a “.csv” File onto Your Local PC

Step6. To import the edited account rule onto the IAR-5000 device, navigate to **IM Management** → **Rule** → **Default Rule** and then follow the steps below:

- Run Excel to edit the previously downloaded account rule. (default file name: IM_Rule_List.csv) (Figure 7-11)
- Modify specific MSN account information. (customize accordingly)
 - ◆ Change the rule from **Default** into **Accept**. (Figure 7-12)

- ◆ Modify the IP and MAC addresses. (Figure 7-13)
- Create a new Yahoo account: Insert a blank row right beneath the last row of MSN accounts and type all necessary information. (Figure 7-14)
- After edited, click on **File** → **Save** on the menu bar and save the file as “IM_Rule_List.csv”.
- Click on **Browse** button on the right of **Import IM Account Rule Settings** to locate the edited account rule and then click on **OK**. (Figure 7-15)
- In the confirmation conversation box, click on **OK** to confirm the import process. (Figure 7-16)

#####						
#Format 1:						
# IM_Type	Account	Rule	AuthName	IP	MAC	AuthType
#						
#						
#####						
MSN	airlive_test01@hotmail.com	Default	sales	172.19.50.24	00:0C:29:8A:BB:46	USER
MSN	airlive_test02@hotmail.com	Default	account	172.19.70.201	00:0A:48:0C:A6:20	-
MSN	airlive_test03@hotmail.com	Accept	account	172.19.50.26	00:0A:48:0C:A6:20	-
MSN	airlive_test04@hotmail.com	Drop	support	172.19.70.204	00:05:5D:95:5B:C6	-
Yahoo	airlive_test01	Default	support	172.19.70.202	00:0A:48:0C:A6:20	USER
Yahoo	airlive_test04	Default	support	172.19.70.204	00:05:5D:95:5B:C6	POP3
QQ	539236964	Default	-	172.19.70.203	00:05:5D:95:5B:C6	-
QQ	539330473	Default	sales	172.19.50.25	00:0B:DC:29:8A:CC	-
QQ	539337471	Default	sales	172.19.70.203	00:05:5D:95:5B:C6	-
ICQ	292420150	Default	-	172.19.50.26	00:0A:48:0C:A6:20	-

Figure 7-11 Rules Shown on the Account List

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


Figure 7-12 Rule Changed


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

Figure 7-13 IP and MAC Addresses Changed

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

Figure 7-14 New Yahoo Account

 Whether an account is purposely or accidentally deleted during editing, it does not affect the existing account rule on IAR-5000 after imported the edited file. Only newly added account(s) or account(s) had been modified makes changes in the account rule.

 The authentication method should not be modified. When authentication is used, the user must set the appropriate authentication data in the authentication interface.

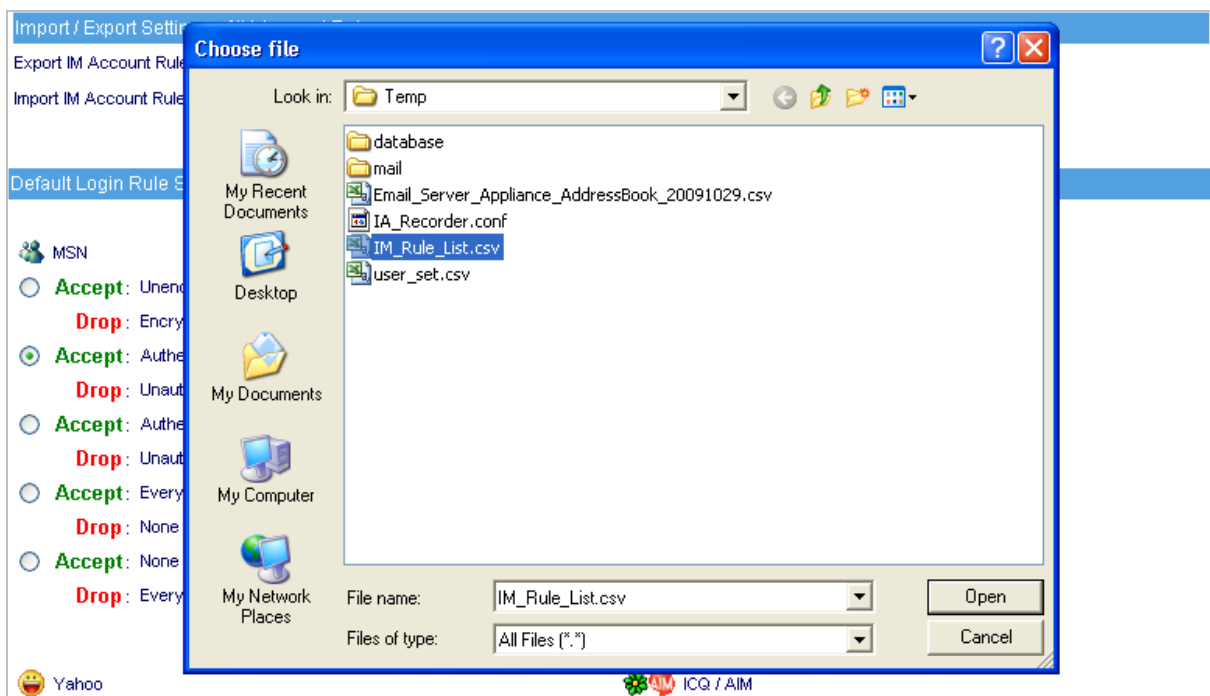


Figure 7-15 Choosing the Edited Account Rule

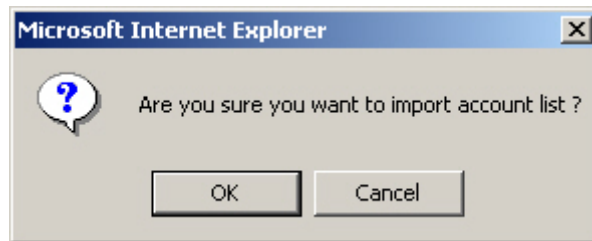


Figure 7-16 Confirming to Import the Account Rule

- Step7.** Navigate to **IM Management** → **Rule** → **Account Rule**, and then follow the steps below:
- On the **Default ... Accounts (Rule Status)** list, grant IM access to the specific accounts by ticking them.
 - Click on **To the accepted** and then click on **OK** on the confirmation conversation. (Figure 7-17)
 - On the **Default ... Accounts (Rule Status)** list, block file transfer of specific accounts by ticking them.
 - Click on **To the accepted (no file transfer)** and then click on **OK** on the confirmation conversation. (Figure 7-18)
 - On the **Default ... Accounts (Rule Status)** list, deny IM access to the specific accounts by ticking them.
 - Click on **To the dropped** and then click on **OK** on the confirmation conversation. (Figure 7-19)
 - On the **Default ... Accounts (Rule Status)** list, click on **Add** to add a new account.
 - In the **Add Account Policy** screen, type the new account to be added and then tick the desirable rule for it. (Figure 7-20, 21)
 - Click on **OK** to complete adding a new account.
 - To delete unwanted accounts, tick the specific accounts and then click on **Remove**. (Figure 7-22)
 - Modification is completed. (Figure 7-23)

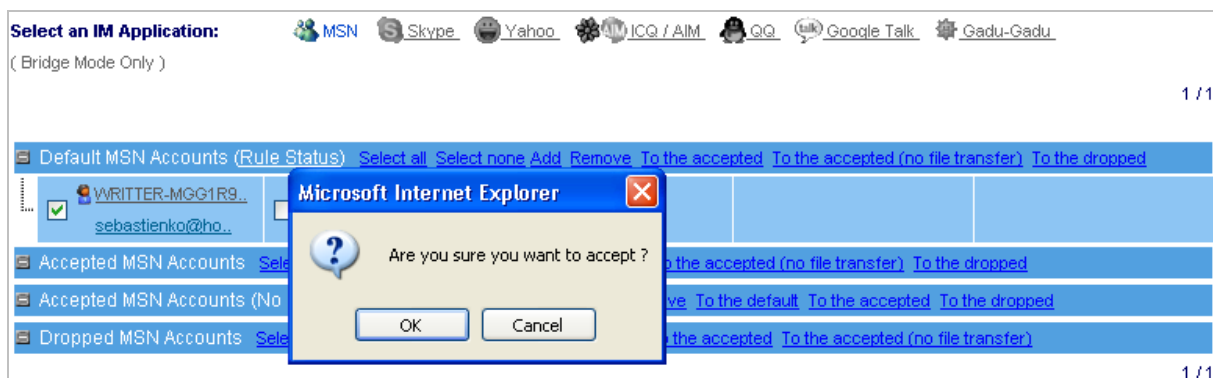


Figure 7-17 Granting IM Access to Specific Accounts

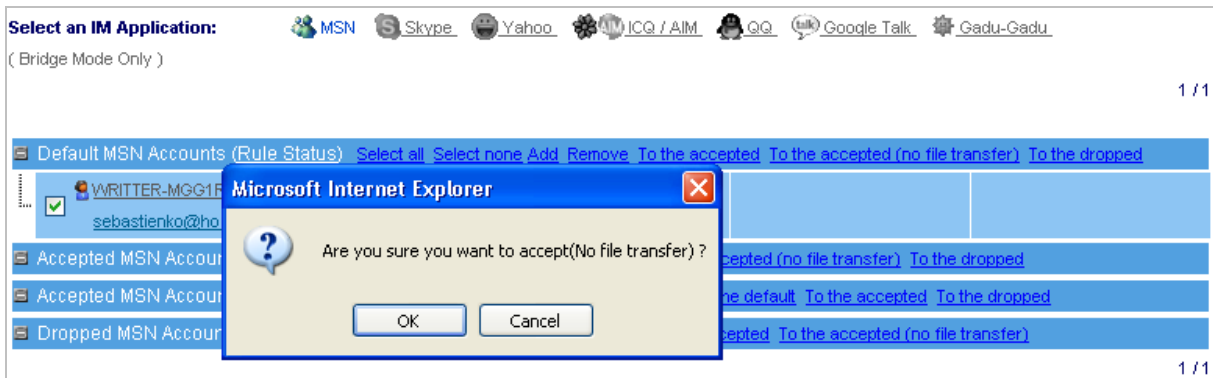


Figure 7-18 Blocking File Transfer of Specific Accounts

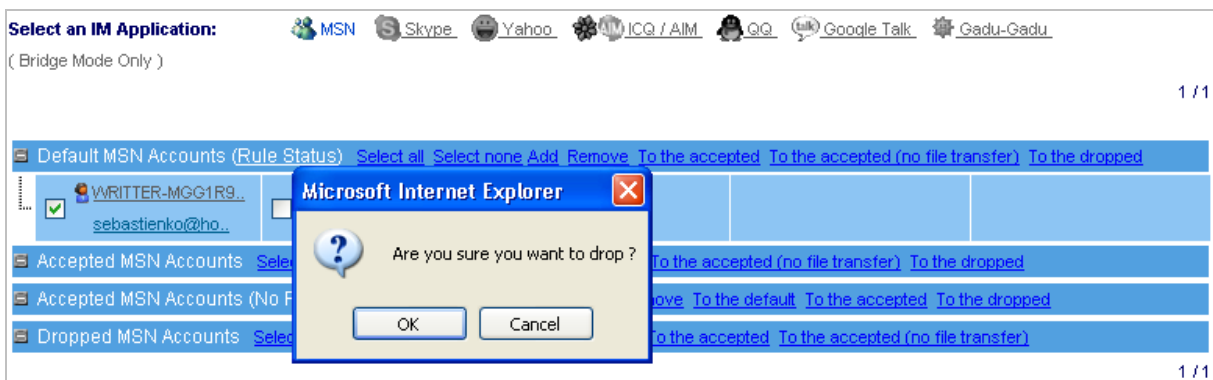


Figure 7-19 Denying IM Access to Specific Accounts

Add Account Policy	
IM Protocol	MSN
Account	airlive@hotmail.com (Max. 128 characters)
Policy	<input checked="" type="checkbox"/> Default <input type="checkbox"/> Accept <input type="checkbox"/> Accept (No file transfer) <input type="checkbox"/> Drop

Figure 7-20 Denying IM Access to Specific Accounts

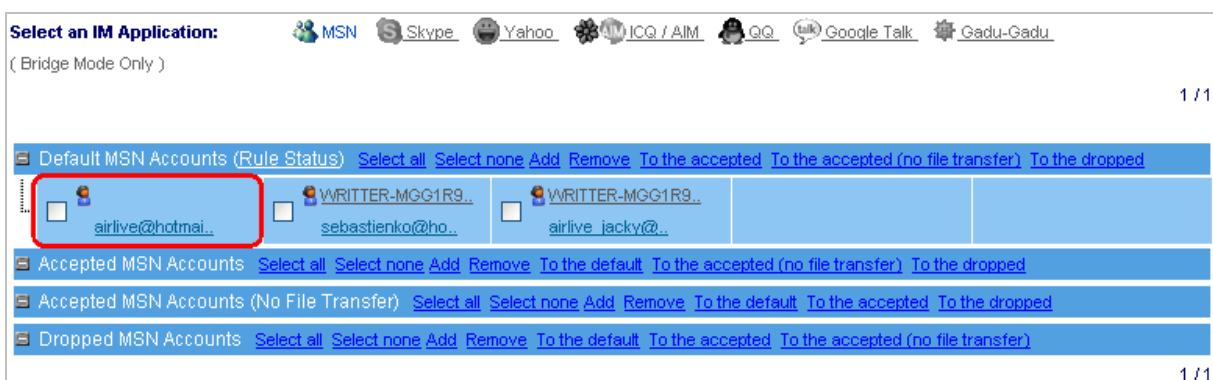


Figure 7-21 Denying IM Access to Specific Accounts

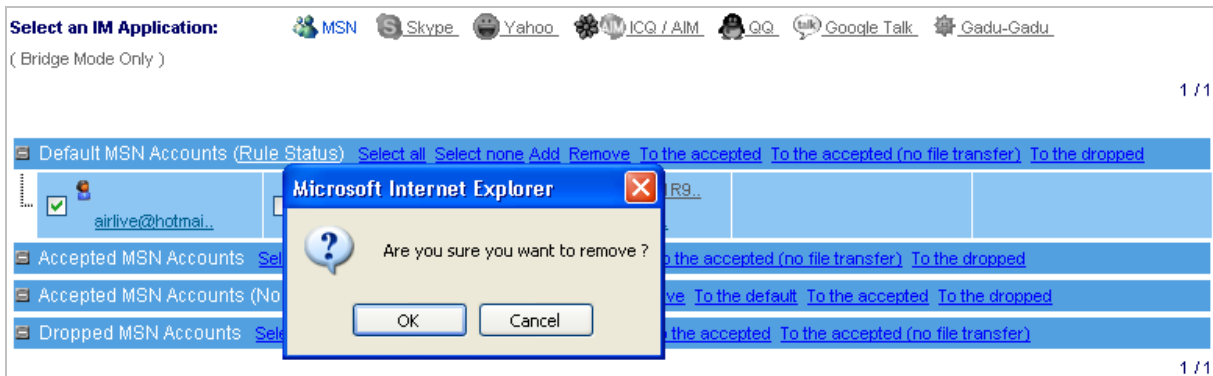



Figure 7-22 Confirming to Remove an Account



Figure 7-23 Modification Completed



IAR-5000 will use default rule (see Rule Status) on newly added IM accounts.

8

Application Management

Application Management determines the users' right to access applications (peer-to-peer sharing, multimedia streaming, online gaming, VPN tunneling and remote controlling). System administrator may grant or deny access to applications based on which application is used or who the user is.

Application Management comprises two major settings:

1. **Default Rule:** IAR-5000 is now capable of controlling the access to five kinds of applications, namely peer-to-peer sharing, multimedia streaming, online gaming, VPN tunneling and remote controlling. Newly detected application users will be subject to default rule.
2. **Custom Rule:** Accounts are classified into three categories, namely default account, accept account and drop account. System administrator may regulate application access by arranging users into different accounts.



1. Application Management **"ONLY"** functions when IAR-5000 is deployed as Bridge mode.
2. **Peer-to-Peer Sharing:** eMule/eDonkey, BitTorrent, WinMX, Foxy, KuGoo, AppleJuice, AudioGalaxy, DirectConnect, iMesh, MUTE, Thunder 5, GoGoBox, QQDownload, Ares, Shareaza, BearShare, Morpheus, LimeWire, KaZaa.
3. **Multimedia Streaming:** PPLive, PPStream, UUSee, QQLive, ezPeer, QvodPlayer.
4. **Online Gaming:** GL World, QQGame.
5. **VPN Tunneling:** VNN Client, Ultra-Surf, Tor, Hamachi.
6. **Remote Controlling:** TeamViewer, VNC, Remote Desktop.

8.1 Default Rule

Default Rule for Applications (Bridge Mode Only)

- Permits or blocks the access to peer-to-peer sharing, multimedia streaming, online gaming, VPN tunneling and remote controlling.

Configuring the Default Rule for Application Access

Step1. Navigate to **Application Management** → **Default Rule**, and then set as below: (Figure 8-1)

- Select **Drop** for all Peer-to-Peer sharing applications.

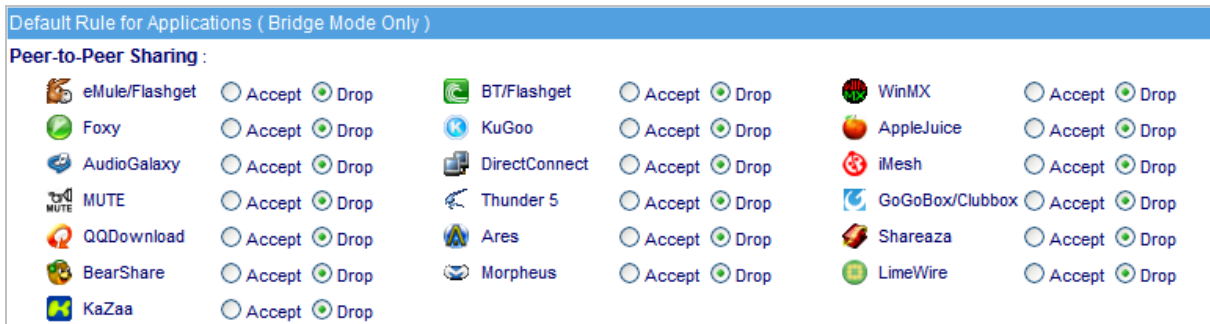


Figure 8-1 Configuring the Default Rule for Application Access

Step2. After configured the default rule, eMule will not be accessible. (Figure 8-2)

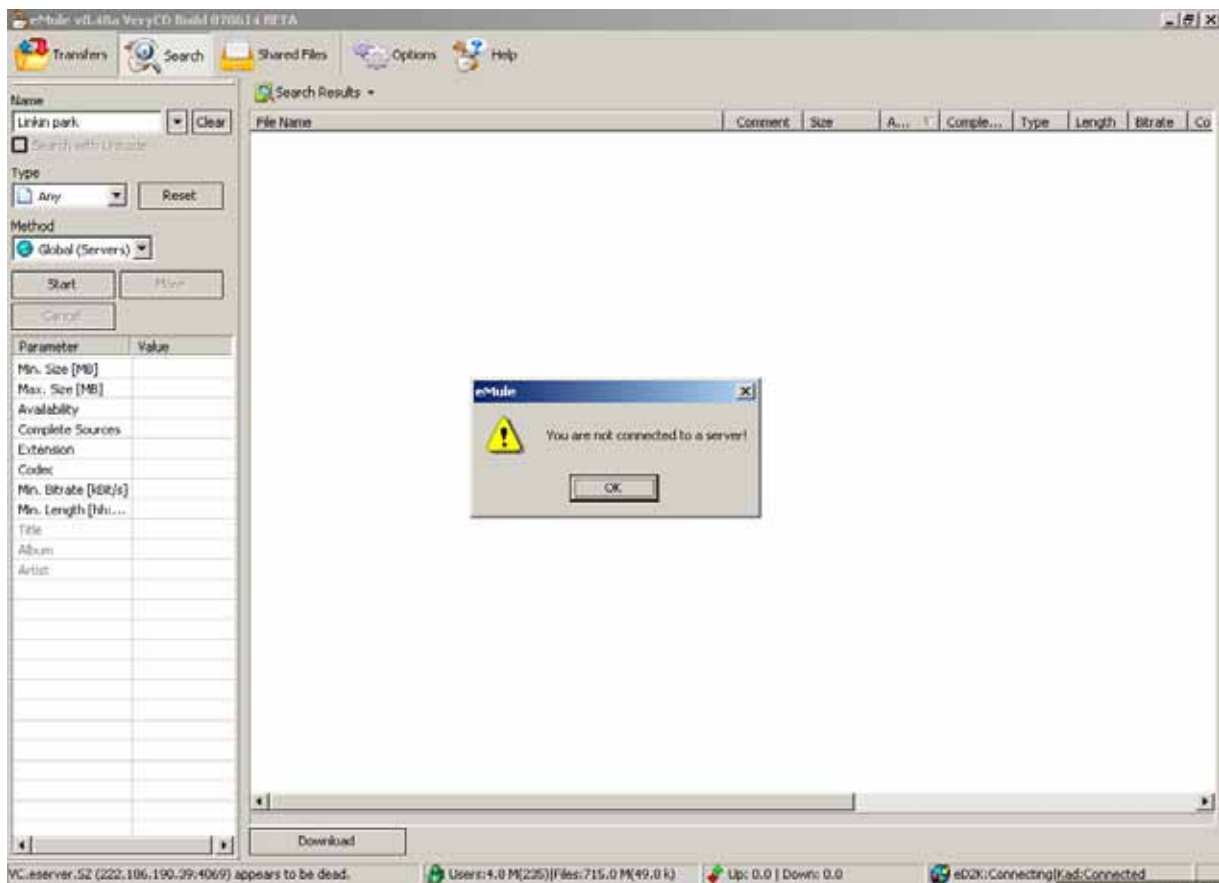


Figure 8-2 eMule Failed in Connecting to the Server



IAR-5000 cannot block Thunder 5 from downloading if it is just simply using HTTP or FTP protocols.

8.2 Custom Rule

... Users under Default Rule (Rule Status)

- Users resided in this category are subject to default rule.

Accepted ... Account

- Accounts resided in this category are granted with application access.

Dropped ... Account

- Accounts resided in this category are denied with application access.

Configuring the Custom Rule for Application Access

Step1. Navigate to **Application Management** → **Custom Rule**, and then set as below:

- From the **Select an Application** drop-down list, select **Peer-to-Peer Sharing**.
- In the **Default eMule/eDonkey Accounts** list, grant P2P access to the specific accounts by ticking them.
- Click on **To the accepted** and then click on **OK** on the confirmation conversation. (Figure 8-3)
- On the **... Users under Default Rule (Rule Status)** list, deny P2P access to the specific accounts by ticking them.
- Click on **To the dropped** and then click on **OK** on the confirmation conversation. (Figure 8-4)
- Modification is completed. (Figure 8-5)

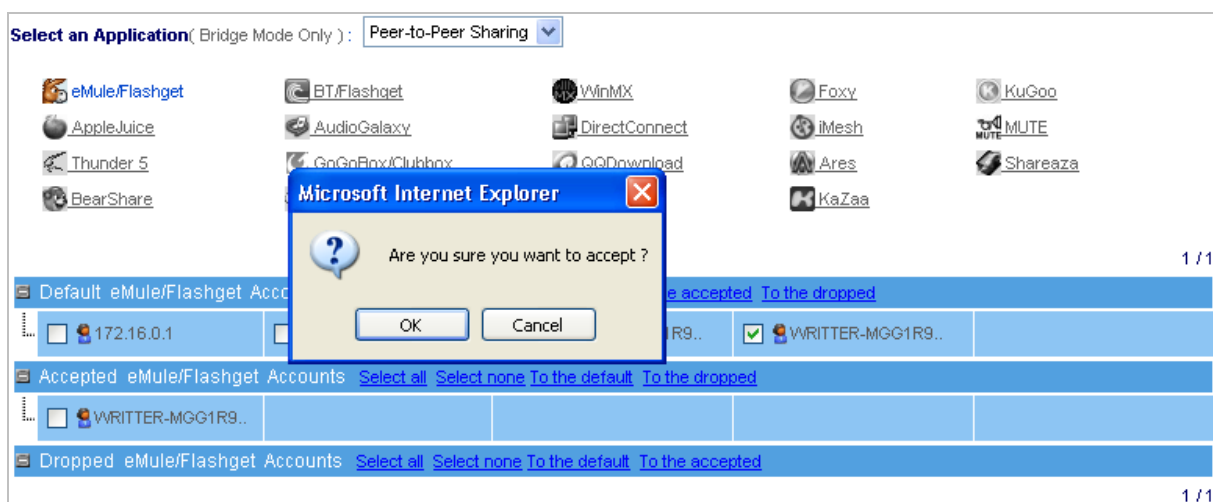


Figure 8-3 Granting P2P Access to Specific Accounts

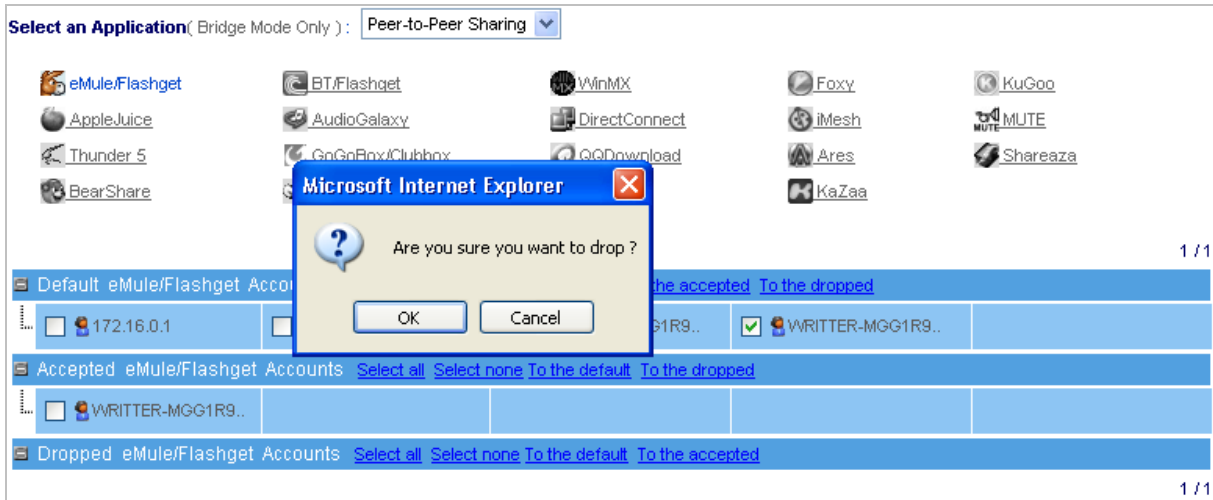


Figure 8-4 Denying P2P Access to Specific Accounts

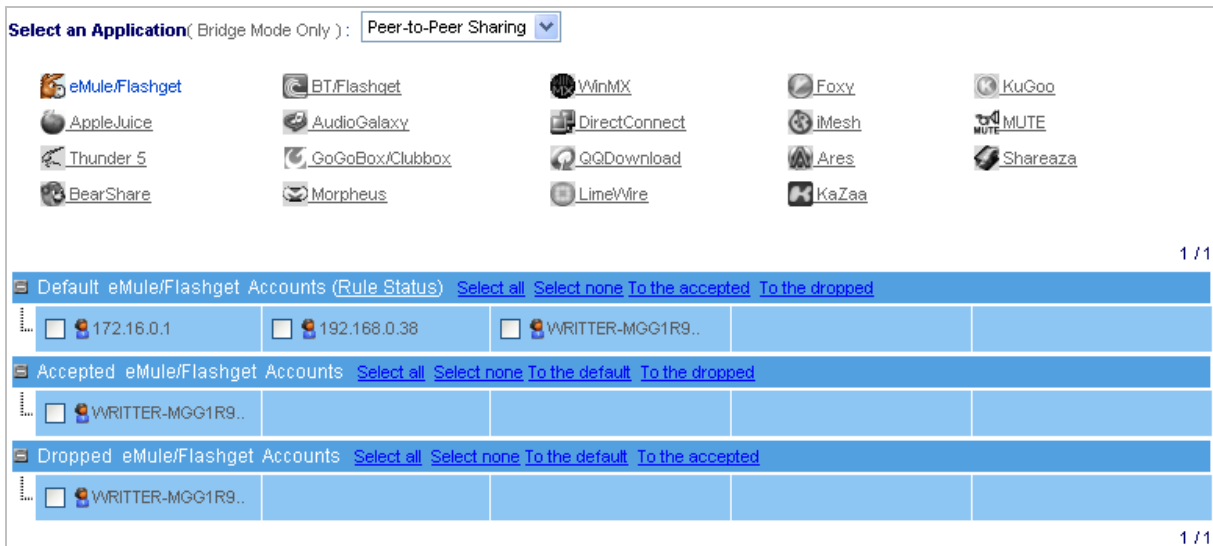



Figure 8-5 Modification Completed



IAR-5000 will use default rule (see Rule Status) on newly added P2P accounts.

9

Record: Settings

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.

9.1 Settings

Signature Definition Status (Web Mail / IM / Application):

- Signature definitions will be updated to reflect any changes to the packet transfer mechanisms of web mail, IM and application to ensure the devices functionality remains up-to-date.
- IAR-5000 automatically checks for the availability of newer signature patterns every hour. It features two ways to update your device, automatic update and manual update.

Username Binding:

- For companies using fixed IP addresses, select **IP Addresses (Username-IP Binding)**. Network packets from the same IP address will be treated as one user.
- For companies using dynamic addressing, such as DHCP addressing, select **MAC addresses (Username-MAC Binding)**. Binding user names to MAC addresses effectively prevents users with malicious intentions and untraceable IP addresses from tampering with the system.
- For companies using Active Directory (AD) server, select **AD Server (Username – Loginname Binding)**. The user name, i.e. the AD account name, is not only used for logging on to Windows, but also for the basis of recording IP services.
- **Authentication names (Username-Authname Binding)** can be used as the basis of recording. Any recordings from the authenticated account will be associated with the same user. It can be used for users who also require authentication to access the Internet. (Note: Requires Bridge mode deployment)



When the router is connected between the LAN user and the IAR-5000 device, the MAC IP address of the packets will be replaced with the MAC address of the router before being sent to the IAR-5000 device. Therefore, if this is the case, please select Username-IP Binding.

Plug-In for Binding Username to AD Server and Recording Skype Conversations (Text & Voice)

■ Plug-In installation location:

◆ AD Server:

- The user's computer will automatically install and run the plug-in when the user logs on to the AD server. Skype text and conversation will be recorded.

◆ On the user's computer:

- When **AD server (Username-Loginname Binding)** is chosen as the recording basis, but the network is not operating with an AD server, the local PC's login will be used as the basis to record Skype text and conversation.
- When using **MAC addresses (Username-MAC Binding)**, **AD server (Username-Loginname Binding)** or **Authentication names (Username-Authname Binding)** as the recording basis, the device will record Skype text and conversation.

Choosing the recording basis, in combination with the plug-in's installation location will produce the following scenarios:

- When **IP addresses (Username-IP Binding)** is chosen as the recording basis the installation of the plug-in becomes irrelevant. The user's IP address forms the basis of recording.
- When **MAC addresses (Username-MAC Binding)** is chosen as the recording basis the installation of the plug-in becomes irrelevant. The user's MAC address forms the basis of recording.
- When **AD server (Username-Loginname Binding)** is chosen as the recording basis the installation of the plug-in becomes irrelevant. The user's AD server login name forms the basis of recording.

Installation Location of the Plug-In	Login used	Recording Basis when an AD Server is Used
Installed on the AD server	AD login	AD login is used as the recording basis
	Local computer's login	User's IP address is used as the recording basis
Installed on User's Computers	AD login	User's AD login is used as the recording basis
	Local computer's login	User's local computer's login is used as the recording basis
Not Installed	AD login	User's IP address is used as the recording basis
	Local computer's login	User's IP address is used as the recording basis

- When **Authentication names (Username-Authname Binding)** is chosen as the recording basis the installation of the plug-in becomes irrelevant.



The IAR-5000 automatically modifies the plug-in file to suite the currently attached network. Thus, it is important to download the plug-in only once the network has been deployed.

LAN to LAN Activity Recording:

IAR-5000 is capable of recording the data transmission among LANs. Supposing users must access the Internet through an on-site proxy server, then that is the case it is used.

Service Content / Log Recording Settings:

- Enables you to decide whether to record a service completely. You may record an IP service completely, or simply the log, or nothing at all.
 - ◆ If set to “Content”, then both the contents and logs of the service will be available for viewing. Accordingly, it takes up more hard disk space.
 - ◆ If set to “Log”, then merely the logs of the service will be available for viewing. It takes only a few bytes (a couple of hundred bytes at most) in size per each service log.
 - ◆ If set to “Not Recording”, then the 8 major services will not be recorded.

Service Log Display Setting:

- Determines the maximum entries displayed per page.

Report Browsing Settings (Search Results / Audit Report):

- Provides users with access to service contents by hyperlinks. Service contents are accessible through the designated IP address and port number within a specific period of time.

Default Character Encoding for Recording:

- The default setting will be applied to data of an unidentified character encoding.

9.2 Settings Example

Binding User Names to IP Addresses:

Step1. Navigate to **Record** → **Settings** → **Settings**, and then set as below:
(Figure 9-1)



Figure 9-1 Record Analysis Settings

Step2. Under **User List** → **Logged**, you will see: (Figure 9-2)

- Users are identified by computer name or DNS name.
- IP address is used for user identification if no information (e.g., user name, DNS name, etc.) is available for displaying.

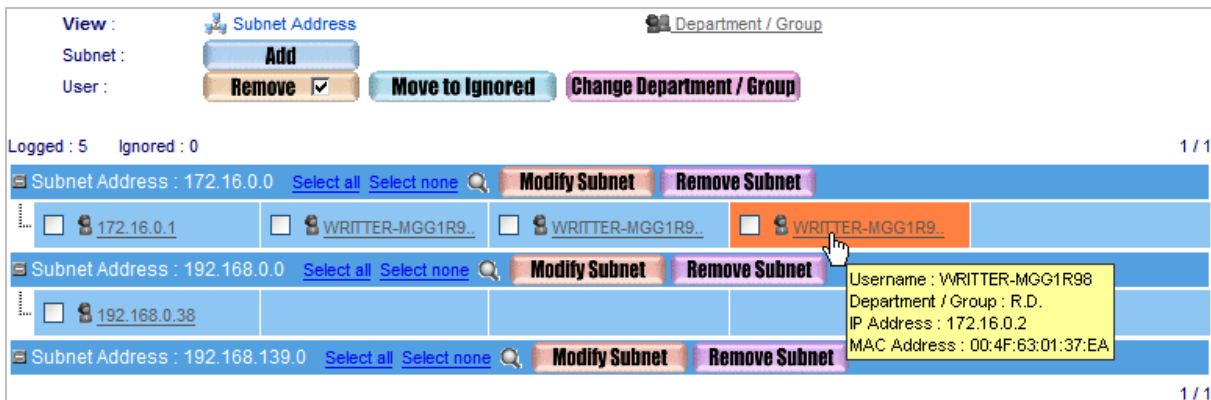


Figure 9-2 User Names Binding to IP Addresses

Step3. User name helps track and control user's online activities. Eight kinds of IP service logs are available under **Record** → **Service**. (Figure 9-3)



Date/Time	Username	Web Site
11/30 15:23	WRITTER-MGG1R98	http://tools.google.com/...
11/30 14:23	WRITTER-MGG1R98	...
11/30 14:07	WRITTER-MGG1R98	...
11/30 13:57	WRITTER-MGG1R98	...
11/30 13:57	WRITTER-MGG1R98	...
11/30 13:52	WRITTER-MGG1R98	servers.def.vpu.stamp
11/30 13:52	WRITTER-MGG1R98	prod-av_pro.vpu.stamp

Figure 9-3 User's Online Activities

Binding User Names to MAC Addresses:

Step1. Navigate to **Record** → **Settings** → **Settings**, and then set as below: (Figure 9-4)

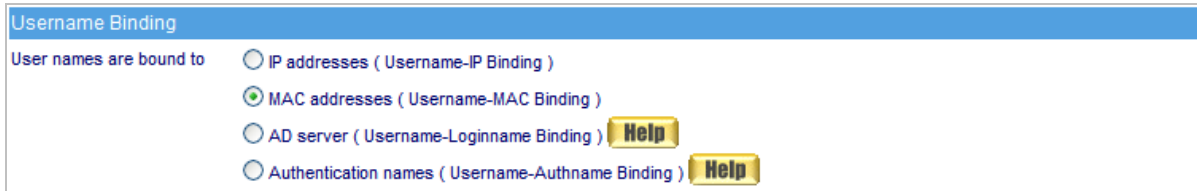


Figure 9-4 Record Analysis Settings

Step2. Under **User List** → **Logged**, you will see: (Figure 9-5)

- Users are identified by computer name or DNS name.
- MAC address is used for user identification if no information (e.g., user name, DNS name, etc.) is available for displaying.

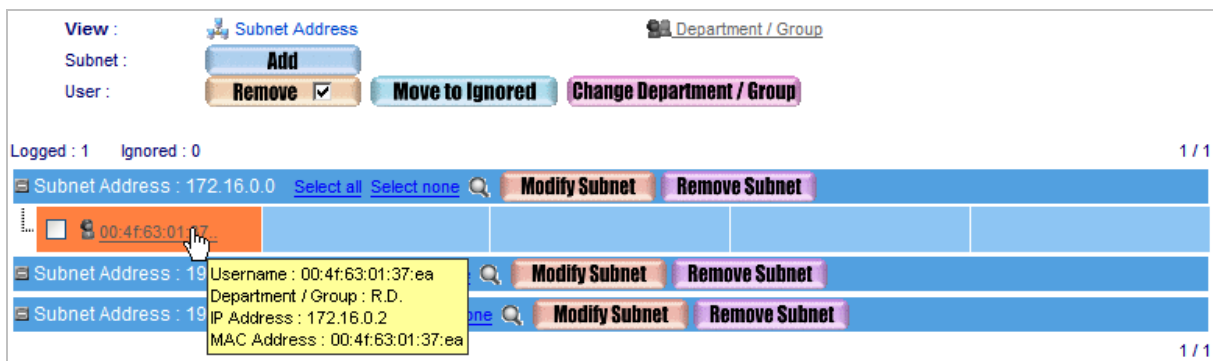


Figure 9-5 User Names Binding to MAC Addresses

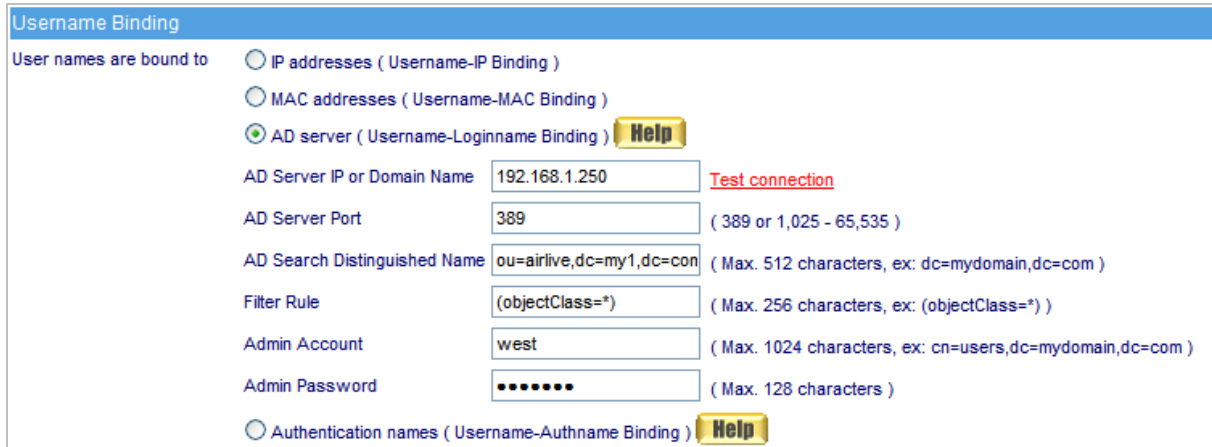
Step3. User name helps track and control user's online activities. Eight kinds of IP service logs are available under **Record** → **Service**. (Figure 9-6)

Date/Time	Username	Web Site
11/30 15:23	JACKY	http://tools.google.com/...
11/30 15:23	WRITTER-MG	http://tools.google.com/...
11/30 15:23	00:4f63:01:37:ea	http://tools.google.com/...
11/30 14:23	JACKY	5.184.155
11/30 14:23	WRITTER-MG	5.184.155
11/30 14:23	00:4f63:01:37:ea	https://65.55.184.155

Figure 9-6 User's Online Activities

Binding User Names to AD Server:

Step1. Navigate to **Record** → **Settings** → **Settings**, and then set as below:
(Figure 9-7)



Username Binding

User names are bound to

- IP addresses (Username-IP Binding)
- MAC addresses (Username-MAC Binding)
- AD server (Username-Loginname Binding) **Help**
- Authentication names (Username-Authname Binding) **Help**

AD Server IP or Domain Name: [Test connection](#)

AD Server Port: (389 or 1,025 - 65,535)

AD Search Distinguished Name: (Max. 512 characters, ex: dc=mydomain,dc=com)

Filter Rule: (Max. 256 characters, ex: (objectClass=*))

Admin Account: (Max. 1024 characters, ex: cn=users,dc=mydomain,dc=com)

Admin Password: (Max. 128 characters)

Figure 9-7 Record Analysis Settings

Step2. Right-click on your domain, point to **New**, and then click on **Organizational Unit**. Next, create as many users as desirable in the newly created **Organizational Unit** folder. (Figure 9-8)

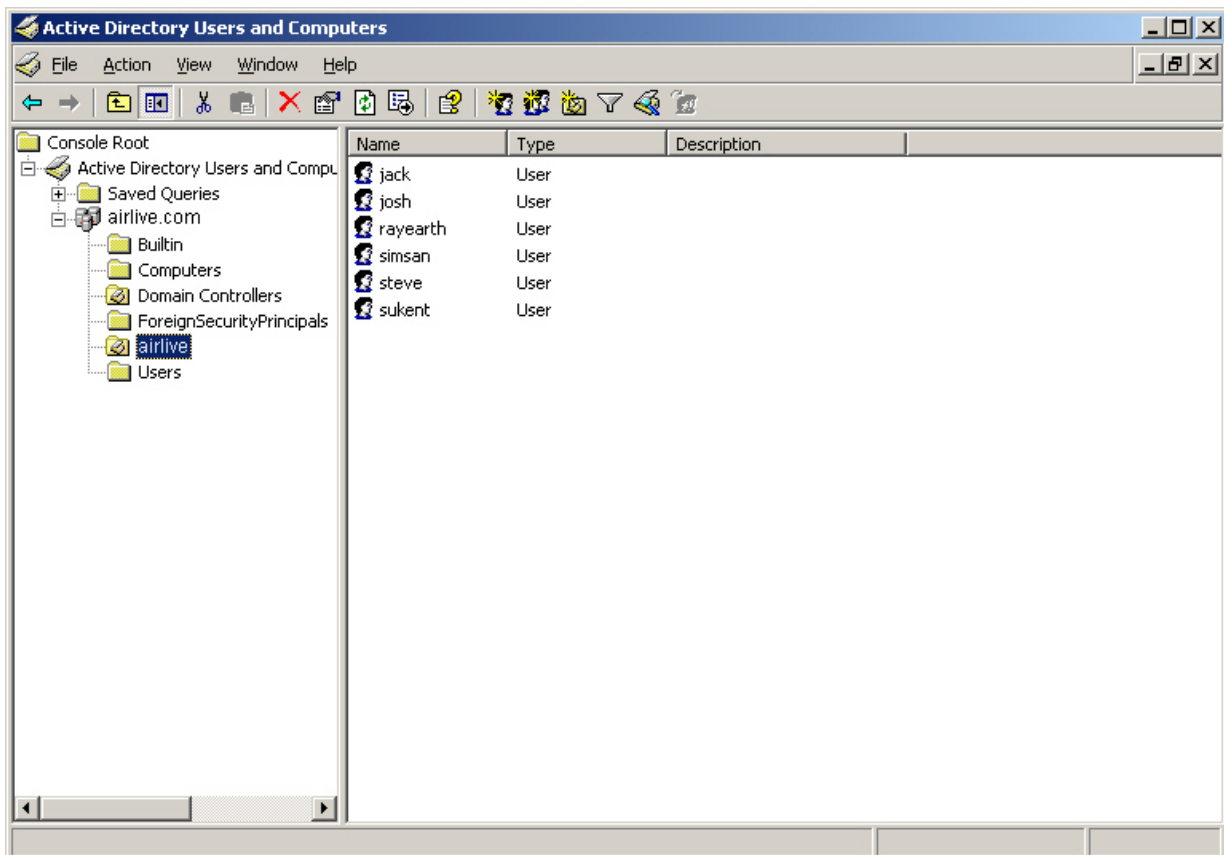


Figure 9-8 Creating an Organizational Unit and Its Members



1. Each AD object has a unique identifier known as a Distinguished Name (DN). DNs are used to uniquely identify entries in an LDAP directory. The following string-type attributes represent the set of standardized attribute types for accessing an LDAP directory.
 - DC - DomainComponent
 - CN - CommonName
 - OU - OrganizationalUnitName
 - O - OrganizationName
 - STREET – StreetAddress
 - L - LocalityName
 - ST - StateOrProvinceName
 - C – CountryName
 - UID : Userid

2. Attribute Values Based Upon AD Server Data
 - dc=my1, dc=com refers to the domain name my1.com (Figure 9-9)
 - cn=Administrator,cn=Users,dc=my1, dc=com refers to the User named Administrator (Figure 9-10)
 - cn=josh,ou=airlive,dc=my1,dc=com refers to the User named josh under the organizational unit name airlive (Figure 9-11)

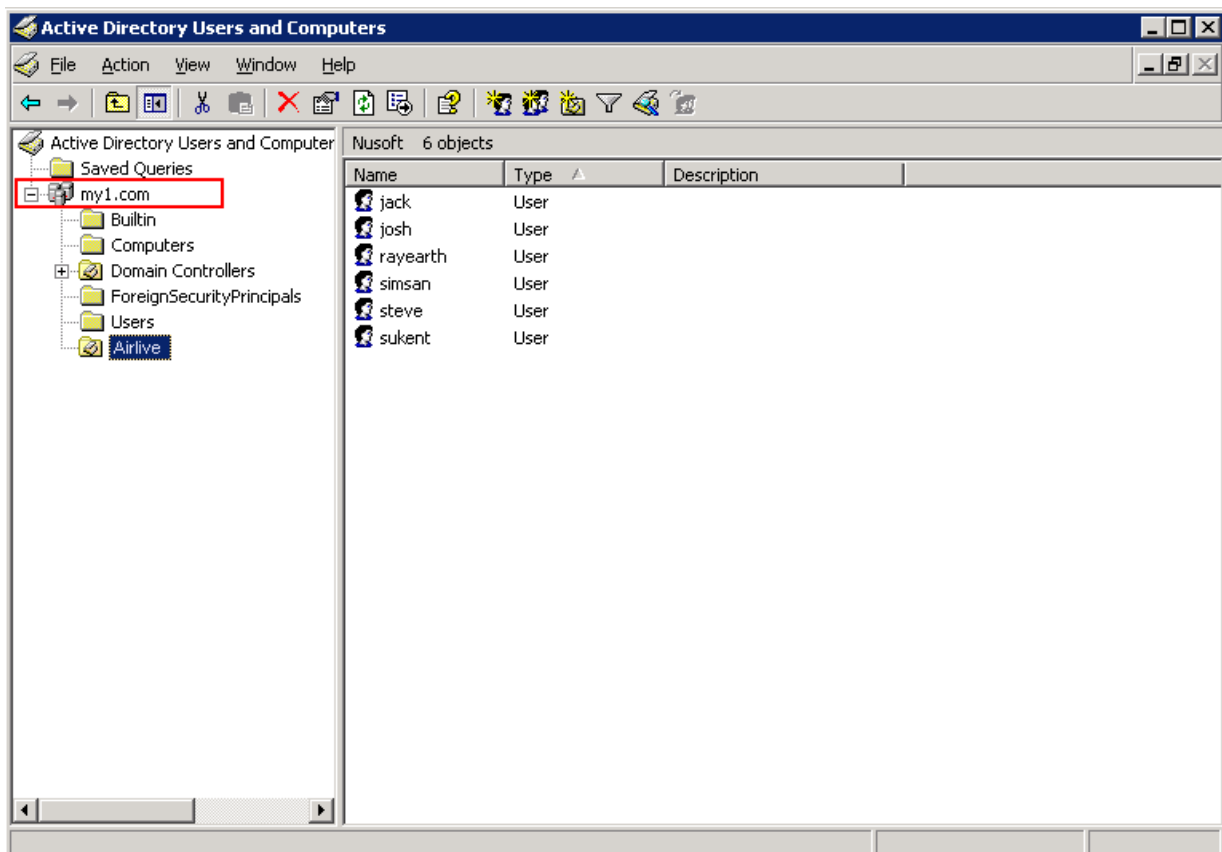


Figure 9-9 Searching for Users by AD Logon Name

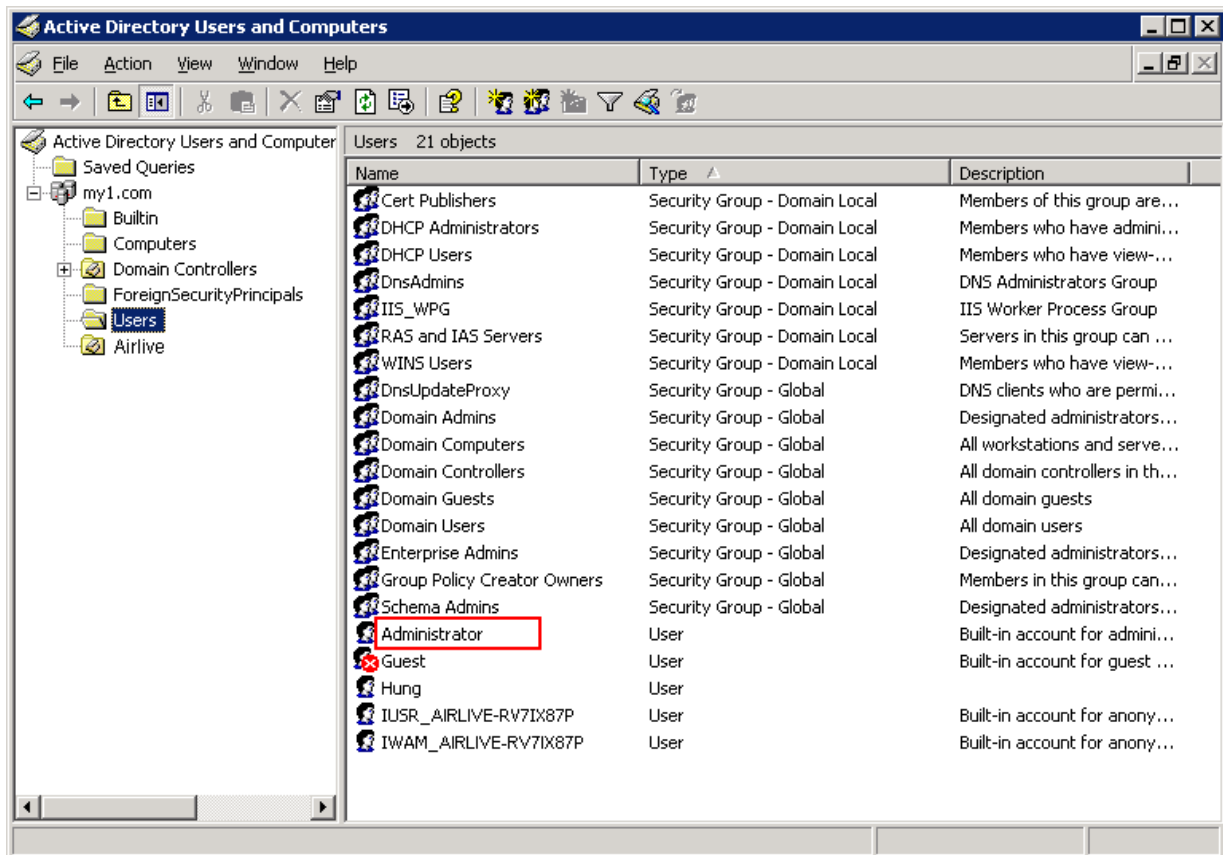


Figure 9-10 Searching for Users Inside Containers

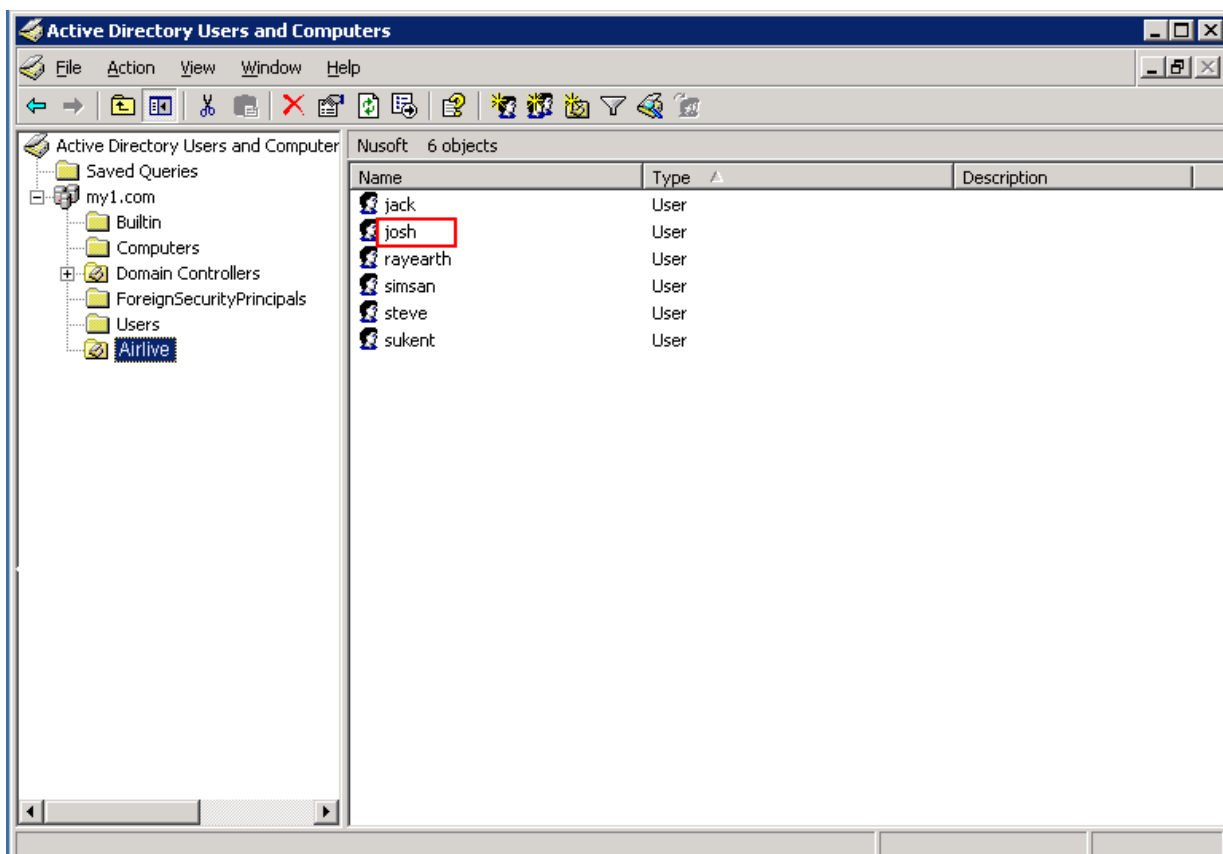


Figure 9-11 Searching for Users Inside Organizations Units

Step3. Under **User List** → **Logged**, you will see: (Figure 9-12)

- Users are displayed by the given name from the **Organizational Unit** in the AD server.
- IP address is used for user identification if the plug-in has not been installed onto the client's computer or user itself has not been authenticated.

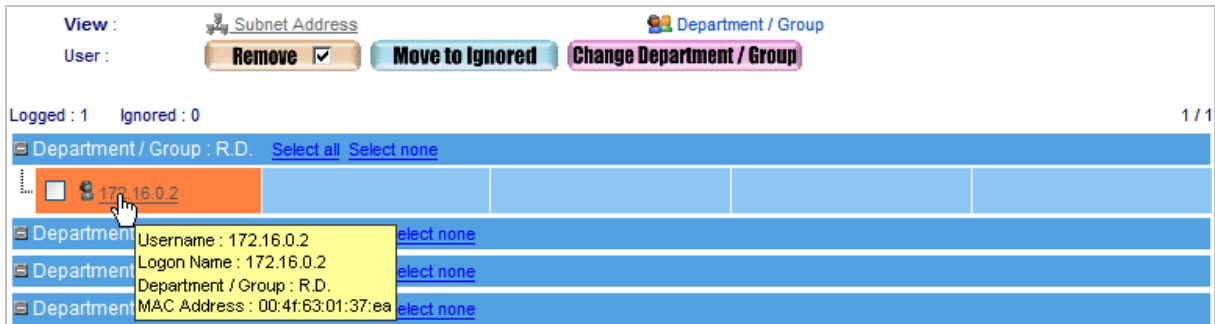


Figure 9-12 User Names Binding to AD Server

Step4. Download the plug-in from the device and install it into your AD server. (Figure 9-13, 14)

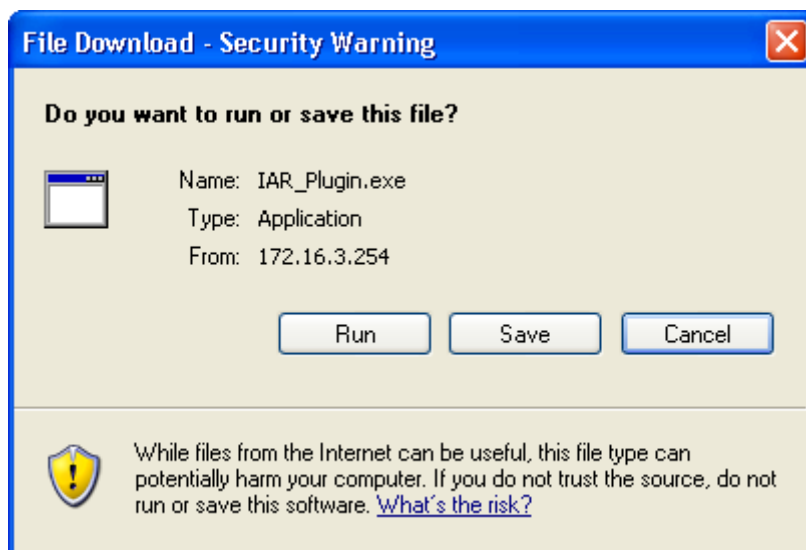


Figure 9-13 Downloading the Plug-In from the Device

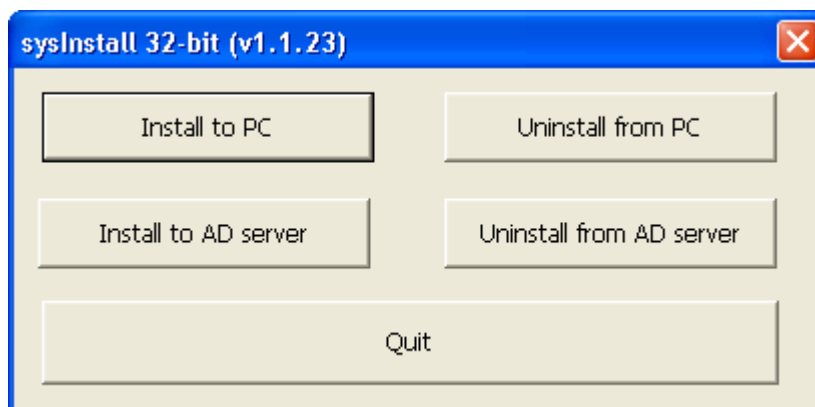


Figure 9-14 Installing the Plug-In onto AD Server

- Step5.** Download the plug-in and installed it onto the AD server:
- Navigate to **Start → All Programs → Administrative Tools → Active Directory Users and Computers**, and then right-click on the domain and choose **Properties**. (Figure 9-15)
 - Select the **Default Domain Policy** and then click on **Edit**. (Figure 9-16)
 - In the **Group Policy Object Editor** window, select **User Configuration → Windows Settings → Scripts (Logon/Logoff)**. After that, double-click on **Logon** scripts. (Figure 9-17)
 - Select the “sysProtect.exe” and then click on **Edit**. (Figure 9-18)
 - Click on **OK** after finish editing. (Figure 9-19)
 - Click on **OK** in the **Logon Properties** window. (Figure 9-20)
 - Setting completed. The plug-in will be automatically installed onto and executed on all AD clients’ computers when they have logged on to AD server.

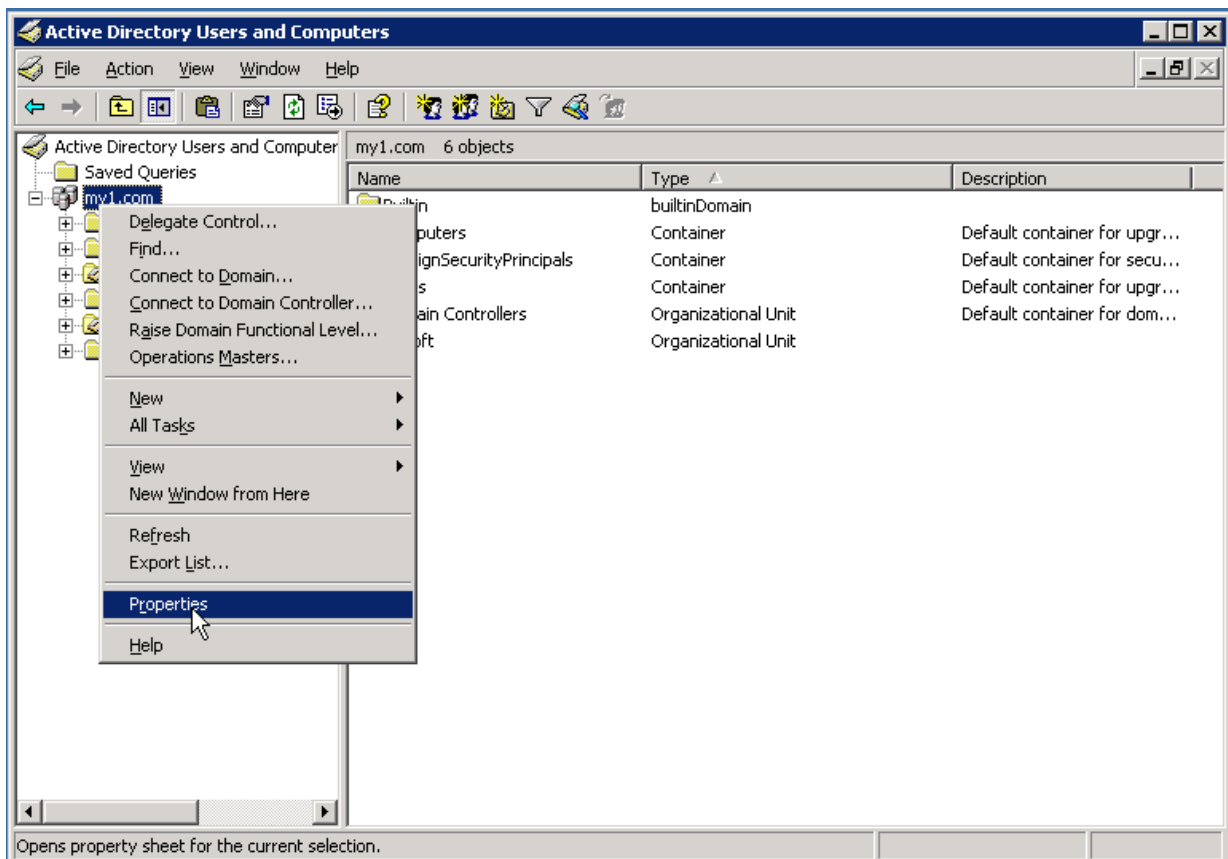


Figure 9-15 Active Directory Users and Computers

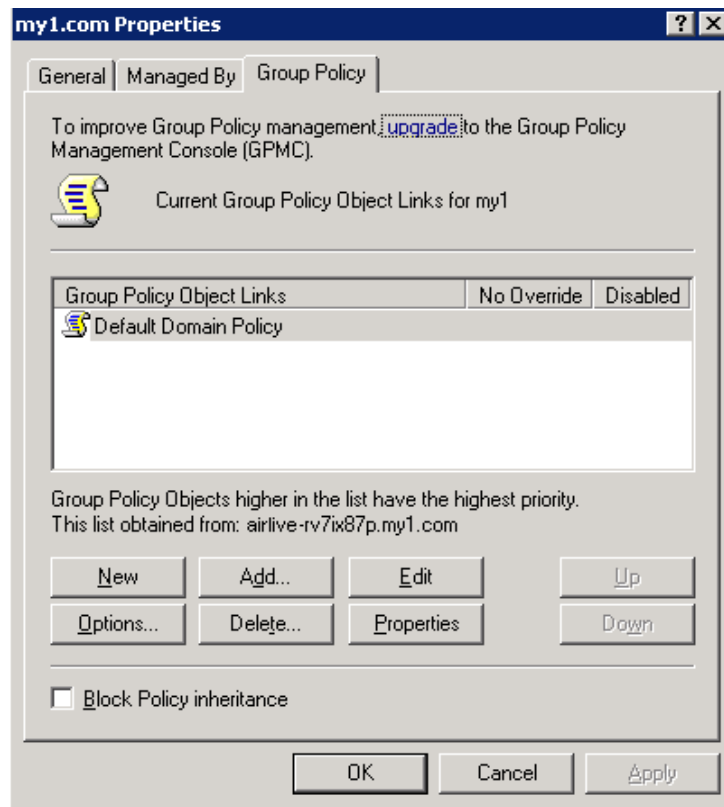


Figure 9-16 Domain Properties

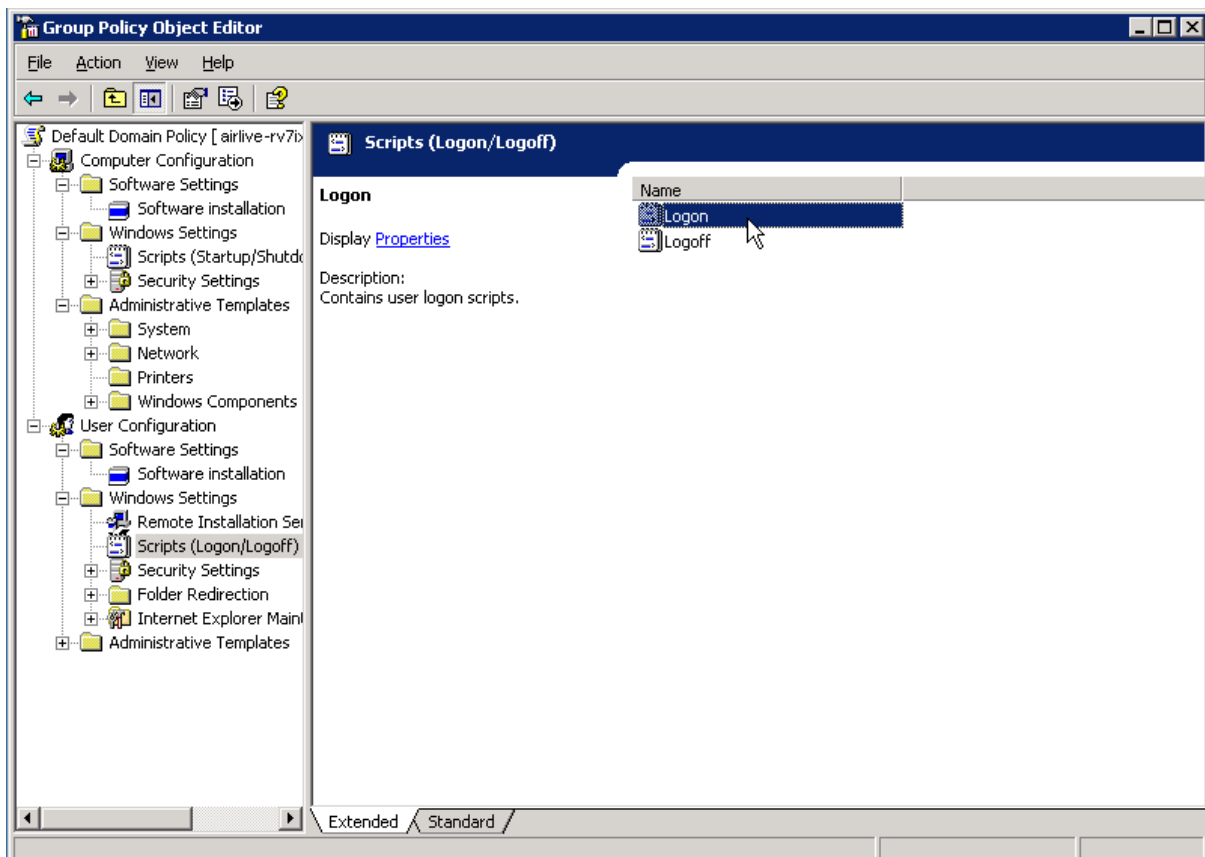


Figure 9-17 Group Policy Object Editor

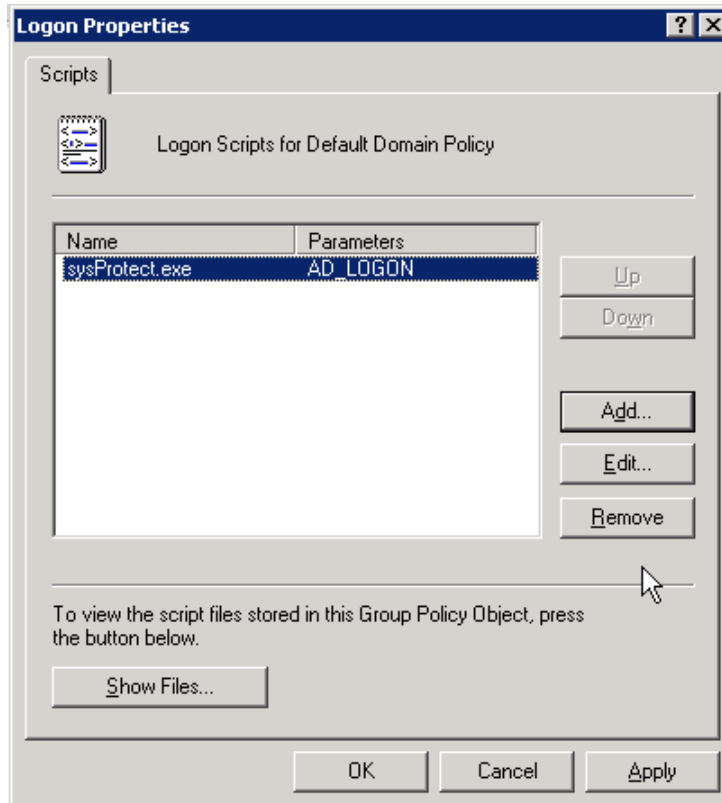


Figure 9-18 Logon Properties

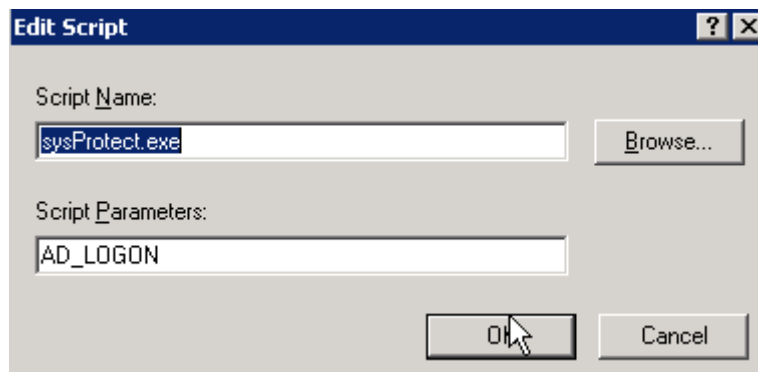


Figure 9-19 Editing Logon Script

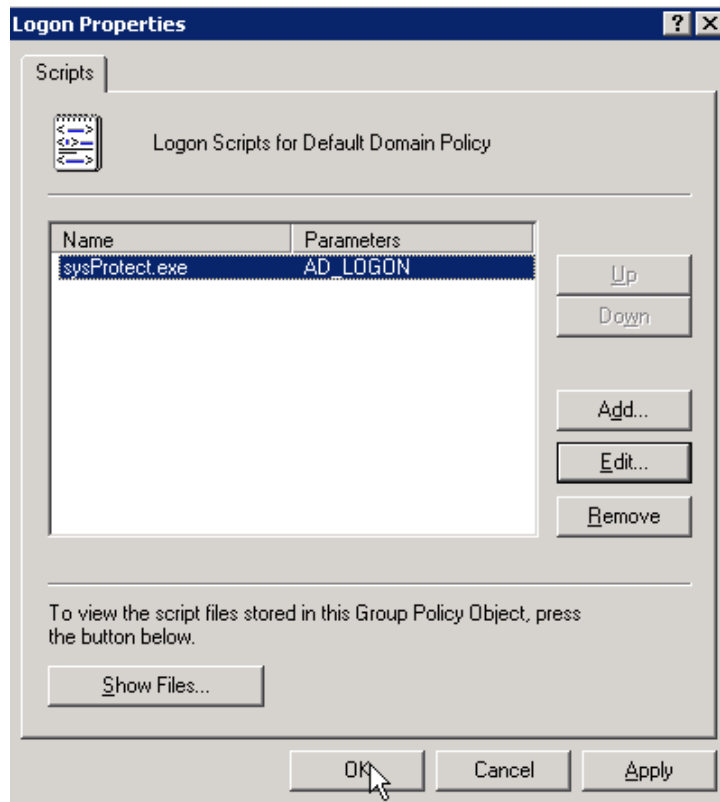



Figure 9-20 Logon Script Configuration Completed

Step6. A user logs on to Windows using Active Directory authentication. (Figure 9-21)



Figure 9-21 Logging on to an AD Domain



For non-AD client users, you may download the plug-in yourself and install it onto your computer. The device will then be able to use your user name, namely the name you use to log on to Windows, as a basis for recording online activities. (Figure 9-22, 23, 24)



Figure 9-22 User Using an AD Account to Log on to Windows

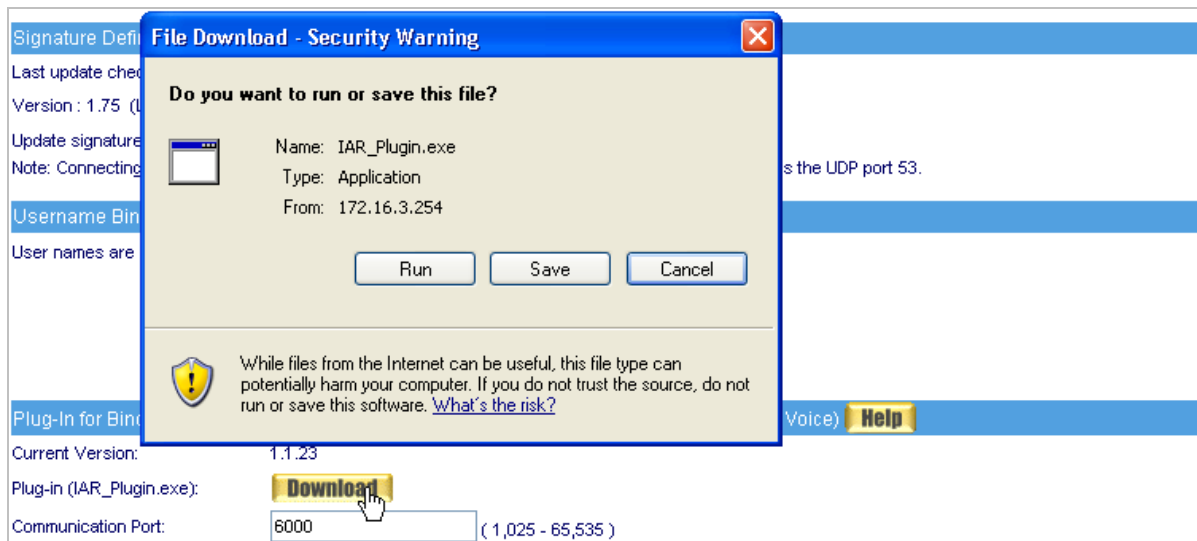


Figure 9-23 Downloading the Plug-In from the Device

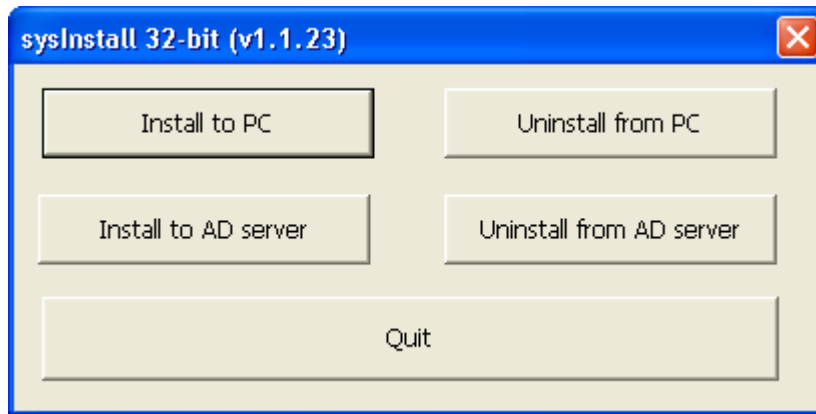


Figure 9-24 Installing the Plug-In onto Client PC

Step7. User name helps track and control user's online activities. Eight kinds of IP service logs are available under **Record** → **Service**. (Figure 9-25)

2009-12-02 (38 records) 1/1			
<input type="checkbox"/>	Date/Time	Username	Web Site
<input type="checkbox"/>	12/02 14:26	172.16.0.2	http://tools.google.com/...
<input type="checkbox"/>	12/02 14:06	WRITTER-MC	http://...
<input type="checkbox"/>	12/02 13:54	172.16.0.2	
<input type="checkbox"/>	12/02 13:54	172.16.0.2	
<input type="checkbox"/>	12/02 12:26	172.16.0.2	https://207.46.113.93
<input type="checkbox"/>	12/02 12:26	172.16.0.2	https://207.46.113.93

Figure 9-25 User's Online Activities

Binding User Names to Authentication Names:

Step1. Navigate to **Record** → **Settings** → **Settings**, and then set as below: (Figure 9-26)

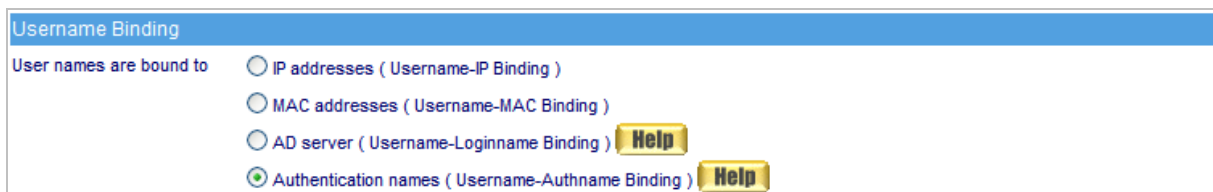


Figure 9-26 Record Analysis Settings

Step2. Under **User List** → **Logged**, you will see: (Figure 9-27)

- Users are identified by authentication name.
- IP address is used for user identification if no information (e.g., user name, DNS name, etc.) is available for displaying.

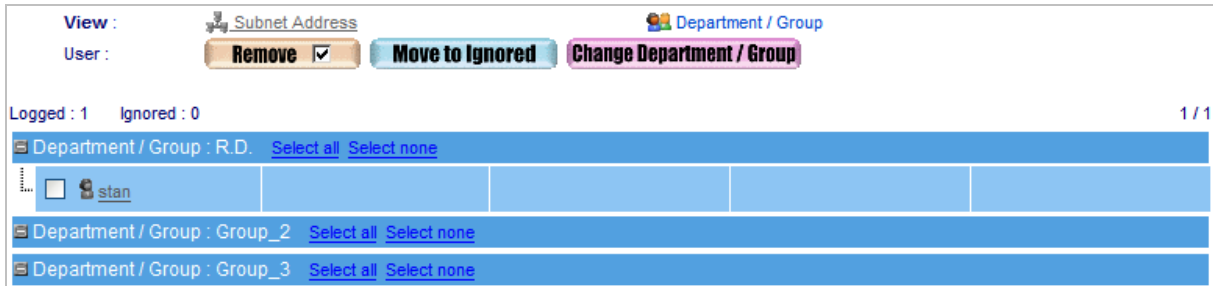
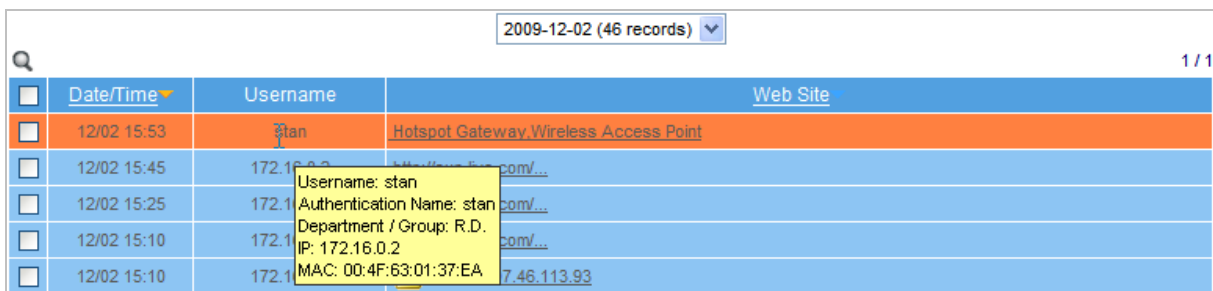


Figure 9-27 User Names Binding to Authentication Name

Step3. User name helps track and control user's online activities. Eight kinds of IP service logs are available under **Record** → **Service**. (Figure 9-28)



The screenshot shows a table of service logs. At the top right, there is a dropdown menu showing '2009-12-02 (46 records)'. The table has columns for 'Date/Time', 'Username', and 'Web Site'. The first row is highlighted in orange and shows '12/02 15:53', 'stan', and 'Hotspot Gateway Wireless Access Point'. A tooltip is visible over the 'stan' username, showing 'Username: stan', 'Authentication Name: stan', 'Department / Group: R.D.', 'IP: 172.16.0.2', and 'MAC: 00:4F:63:01:37:EA'. The last row shows '12/02 15:10', '172.16.0.2', and '7.46.113.93'.

Date/Time	Username	Web Site
12/02 15:53	stan	Hotspot Gateway Wireless Access Point
12/02 15:45	172.16.0.2	...
12/02 15:25	172.16.0.2	...
12/02 15:10	172.16.0.2	...
12/02 15:10	172.16.0.2	7.46.113.93

Figure 9-28 User Names Binding to Authentication Name

10

Record: User and Service

The AirLive IAR-5000 classifies the most frequently seen online activities into 8 services. By monitoring 8 services of each user, system administrator may easily secure the corporate information assets and also avoid network bandwidth from being abused for private purposes.

Today Log:

- The recording of a user's online activities via SMTP, POP3/ IMAP, HTTP, IM (MSN, Yahoo Messenger, QQ, ICQ, AIM, Skype, Gadu-Gadu), Web SMTP, Web POP3, FTP and Telnet of the day is obtainable through the Today Log menu.

10.1 SMTP

Search Emails Sent via SMTP:

- Records are available if searched by criteria, such as recipient, sender, subject, content, session direction, no attached file, attached file and date, as keyword or pattern.
 - ◆ Under **System → Settings**, tick **Enable email notification** and configure its related settings; and then navigate to **Record → Settings → Settings** to **Enable report hyperlinks** as well as configure its related settings. Refer to the steps below to start a search:
 1. **Sender:** Type a key word from the email address
 2. **Username:** Type a key word from the user name
 3. Enable the searching duration and specify a period of time to search within.
 4. Click on **Search**. (Figure 10-1)
 5. Click on **Send Report**.
 6. Mail out the search results to the designated recipient. (Figure 10-2)
 7. Click on **Download Report** to download the search results as a “.txt” file onto local computer. (Figure 10-3, 4)
 8. Click on **Export Mail** to download the search results as a “.mbx” file onto local computer. (Figure 10-5)

Search Emails Sent via SMTP

Enter your search criteria :

Recipient : (Max. 100 characters)

Sender : (Max. 100 characters)

Subject : (Max. 100 characters)

Content : (Max. 100 characters)

Username : (Max. 80 characters)

IP Address :

No Attachment

Attachment File Name : (Max. 100 characters)

Start a search from: 2009 / 12 / 01 00 : 00

To: 2009 / 12 / 02 17 : 04

Search **Mail Report** **Download Report** **Export Mail**

Help

Results

2009-12-02 (12 records) ▾

<input type="checkbox"/>	Date / Time ▾	Username	Sender	Recipient	Subject (Click to view details)
<input type="checkbox"/>	12/02 16:42	JACKY	pm3@airlive.com	stan@test.com	- RE: MW-2000S
<input type="checkbox"/>	12/02 16:42	JACKY	pm3@airlive.com	michael@test.com	- RE: MW-2000S

Figure 10-1 Searching for a Specific Log

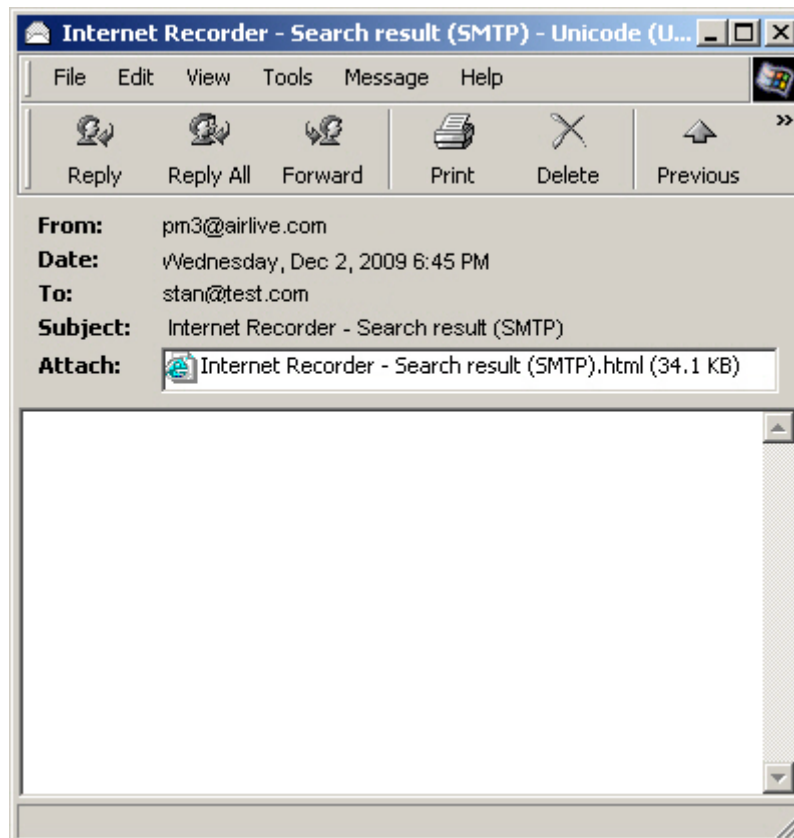


Figure 10-2 The Search Results of SMTP Attached to an Email

IAR-5000 - Search result (SMTP)

Date / Time	Username	Sender	Recipient	Subject
12/02 16:42	JACKY	pm3@airlive.com	stan@test.com	RE: MW-2000S
12/02 16:42	JACKY	pm3@airlive.com	michael@test.com	RE: MW-2000S

Figure 10-3 The Search Results of SMTP

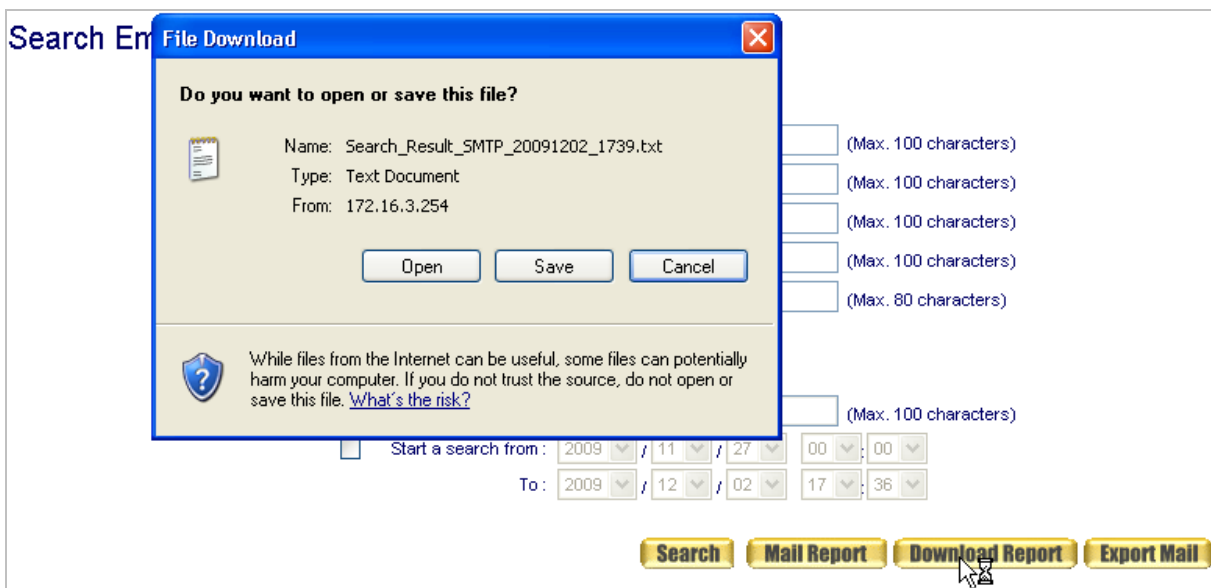
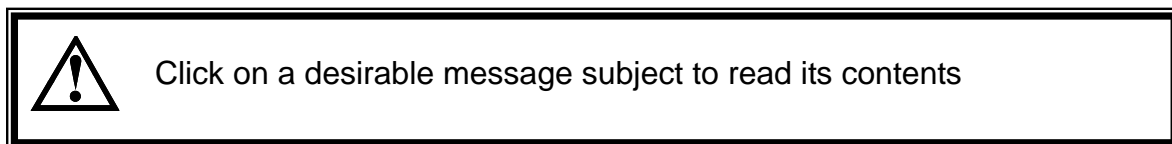


Figure 10-4 Downloading the Search Results as a ".txt" File

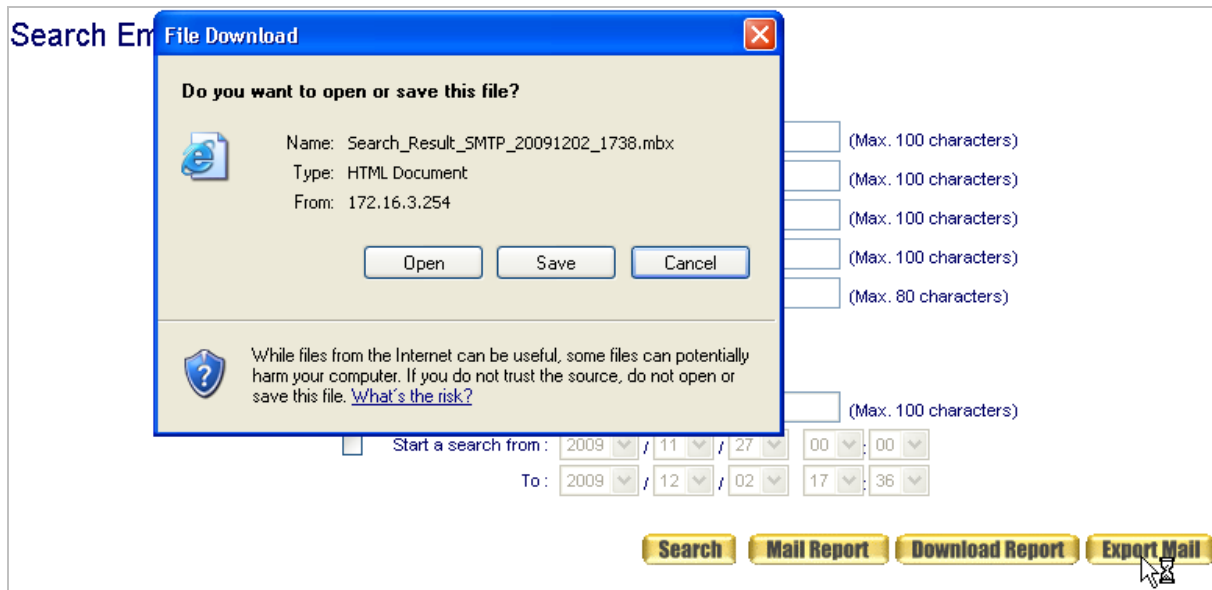


Figure 10-5 Exporting the Search Results as a “.mbx” File



How to open a “.mbx” file on your local computer:

- Convert the “.mbx” file into a “.eml” file with a mbx2eml application (e.g., IMAPSize) and then run Outlook Express to open the “.eml” file.
- Run IMAPSize, navigate to **Tools** → **mbx2eml** on the menu bar, and then click on it. (Figure 10-6)
- In the mbx2eml window, click on **“Select mbox files to convert”** button, locate the “.mbx” file, click on **Open**, and then click on **Convert** to start converting the file into “.eml” file. (Figure 10-7, 8, 9)
- Run Outlook Express to open the “.eml” file. (Figure 10-10)

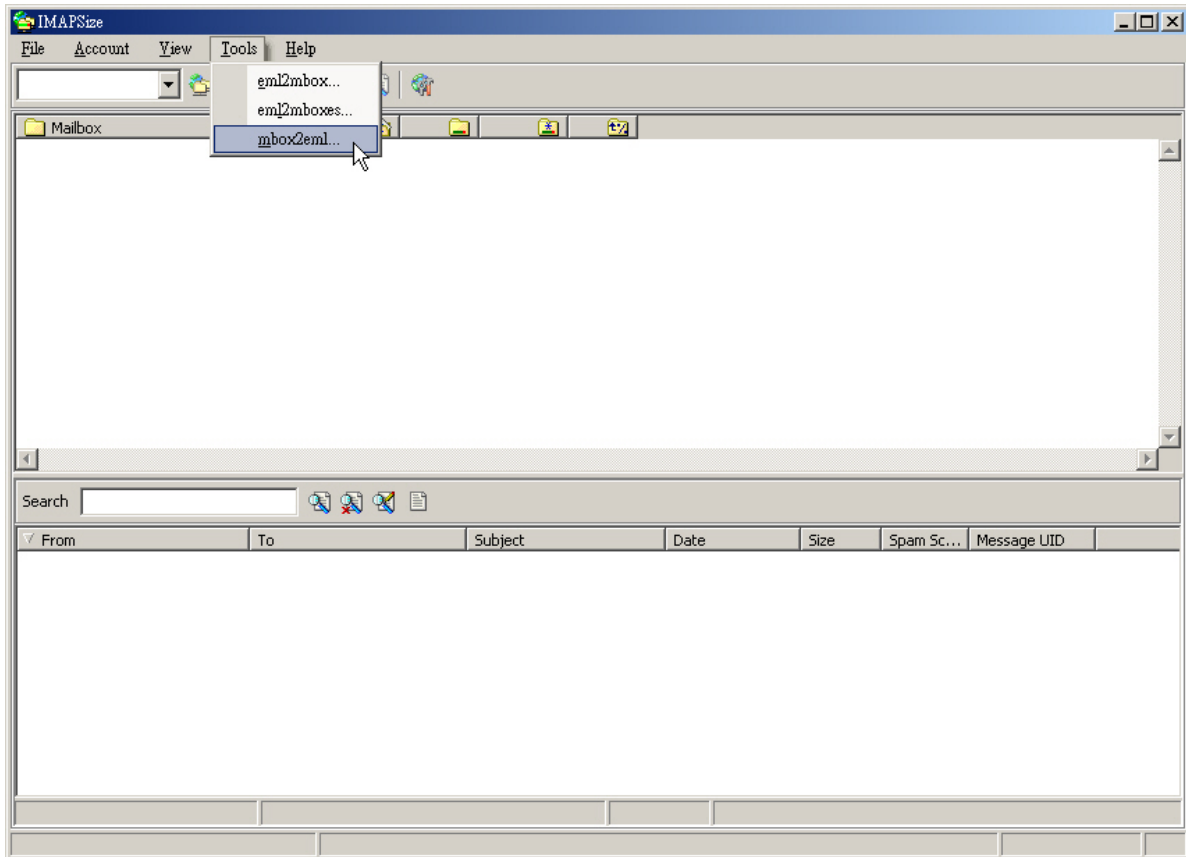


Figure 10-6 Navigating to Tools → Mbox2eml on the Menu Bar

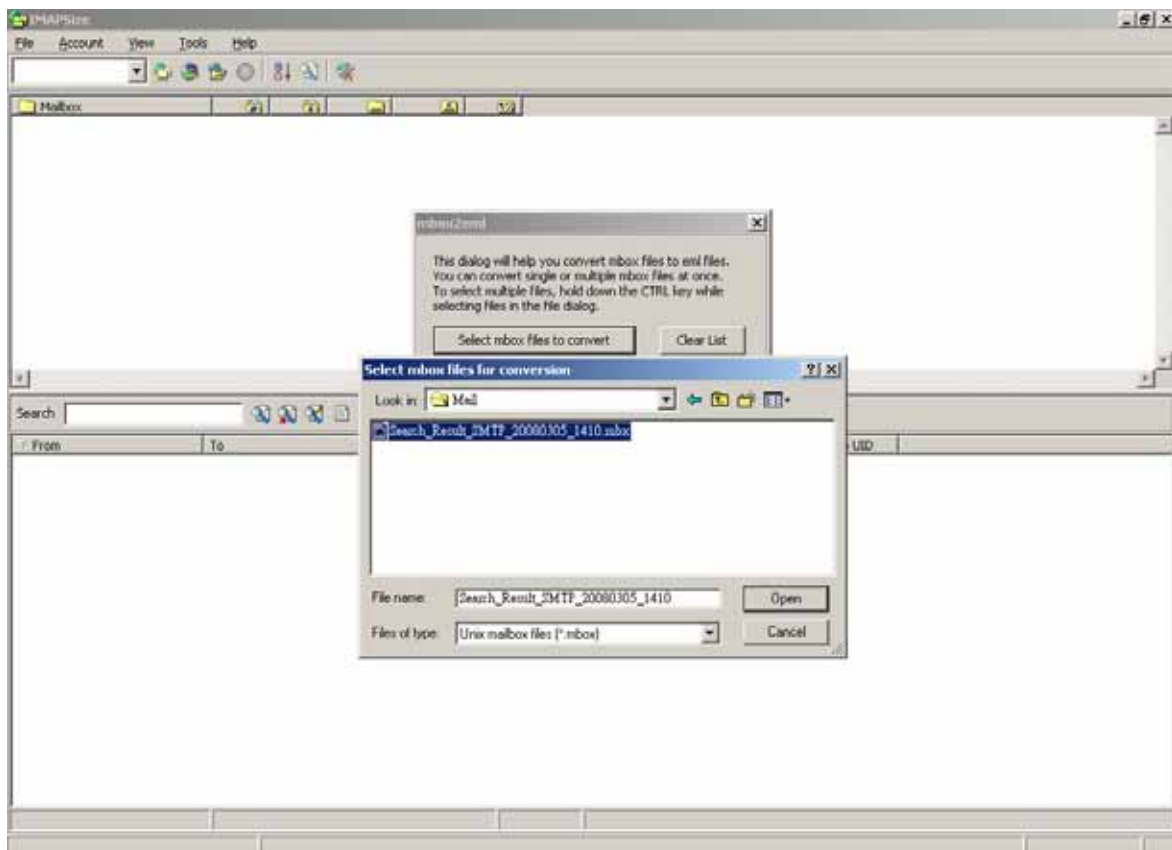


Figure 10-7 Specifying the “.mbx” File to be Converted

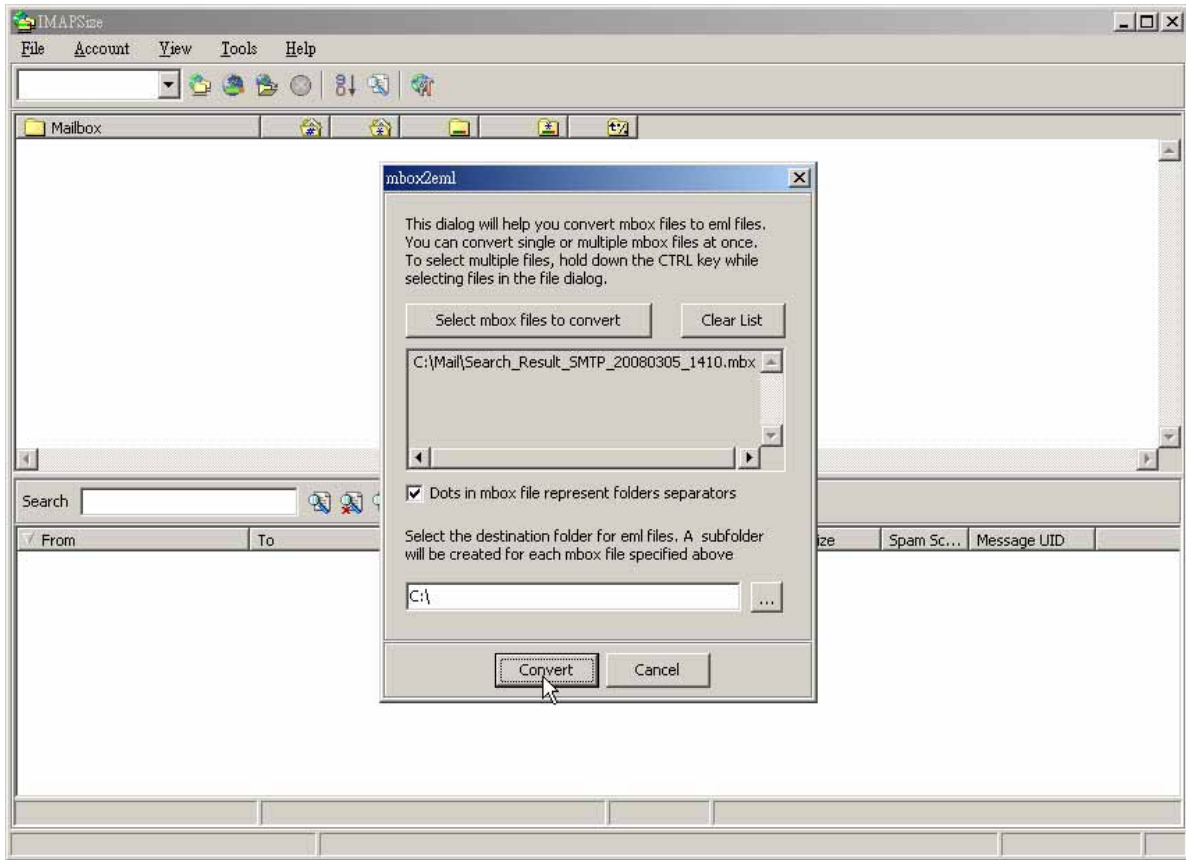


Figure 10-8 Converting the “.mbx” File into a “.eml” File

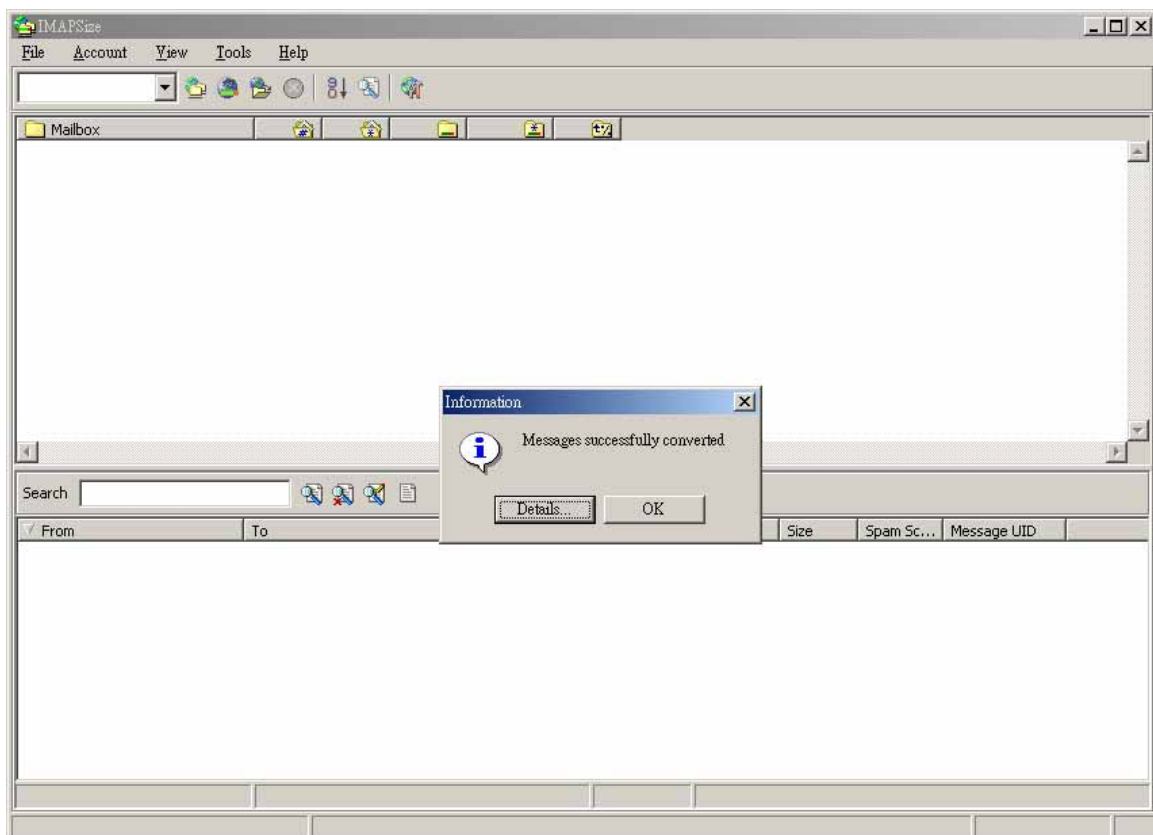


Figure 10-9 File Conversion Completed

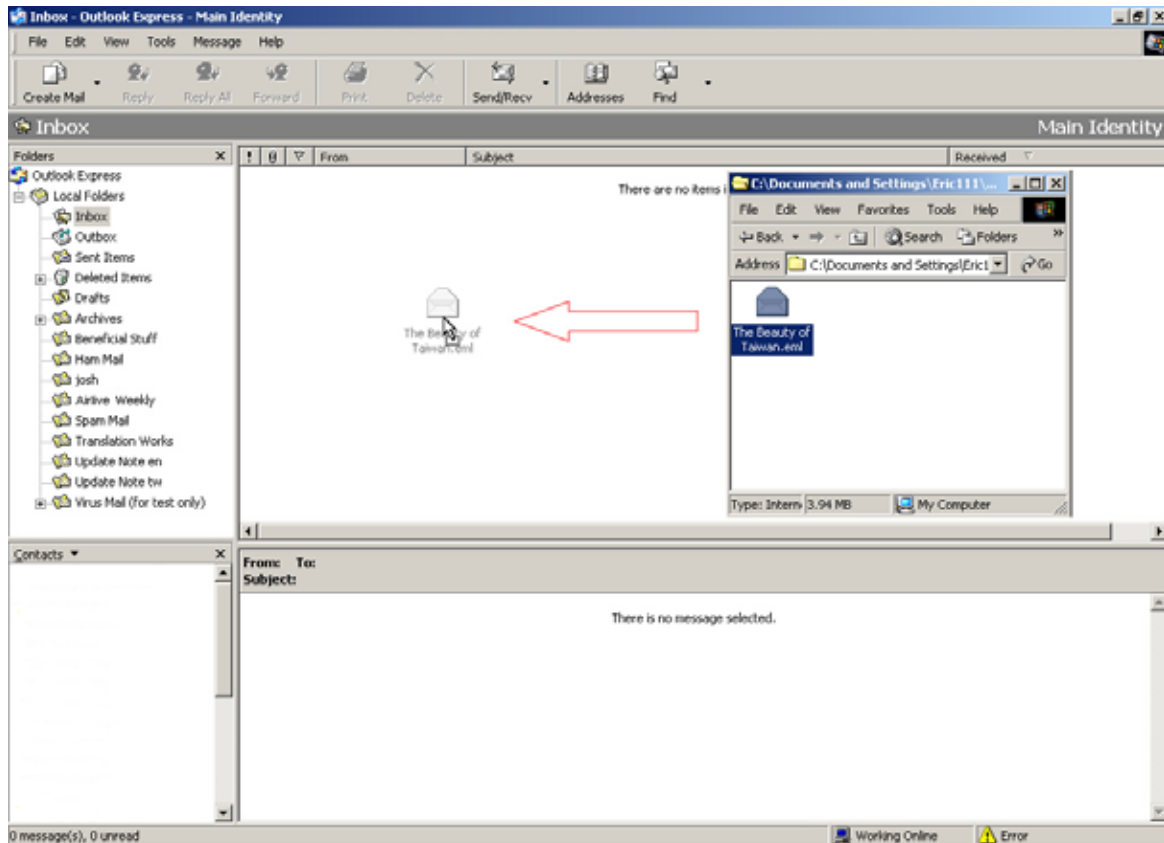


Figure 10-10 Click oning and Dragging the “.eml” File into Outlook Express to Open It

10.2 HTTP

Search Visited Webpages via HTTP:

- Records are available if searched by criteria, such as Web site address, content, session direction, transmission direction and date, as keyword or pattern.
- ◆ Under **System** → **Settings**, tick **Enable email notification** and configure its related settings; and then navigate to **Record** → **Settings** → **Settings** to **Enable report hyperlinks** as well as configure its related settings. Refer to the steps below to start a search:
 1. **Web Site:** Type a key word from the Web site address.
 2. **Username:** Type a key word from the user name.
 3. **File Transfer:** Tick both **Upload** and **Download**.
 4. Enable the searching duration and specify a period of time to search within.
 5. Click on **Search**. (Figure 10-11)
 6. Click on **Send Report**.
 7. Mail out the search results to the designated recipient. (Figure 10-12, 13)
 8. Click on **Download Report** to download the search results as a “.txt” file onto local computer. (Figure 10-14)

Search Visited Webpages via HTTP

Enter your search criteria :

Web Site : (Max. 80 characters)
 Username : (Max. 80 characters)
 IP Address :
 Content : (Max. 80 characters)

File Transfer : Upload Download

Start a search from : 2009 / 12 / 02 00 : 00
 To : 2009 / 12 / 02 18 : 13

Search **Mail Report** **Download**

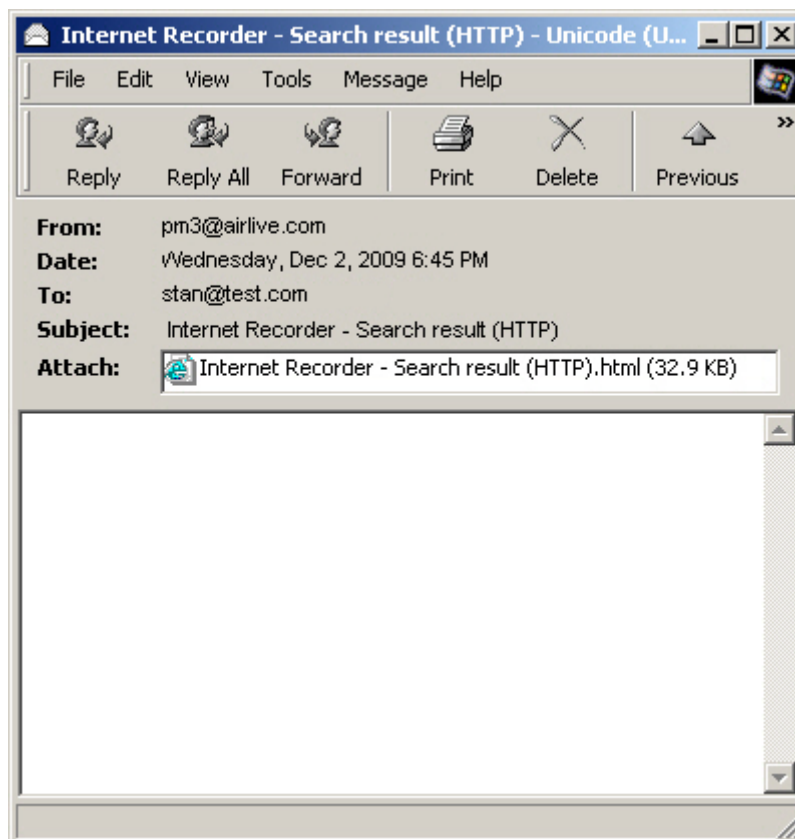
Results

2009-12-02 (8 records) 1 / 1

<input type="checkbox"/>	Date/Time	Username	Web Site
<input type="checkbox"/>	12/02 17:02	JACKY	servers.def.vpu.stamp
<input type="checkbox"/>	12/02 17:02	JACKY	prod-av_pro.vpu.stamp
<input type="checkbox"/>	12/02 17:02	JACKY	microsoftrootcert.crl
<input type="checkbox"/>	12/02 17:02	JACKY	MSNContentPCA.crl
<input type="checkbox"/>	12/02 17:02	JACKY	MSNContentCA.crl
<input type="checkbox"/>	12/02 17:02	JACKY	MSNContentCA.crl
<input type="checkbox"/>	12/02 17:02	JACKY	MSNContentPCA.crl
<input type="checkbox"/>	12/02 17:02	JACKY	microsoftrootcert.crl

1 / 1
Clear **Clear All**

Figure 10-11 Searching for a Specific Log



Internet Recorder - Search result (HTTP) - Unicode (U...

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous

From: pm3@airlive.com
Date: Wednesday, Dec 2, 2009 6:45 PM
To: stan@test.com
Subject: Internet Recorder - Search result (HTTP)
Attach: Internet Recorder - Search result (HTTP).html (32.9 KB)

Figure 10-12 The Search Results of HTTP Attached to an Email

IAR-5000 - Search result (POP3 / IMAP)

Date / Time	Username	Web Site
12/02 17:02	JACKY	servers.def.vpu.stamp
12/02 17:02	JACKY	prod-av_pro.vpu.stamp
12/02 17:02	JACKY	microsoftrootcert.crl
12/02 17:02	JACKY	MSNContentPCA.crl
12/02 17:02	JACKY	MSNContentCA.crl

Figure 10-13 The Search Results of HTTP



Click on a desirable Web site log to view the visited page.

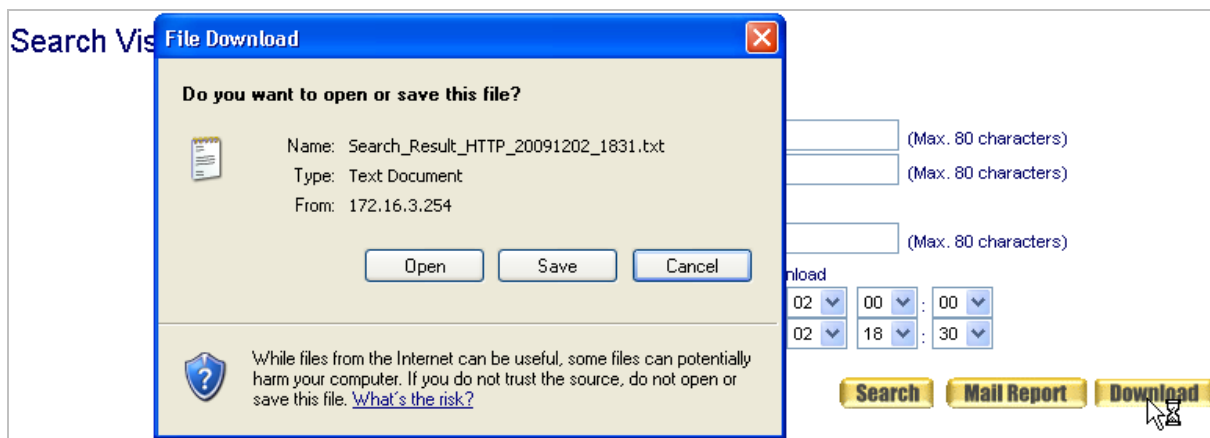


Figure 10-14 Downloading the Search Results as a ".txt" File

10.3 IM

Search IM Conversations:

- Records are available if searched by criteria, such as type, session direction, user account, participants, content, file name, auth name and date, as keyword or pattern.
- ◆ Under **System → Settings**, tick **Enable email notification** and configure its related settings; and then navigate to **Record → Settings → Settings** to **Enable report hyperlinks** as well as configure its related settings. Refer to the steps below to start a search:
 1. **IM Application:** Select “All”.
 2. **Username:** Type a key word from the user name.
 3. **IM Account:** Type a key word from the user account.
 4. Enable the searching duration and specify a period of time to search within.
 5. Click on **Search**. (Figure 10-15)
 6. Click on **Send Report**.
 7. Mail out the search results to the designated recipient. (Figure 10-16, 17)
 8. Click on **Download Report** to download the search results as a “.txt” file onto local computer. (Figure 10-18)

Search IM Conversations

Enter your search criteria :

IM Application : All

IP Address :

Username : (Max. 80 characters)

IM Account : (Max. 100 characters)

Participant : (Max. 100 characters)

Content : (Max. 100 characters)

Transferred File Name : (Max. 100 characters)

Start a search from : 2009 / 12 / 02 00 : 00

To : 2009 / 12 / 02 18 : 40

Results

2009-12-02 (1 records)

← 1 / 1

<input type="checkbox"/>	Conversation Duration	Username	Participant	
<input type="checkbox"/>	18:39:52 – 18:39:52 (0.0 min.)	JACKY	-	sebastienko@hotmail... ↔ airlive_jacky@hotmail.com 1

← 1 / 1

Figure 10-15 Searching for a Specific Log

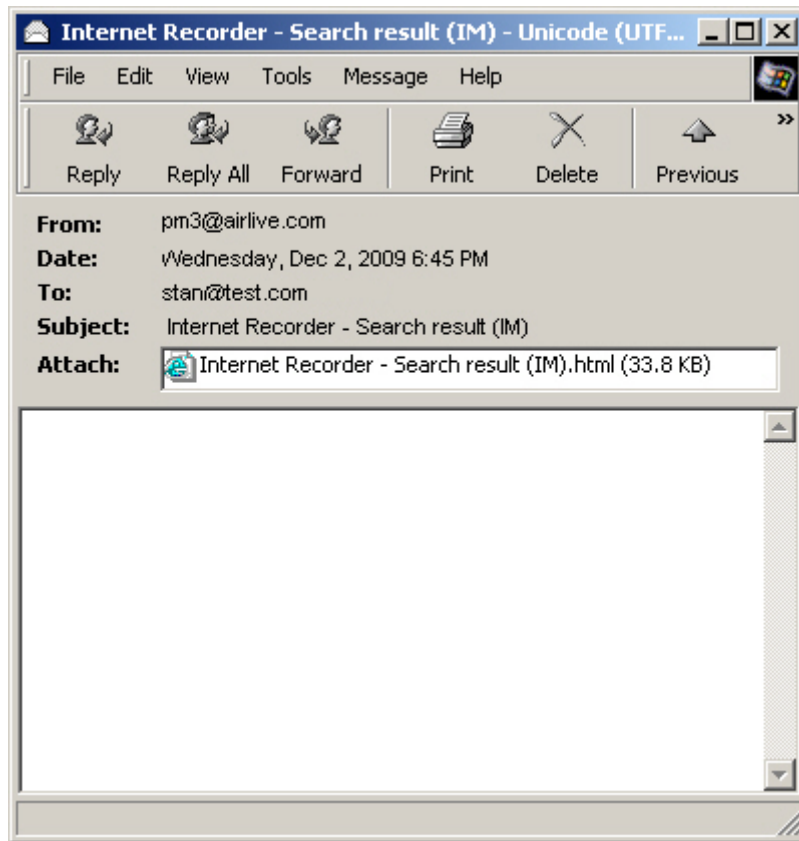



Figure 10-16 The Search Results of IM Attached to an Email

IAR-5000 - Search result (IM)			
Conversation Duration	Username	Participant	P <-> P
18:39:52 -- 18:39:52 (0.0min.)	JACKY	- (MSN) sebastienko@hotmail.. <-> airlive_jacky@hotmail..	2

Figure 10-17 The Search Results of IM

1



Click on the frequency number of a conversation to view its conversation

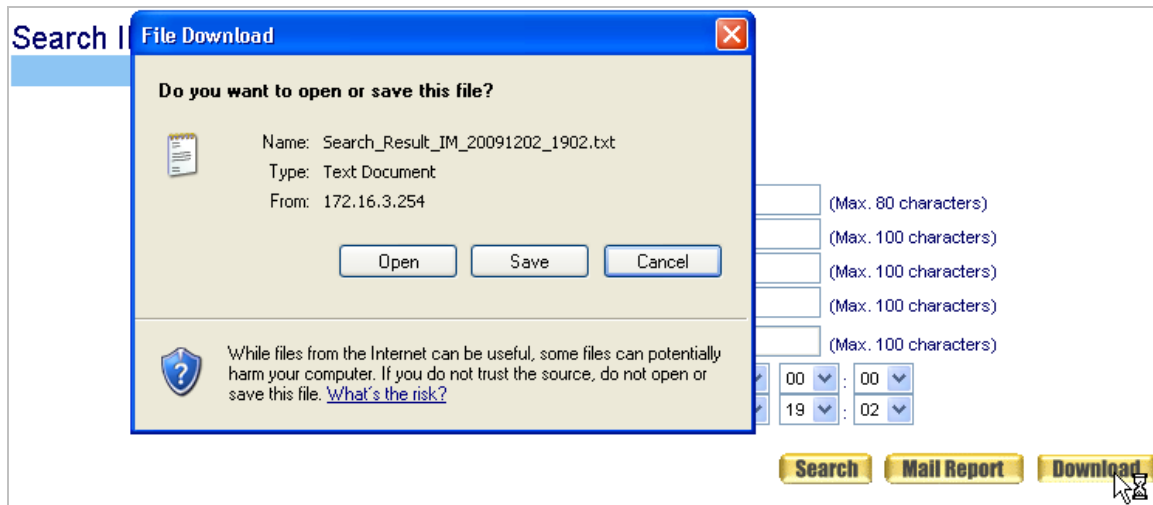


Figure 10-18 Downloading the Search Results as a “.txt” File

10.4 Web SMTP

Search Emails Sent via Web-Based Email Services:

- Records are available if searched by criteria, such as recipient, sender, subject, content, session direction, no attached file, attached file and date, as keyword or pattern.
- ◆ Under **System → Settings**, tick **Enable email notification** and configure its related settings; and then navigate to **Record → Settings → Settings** to **Enable report hyperlinks** as well as configure its related settings. Refer to the steps below to start a search:
 1. **Username:** Type a key word from the user name.
 2. **Session Direction:** Select “All”.
 3. Enable the searching duration and specify a period of time to search within.
 4. Click on **Search**. (Figure 10-19)
 5. Click on **Send Report**.
 6. Mail out the search results to the designated recipient. (Figure 10-20, 21)
 7. Click on **Download Report** to download the search results as a “.txt” file onto local computer. (Figure 10-22)
 8. Click on **Export Mail** to download the search results as a “.mbx” file onto local computer. (Figure 10-23)

Search Emails Sent via Web-Based Email Services

Enter your search criteria :

Recipient : (Max. 100 characters)

Sender : (Max. 100 characters)

Subject : (Max. 100 characters)

Content : (Max. 100 characters)

Username : (Max. 100 characters)

IP Address :

No Attachment

Attachment File : (Max. 100 characters)

Start a search from : 2009 / 12 / 04 00 00

To : 2009 / 12 / 04 10 51

Search **Mail Report** **Download Report** **Export Mail**

Help

Results

2009-12-04 (1 records)

<input type="checkbox"/>	Date / Time	Username	Sender	Recipient	Subject (Click to view the content)
<input type="checkbox"/>	12/04 10:50	JACKY	airlive_jacky@hotmail...	jacky.ko@airlive.com	- IAR-5000 demo for WebSMTP connection

Clear **Clear All**

Figure 10-19 Searching for a Specific Log

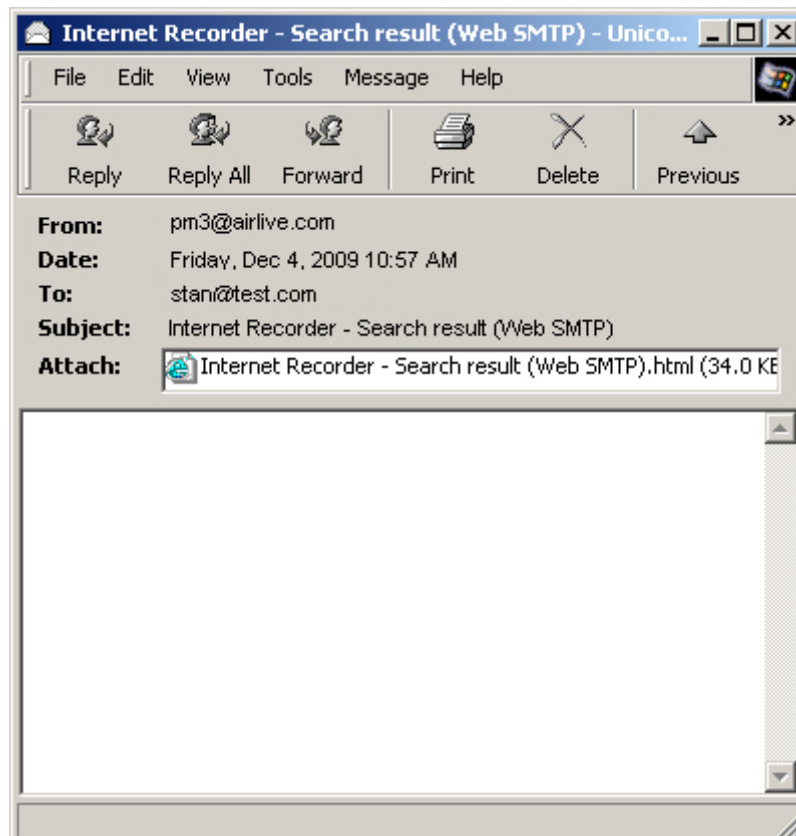



Figure 10-20 The Search Results of Web SMTP Attached to an Email

IAR-5000 - Search result (Web SMTP)				
Date / Time	Username	Sender	Recipient	Subject
12/04 10:50	JACKY	airlive_jacky@hotmail..	jacky.ko@airlive.com	IAR-5000 demo for WebSMTP connection

Figure 10-21 The Search Results of Web SMTP




Click on a desirable message subject to read its contents.


Search Emails Sent via Web-Based Email Services

File Download ✕

Do you want to open or save this file?



Name: Search_Result_Web SMTP_20091204_1125.txt
 Type: Text Document
 From: airtlive98.dyndns.org



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. [What's the risk?](#)

(Max. 100 characters)
 (Max. 100 characters)
 (Max. 100 characters)
 (Max. 100 characters)
 (Max. 100 characters)
 (Max. 100 characters)

Start a search from: 2009 / 12 / 04 00:00
 To: 2009 / 12 / 04 11:24

Figure 10-22 Downloading the Search Results as a ".txt" File

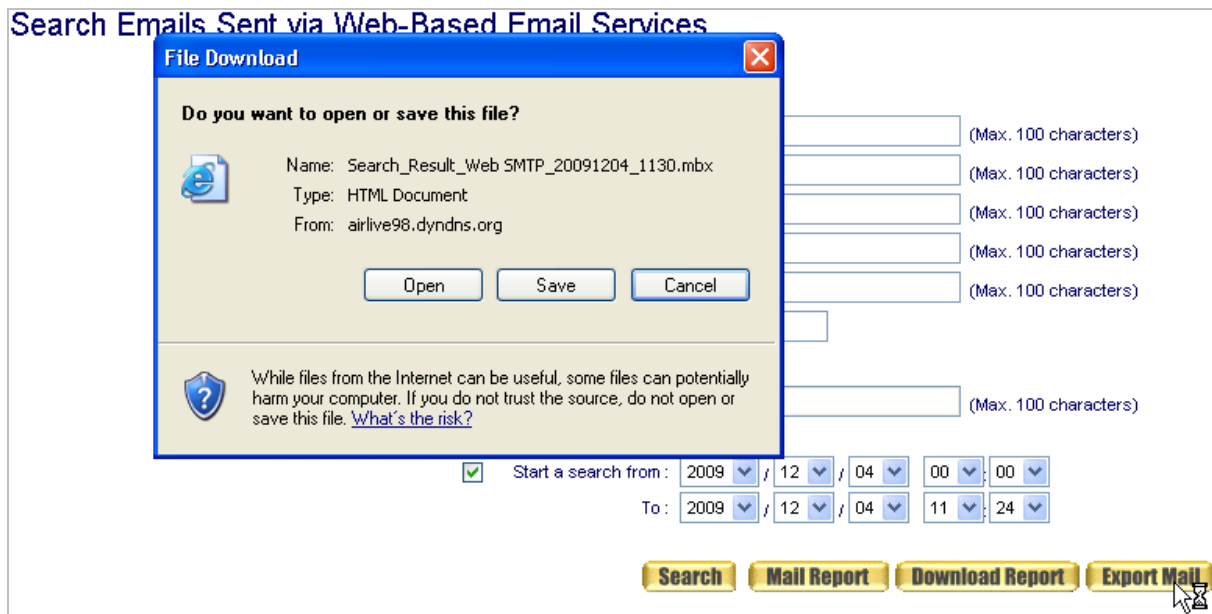
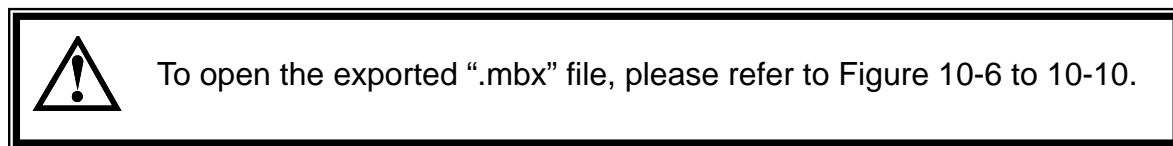


Figure 10-23 Exporting the Search Results as a “.mbx” File



10.5 Web POP3

Search Emails Received via Web-Based Email Services:

- Records are available if searched by criteria, such as recipient, sender, subject, content, session direction, no attached file, attached file and date, as keyword or pattern.
- ◆ Under **System** → **Settings**, tick **Enable email notification** and configure its related settings; and then navigate to **Record** → **Settings** → **Settings** to **Enable report hyperlinks** as well as configure its related settings. Refer to the steps below to start a search:
 1. **Username:** Type a key word from the user name.
 2. Enable the searching duration and specify a period of time to search within.
 3. Click on **Search**. (Figure 10-24)
 4. Click on **Send Report**.
 5. Mail out the search results to the designated recipient. (Figure 10-25, 26)
 6. Click on **Download Report** to download the search results as a “.txt” file onto local computer. (Figure 10-27)
 7. Click on **Export Mail** to download the search results as a “.mbx” file onto local computer. (Figure 10-28)

Search Emails Received via Web-Based Email Services

Enter your search criteria :

Recipient : (Max. 100 characters)

Sender : (Max. 100 characters)

Subject : (Max. 100 characters)

Content : (Max. 100 characters)

Username : (Max. 100 characters)

IP Address :

No Attachment

Attachment File : (Max. 100 characters)

Start a search from: 2009 / 12 / 04 00:00

To: 2009 / 12 / 04 11:42

Search **Mail Report** **Download Report** **Export Mail**

Help

Results

2009-12-04 (5 records) ▾

<input type="checkbox"/>	Date / Time ▾	Username	Sender	Recipient	Subject (Click to view the content)
<input type="checkbox"/>	12/04 10:36	JACKY	notification+2mk24..	sebastienko@hotmail..	- Jennifer Lu commented on her..

← 1 / 1

Figure 10-24 Searching for a Specific Log

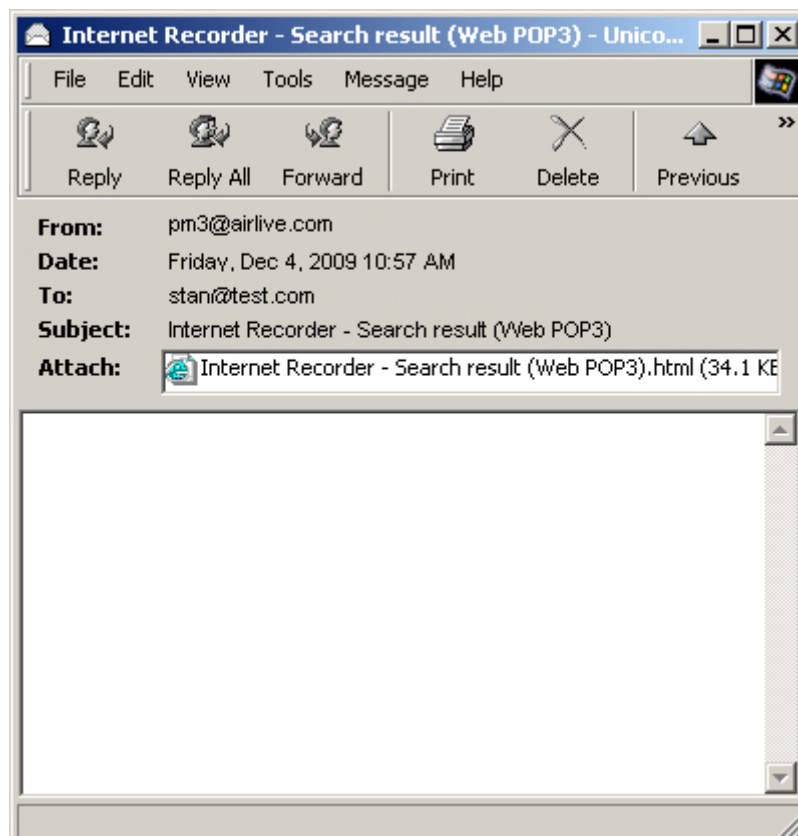



Figure 10-25 The Search Results of Web POP3 Attached to an Email

IAR-5000 - Search result (Web POP3)

Date / Time	Username	Sender	Recipient	Subject
12/04 12:35	JACKY	notification + 2mk24	sebastienko@hotmai..	Jennifer Lu command on her..

Figure 10-26 The Search Results of Web POP3




Click on a desirable message subject to read its contents.

Search Emails Received via Web-Based Email Services

File Download ✖


Do you want to open or save this file?



Name: Search_Result_Web POP3_20091204_1203.txt

Type: Text Document

From: airlive98.dyndns.org

 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. [What's the risk?](#)

Start a search from: 2009 / 12 / 04 00:00

To: 2009 / 12 / 04 12:03

Figure 10-27 Downloading the Search Results as a ".txt" File

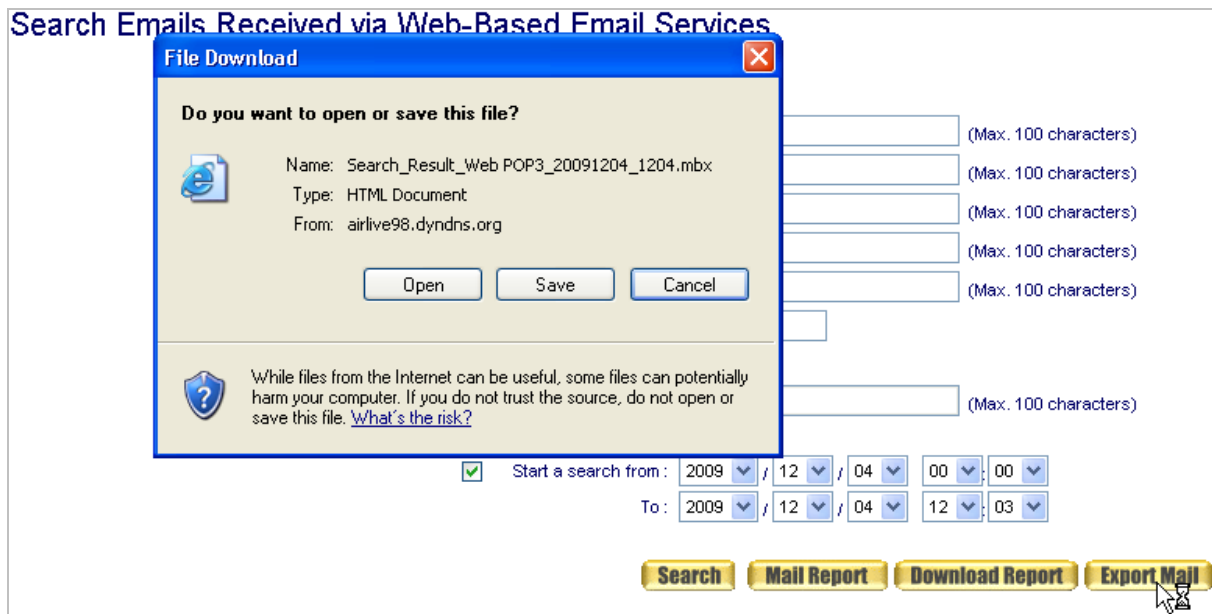


Figure 10-28 Exporting the Search Results as a “.mbx” File



To open the exported “.mbx” file, please refer to Figure 10-6 to 10-10.

10.6 FTP

Search Files Transferred via FTP:

- Records are available if searched by criteria, such as file name, host name, user name, size, session direction and date, as keyword or pattern.
- ◆ Under **System** → **Settings**, tick **Enable email notification** and configure its related settings; and then navigate to **Record** → **Settings** → **Settings** to **Enable report hyperlinks** as well as configure its related settings. Refer to the steps below to start a search:
 1. **Username:** Type a key word from the user name.
 2. Enable the searching duration and specify a period of time to search within.
 3. Click on **Search**. (Figure 10-29)
 4. Click on **Send Report**.
 5. Mail out the search results to the designated recipient. (Figure 10-30, 31)
 6. Click on **Download Report** to download the search results as a “.txt” file onto local computer. (Figure 10-32)

Search Files Transferred via FTP

Enter your search criteria :

File Name : (Max. 80 characters)

Hostname : (Max. 80 characters)

Username : (Max. 80 characters)

IP Address :

File Size : Larger than KBytes (1 - 9999)

Start a search from : 2009 / 12 / 4 0 : 0

To : 2009 / 12 / 4 13 : 18

Search **Mail Report** **Download**

Results

2009-12-04 (4 records) 1 / 1

<input type="checkbox"/>	Date / Time	Username	Hostname	Login Name : Password	Direction	File Name	File Size
<input type="checkbox"/>	12/04 12:05	JACKY	59.115.100.67	jacky : KB115	Download	IAR-5K_45.png	27 KB

Figure 10-29 Searching for a Specific Log

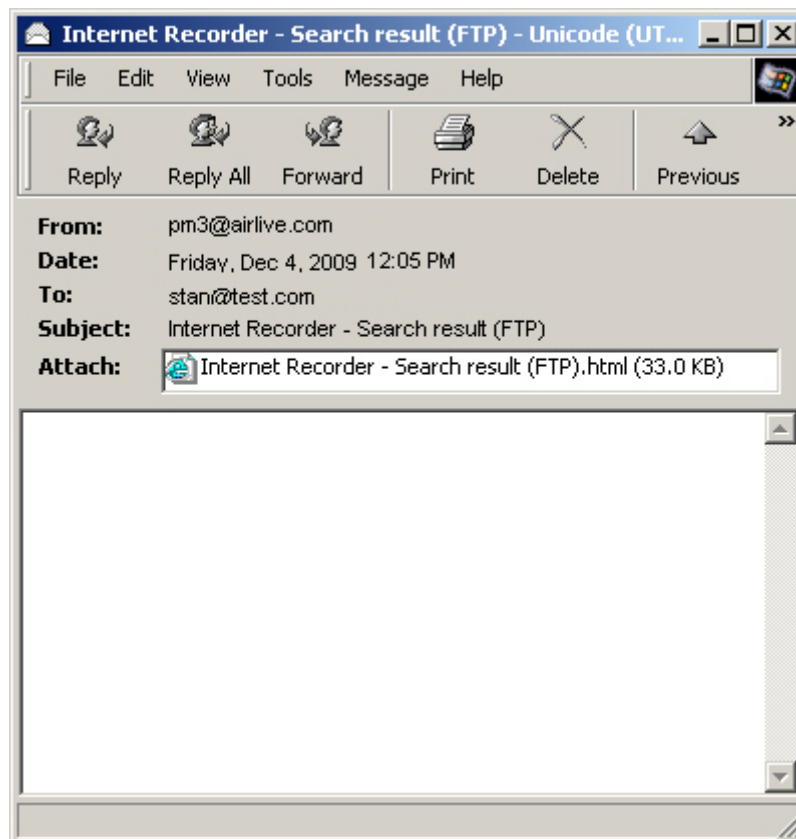


Figure 10-30 The Search Results of FTP Attached to an Email

Date / Time	Username	Hostname	Login Name : Password	Direction	File Name	File Size
12/04 15:22	JACKY	airlive15.dyndns.org	jacky : *****	Download	IAR-5K_48.png	33 KB
12/04 14:37	JACKY	airlive15.dyndns.org	jacky : *****	Download	IAR-5K_47.png	24 KB
12/04 13:51	JACKY	airlive15.dyndns.org	jacky : *****	Download	IAR-5K_46.png	21 KB
12/04 12:05	JACKY	59.115.100.67	jacky : *****	Download	IAR-5K_45.png	27 KB
12/04 12:05	JACKY	59.115.100.67	jacky : *****	Download	IAR-5K_44.png	28 KB
12/04 11:31	JACKY	59.115.100.67	jacky : *****	Download	IAR-5K_43.png	27 KB
12/04 11:28	JACKY	59.115.100.67	jacky : *****	Download	IAR-5K_42.png	26 KB

Figure 10-31 The Search Results of FTP

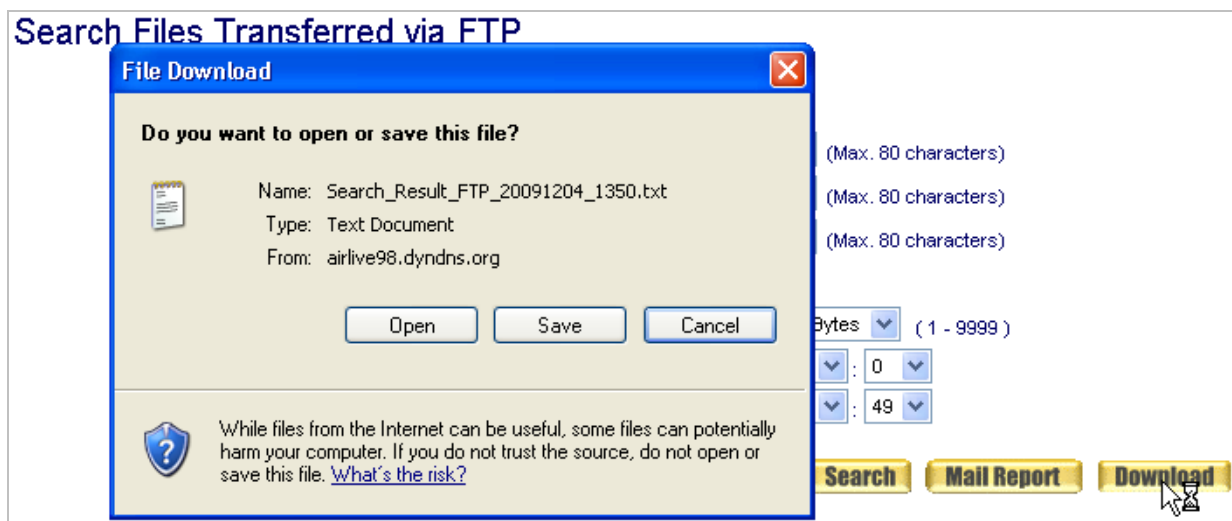


Figure 10-32 Downloading the Search Results as a ".txt" File

10.7 Telnet

Search Sessions Established via TELNET:

- Records are available if searched by criteria, such as user name, host name, session direction and date, as keyword or pattern.
 - ◆ Under **System** → **Settings**, tick **Enable email notification** and configure its related settings; and then navigate to **Record** → **Settings** → **Settings** to **Enable report hyperlinks** as well as configure its related settings. Refer to the steps below to start a search:
 1. **Username:** Type a key word from the user name.
 2. Enable the searching duration and specify a period of time to search within.
 3. Click on **Search**. (Figure 10-33)
 4. Click on **Send Report**.
 5. Mail out the search results to the designated recipient. (Figure 10-34, 35)
 6. Click on **Download Report** to download the search results as a “.txt” file onto local computer. (Figure 10-36)

Enter your search criteria :

Username : (Max. 80 characters)

IP Address :


Hostname : (Max. 100 characters)

Start a search from : 2009 / 12 / 04 00 : 00

To : 2009 / 12 / 04 14 : 17

Results

2009-12-04 (1 records) ← 1 / 1

	Date / Time	Username	Hostname	Details
<input type="checkbox"/>	12/04 14:17 -- 12/04 14:17 (0.9 min.)	JACKY	bbs.ntu.edu.tw	

← 1 / 1

Figure 10-33 Searching for a Specific Log

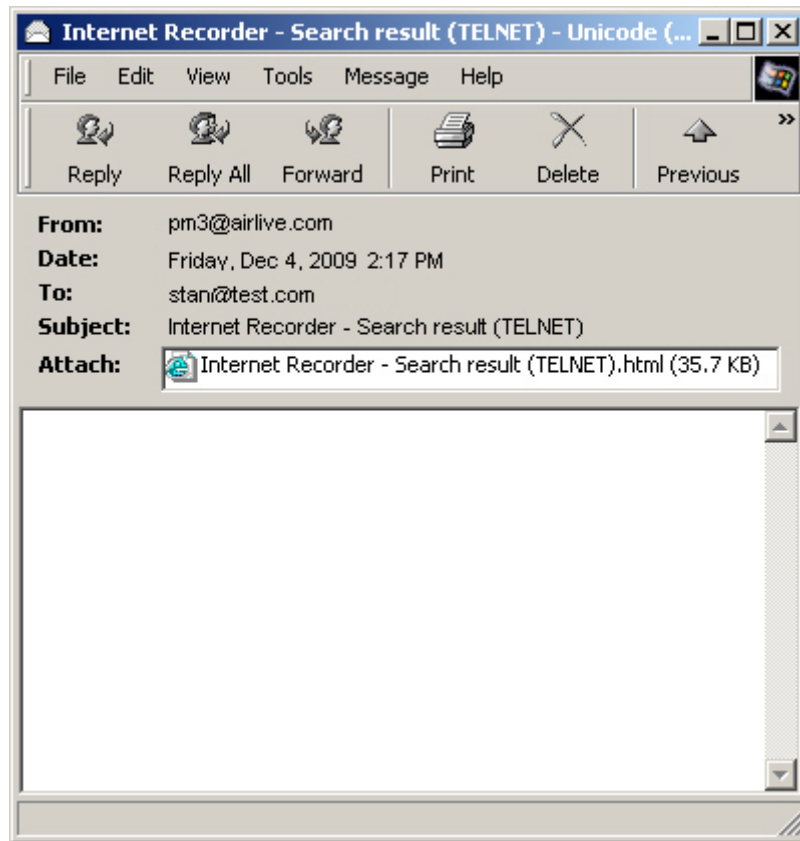



Figure 10-34 The Search Results of TELNET Attached to an Email

IAR-5000 - Search result (TELNET)			
Date / Time	Username	Hostname	Details
12/04 14:17 -- 12/04 14:17 (0.9 min.)	JACKY	bbs.ntu.edu.tw	Ⓢ

Figure 10-35 The Search Results of TELNET

 Click on the detail symbol "Ⓢ" to view the captured image of a TELNET session.

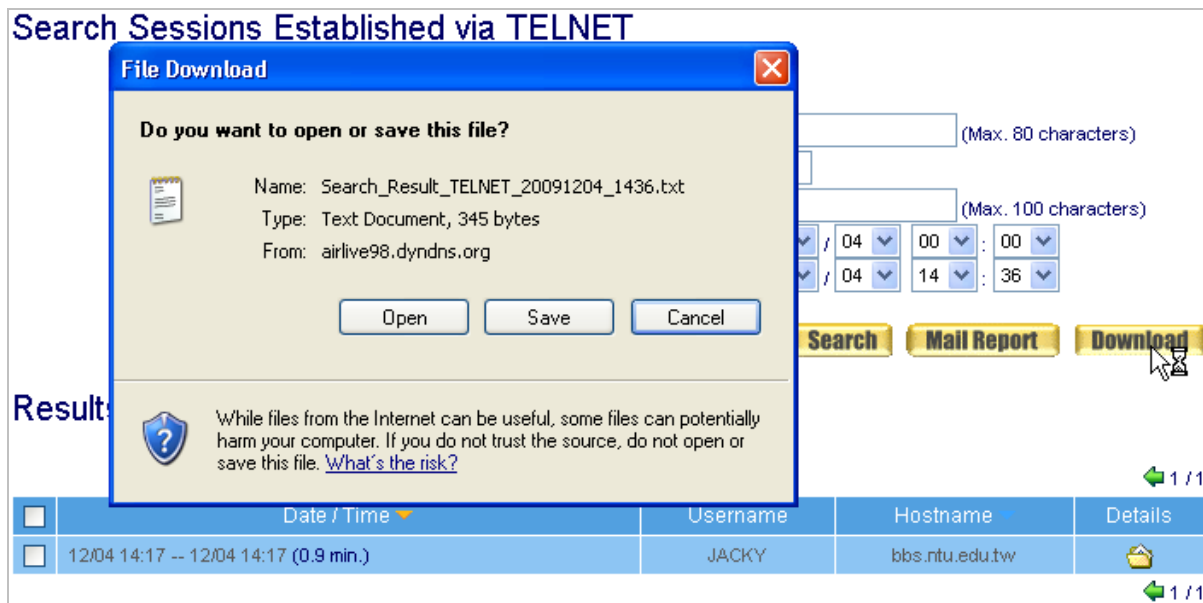


Figure 10-36 Downloading the Search Results as a ".txt" File

10.8 Custom Log

- The recording of a user's online activities via SMTP, POP3/ IMAP, HTTP, IM (MSN, Yahoo Messenger, QQ, ICQ, AIM, Skype, Gadu-Gadu), Web SMTP, Web POP3, FTP and Telnet for a specified date is obtainable through the Custom Log.
- Records are produced based on search criteria, such as user name, host name, session direction, date, keyword or pattern.
 - ◆ Navigate to **Record** → **User** → **Logged**, click the user you want to search and choose **Custom Log**. (Figure 10-37)
 - Select all recorded services.
 - Specify a period of time to search within.
 - Click **Search**. (Figure 10-38)
 - Click **Send Report**.
 - The device will mail out the search results to the designated recipient. (Figure 10-39, 40)
 - Click on **Download Report** to download the search results as a ".txt" file onto the local computer. (Figure 10-41)

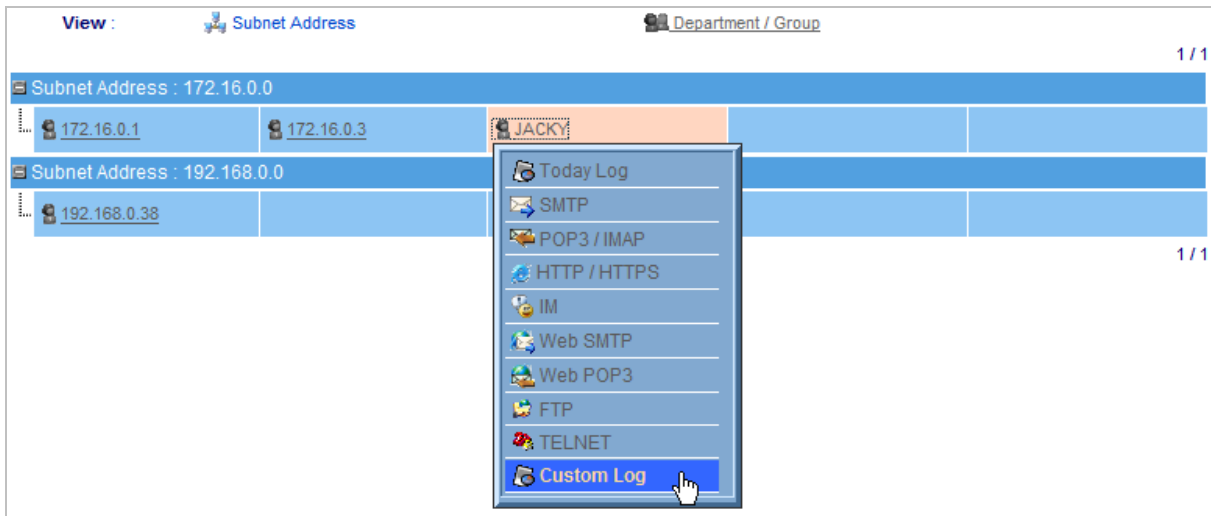


Figure 10-37 Custom Log

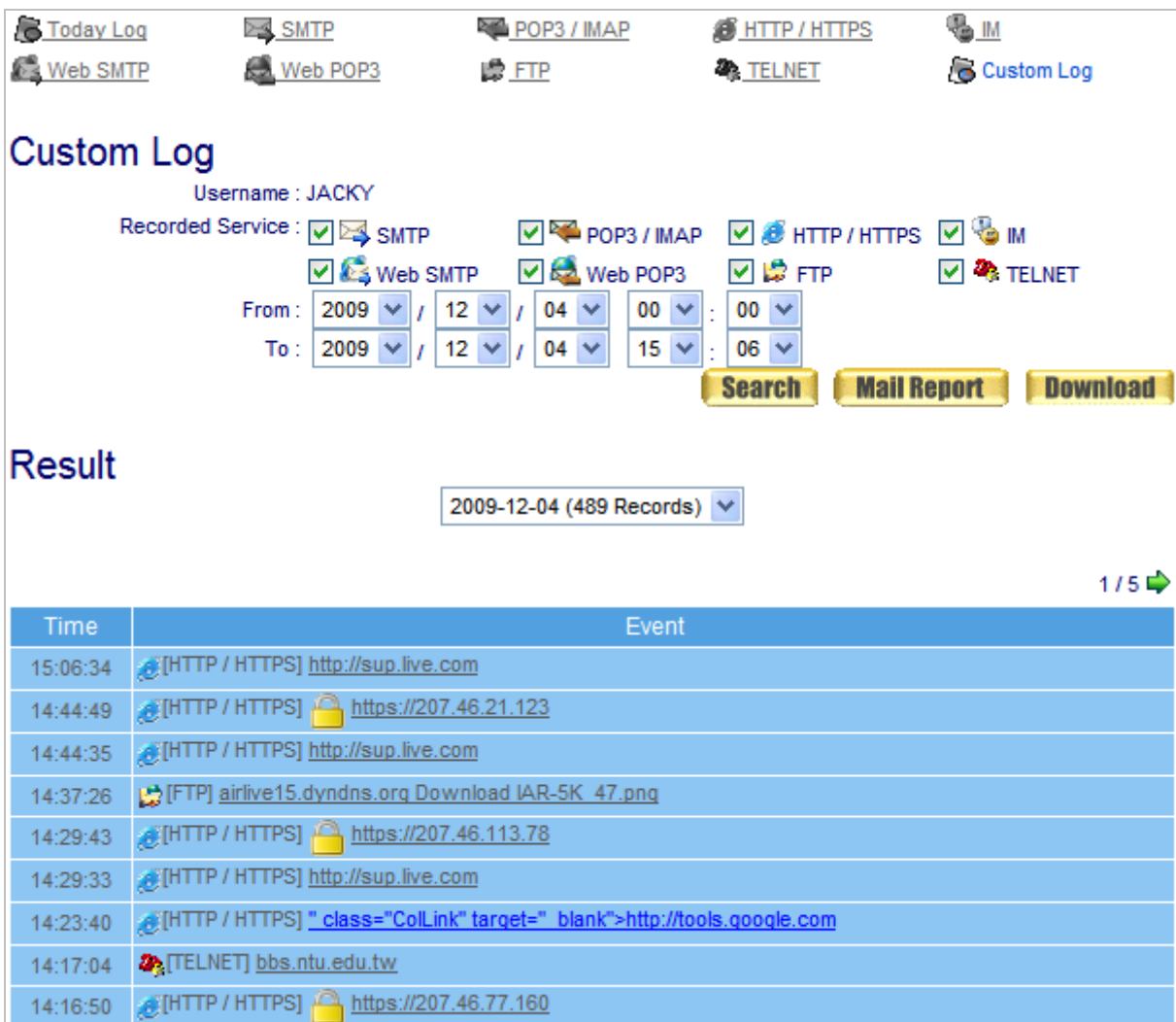


Figure 10-38 Searching for Specific Records

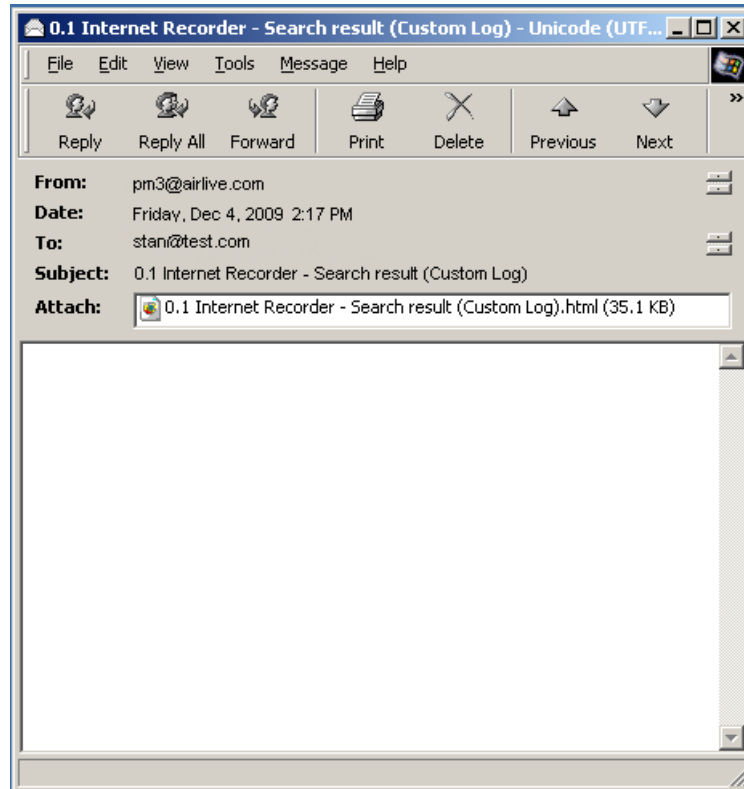


Figure 10-39 Receiving the Searching Results

IAR-5000 - Search result (Custom Log)	
JACKY	
Time	Event
12-04 15:12:46	[HTTP / HTTPS] https://207.46.113.93
12-04 15:12:45	[HTTP / HTTPS] https://207.46.113.93
12-04 15:06:34	[HTTP / HTTPS] http://sup.live.com
12-04 14:44:49	[HTTP / HTTPS] https://207.46.21.123
12-04 14:44:35	[HTTP / HTTPS] http://sup.live.com
12-04 14:37:26	[FTP] airlive15.dyndns.org Download IAR-5K_47.png
12-04 14:29:43	[HTTP / HTTPS] https://207.46.113.78
12-04 14:29:33	[HTTP / HTTPS] http://sup.live.com
12-04 14:23:40	[HTTP / HTTPS] " class="ColLink" target=" blank">http://tools.google.com
12-04 14:17:04	[TELNET] bbs.ntu.edu.tw
12-04 14:16:50	[HTTP / HTTPS] https://207.46.77.160

Figure 10-40 Custom Searching Results

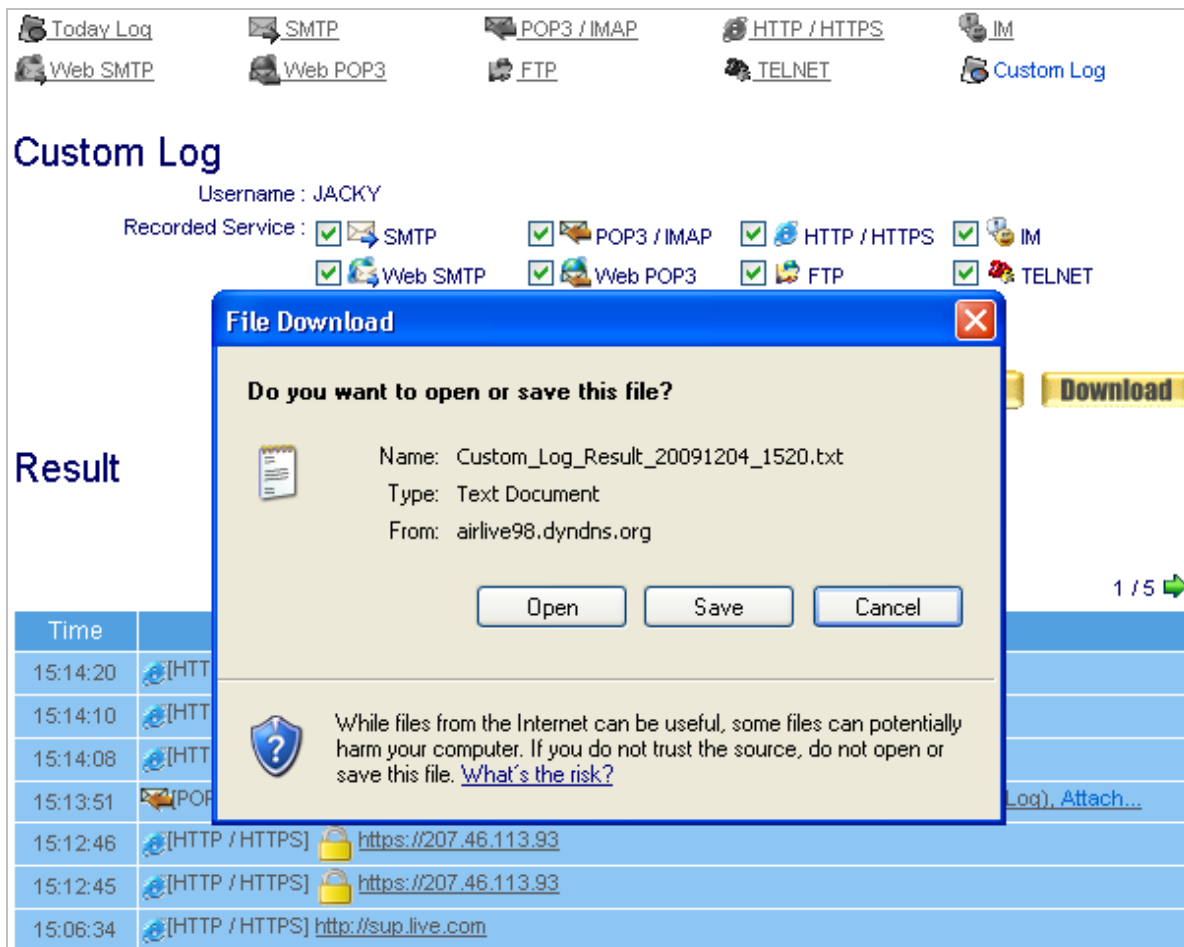





Figure 10-41 Downloading the Records

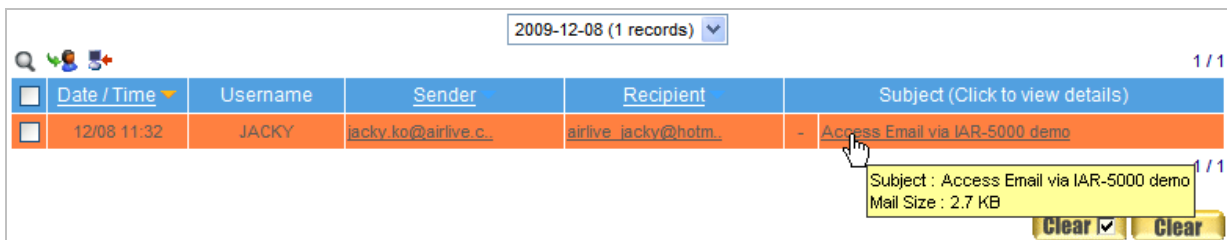
11

Record: Access Record

11.1 Accessing Emails Sent via SMTP Protocol

Navigate to **Record** → **Service** → **SMTP** to obtain the details of user's using SMTP protocol.

- To view an archived email, click on the desirable email subject. (Figure 11-1)
- Then it displays the content of the email. (Figure 11-2)
- To retrieve an archived email, tick the corresponding box and then click on  (**Forward**) at the top of the chart icon.
- Designate both the sender and recipient email address in the **Retrieve Mail** window, and then click on **OK**.
- The email is sent to the assigned recipient. (Figure 11-3)
- To remove unwanted emails, tick the corresponding boxes and then click on  icon.
- Click on **OK** to confirm to remove selected emails.
- The selected emails are removed. (Figure 11-4)
- To clean up emails by date, click on  in the lower right corner.
- Define the date and click on **OK** to confirm to clean up emails.
- All emails (SMTP logs) are cleaned up. (Figure 11-5)



2009-12-08 (1 records) ▾					
<input type="checkbox"/>	Date / Time ▾	Username	Sender	Recipient	Subject (Click to view details)
<input type="checkbox"/>	12/08 11:32	JACKY	jacky_ko@airlive.c_	airlive_jacky@hotmail_	- Access Email via IAR-5000 demo

Subject : Access Email via IAR-5000 demo
 Mail Size : 2.7 KB

Figure 11-1 Click on the Desirable Email to View

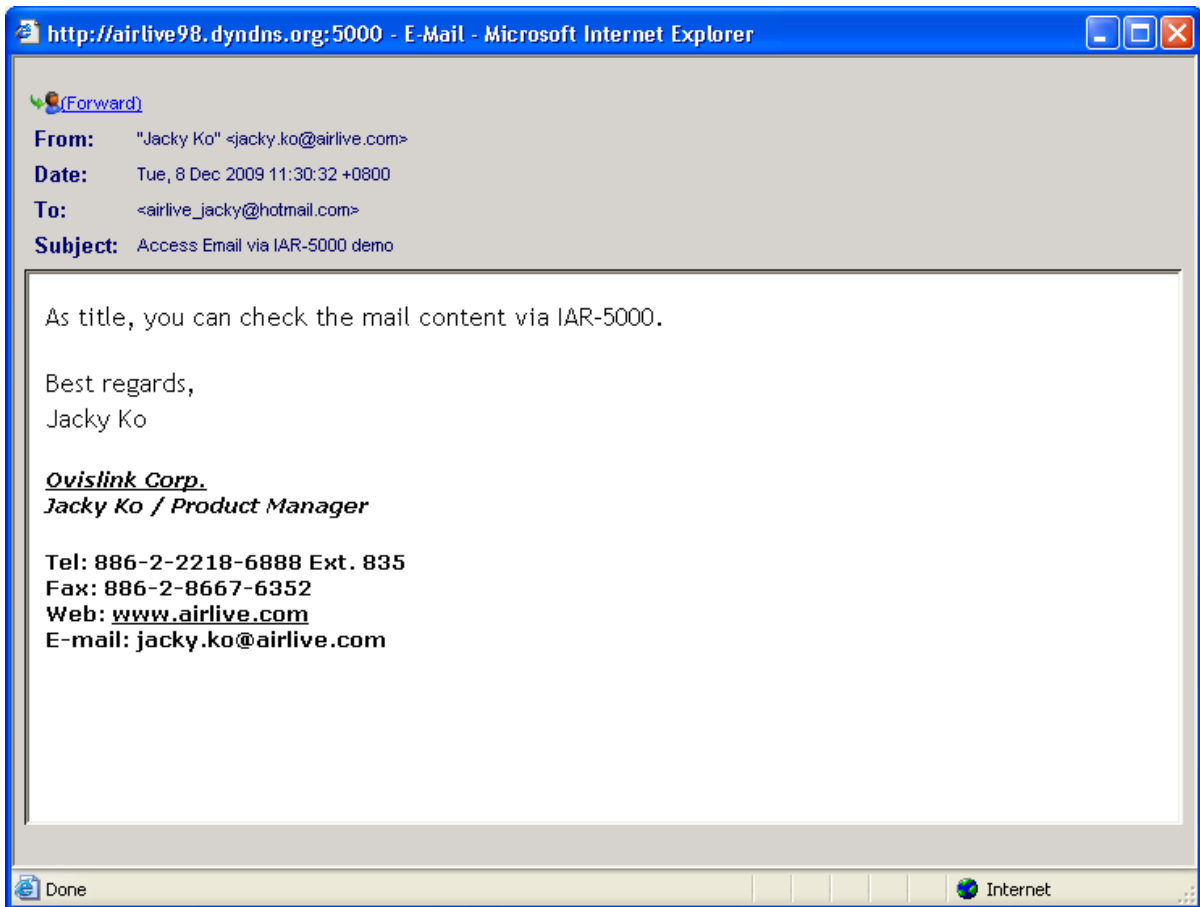



Figure 11-2 An Archived Email

 This window offers users not only a view of email content but also the function to forward the email or to save the attachment.

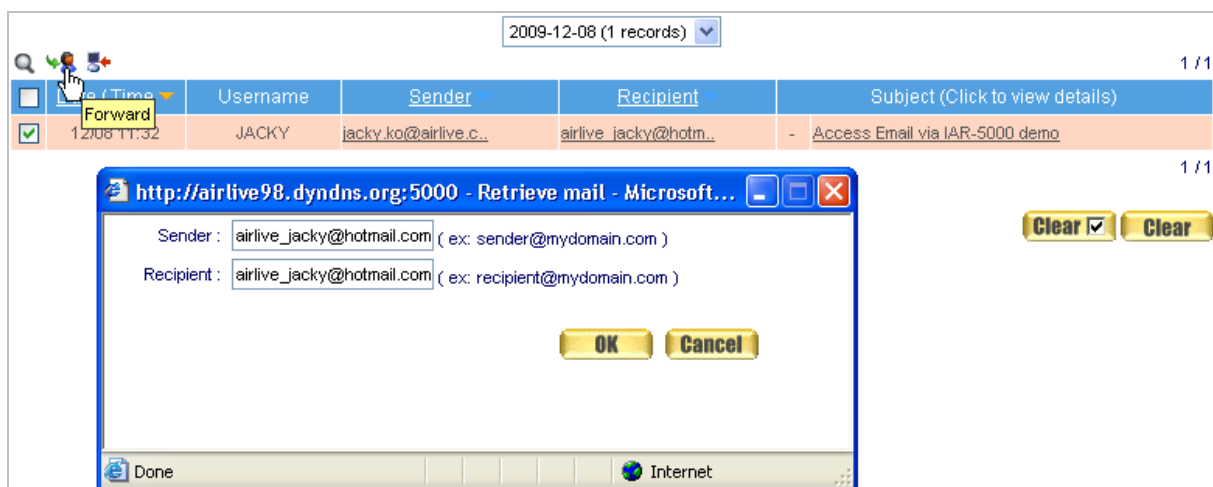


Figure 11-3 Configuring to Retrieve the Archived Email

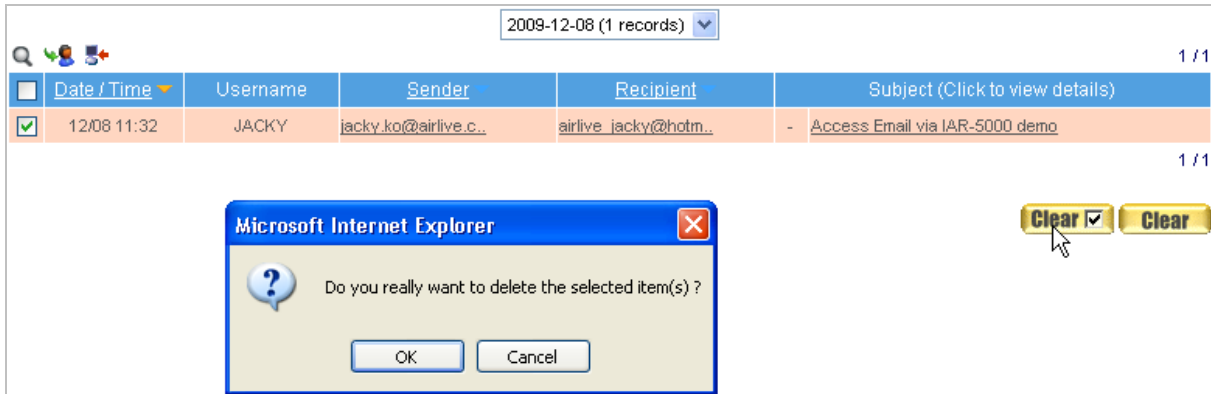


Figure 11-4 Confirming to Remove the Selected Email

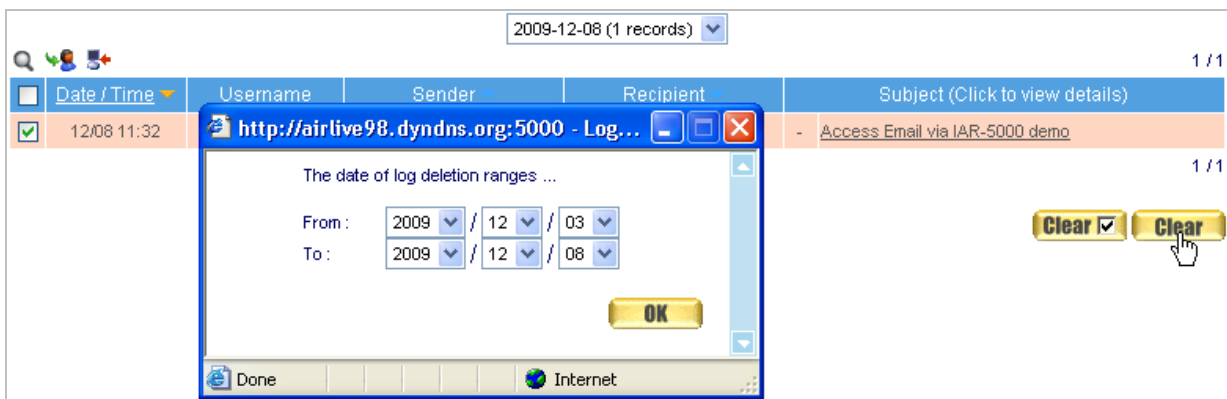




Figure 11-5 Confirming the date of log deletion ranges



To import emails from MS Outlook (including Outlook Express) or other email applications:

- Click on  to import the emails. (Figure 11-6)
- In the Email Import Settings window, specify the location and file extension of the messages file. (Figure 11-7)
- Emails are chronologically archived according to their sending or receiving time.
- The imported emails can be located under **Record** → **Service** → **SMTP**. (Figure 11-8, 9)

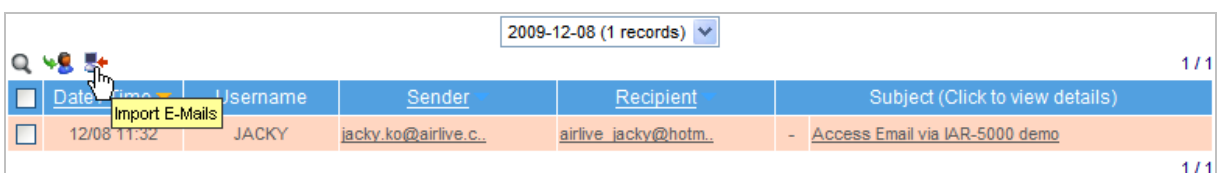


Figure 11-6 Click on the Symbol to Import Email Messages

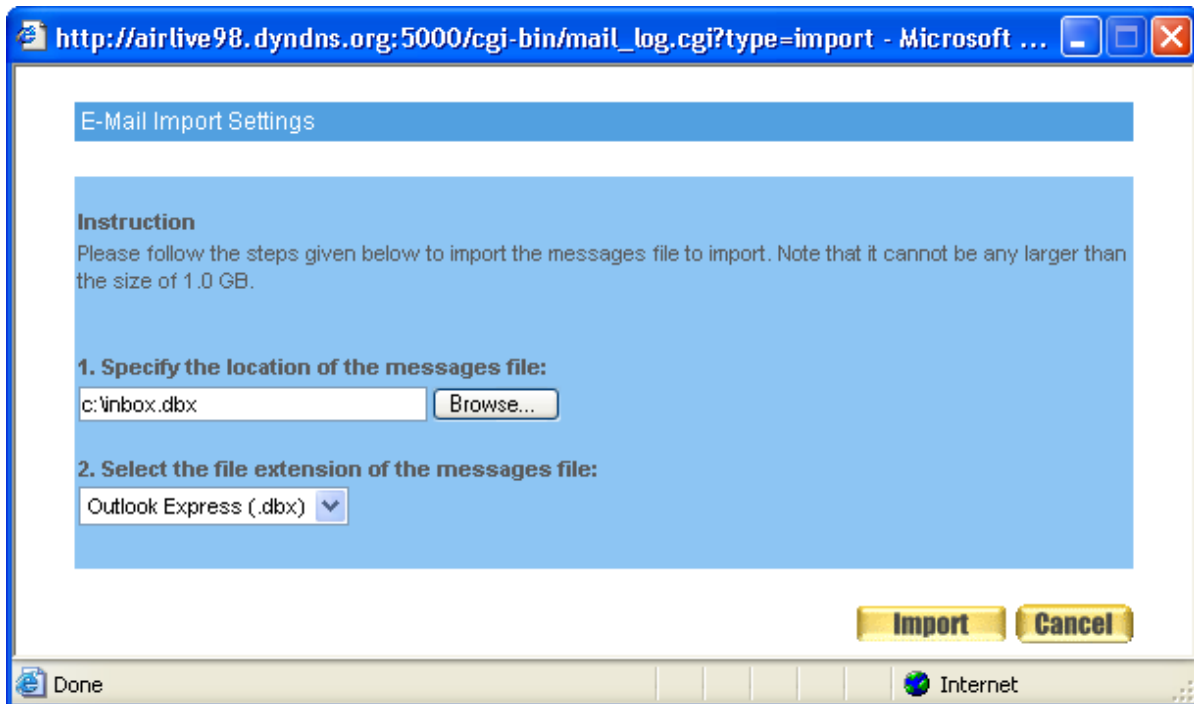


Figure 11-7 Importing a Messages File

2009-12-04 (4 records) ▼				
Date / Time	Username	Sender	Recipient	Subject (Click to view details)
12/04 15:25	---	test@airlive.com	jacky.ko@airlive.c...	- test

Figure 11-8 Imported Email Messages

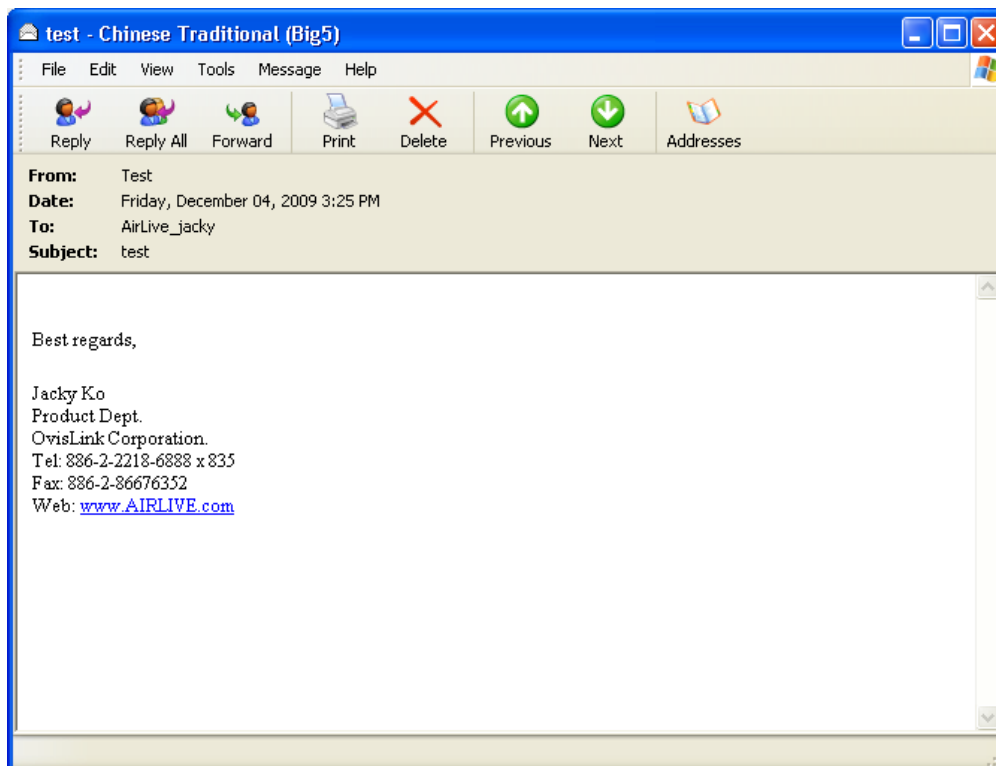





Figure 11-9 Reading the Imported Email

11.2 Accessing Emails Sent via POP3/IMAP Protocol

Navigate to **Record** → **Service** → **POP3/IMAP** to obtain the details of user's using POP3/IMAP protocol.

- To view an archived email, click on the desirable email subject. (Figure 11-10)
- Then it displays the content of the email. (Figure 11-11)
- To retrieve an archived email, tick the corresponding box and then click on  (**Forward**) at the top of the chart icon.
- Designate both the sender and recipient email address in the **Retrieve Mail** window, and then click on **OK**.
- The email is sent to the assigned recipient. (Figure 11-12)
- To remove unwanted emails, tick the corresponding boxes and then click on  icon.
- Click on **OK** to confirm to remove selected emails.
- The selected emails are removed. (Figure 11-13)
- To clean up emails by date, click on  in the lower right corner.
- Define the date and click on **OK** to confirm to clean up emails.
- All emails (POP3 / IMAP logs) are cleaned up. (Figure 11-14)

2009-12-08 (1 records) ▾					
<input type="checkbox"/>	Date / Time ▾	Username	Sender	Recipient	Subject (Click to view details)
<input type="checkbox"/>	12/08 12:05	JACKY	leo_chen@airlive.c_	jacky_ko@airlive.c_	- Re: outgoing mail server

Subject : Re: outgoing mail server
 Mail Size : 3.9 KB



 

Figure 11-10 Click on the Desirable Email to View

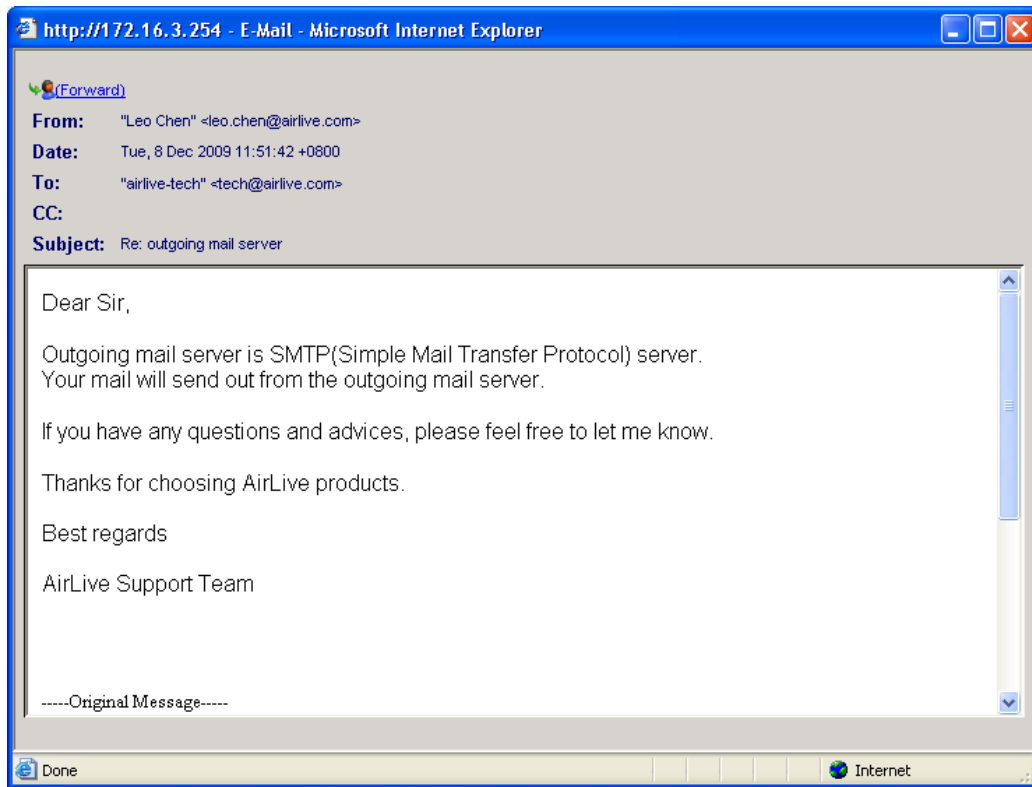



Figure 11-11 An Archived Email



This window offers users not only a view of email content but also the function to forward the email or to save the attachment.

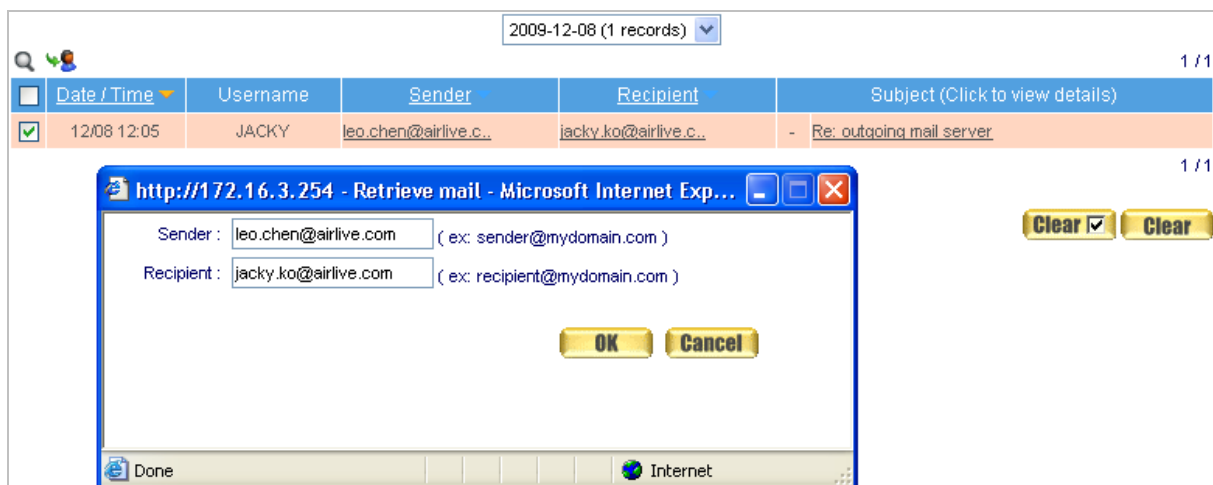


Figure 11-12 Configuring to Retrieve the Archived Email

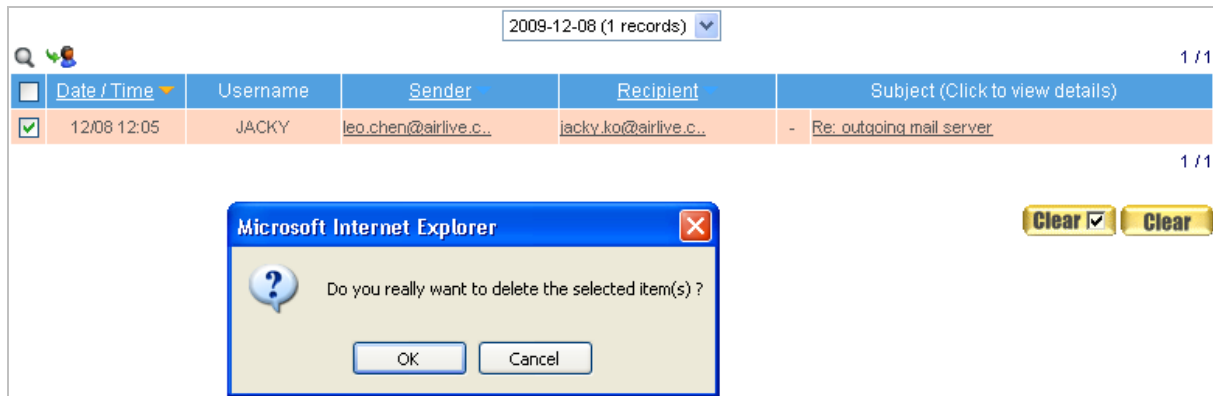


Figure 11-13 Confirming to Remove the Selected Email

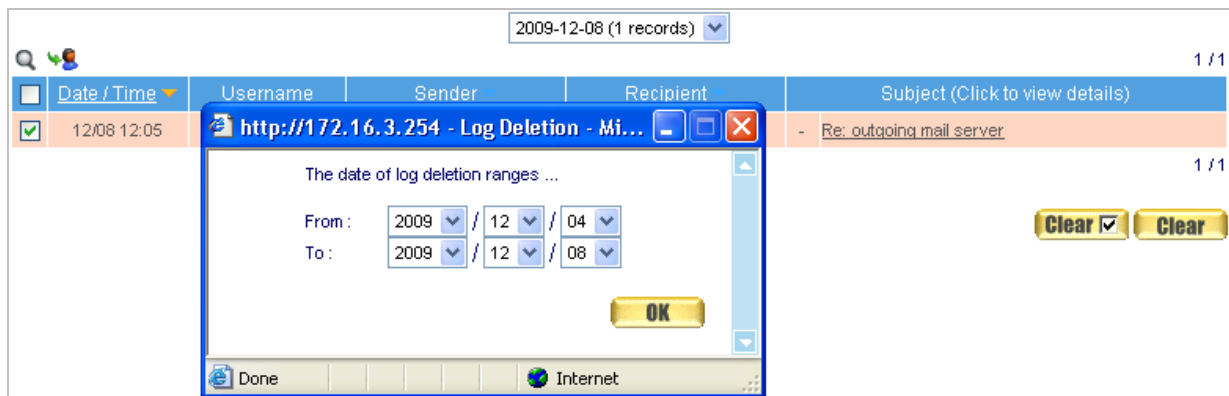


Figure 11-14 Confirming the date of log deletion ranges

11.3 Accessing Visited Webpages via HTTP Protocol

Navigate to **Record** → **Service** → **HTTP** to obtain the details of user's using HTTP protocol.

- To view a visited page, click on the desirable page. (Figure 11-15)
- Then it displays the visited page. (Figure 11-16)
- To remove unwanted visited pages, tick the corresponding boxes and then click on **Clear** icon.
- Click on **OK** to confirm to remove selected visited pages.
- To clean up visited pages by date, click on **Clear** in the lower right corner.
- Define the date and click on **OK** to confirm to clean up visited pages.
- All emails (HTTP logs) are cleaned up. (Figure 11-18)



Figure 11-15 Click on the Desirable Page to View



Figure 11-16 An Archived Page

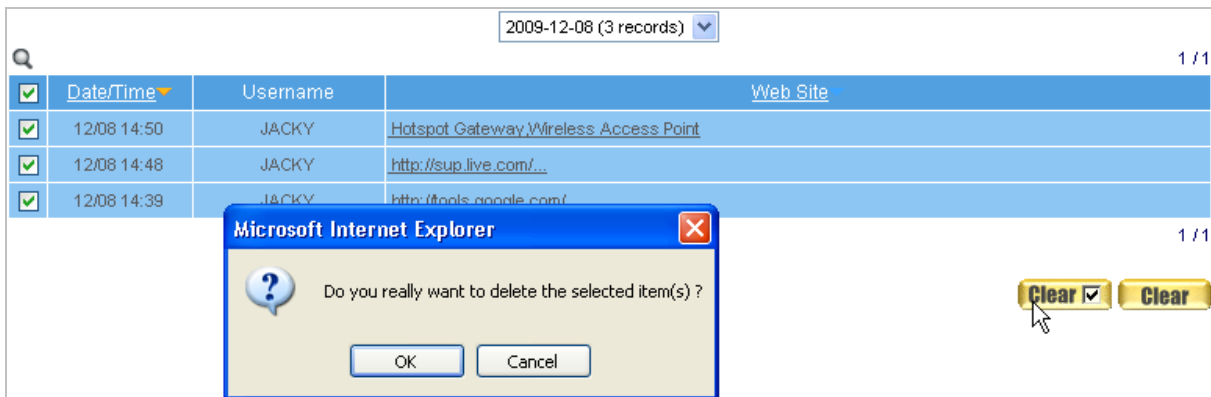


Figure 11-17 Confirming to Remove the Selected Pages

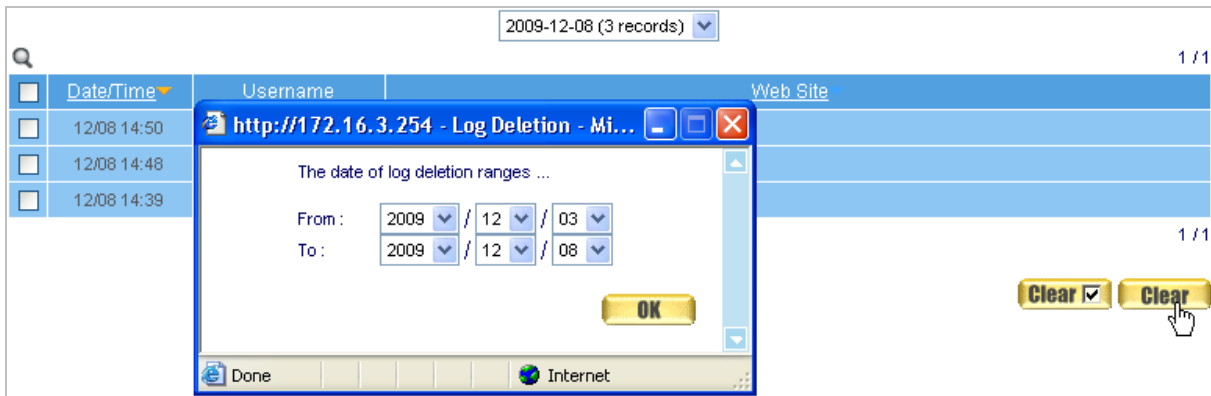


Figure 11-18 Confirming the date of log deletion ranges

11.4 Accessing Details of an IM Conversation

Navigate to **Record** → **Service** → **IM** to obtain the details of user's using instant messaging applications.

- Click on the corresponding total message entries on the right to access to the history messages. (Figure 11-19)
- Then it displays the conversation between the two participants. (Figure 11-20)
- To remove unwanted conversations, tick the corresponding boxes and then click on **Clear** icon.
- Click on **OK** to confirm to remove selected conversations.
- The selected conversations are removed. (Figure 11-21)
- To clean up conversations by date, click on **Clear** in the lower right corner.
- Define the date and click on **OK** to confirm to clean up conversations.
- All emails (IM logs) are cleaned up. (Figure 11-22)

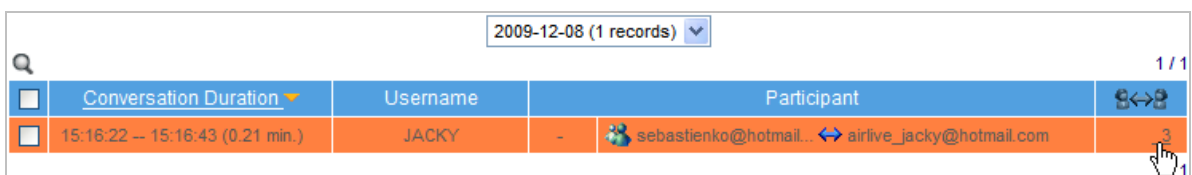


Figure 11-19 Click on the Desirable Conversation to View

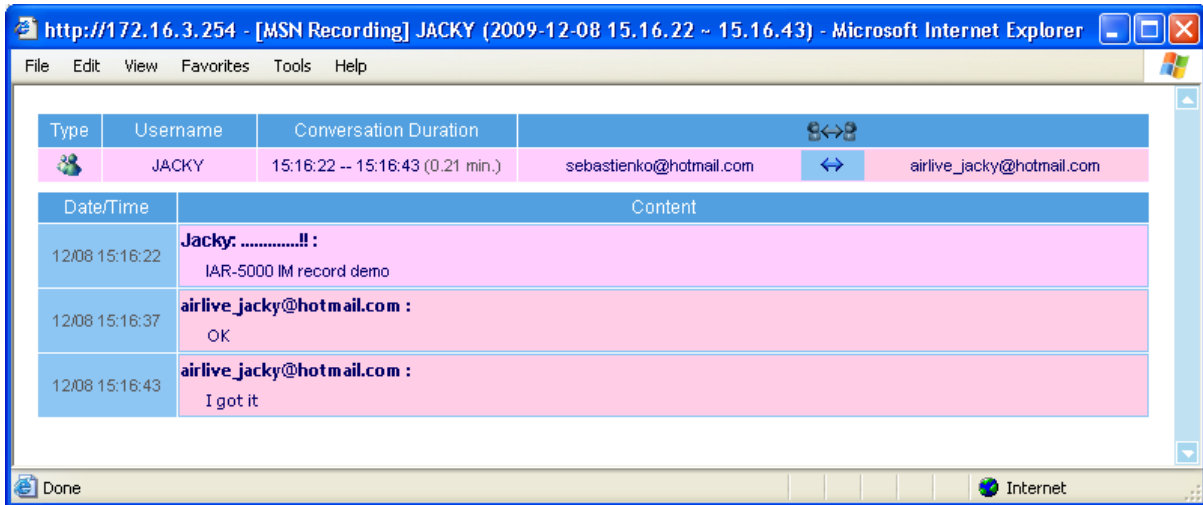


Figure 11-20 History Messages

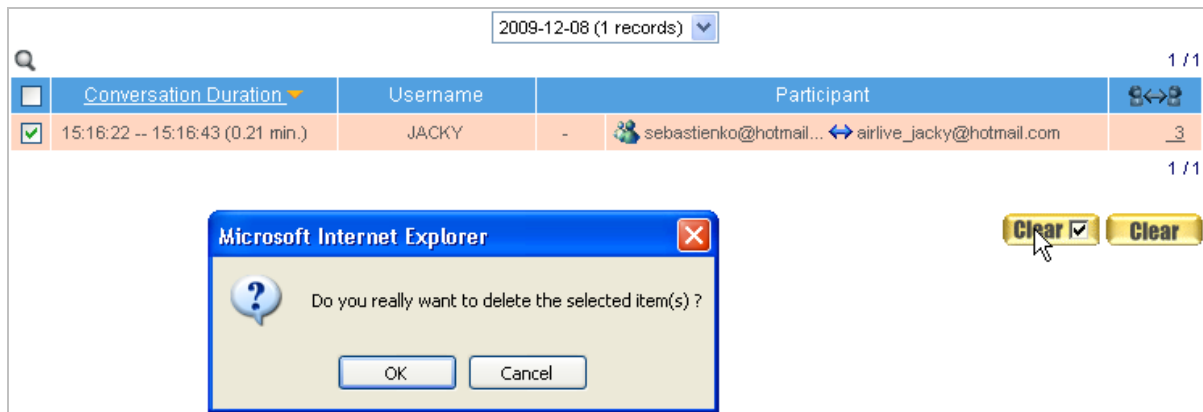


Figure 11-21 Confirming to Remove the Selected Conversations

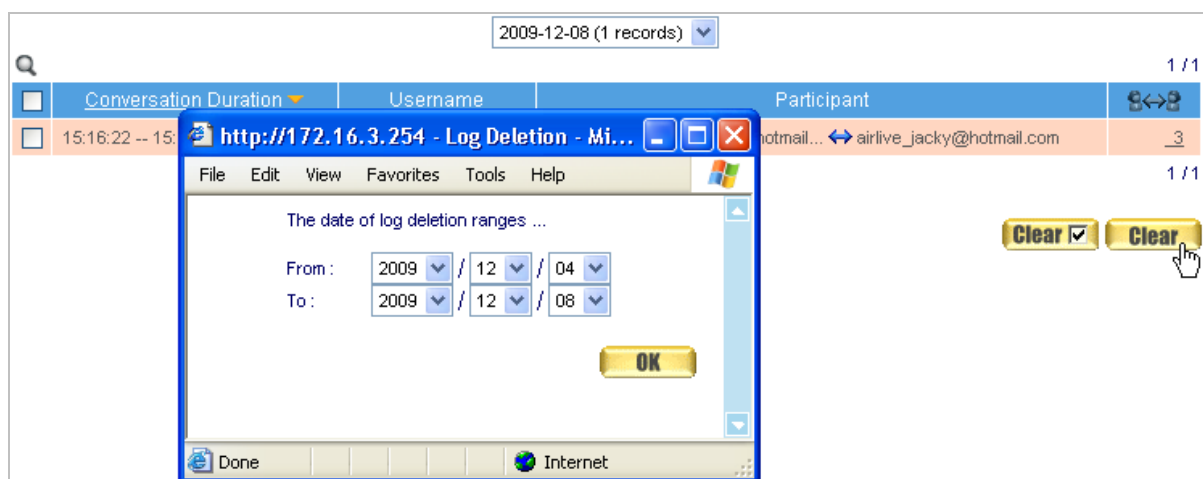




Figure 11-22 Confirming the date of log deletion ranges



Checking Skype voice conversations:

1. The symbol  indicates a voice conversation. (Figure 11-23)
2. The voice conversation can be played online or downloaded onto a local PC. (Figure 11-24, 25)

2009-12-08 (5 records) 1 / 1					
<input type="checkbox"/>	<input type="checkbox"/>	Conversation Duration	Username	Participant	
<input type="checkbox"/>	<input type="checkbox"/>	21:15:15 -- 21:43:00 (27.45 min.)	172.19.100.85	-	airlive_jacky@hotmail.. ↔ support@test.com
<input type="checkbox"/>	<input checked="" type="checkbox"/>	16:38:53 -- 16:39:33 (0.40 min.)	172.19.50.16		airlive1_testlab ↔ airtive2_testlab
<input type="checkbox"/>	<input type="checkbox"/>	16:19:13 -- 16:27:01 (7.48 min.)	172.19.20.12	-	airlive_jacky@hotmail.. ↔ chokchai_j@hotmail.com
<input type="checkbox"/>	<input type="checkbox"/>	11:12:06 -- 15:23:50 (251.44 min.)	172.19.20.12	-	airlive_jacky@hotmail.. ↔ ulisis2@hotmail.com
<input type="checkbox"/>	<input type="checkbox"/>	10:02:30 -- 10:08:40 (6.10 min.)	172.19.20.12	-	airlive_jacky@hotmail.. ↔ mailto_anuchit@chaiyo.com

1 / 1

Clear Clear

Figure 11-23 Skype Voice Conversations

Type	Username	Conversation Duration		
	172.19.50.16	16:38:53 -- 16:39:33 (0.40 min.)	airlive1_testlab	airlive2_testlab


Date/Time	Content
06/02 16:38:53	airtive2_testlab : <partlist alt=""> <part identity="airlive1_testlab"> <name>airlive1_testlab</name> </part> <part identity="airlive2_testlab"> <name>airlive2_testlab</name> </part> </partlist>
06/02 16:38:53	airtive2_testlab :  (00:00:37) (214.9 KB)

Figure 11-24 Playing the Voice Conversation

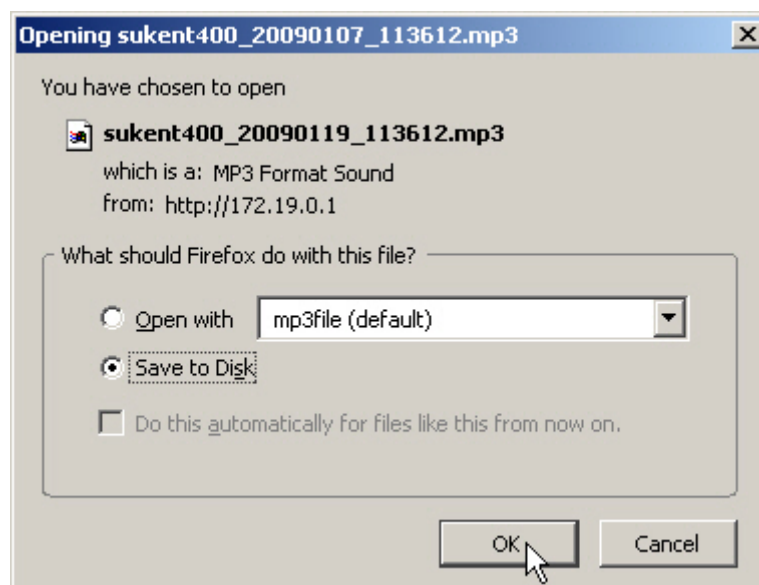


Figure 11-25 Downloading the Voice Conversation

11.5 Accessing Emails Sent via Web-Based Email Service

Navigate to **Record** → **Service** → **Web SMTP** to obtain the details of user's using Web SMTP protocol.

- To view an archived email, click on the desirable email subject. (Figure 11-26)
- Then it displays the content of the email. (Figure 11-27)
- To remove unwanted emails, tick the corresponding boxes and then click on **Clear** icon.
- Click on **OK** to confirm to remove selected emails.
- The selected emails are removed. (Figure 11-28)
- To clean up emails by date, click on **Clear** in the lower right corner.
- Define the date and click on **OK** to confirm to clean up emails.
- All emails (Web SMTP logs) are cleaned up. (Figure 11-29)

2009-12-04 (2 records) ▾					
<input type="checkbox"/>	Date / Time ▾	Username	Sender	Recipient	Subject (Click to view the content)
<input type="checkbox"/>	12/04 15:33	JACKY	sebastienko@hotmail.co..	jacky.ko@airlive.com	- FW: IAR-5000 - Search result (TELNET)
<input type="checkbox"/>	12/04 10:50	JACKY	airlive_jacky@hotmail...	jacky.ko@airlive.com	- IAR-5000 demo for WebSMTP connection

1 / 1

Clear **Clear**

Figure 11-26 Click on the Desirable Email to View

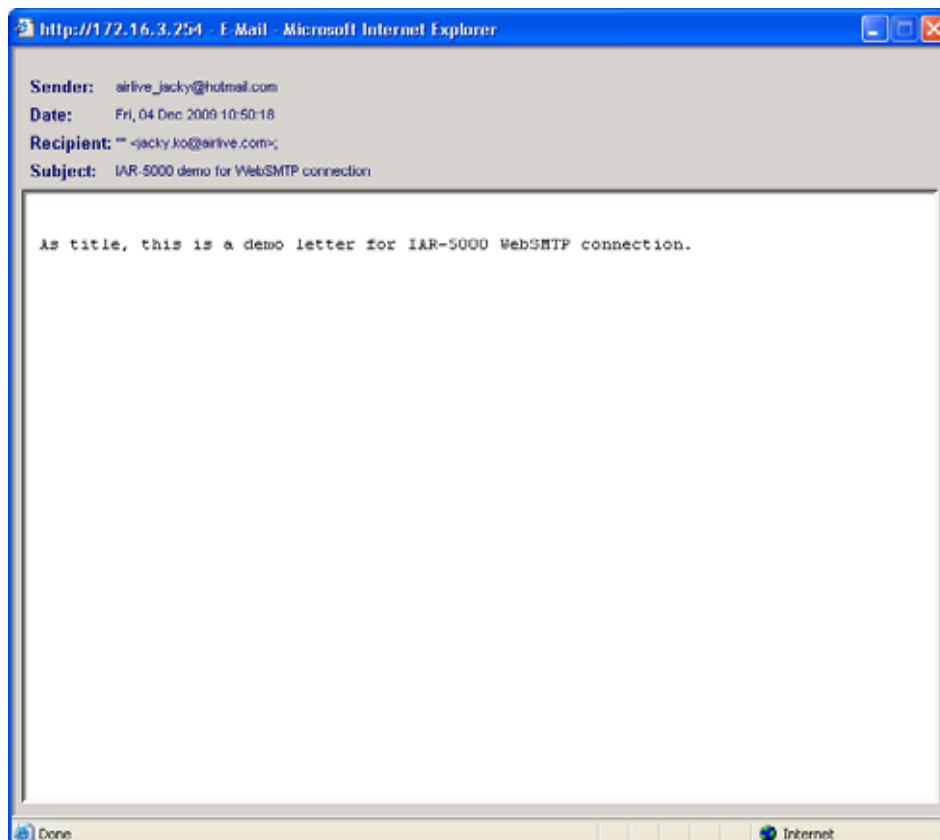


Figure 11-27 An Archived Email

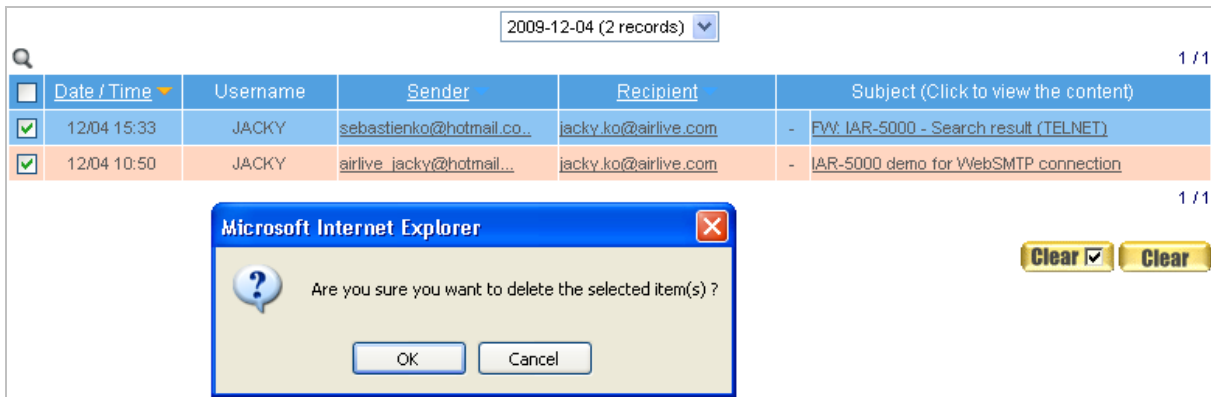
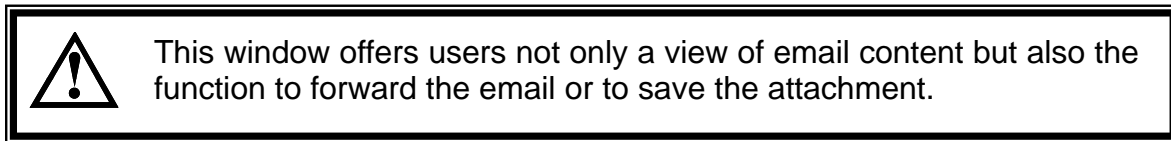


Figure 11-28 Confirming to Remove the Selected Emails

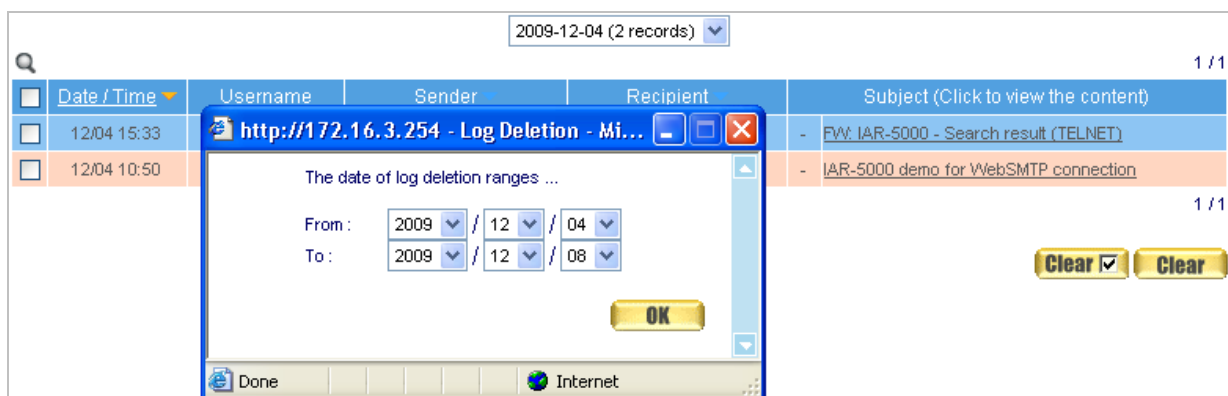




Figure 11-29 Cleaning up Archived Emails (Web SMTP Logs)

11.6 Accessing Emails Received via Web-Based Email Service

Navigate to **Record** → **Service** → **Web POP3** to obtain the details of user's using Web POP3 protocol.

- To view an archived email, click on the desirable email subject. (Figure 11-30)
- Then it displays the content of the email. (Figure 11-31)
- To remove unwanted emails, tick the corresponding boxes and then click on  icon.
- Click on **OK** to confirm to remove selected emails.
- The selected emails are removed. (Figure 11-32)
- To clean up emails by date, click on  in the lower right corner.
- Define the date and click on **OK** to confirm to clean up emails.
- All emails (Web POP3 logs) are cleaned up. (Figure 11-33)

2009-12-04 (3 records) ▾					
<input type="checkbox"/>	Date / Time ▾	Username	Sender	Recipient	Subject (Click to view the content)
<input type="checkbox"/>	12/04 17:29	JACKY	jacky.ko@airlive.c.	sebastienko@hotmail.	- IAR-5000 - Search result (SMTP..
<input type="checkbox"/>	12/04 17:11	JACKY	jacky.ko@airlive.c.	sebastienko@hotmail.	- IAR-5000 - Search result (FTP..
<input type="checkbox"/>	12/04 17:11	JACKY	jacky.ko@airlive.c.	sebastienko@hotmail.	- IAR-5000 - Search result (FTP..

Figure 11-30 Click on the Desirable Email to View

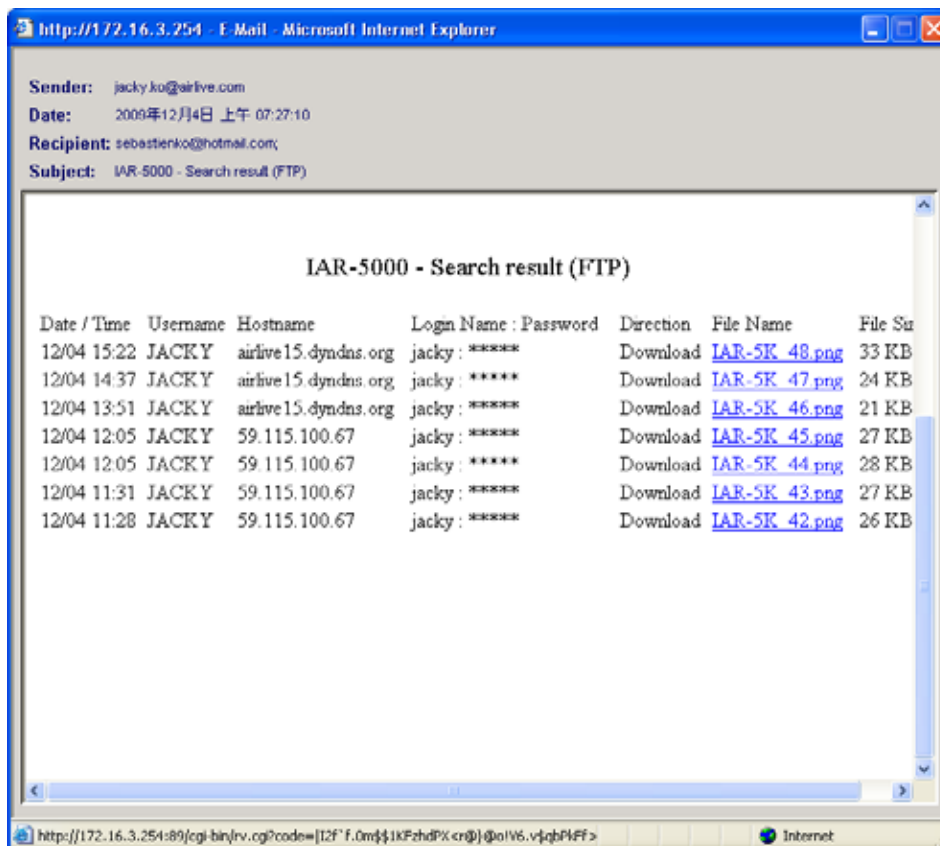


Figure 11-31 An Archived Email



This window offers users not only a view of email content but also the function to forward the email or to save the attachment.



The attachment, if any, will not be archived, provided that it had not been opened or downloaded. IAR-5000 merely records its file name for users' reference.

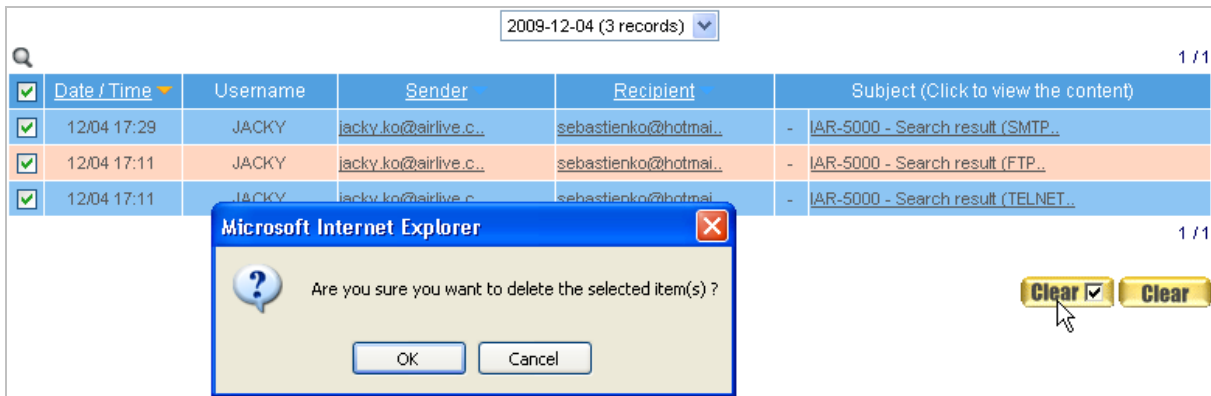


Figure 11-32 Confirming to Remove the Selected Emails

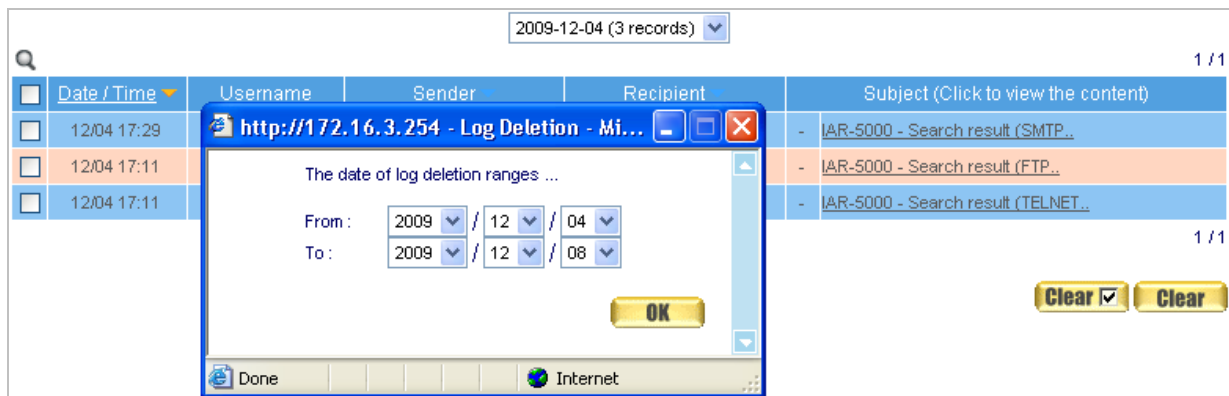




Figure 11-33 Cleaning up Archived Emails (Web POP3 Logs)

11.7 Accessing Files Transferred via FTP Protocol

Navigate to **Record** → **Service** → **FTP** to obtain the details of user's using FTP protocol.

- To open or download a transferred file, click on its file name. (Figure 11-34)
- Then a conversation box prompts you to open or save the file. (Figure 11-35)
- To remove unwanted files, tick the corresponding boxes and then click on  icon.
- Click on **OK** to confirm to remove selected files.
- The selected files are removed. (Figure 11-36)
- To clean up files by date, click on  in the lower right corner.
- Define the date and click on **OK** to confirm to clean up files.
- All emails (FTP logs) are cleaned up. (Figure 11-37)

2009-12-08 (3 records) 1/1

<input type="checkbox"/>	Date / Time	Username	Hostname	Login Name : Password	Direction	File Name	File Size
<input type="checkbox"/>	12/08 16:52	JACKY	192.168.110.1	jacky : cm4352	Download	IAR-5K_70.png	18 KB
<input type="checkbox"/>	12/08 16:52	JACKY	192.168.110.1	jacky : cm4352	Download	IAR-5K_71.png	20 KB
<input type="checkbox"/>	12/08 16:47	JACKY	192.168.110.1	jacky : cm4352	Download	IAR-5K_69.png	29 KB


1/1

Figure 11-34 Click on the File Name to Access the File

2009-12-08 (3 records) 1/1

File Download

Do you want to open or save this file?

 Name: IAR-5K_70.png
Type: PNG Image, 18.2 KB
From: 172.16.3.254

Open Save Cancel

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. [What's the risk?](#)

Direction	File Name	File Size
Download	IAR-5K_70.png	18 KB
Download	IAR-5K_71.png	20 KB
Download	IAR-5K_69.png	29 KB

1/1

Clear Clear

Figure 11-35 Saving the Archived File

2009-12-08 (3 records) 1/1

<input checked="" type="checkbox"/>	Date / Time	Username	Hostname	Login Name : Password	Direction	File Name	File Size
<input checked="" type="checkbox"/>	12/08 16:52	JACKY	192.168.110.1	jacky : cm4352	Download	IAR-5K_70.png	18 KB
<input checked="" type="checkbox"/>	12/08 16:52	JACKY	192.168.110.1	jacky : cm4352	Download	IAR-5K_71.png	20 KB
<input checked="" type="checkbox"/>	12/08 16:47	JACKY	192.168.110.1	jacky : cm4352	Download	IAR-5K_69.png	29 KB

Microsoft Internet Explorer

Do you really want to delete selected item(s)?

OK Cancel

1/1

Clear Clear

Figure 11-36 Confirming to Remove the Selected Files

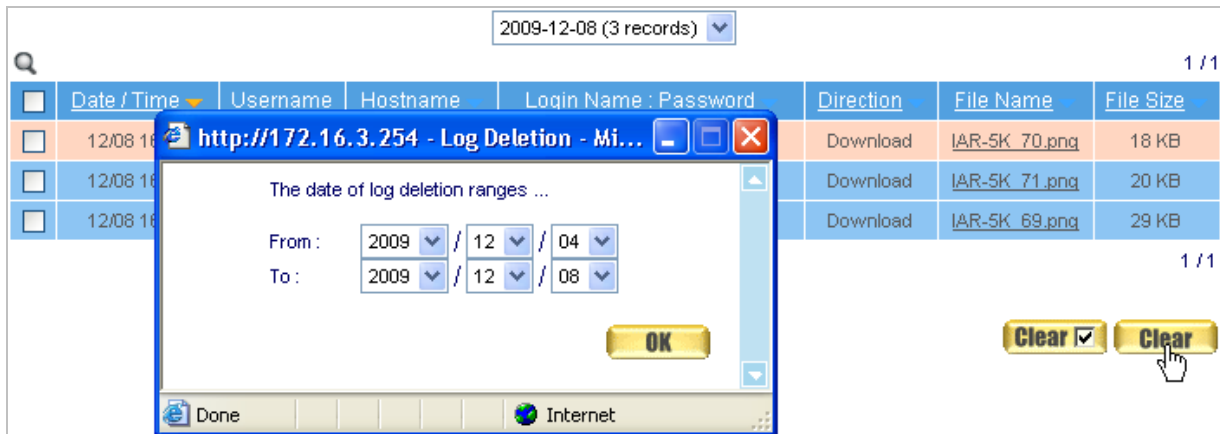


Figure 11-37 Cleaning up Archived Files (FTP Logs)

11.8 Accessing Details of Sessions Established via TELNET Protocol

Navigate to **Record** → **Service** → **Telnet** to obtain the details of user's using Telnet protocol.

- To view the details of a session, click on the **Details** icon corresponding to the desirable session. (Figure 11-38)
- Then it displays the session in details. (Figure 11-39)
- To remove unwanted session details, tick the corresponding boxes and then click on **Clear** icon.
- Click on **OK** to confirm to remove selected session details.
- The selected session details are removed. (Figure 11-40)
- To clean up session details by date, click on **Clear** in the lower right corner.
- Define the date and click on **OK** to confirm to clean up session details.
- All emails (Telnet logs) are cleaned up. (Figure 11-41)

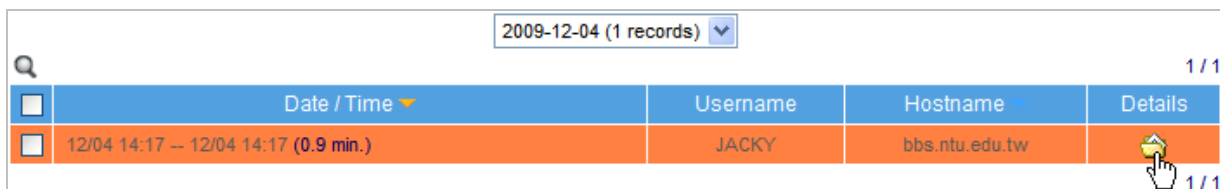


Figure 11-38 Click on the Desirable Session Details to View

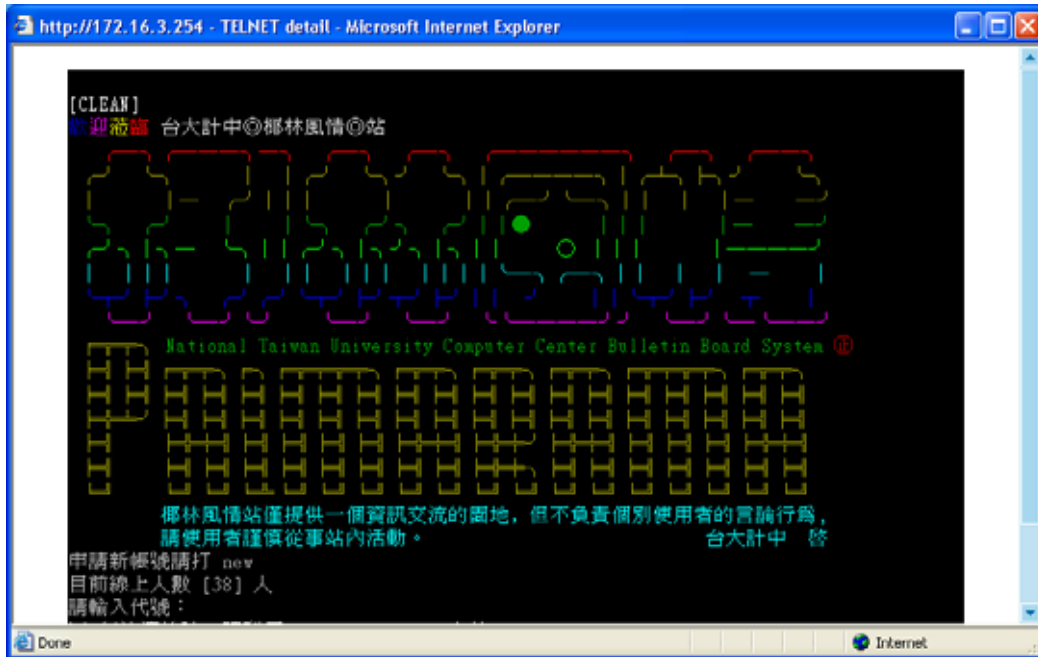


Figure 11-39 Session Log

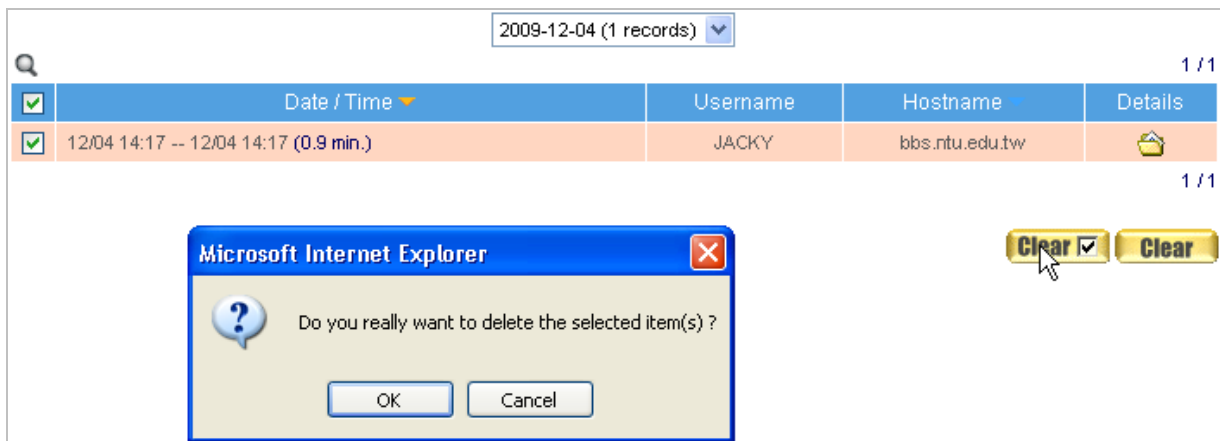


Figure 11-40 Confirming to Remove the Selected Session Log

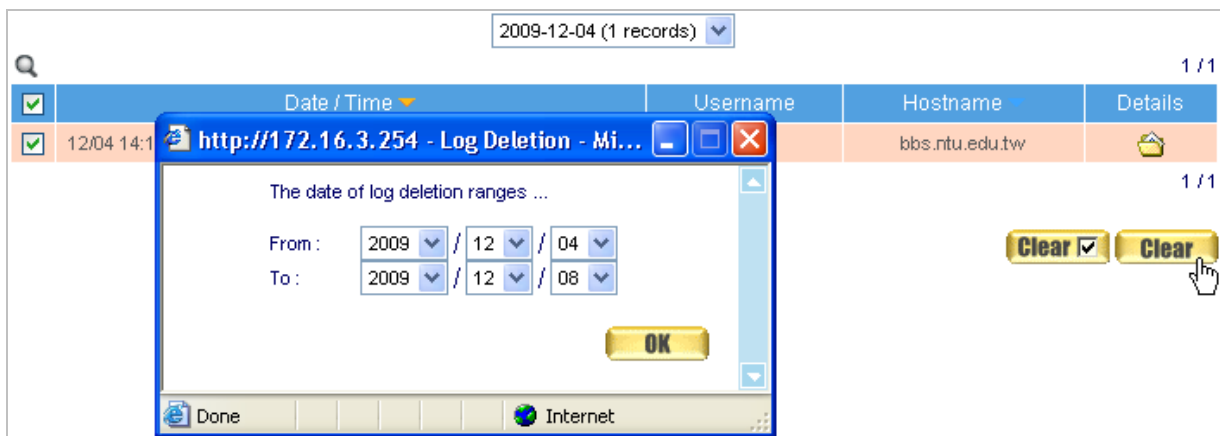


Figure 11-41 Cleaning up Session Logs (TELNET Logs)

12

Content Auditing

Internet services can be regulated through specifying inspection criteria for SMTP, POP3, HTTP, IM, Web SMTP, Web POP3, FTP and TELNET respectively; IAR-5000 allows system administrator to determine whether a service is subject to company policies.

Name:

- The name for audit rule.

Service:

- **SMTP:** When selected, IAR-5000 will inspect each SMTP session for sender, recipient, subject, content, attachment, session direction, recipient's / sender's department / group and user name. A corresponding audit report will be generated and sent to the designated recipient.
- **POP3:** When selected, IAR-5000 will inspect each POP3 session for sender, recipient, subject, content, attachment, session direction, recipient's / sender's department / group and user name. A corresponding audit report will be generated and sent to the designated recipient.
- **HTTP:** When selected, IAR-5000 will inspect each HTTP session for Web site, content, transmission direction, session direction, browser's department / group and user name. A corresponding audit report will be generated and sent to the designated recipient.
- **IM:** When selected, IAR-5000 will inspect each IM session for type, user account, participants, content, file name, auth name, session direction, participant's department / group and user name. A corresponding audit report will be generated and sent to the designated recipient.
- **Web SMTP:** When selected, IAR-5000 will inspect each Web SMTP session for sender, recipient, subject, content, attachment, session direction, recipient's / sender's department / group and user name. A corresponding audit report will be generated and sent to the designated recipient.
- **Web POP3:** When selected, IAR-5000 will inspect each Web POP3 session for sender, recipient, subject, content, attachment, session direction, recipient's / sender's department / group and user name. A corresponding audit report will be generated and sent to the designated recipient.
- **FTP:** When selected, IAR-5000 will inspect each FTP session for file name, host name, size, session direction, user's department / group and user name. A corresponding audit report will be generated and sent to the designated recipient.
- **TELNET:** When selected, IAR-5000 will inspect each TELNET session for host name, session direction, user's department / group and user name. A corresponding audit report will be generated and sent to the designated recipient.

Send Audit Report to:

- Assigns a recipient to receive the audit report.



Everyday at 00:30 a.m., the device automatically searches for logs of the previous day that meet audit criteria, and then sends a summary report to the designated recipient.



Apart from existing criteria, you may use Perl-compatible regular expressions to search for more detailed information.



Regular Expression (RE): An expression that describes a set of strings, giving a concise description without having to list all elements. The following table shows the most commonly seen characters used in regular expression:

(Reference source: <http://docs.python.org/lib/re-syntax.html>)

Character	Description
^	Matches the start of the string.
\$	Matches the end of the string or just before the newline at the end of the string. E.g., foo matches both 'foo' and 'foobar', while the regular expression foo\$ matches only 'foo'.
.	Matches any character except a newline.
\	Either takes away the special meaning of the character following it, or it is the start of a backslash or escape sequence.
*	Causes the resulting RE to match 0 or more repetitions of the preceding RE, as many repetitions as are possible. E.g., Ab* will match 'a', 'ab', or 'a' followed by any number of 'b's.
{n,m}	Matches the preceding element at least <i>n</i> and not more than <i>m</i> times. E.g., b{2,4} matches only "bb", "bbb", and "bbbb".
[]	Used to indicate a set of characters. Characters can be listed individually, or a range of characters can be indicated by giving two characters and separating them by a "-". Special characters are not active inside sets. For example, [akm\$] will match any of the characters "a", "k", "m", or "\$"; [a-z] will match any lowercase letter, and [a-zA-Z0-9] matches any letter or digit. Character classes such as \w or \S (defined below) are also acceptable inside a range. If you want to include a "]" or a "-" inside a set, precede it with a backslash, or place it as the first character. The pattern [)] will match ']', for example.
+	Causes the resulting RE to match 1 or more repetitions of the preceding RE. ab+ will match 'a' followed by any non-zero number of 'b's; it will not match just 'a'.
?	Causes the resulting RE to match 0 or 1 repetitions of the preceding RE. E.g., ab? will match either 'a' or 'ab'.

	Matches either the expression before or the expression after the operator. E.g., abc def matches "abc" or "def".
()	Allows the regular expression in the parentheses to be treated as a single unit. E.g., severity:(1 2) matches the pattern severity:1 or severity:2.

Example:

Creating the Audit Rules for Services of SMTP, POP3, HTTP, IM, Web SMTP, Web POP3, FTP and TELNET

Prior to creating audit rules, please enable "Enable report hyperlinks" and configure its related settings under **Record** → **Settings** → **Settings**.

Step1. Under **Content Auditing** → **Settings**, create an audit rule for SMTP service: (Figure 12-1)

- Click on **New Entry**.
- Type "SMTP_Audit" in the **Name** field.
- Select "SMTP" for **Service**.
- Type "[0-9a-zA-Z_-.]+@[a-zA-Z_0-9.-]+\.[a-zA-Z_0-9.-]+" in the **Content** field. (In the search of any email address)



More example for the content, "[0-9]{4}.){3}[0-9]{4}" indicates with using RE to match the content of 1234-5678-9012-3456, 1234 5678 9012 3456, 4585-4566-3792-5616, 4585 4566 3792 5616, ...

- Select "No" for **Attachment**.
- Select "All" for **Department / Group**.
- Specify a recipient in the **Send Audit Report to** field.
- Click on **OK** to complete the audit rule. (Figure 12-2)
- The device automatically searches for logs according to the criteria and generates a corresponding report. Designated recipient will be receiving the report once it is generated. (Figure 12-3, 4)

Modify Audit Rule	
Name :	SMTP_Audit (Max. 20 characters)
Service :	SMTP
Sender :	(Max. 100 characters)
Recipient :	(Max. 100 characters)
Subject :	(Max. 100 characters) Help
Content :	[0-9a-zA-Z_-.]+@[a-zA-Z_0-9.-]+\.[a-zA-Z_0-9.-]+ (Max. 100 characters) Help
Attachment :	<input checked="" type="checkbox"/> No
Attachment File Name :	(Max. 100 characters)
Department / Group :	All
Username :	(Max. 100 characters)
Send Audit Report to :	mis@airlive.com (Max. 100 characters)

Figure 12-1 Creating an Audit Rule for SMTP Service

Rule Name	Service	Send Audit Report to	Configuration
SMTP_Audit	SMTP	mis@airlive.com	<div style="text-align: right;"> Help Modify Remove </div>

Figure 12-2 The Audit Rule Created for SMTP Service

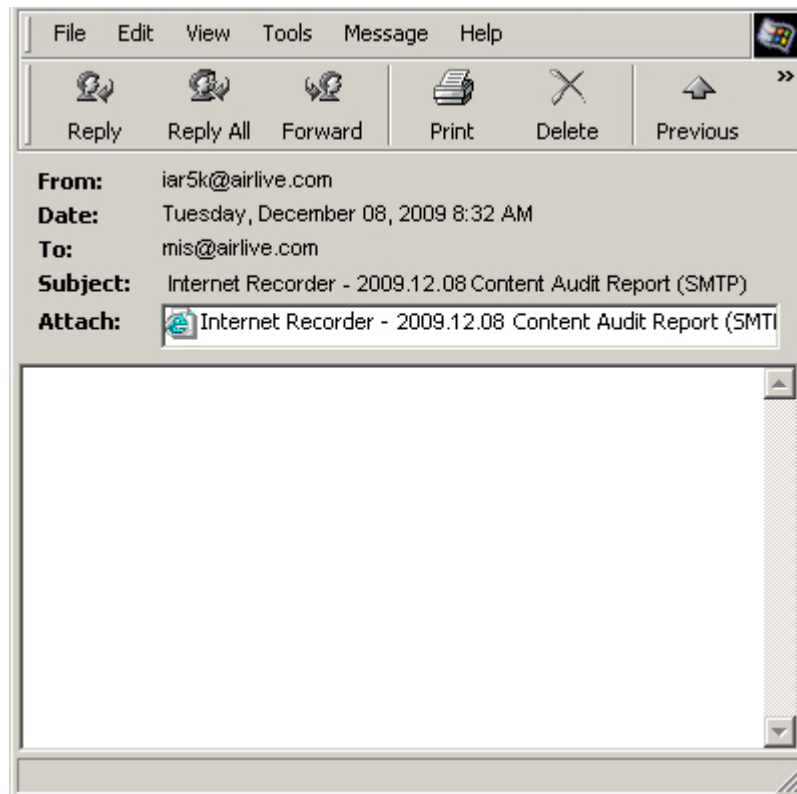


Figure 12-3 The Audit Report of SMTP Service

IAR-5000 - 2009.12.08 Content Audit Report (SMTP)				
Name :: SMTP_Audit				
Date / Time	Username :	Sender :	Recipient :	Subject :
12/08 18:52	JACKY	jacky.ko@airlive.com	airlive_jacky@hotmail..	- Demo for SMTP Content Auditing

Figure 12-4 The Audit Result of SMTP Service

Step2. Under **Content Auditing** → **Settings**, create an audit rule for POP3 service: (Figure 12-5)

- Click on **New Entry**.
- Type "POP3_Audit" in the **Name** field.
- Select "POP3" for **Service**.
- Type "[0-9a-zA-Z_.-]+@[a-zA-Z_0-9.-]+\.[a-zA-Z_0-9.-]+" in the **Content** field. (In the search of any email address)



More example for the content, "[0-9]{3}.){2}[0-9]{3}" indicates with using RE to match the content of 645-564-789, 645 564 789, 618-213-481, 618 213 481, ...

- Select "No" for **Attachment**.
- Select "All" for **Department / Group**.
- Specify a recipient in the **Send Audit Report to** field.
- Click on **OK** to complete the audit rule. (Figure 12-6)
- The device automatically searches for logs according to the criteria and generates a corresponding report. Designated recipient will be receiving the report once it is generated. (Figure 12-7, 8)

Modify Audit Rule	
Name :	POP3_Audit (Max. 20 characters)
Service :	POP3 / IMAP
Sender :	(Max. 100 characters)
Recipient :	(Max. 100 characters)
Subject :	(Max. 100 characters) Help
Content :	[0-9a-zA-Z_~]+@[a-zA-Z_0-9. (Max. 100 characters) Help
Attachment :	<input checked="" type="checkbox"/> No
Attachment File Name :	(Max. 100 characters)
Department / Group :	All
Username :	(Max. 100 characters)
Send Audit Report to :	mis@airlive.com (Max. 100 characters)

Figure 12-5 Creating an Audit Rule for POP3 Service

Rule Name	Service	Send Audit Report to	Configuration
POP3_Audit	POP3 / IMAP	mis@airlive.com	Help Modify Remove

Figure 12-6 The Audit Rule Created for POP3 Service

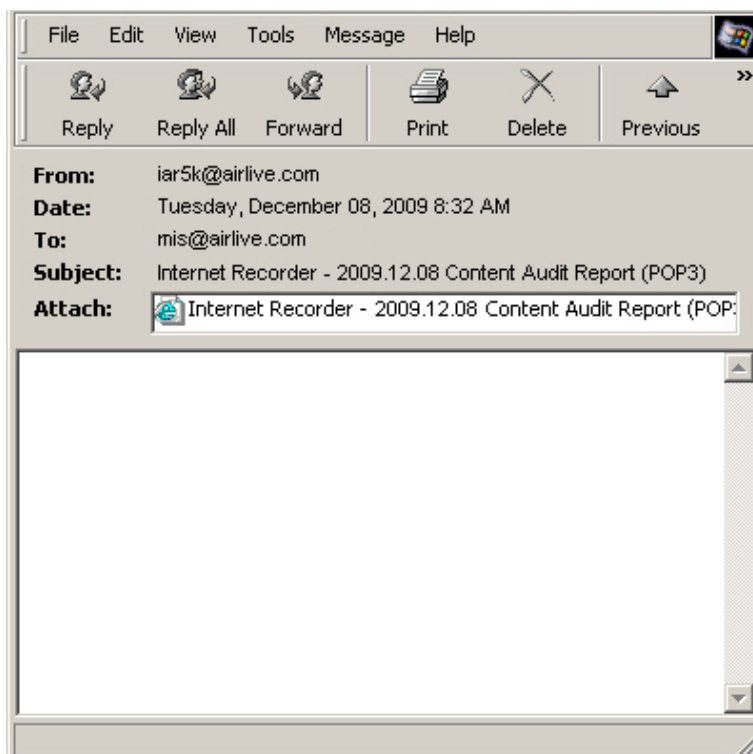


Figure 12-7 The Audit Report of POP3 Service

IAR-5000 - 2009.12.08 Content Audit Report (POP3 / IMAP)				
Name :: POP3_Audit				
Date / Time	Username :	Sender :	Recipient :	Subject :
12/08 17:25	JACKY	leo.chen@airlive.com	jacky.ko@airlive.com	- Re: MW-2000S fail-over questio..
12/08 16:49	JACKY	leo.chen@airlive.com	jacky.ko@airlive.com	- Re: MW-2000S fail-over questio..
12/08 15:23	JACKY	market@digitimes.com	jacky.ko@airlive.com	- □□□y□s□□□□□q/DIGITIMES Global..
12/08 14:58	JACKY	leo.chen@airlive.com	jacky.ko@airlive.com	- Re: Clen AUTENTIFIKATION PROB..

Figure 12-8 The Audit Result of POP3 Service

Step3. Under **Content Auditing** → **Settings**, create an audit rule for HTTP service: (Figure 12-9)

- Click on **New Entry**.
- Type “HTTP_Audit” in the **Name** field.
- Select “HTTP” for **Service**.
- Type “(yahoo|google).com” in the **Content** field. (Using RE to match the content of “www.google.com” or “www.yahoo.com”)
- Select “No” for **Attachment**.
- Select “All” for **Department / Group**.
- Specify a recipient in the **Send Audit Report to** field.
- Click on **OK** to complete the audit rule. (Figure 12-10)
- The device automatically searches for logs according to the criteria and generates a corresponding report. Designated recipient will be receiving the report once it is generated. (Figure 12-11, 12)

Modify Audit Rule	
Name :	HTTP_Audit (Max. 20 characters)
Service :	HTTP / HTTPS
Web Site :	(Max. 100 characters)
Content :	(Google yahoo).com (Max. 100 characters) Help
File Transfer :	<input type="checkbox"/> Upload <input type="checkbox"/> Download
Department / Group :	All
Username :	(Max. 100 characters)
Send Audit Report to :	mis@airlive.com (Max. 100 characters)

Figure 12-9 Creating an Audit Rule for HTTP Service

Rule Name	Service	Send Audit Report to	Configuration
HTTP_Audit	HTTP / HTTPS	mis@airlive.com	Modify Remove

Figure 12-10 The Audit Rule Created for HTTP Service

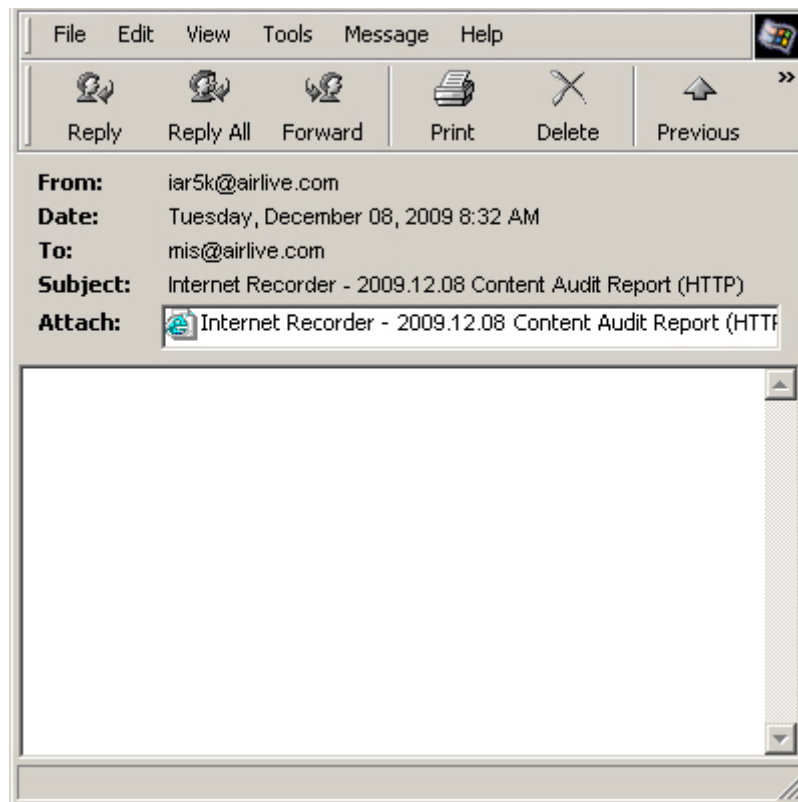


Figure 12-11 The Audit Report of HTTP Service

IAR-5000 - 2009.12.08 Content Audit Report (HTTP / HTTPS)		
Name : : HTTP_Audit		
Date / Time	Username :	Web Site
12/08 18:50	JACKY	http://tw.rd.yahoo.com/
12/08 18:50	JACKY	Google
12/08 18:50	JACKY	Yahoo! □ □ □
12/08 18:50	JACKY	http://www.yahoo.com/
12/08 18:50	JACKY	302 Moved
12/08 18:47	JACKY	Google
12/08 18:47	JACKY	302 Moved

Figure 12-12 The Audit Result of HTTP Service

Step4. Under **Content Auditing** → **Settings**, create an audit rule for IM service: (Figure 12-13)

- Click on **New Entry**.
- Type "IM_Audit" in the **Name** field.
- Select "IM" for **Service**.
- Select "All" for **IM Application**
- Type "(iar|rs|es)-?[0-9]+" in the **Content** field. (Using RE to match the content of IAR-5000, RS-3000, RS-2500, RS-1200, RS-2000, ES-4000, ES-6000...)
- Select "No" for **Attachment**.

- Select "All" for **Department / Group**.
- Specify a recipient in the **Send Audit Report to** field.
- Click on **OK** to complete the audit rule. (Figure 12-14)
- The device automatically searches for logs according to the criteria and generates a corresponding report. Designated recipient will be receiving the report once it is generated. (Figure 12-15, 16)

Create an Audit Rule	
Name :	IM_Audit (Max. 20 characters)
Service :	IM
IM Application :	All
IM Account :	(Max. 100 characters)
Participant :	(Max. 100 characters)
Content :	(iar rs es)-?[0-9]+ (Max. 100 characters) Help
Transferred File Name :	(Max. 100 characters)
Authentication Name :	(Max. 100 characters)
Department / Group :	All
Username :	(Max. 100 characters)
Send Audit Report to :	mis@airlive.com (Max. 100 characters)

Figure 12-13 Creating an Audit Rule for IM Service

Rule Name	Service	Send Audit Report to	Configuration
IM_Audit	IM	mis@airlive.com	Modify Remove

Figure 12-14 The Audit Rule Created for IM Service

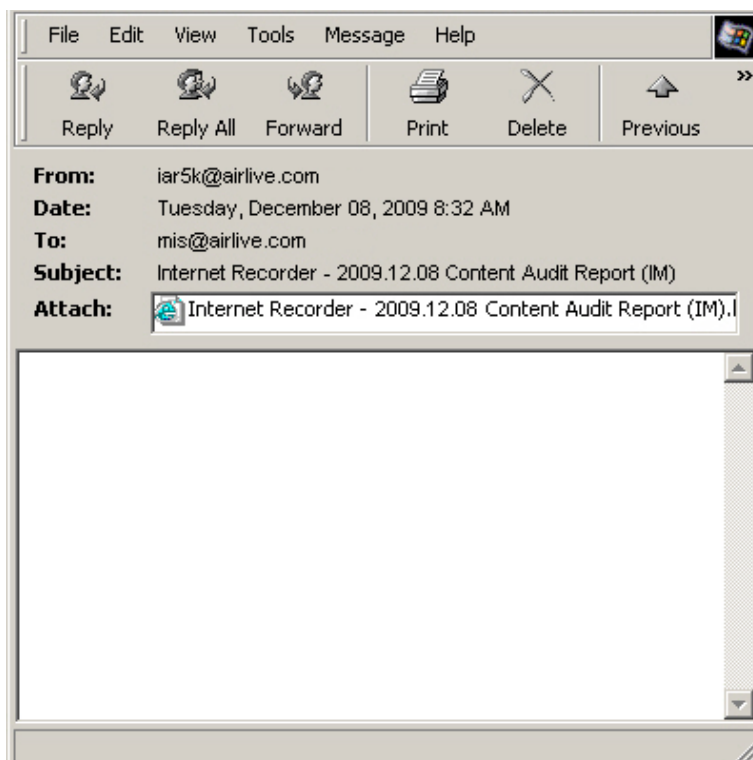


Figure 12-15 The Audit Report of IM Service

IAR-5000 - 2009.12.08 Content Audit Report (IM)			
Name : IM_Audit			
Dialogue Duration	Username :	Participant :	P↔P
12/08 15:16 -- 12/08 19:30 (254.27 min.)	JACKY	(MSN) sebastienko@hotmail... <-> airlive_jacky@hotmail..	4

Figure 12-16 The Audit Result of IM Service

Step5. Under **Content Auditing** → **Settings**, create an audit rule for Web SMTP service: (Figure 12-17)

- Click on **New Entry**.
- Type “WebSMTP_Audit” in the **Name** field.
- Select “Web SMTP” for **Service**.
- Type “[A-Z][0-9]” in the **Content** field, it indicates with using RE to match the content of A2, B368, S2693548, ...
- Select “No” for **Attachment**.
- Select “All” for **Department / Group**.
- Specify a recipient in the **Send Audit Report to** field.
- Click on **OK** to complete the audit rule. (Figure 12-18)
- The device automatically searches for logs according to the criteria and generates a corresponding report. Designated recipient will be receiving the report once it is generated. (Figure 12-19, 20)

Modify Audit Rule	
Name :	WebSMTP_Audit (Max. 20 characters)
Service :	Web SMTP
Sender :	(Max. 100 characters)
Recipient :	(Max. 100 characters)
Subject :	(Max. 100 characters) Help
Content :	[A-Z][0-9] (Max. 100 characters) Help
Attachment :	<input checked="" type="checkbox"/> No
Attachment File Name :	(Max. 100 characters)
Department / Group :	All
Username :	(Max. 100 characters)
Send Audit Report to :	mis@airlive.com (Max. 100 characters)

Figure 12-17 The Audit Result of IM Service

Rule Name	Service	Send Audit Report to	Configuration
WebSMTP_Audit	Web SMTP	mis@airlive.com	<div style="text-align: right;"> Help Modify Remove </div>

Figure 12-18 The Audit Rule Created for Web SMTP Service

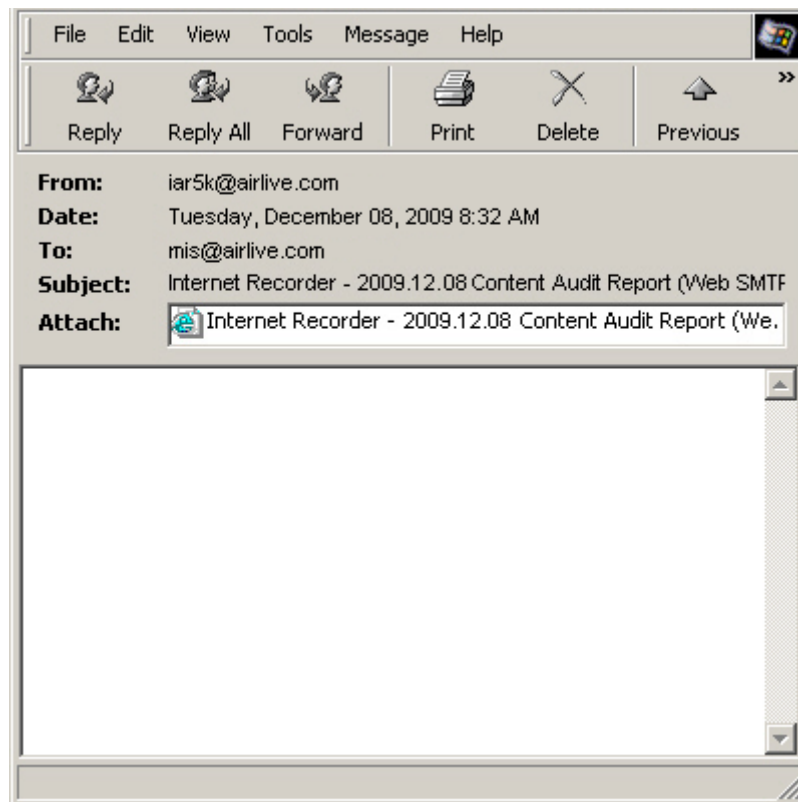


Figure 12-19 The Audit Report of Web SMTP Service

IAR-5000 - 2009.12.08 Content Audit Report (Web SMTP)				
Name :: WebSMTP_Audit				
Date / Time	Username :	Sender :	Recipient :	Subject :
12/08 17:25	JACKY_PC	jacky.ko@airlive.com	sebastienko@hotmail...	- Fw: Demo: IAR-5000 Content Aud..
12/08 16:49	JACKY_PC	jacky.ko@airlive.com	airlive_jacky@hotma..	- Fw: Demo: IAR-5000 Content Aud..
12/08 15:23	JACKY_PC	jacky.ko@airlive.com	airlive_jacky@hotmai..	- Demo: IAR-5000 Content Audit f..
12/08 14:58	JACKY_PC	jacky.ko@airlive.com	airlive_jacky@airliv..	- Demo: IAR-5000 Content Audit f..

Figure 12-20 The Audit Result of Web SMTP Service

Step6. Under **Content Auditing** → **Settings**, create an audit rule for Web POP3 service: (Figure 12-21)

- Click on **New Entry**.
- Type “WebPOP3_Audit” in the **Name** field.
- Select “Web POP3” for **Service**.
- Type “[0-9a-zA-Z_.-]+@[a-zA-Z_0-9.-]+\.[a-zA-Z_0-9.-]+” in the **Content** field. (In the search of any email address)



More example for the content, “http://.?.?.?.?.?.?.?” indicates with using RE to match the content of http://x.x., http://x.xx, http://x.xxx, http://xx.x, http://xx.xx, http://xx.xxx, http://xxx.x, http://xxx.xx, http://xxx.xxx, ...

- Select “No” for **Attachment**.
- Select “All” for **Department / Group**.
- Specify a recipient in the **Send Audit Report to** field.
- Click on **OK** to complete the audit rule. (Figure 12-22)
- The device automatically searches for logs according to the criteria and generates a corresponding report. Designated recipient will be receiving the report once it is generated. (Figure 12-23, 24)

Modify Audit Rule	
Name :	WebPOP3_Audit (Max. 20 characters)
Service :	Web POP3
Sender :	(Max. 100 characters)
Recipient :	(Max. 100 characters)
Subject :	(Max. 100 characters) Help
Content :	[0-9a-zA-Z_.-]+@[a-zA-Z_0-9. (Max. 100 characters) Help
Attachment :	<input checked="" type="checkbox"/> No
Attachment File Name :	(Max. 100 characters)
Department / Group :	All
Username :	(Max. 100 characters)
Send Audit Report to :	mis@airlive.com (Max. 100 characters)

Figure 12-21 Creating an Audit Rule for Web POP3 Service

Help			
Rule Name	Service	Send Audit Report to	Configuration
WebPOP3_Audit	Web POP3	mis@airlive.com	Modify Remove

Figure 12-22 The Audit Rule Created for Web POP3 Service

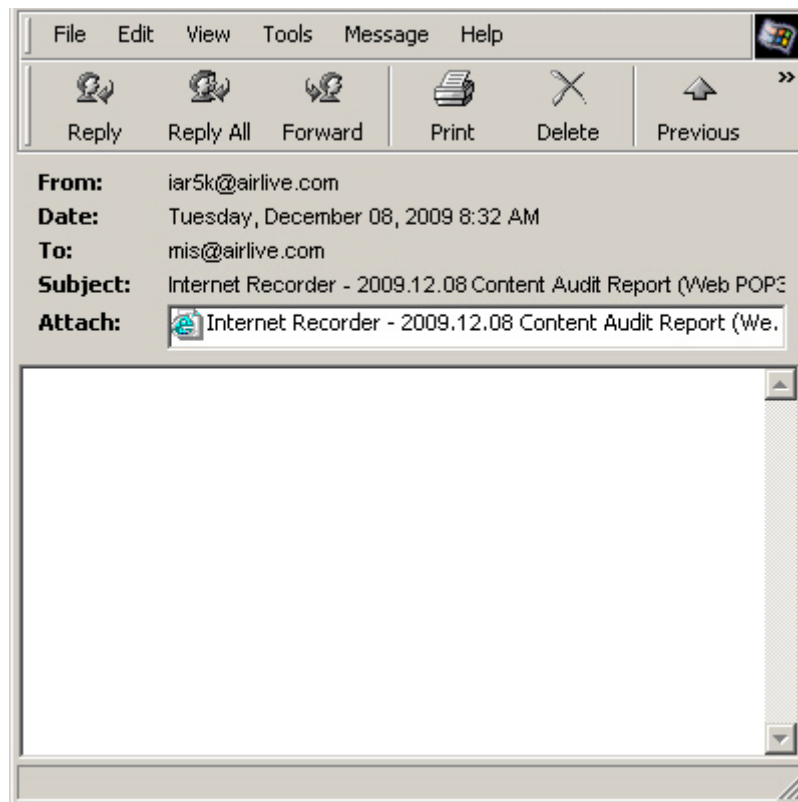


Figure 12-23 The Audit Report of Web POP3 Service

IAR-5000 - 2009.12.08 Content Audit Report (Web POP3)				
Name :: WebPOP3_Audit				
Date / Time	Username :	Sender :	Recipient :	Subject :
12/08 17:25	JACKY_PC	airlive_jacky@hotmail..	---	- RE: Demo for IAR-5000 Gmail We..
12/08 16:49	JACKY_PC	airlive_jacky@hotmail..	---	- RE: Demo for IAR-5000 Gmail We..

Figure 12-24 The Audit Result of Web POP3 Service

Step7. Under **Content Auditing** → **Settings**, create an audit rule for FTP service: (Figure 12-25)

- Click on **New Entry**.
- Type "FTP_Audit" in the **Name** field.
- Select "FTP" for **Service**.
- Select "All" for **Department / Group**.
- Specify a recipient in the **Send Audit Report to** field.
- Click on **OK** to complete the audit rule. (Figure 12-26)
- The device automatically searches for logs according to the criteria and generates a corresponding report. Designated recipient will be receiving the report once it is generated. (Figure 12-27, 28)

Modify Audit Rule	
Name :	FTP_Audit (Max. 20 characters)
Service :	FTP
Transferred File Name :	(Max. 100 characters)
Hostname :	(Max. 100 characters)
Transferred File Size:	Larger than [] Bytes [] (1 - 9999)
Department / Group :	All
Username :	(Max. 100 characters)
Send Audit Report to :	mis@airlive.com (Max. 100 characters)

Figure 12-25 Creating an Audit Rule for FTP Service

Rule Name	Service	Send Audit Report to	Configuration
FTP_Audit	FTP	mis@airlive.com	Modify Remove

Figure 12-26 The Audit Rule Created for FTP Service

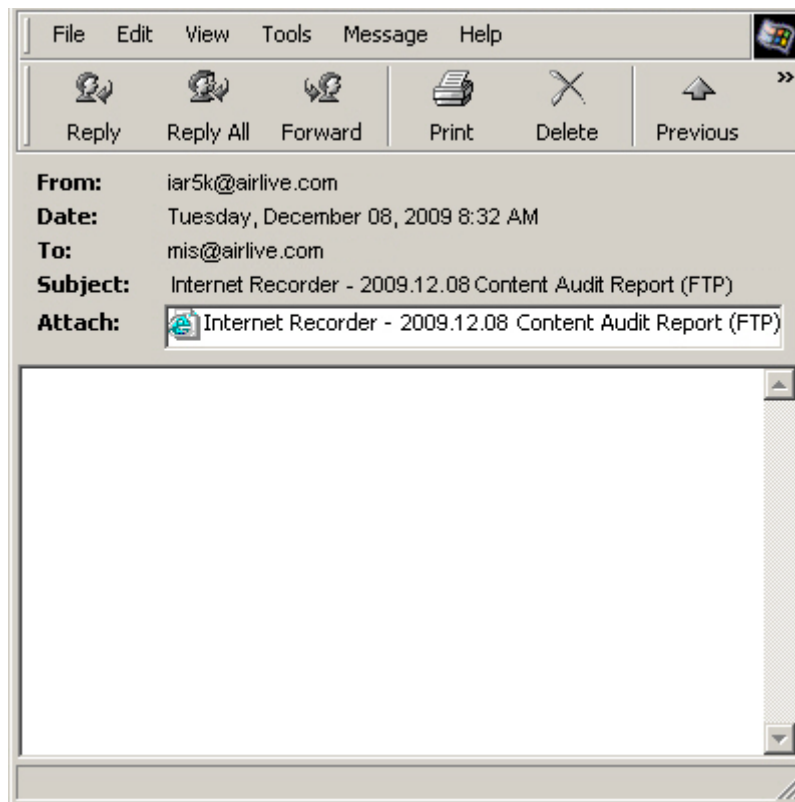


Figure 12-27 The Audit Report of FTP Service

IAR-5000 - 2009.12.08 Content Audit Report (FTP)						
Name : : FTP_Audit						
Date / Time	Username :	Hostname :	Login ID : Password	Direction	Transferred File Name :	Transferred File Size:
12/08 19:33	JACKY	192.168.110.1	jacky : *****	Download	New Text Document.txt	66 KB
12/08 17:33	JACKY	192.168.110.1	jacky : *****	Download	IAR-5K_77.png	19 KB
12/08 17:33	JACKY	192.168.110.1	jacky : *****	Download	IAR-5K_76.png	15 KB
12/08 17:33	JACKY	192.168.110.1	jacky : *****	Download	IAR-5K_75.png	21 KB
12/08 17:07	JACKY	192.168.110.1	jacky : *****	Download	IAR-5K_73.png	17 KB
12/08 17:07	JACKY	192.168.110.1	jacky : *****	Download	IAR-5K_74.png	20 KB
12/08 17:07	JACKY	192.168.110.1	jacky : *****	Download	IAR-5K_72.png	19 KB
12/08 16:52	JACKY	192.168.110.1	jacky : *****	Download	IAR-5K_71.png	20 KB
12/08 16:52	JACKY	192.168.110.1	jacky : *****	Download	IAR-5K_70.png	18 KB
12/08 16:47	JACKY	192.168.110.1	jacky : *****	Download	IAR-5K_69.png	29 KB

Figure 12-28 The Audit Report of FTP Service

Step8. Under **Content Auditing** → **Settings**, create an audit rule for TELNET service: (Figure 12-29)

- Click on **New Entry**.
- Type “Telnet_Audit” in the **Name** field.
- Select “TELNET” for **Service**.
- Select “All” for **Department / Group**.
- Specify a recipient in the **Send Audit Report to** field.
- Click on **OK** to complete the audit rule. (Figure 12-30)
- The device automatically searches for logs according to the criteria and generates a corresponding report. Designated recipient will be receiving the report once it is generated. (Figure 12-31, 32)

Modify Audit Rule	
Name :	<input type="text" value="Telnet_Audit"/> (Max. 20 characters)
Service :	<input type="text" value="TELNET"/>
Hostname :	<input type="text"/> (Max. 100 characters)
Department / Group :	<input type="text" value="All"/>
Username :	<input type="text"/> (Max. 100 characters)
Send Audit Report to :	<input type="text" value="mis@airlive.com"/> (Max. 100 characters)

Figure 12-29 Creating an Audit Rule for TELNET Service

				Help
Rule Name	Service	Send Audit Report to	Configuration	
Telnet_Audit	TELNET	mis@airlive.com	Modify	Remove

Figure 12-30 The Audit Rule Created for TELNET Service

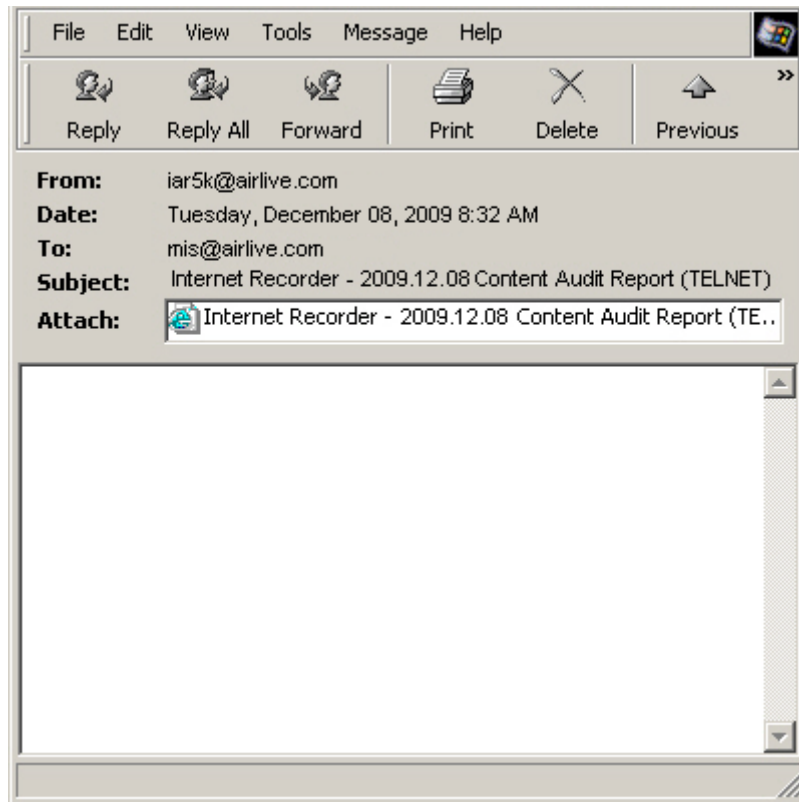


Figure 12-31 The Audit Report of TELNET Service

IAR-5000 - 2009.12.08 Content Audit Report (TELNET)			
Name : Telnet_Audit			
Date / Time	Username :	Hostname :	Detail
12/08 19:34 -- 12/08 19:34 (0.22 min.)	JACKY	bbs.ntu.edu.tw	@

Figure 12-32 The Audit Report of TELNET Service

13

Anomaly Flow IP

When the corporate network is under an attack (which causes excessive network traffic), IAR-5000 will take action to against it. Besides, by joining forces with an IDP-enabled switch, you can defend various threats from the Internet, avoiding losing revenue opportunities as a result of the network being paralyzed.

This chapter will be discussing the functionality and application of **Anomaly Flow IP**.

The threshold for anomaly sessions per IP address is ... sessions / sec

- When the number of concurrent sessions from an IP address has exceeded the threshold, IAR-5000 will treat the IP address as an anomaly flow IP. And then, block its packet transmission as well as mail out the alert notification to designated recipient.

Anomaly Flow IP Blocking

- All sessions created by an anomaly flow IP will be dropped for the sake of keeping others' Internet access available.

Email Notification

- The victim user and system administrator will both receive an alert notification through an email message or a NetBIOS broadcast when an anomaly flow occurs.

Safe IP Addresses

- Given that a local server is mistaken as an anomaly flow IP due to providing services to public, then this server is suggested to be classified as a safe IP address.

Configuring to Alerts for Anomaly Flow and Block Intrusion Packets:

Step1. Navigate to **System** → **Settings** → **Settings**, and then select **Enable email notification**. Navigate to **Anomaly Flow IP** → **Settings**, and then configure as below:

- Configure **The threshold for anomaly sessions per IP address is ... sessions / sec** accordingly. (100 by default)
- Tick **Enable anomaly flow IP blocking** and then configure the **Blocking Time (second)** accordingly. (600 by default)
- Tick **Enable email notification**.
- Tick **Enable NetBIOS notification**.
- Type "172.16.0.2" in the **IP address of system administrator** field.
- Click on **OK** to complete the settings. (Figure 13-1)

Anomaly Flow IP Settings

The threshold for anomaly sessions per IP address is sessions / sec (1 - 9999)

Enable anomaly flow IP blocking Blocking time (second) : (1 - 999)

Enable email notification

Enable NetBIOS notification IP address of system administrator :


Enable co-defense system

Switch Model :


Username :

Password :

Figure 13-1 Anomaly Flow IP Settings



To block intrusion packets, enable **co-defense system** to notify the designated switch to act against the attack.



Safe IP Addresses can be used for excluding specific IP from detection.

Step2. When a DDoS attack occurs, IAR-5000 will warn about the anomaly flow under **Anomaly Flow IP → Safe IP Addresses** or alert both the victim user and the system administrator about it through a NetBIOS broadcast. (Figure 13-2, 3, 4)

Threshold Sessions / Sec: 100			
Username	Virus-Infected IP	MAC Address	Alarm Time
JACKY_PC	172.16.0.2	00:4F:63:01:37:EA	2009-12-14 18:24:27

Figure 13-2 Virus Infected IP

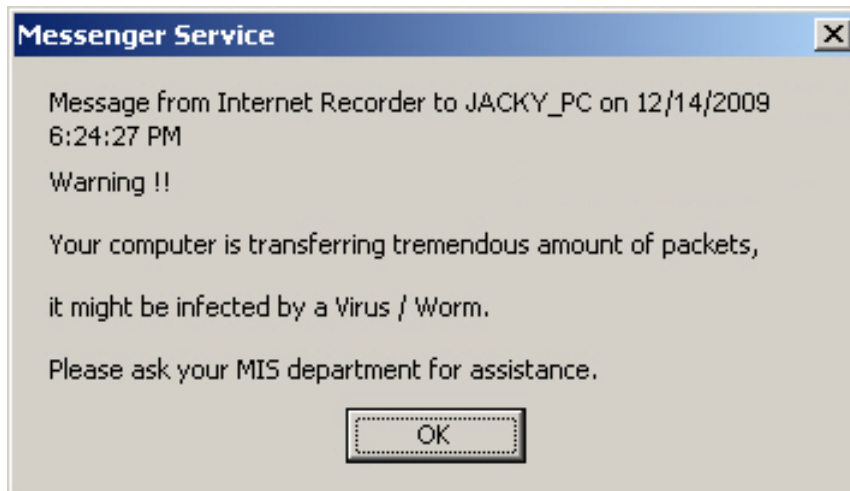


Figure 13-3 NetBIOS Broadcast Shown to the Victim User

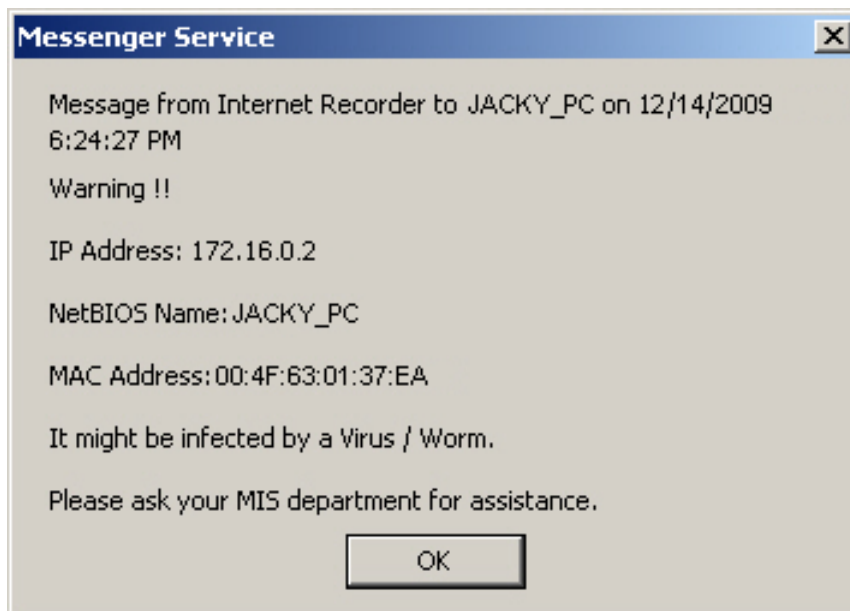


Figure 13-4 NetBIOS Broadcast Shown to the System Administrator

Step3. The figure below shows the system administrator receives the alert notification through an email message. (Figure 13-5)

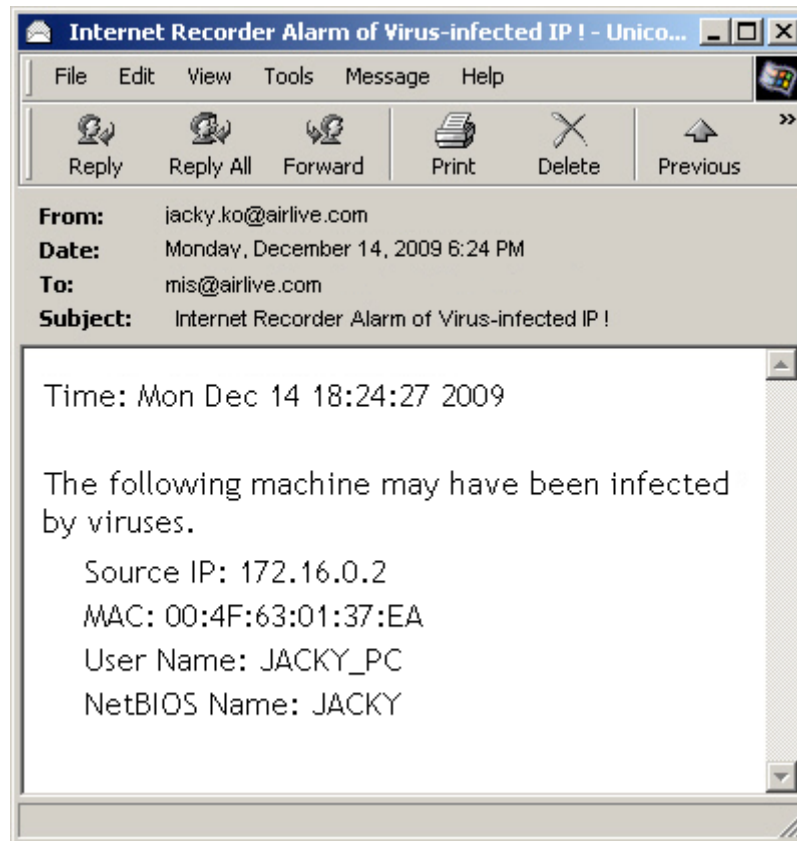


Figure 13-5 The Alert Notification Sent through an Email Message

Step4. When a DDoS attack occurs, IAR-5000 will warn about the anomaly flow under **Anomaly Flow IP** → **Intrusion IP** or alert the intruder and the system administrator about it through a NetBIOS broadcast. (Figure 13-6,7, 8)

Intrusion IP	Alarm Time
192.168.101.103	2007-10-30 14:47:34
58.10.216.188	2007-10-30 14:44:51
192.168.159.30	2007-10-30 14:23:37
192.168.169.30	2007-10-30 14:23:37
192.168.179.30	2007-10-30 14:23:37
192.168.189.30	2007-10-30 14:23:37
192.168.101.103	2007-10-30 14:22:53
58.10.216.188	2007-10-30 14:20:40
188.99.99.1	2007-10-30 14:19:36
192.168.169.1	2007-10-30 14:17:42
192.168.189.111	2007-10-30 14:17:42
192.168.10.1	2007-10-30 14:17:42
192.168.101.20	2007-10-30 14:17:41
172.29.254.254	2007-10-30 14:17:41
192.1.1.1	2007-10-30 14:16:30
192.168.3.1	2007-10-30 14:16:30
192.168.163.1	2007-10-30 14:16:30
192.168.165.1	2007-10-30 14:16:29
192.168.192.192	2007-10-30 14:16:29
192.168.41.33	2007-10-30 14:15:29

Figure 13-6 Intrusion IP Addresses

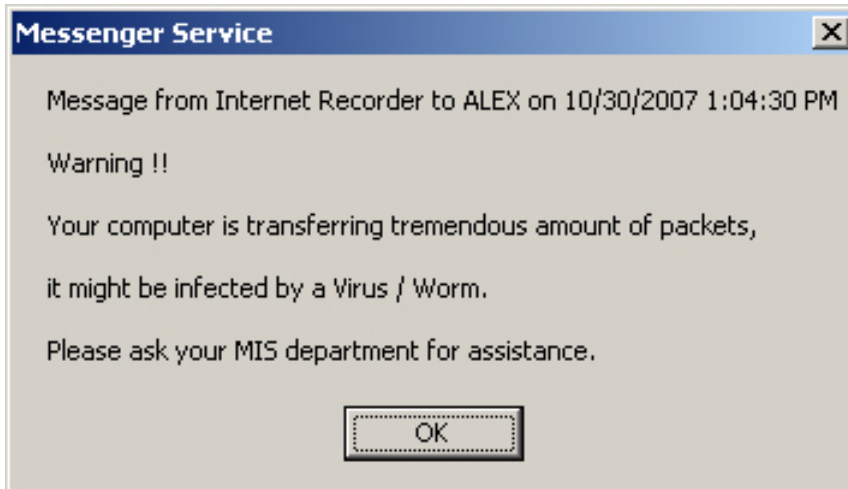


Figure 13-7 A NetBIOS Broadcast Shown to the Intruder

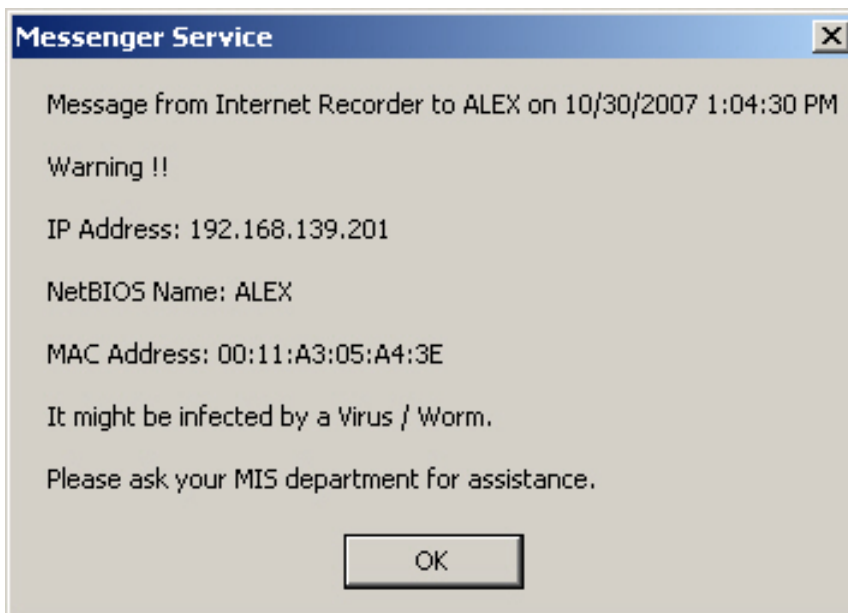


Figure 13-8 A NetBIOS Broadcast Shown to the System Administrator

Step5. The figure below shows the system administrator receives the alert notification through an email message. (Figure 13-9)

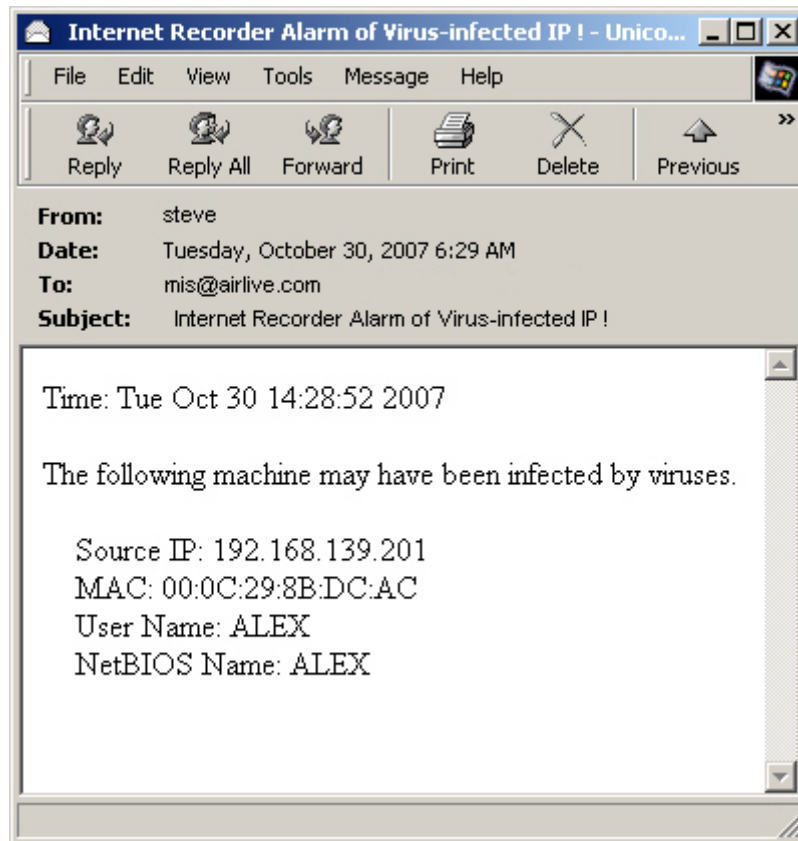


Figure 13-9 The Alert Notification Sent through an Email Message

14

Local Disk

The records of online activities are stored in the built-in hard disk. *Local Disk* has a utilization summary of each service according to which system administrator may decide the storage time for records of every kind separately. This helps optimize the use of built-in hard disk, avoiding insufficient storage space for new records.

14.1 Storage Time

Total Hard Disk Drive Space:

- The total available storage space on IAR-5000's built-in hard disk.

Service:

- The 8 major services to be recorded, namely SMTP, POP3, HTTP, IM, Web SMTP, Web POP3, FTP and TELNET.

Duration (YY/MM/DD):

- The storage duration of records is shown in the format YY/MM/DD.

Avg. Traffic / Day:

- The average traffic per day of a specific service is derived from the storage duration.

Storage Time (0: Not Recording):

- Records of each service can be assigned a storage time and will be deleted when expired.

Estimated Storage Utilization* (Percentage):

- The estimated used storage space is derived from the multiplication of **Avg. Traffic / Day** and **Storage Time**; the percentage in total storage space is given as well.

Configuring the Storage Time Based on the Traffic of Each Service:

Navigate to **Local Disk** → **Storage Time** and then configure accordingly. (Figure 14-1)

Total Hard Disk Drive Space : 140 GB				
Service	Duration (YY/MM/DD)	Avg. Traffic / Day	Storage Time (0: Not Recording)	Estimated Storage Utilization* (Percentage)
SMTP	09/12/08 - 09/12/09	19.36 KB	7 Days	135.49 KB (0.00%)
POP3 / IMAP	09/12/04 - 09/12/09	113.36 KB	7 Days	793.53 KB (0.00%)
HTTP / HTTPS	09/12/09 - 09/12/09	1 KB	7 Days	1 KB (0.00%)
IM	09/12/08 - 09/12/09	1.44 KB	7 Days	10.04 KB (0.00%)
Web SMTP	09/12/04 - 09/12/09	2.94 KB	7 Days	20.59 KB (0.00%)
Web POP3	09/12/04 - 09/12/09	13.74 KB	7 Days	96.22 KB (0.00%)
FTP	09/12/04 - 09/12/09	88.71 KB	7 Days	620.96 KB (0.00%)
TELNET	09/12/04 - 09/12/09	1.15 KB	7 Days	8.04 KB (0.00%)
Total				1.68 MB (0.00%)

*Estimated Storage Utilization = Avg. Traffic * Storage Time [Help](#)

14-1 Configuring the Storage Time for Each Service

14.2 Disk Space

Hard Disk Utilization:

- The indicative bar uses different colors to demonstrate the utilization of storage space. Each color represents a service (the color white means available storage space.); move the cursor over a color and then it shows what service it is and the used storage space.

SMTP:

- Indicates the total used storage space of SMTP records and lists out the top 10 users.

POP3

- Indicates the total used storage space of POP3 records and lists out the top 10 users.

HTTP:

- Indicates the total used storage space of HTTP records and lists out the top 10 users.

IM:

- Indicates the total used storage space of IM records and lists out the top 10 users.

Web SMTP:

- Indicates the total used storage space of Web SMTP records and lists out the top 10 users.

Web POP3:

- Indicates the total used storage space of Web POP3 records and lists out the top 10 users.

FTP:

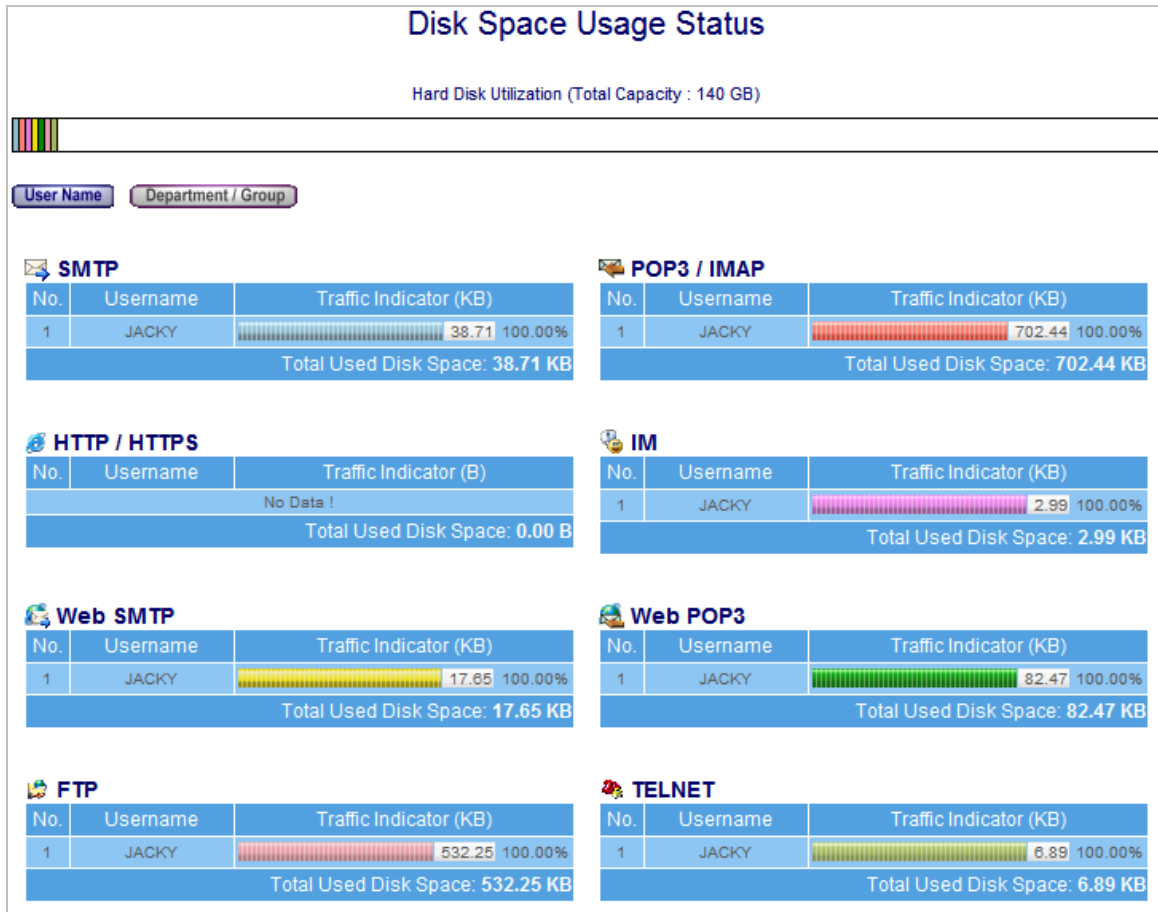
- Indicates the total used storage space of FTP records and lists out the top 10 users.

TELNET:

- Indicates the total used storage space of TELNET records and lists out the top 10 users.

Viewing the Used Storage Space and Top 10 Users of Each Service:

Under **Local Disk** → **Disk Space**, there it shows the details of built-in hard disk usage. (Figure 14-2)



14-2 Viewing the Details of Hard Disk Usage

15

Remote Backup

Running a storage is always a disaster especially when calling for archiving valuable information for a long-term storage. Accordingly, IAR-5000 features *Remote Backup* which helps resolve the storage quandary by periodically duplicating online activity records to a remote storage device, such as a NAS or Samba server.

In this chapter, it will be discussing the functionality and application of *Remote Backup*.



Benefits from using **Remote Backup**:

1. Extending the storage space without bounds.
2. Avoiding data lost caused by human factor or system error.
3. Browsing the archives remotely through a browser from any PC.

15.1 Backup Settings

Connection Status of Backup Storage Device:

- Displays the access validity, assigned access privilege (read/write), space requirement for next backup and current available space of backup storage device.

Mailing Settings:

- Once enabled, the designated recipient(s) will receive a notification about the completion of backup through an email.

Backup Settings:

- Determines of which service, destination and schedule to backup.

Immediate Backup:

- Used for performing a backup for selected service(s) / protocol(s) in a particular period. Once the duration is defined, the required hard drive space will be displayed on the screen.

Configuring IAR-5000 to Transfer Logs to the Designated Storage Device Periodically:

- Step1.** Navigate to **Remote Backup** → **Settings** → **Backup Settings**, and then configure as below: (Figure 15-1)

Connection Status of Backup Storage Device

Connection status: Disconnect (Privilege: ---)

Required disk space for the backup (09/12/01 - 09/12/31): 12.2 MBytes

Hard Disk Utilization (Total Capacity: ---, Free Disk Space: ---)

Mailing Settings

Send a notice upon backup completion

Sent from: mail.airlive.com

Sent to: mis@airlive.com

Backup Settings

Enable Remote Backup

Backup Path :

Remote Server Computer Name / IP :

Shared Directory Name : Help

Login ID :

Password :

Connection status: Test

Service logs / contents to backup :

<input checked="" type="checkbox"/> SMTP	<input checked="" type="checkbox"/> POP3	<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> IM
<input checked="" type="checkbox"/> Web SMTP	<input checked="" type="checkbox"/> Web POP3	<input checked="" type="checkbox"/> TELNET	<input checked="" type="checkbox"/> FTP

Backup starts at

00 : 00 every day
 00 : 00 every
 00 : 00 on the every month

OK Cancel

Immediate Backup

Required disk space for the backup: ---

From: / /

To: / /

Service logs / contents to backup :

<input checked="" type="checkbox"/> SMTP	<input checked="" type="checkbox"/> POP3	<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> IM
<input checked="" type="checkbox"/> Web SMTP	<input checked="" type="checkbox"/> Web POP3	<input checked="" type="checkbox"/> TELNET	<input checked="" type="checkbox"/> FTP

OK

15-1 Backup Settings

Step2. View the storage location and utilization: (Figure 15-2)

Connection Status of Backup Storage Device

Connection status: Succeeded (Privilege: [Read/Write](#))
 Required disk space for the backup (09/12/01 - 09/12/31): 12.2 MBytes
 Hard Disk Utilization (Total Capacity: 55.9 GBytes, Free Disk Space: 38.8 GBytes)

Mailing Settings

Send a notice upon backup completion
 Sent from: mail.airlive.com
 Sent to: mis@airlive.com

Backup Settings

Enable Remote Backup
 Backup Path :
 Remote Server Computer Name / IP :
 Shared Directory Name : Help
 Login ID :
 Password :
 Connection status: Test

Service logs / contents to backup :

<input checked="" type="checkbox"/> SMTP	<input checked="" type="checkbox"/> POP3	<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> IM
<input checked="" type="checkbox"/> Web SMTP	<input checked="" type="checkbox"/> Web POP3	<input checked="" type="checkbox"/> TELNET	<input checked="" type="checkbox"/> FTP

Backup starts at

<input type="radio"/>	<input type="text" value="00 : 00"/> every day
<input type="radio"/>	<input type="text" value="00 : 00"/> every <input type="text" value="Sunday"/>
<input checked="" type="radio"/>	<input type="text" value="00 : 00"/> on the <input type="text" value="first day"/> every month

OK Cancel

Immediate Backup

Required disk space for the backup: ---


From: / /
 To: / /

Service logs / contents to backup :

<input checked="" type="checkbox"/> SMTP	<input checked="" type="checkbox"/> POP3	<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> IM
<input checked="" type="checkbox"/> Web SMTP	<input checked="" type="checkbox"/> Web POP3	<input checked="" type="checkbox"/> TELNET	<input checked="" type="checkbox"/> FTP

OK

15-2 Viewing the Utilization of Backup Storage

 System administrator may backup logs of a specific period of time. (Figure 15-3)

Immediate Backup

Required disk space for the backup (09/12/03 - 09/12/08): 10.5 MBytes

From 2009 / 12 / 03

To 2009 / 12 / 08

Service logs / contents to backup :

<input checked="" type="checkbox"/> SMTP	<input checked="" type="checkbox"/> POP3	<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> IM
<input checked="" type="checkbox"/> Web SMTP	<input checked="" type="checkbox"/> Web POP3	<input checked="" type="checkbox"/> TELNET	<input checked="" type="checkbox"/> FTP

15-3 Immediate Backup Settings


15.2 Browse Settings


Connection Status of Backup Storage Device:

- Displays the status of the connection to the remote storage, and the access privilege (e.g., read / write) of backup storage device.

Browse Settings:

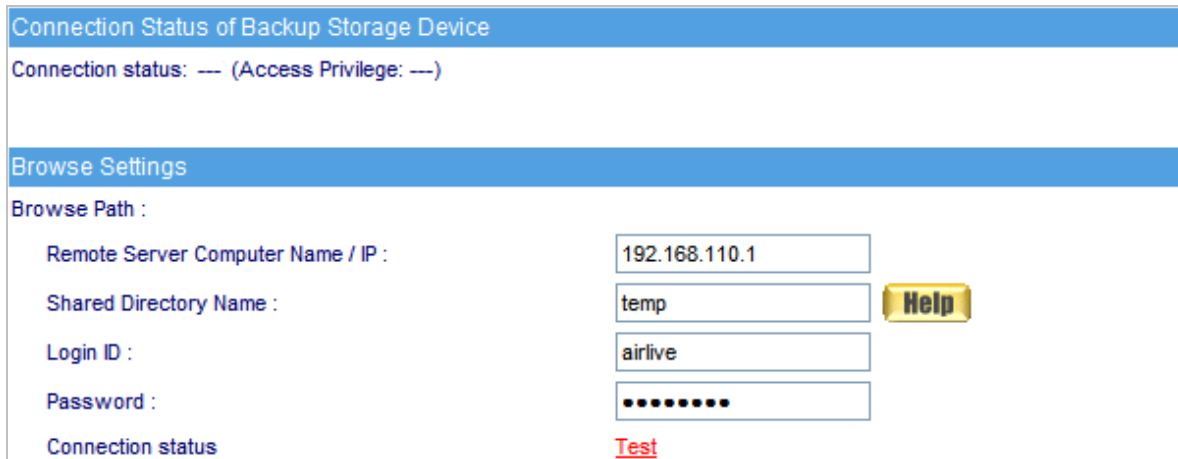
- Determines of which location to access archives.

 Accessing to the service logs under **Remote Backup → Browse** requires configuring the **Browse Settings** under **Remote Backup → Settings → Browse Settings**.

 For guidance on accessing the service archives under **Remote Backup → Browse**, please refer to chapter 10.

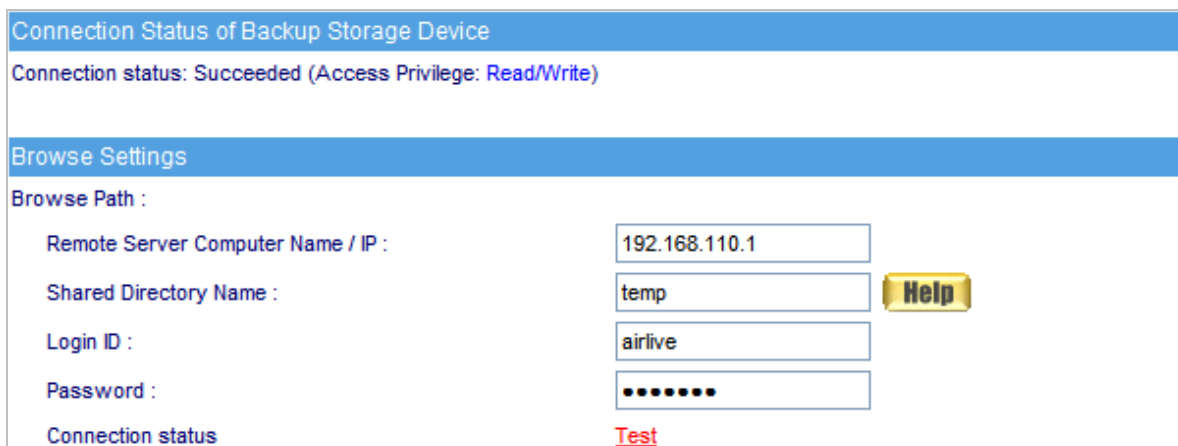
Configuring IAR-5000 to Gain Access to Archives:

Step1. Navigate to **Remote Backup** → **Settings** → **Browse Settings**, and then configure as below: (Figure 15-4)



15-4 Browse Settings

Step2. View the connection status and the access privilege of remote storage. (Figure 15-5)



15-5 Viewing the Connection Status of Backup Storage

Step3. Service logs are sorted by the eight services and duplicated periodically to the designated NAS server or file server.

- Under **Remote Backup** → **Browse**, services are classified into separate submenu items. Click on the desirable submenu item to access the logs. (Figure 15-6)

16

Reporting

Reporting delivers system administrator a quick insight to network traffic and storage space utilization with graphical charts, enhancing the management on a corporate network.

In this chapter, it will be discussing the functionality and application of *Reporting*.

Periodic Report Scheduling Settings:

- It generates and sends out the periodic report to the designated recipient(s) on schedules.

History Report Retrieving Settings:

- It generates the report of a specific date and instantly sends it to the designated recipient(s).
 - ◆ Navigate to **System** → **Settings** → **Settings** to enable **email notification** and configure its related settings. And then refer to the following to adjust settings under **Reporting** → **Settings**:
 1. Tick **Enable the mailing of Periodic Report** and then tick **Yearly report**, **Monthly report**, **Weekly report** and **Daily report**.
 2. Click on **OK**. (Figure 16-1)
 3. Recipient will be receiving reports on schedules. (Figure 16-2, 3)
 4. Under **History Report Retrieving Settings** section, specify the date of issue.
 5. Click on **Send Report**. (Figure 16-4)
 6. Recipient shall receive report(s) by now. (Figure 16-5, 6)



Schedule for periodic report:

1. **Yearly report** is produced at 24 o'clock on January 1st of a year.
2. **Monthly report** is produced at 24 o'clock on the 1st of a month.
3. **Weekly report** is produced at 24 o'clock on the first day of a week.
4. **Daily report** is produced at 24 o'clock of a day.

Periodic Report Scheduling Settings

Enable the mailing of Periodic Report

Yearly report Monthly report Weekly report Daily report

OK **Cancel**

History Report Retrieving Settings

Yearly report 2009

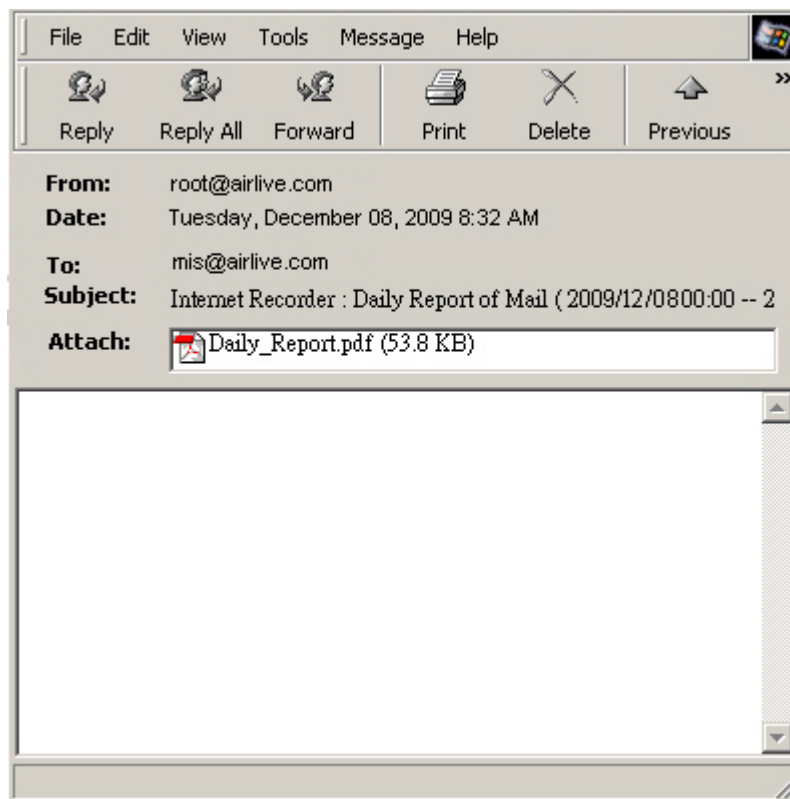
Monthly report 2009 12

Weekly report 2009 12 06

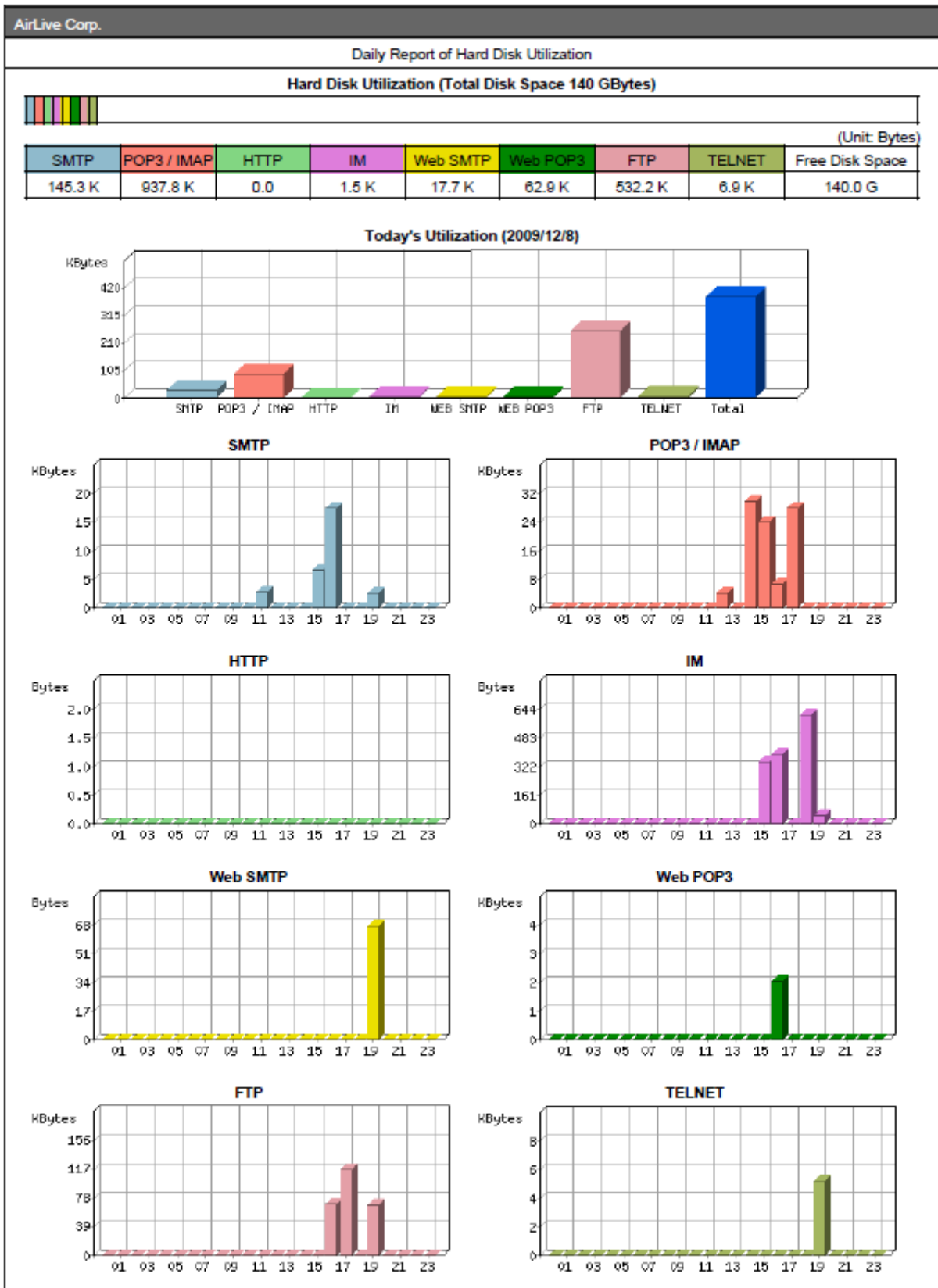
Daily report 2009 12 09

Mail Report

16-1 Periodic Report Scheduling Settings



16-2 Daily Report Sent through an Email Message



16-3 Daily Report

Periodic Report Scheduling Settings

Enable the mailing of Periodic Report

Yearly report Monthly report Weekly report Daily report

OK **Cancel**

History Report Retrieving Settings

Yearly report 2009

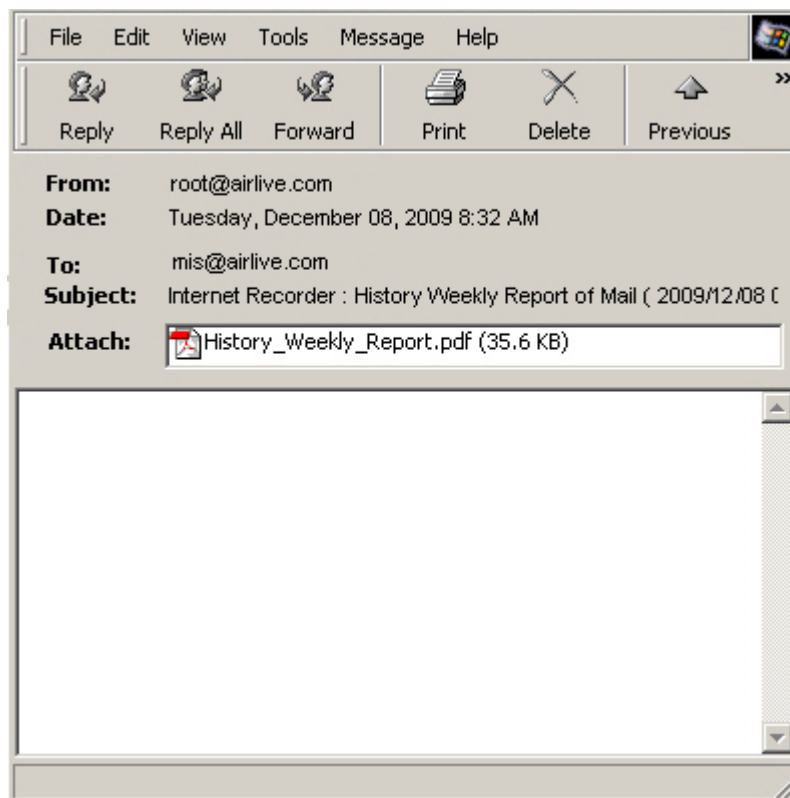
Monthly report 2009 12

Weekly report 2009 12 06

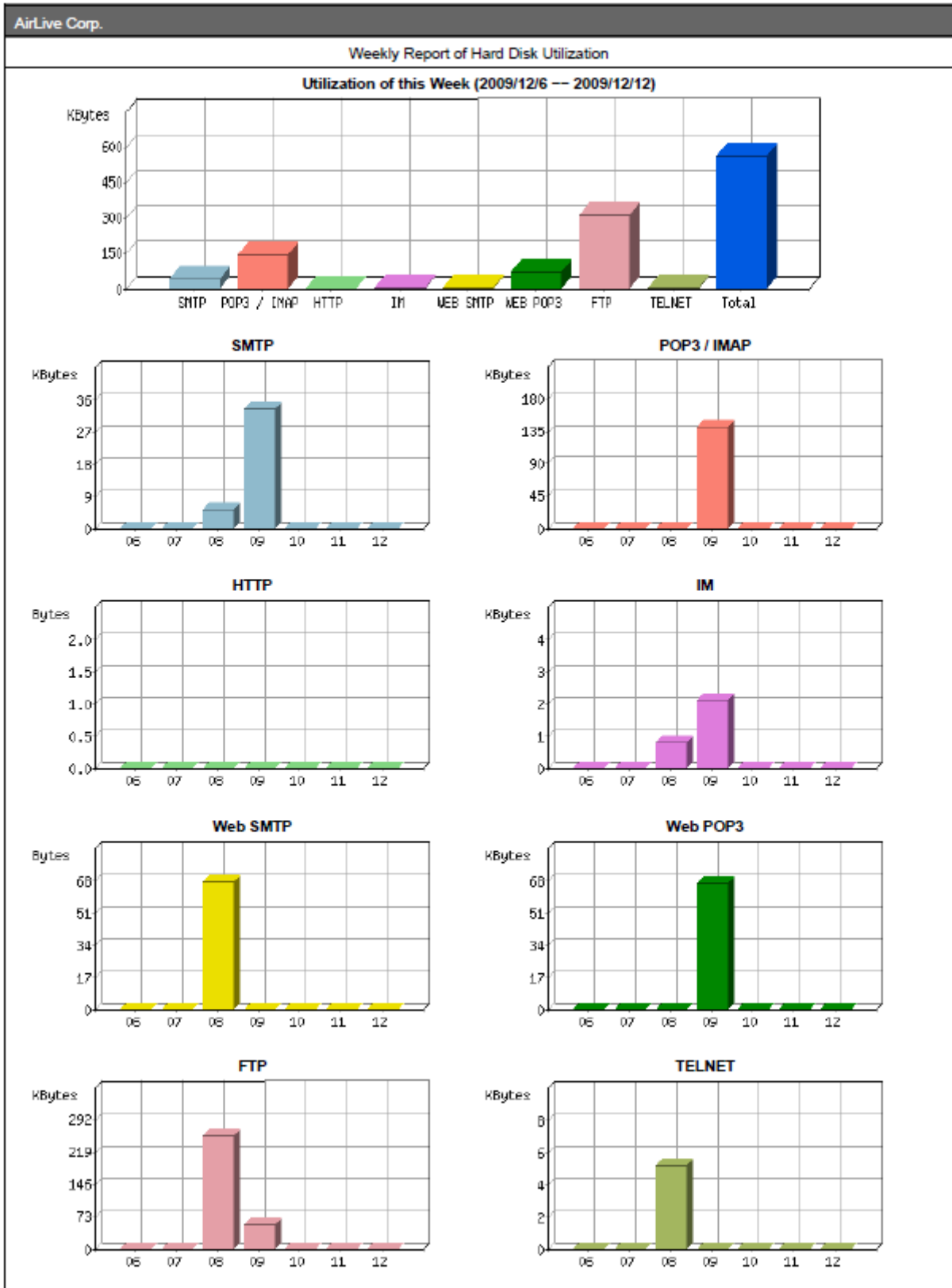
Daily report 2009 12 09

Mail Report

16-4 History Report Retrieving Settings

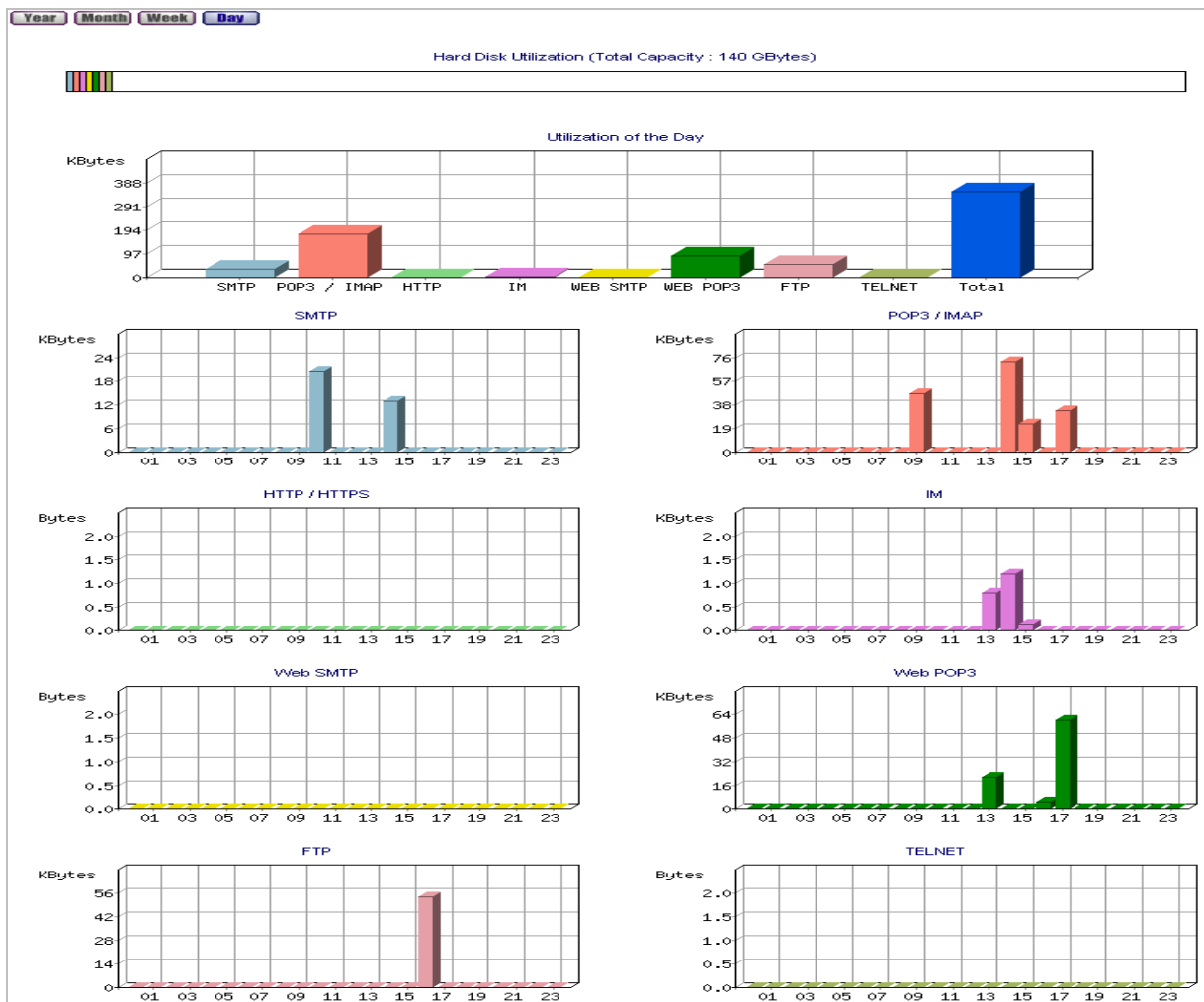


16-5 Weekly History Report Sent through an Email Message



16-6 Weekly Report

- Step1.** Under **Reporting** → **Storage Report**, bar charts indicate the disk space utilization of each service.
- Step2.** In the upper left corner, click on a time unit from which the bar charts are derived. Click on **Day** for bar charts derived from daily operation; click on **Week** for bar charts derived from weekly operation; click on **Month** for bar charts derived from monthly operation; click on **Year** for bar charts derived from yearly operation.
- Step3.** How to read the histograms: (Figure 16-7)
- Y-axis indicates the used disk space in MB.
 - X-axis indicates time



16-7 Storage Report

17

Status

Status presents system administrator with the system performance, authentication, current sessions and event logs.

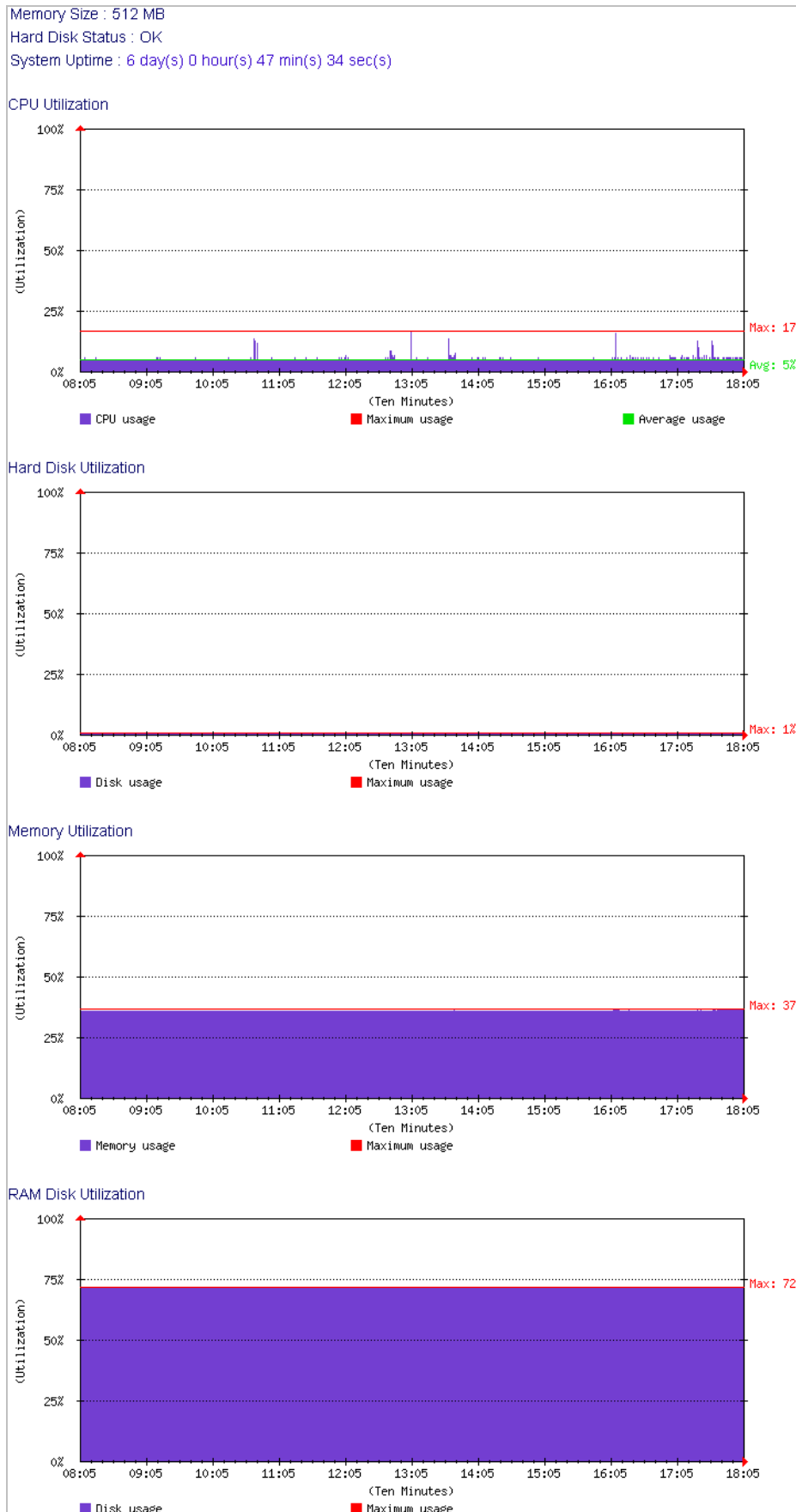
17.1 System Info

System Info:

- The usage of CPU, hard disk, memory and RAM disk are illustrated separately in different histograms. (Figure 17-1)

Under **Status** → **System Info**, there it shows the resource usage and system uptime.

- **System Uptime:** The time the device has been up and running.
- **CPU Utilization:** The resource usage of CPU.
- **Hard Disk Utilization:** The resource usage of hard disk.
- **Memory Utilization:** The resource usage of memory.
- **RAM Disk Utilization:** The resource usage of RAM disk.




17-1 System Info

17.2 Authentication

Authentication:

- The related information of User Authentication, such as client’s IP address, login name, login time, and the remove selection for administrator.

IP Address	Authentication-User Name	Login Time	Configure
172.16.0.2	stan	2009/12/09 18:11:21	

17-2 Authentication Info

17.3 Current Session

Current Session:

- Shows the traffic and amount of sessions created by each service, such as HTTP, FTP, POP3, SMTP, IM, TELNET, Web Mail and applications.

Search Active Sessions:

- Records are available if searched by criteria, such as service, status, protocol, source IP, destination IP and port number, as keyword or pattern.
 - ◆ Refer to the steps below to start a search:
 1. Select “Active” for **Session Status**.
 2. Select “TCP” for **Protocol**.
 3. Click on **Search**. (Figure 17-3)

Search Active Sessions

Enter your search criteria :

IP Service :


Session Status :

Protocol :

Source IP : (Max. 15 characters)









Destination IP : (Max. 15 characters)

Port : -> (1 - 65,535)



Results

Search results : 4 records

IP Service	Source IP	Destination IP	Port	Start Time	Traffic	Session Status
 FTP	JACKY	192.168.110.1	 TCP 3578 => 21	18:02:02	1.9 KB	Active
 POP3 / I.	JACKY	mail.airlive.com	 TCP 3577 => 110	18:01:34	944.0 B	Active
 FTP	JACKY	192.168.110.1	 TCP 3576 => 21	18:00:00	2.9 KB	Active
 MSN	JACKY	65.54.48.85	 TCP 2940 => 1863	14:03:24	438.6 KB	Active

17-3 Searching for a Specific Log

Step1. Under **Status** → **Current Session**, there it shows the sessions created by each service. (Figure 17-4)

IP Service	Traffic	Active / Inactive Sessions	Number of Sessions
TOTAL	535.4 KB	2 / 0	2
POP3 / IMAP	944.0 B	1 / 0	1
IM	534.5 KB	1 / 0	1

17-4 Current Sessions – Overall Information

Step2. Click on **Total** to view the used port number and traffic of each service session. (Figure 17-5)

IP Service	Source IP	Destination IP	Port	Start Time	Traffic	Session Status
MSN	JACKY	65.54.48.85	TCP 2940 => 1863	14:03:24	546.7 KB	Active

17-4 Current Sessions – Specific Details

Step3. In the **Total IP Service** screen, a mouse click on a **Source IP** or **Destination IP** will show its corresponding IP address, host name, domain name, port number and traffic in a pop-up window. (Figure 17-6)

IP Service	Source IP	Destination IP	Port	Start Time	Traffic	Session Status
POP3 / I.	JACKY	mail.airlive.com	TCP 3717 => 110	18:41:55	944.0 B	Active
MSN	JACKY	65.54.48.85	TCP 2940 => 1863	14:03:24	560.7 KB	Active

17-5 Current Sessions - Detailed Information of an IP Address

17.4 IM / Application Log

IM / Application Log:

- Depicts the status of each IM / application used.

Search IM / Application Logs:

- Records are available if searched by criteria, such as date, IM/ application event, IM account and action, as keyword or pattern.
 - ◆ Refer to the steps below to start a search:
 1. Specify the time duration to search within.
 2. Select "Ignore" for **Access**.
 3. Click on **Search**. (Figure 17-6)

Search IM / Applications Logs

Enter your search criteria :

Start a search from: 2009 / 12 / 04 00 : 00
 To: 2009 / 12 / 09 18 : 16

IM / Applications: (Max. 80 characters)

IM Account: (Max. 80 characters)


Access:

Search **Download**

Results

2009-12-09 (1 Record)

← 1 / 1

Date / Time	Username	IM / Applications	IM Account	Access
Dec 09 18:16:06	JACKY	[IM] MSN Messenger	sebastienko@hotmail.com	

← 1 / 1


17-6 Searching for a Specific Log

17.5 Even Log

Event Log:

- Records all modifications on IAR-5000, such as deleting a setting.

Search Event Logs:

- Records are available if searched by criteria, such as event and date, as keyword or pattern.
 - Refer to the steps below to start a search:
 - Enable the searching duration and specify a period of time to search within.
 - Click on **Search**. (Figure 17-7)
 - Click on **Download** to download the search results onto local computer. (Figure 17-8)
 - Click on  icon to view the detailed event information. (Figure 17-9)

Search Event Logs

Enter your search criteria :

Event :

Start a search from : 2009 / 12 / 3 17 : 18

To : 2009 / 12 / 9 18 : 14

Search

Results

Search result: 186 records

Download View: 1 - 100 ← 1 / 2 →


Date / Time	Admin Name	IP Address	Event	Details
Dec 9 18:14:43	---	172.16.0.2	[Authentication] User 172.16.0.2 Logout success	-
Dec 9 18:11:20	---	172.16.0.2	[Authentication] User stan Login success	-
Dec 9 17:38:28	admin	172.16.0.2	[Report] Send History Report (2009/12/8)	-
Dec 9 17:32:45	admin	172.16.0.2	[Report] Send History Report (2009/12/6)	-
Dec 9 17:32:30	admin	172.16.0.2	[System] Modify Setting	
Dec 9 17:32:17	admin	172.16.0.2	[System] Modify Setting	


17-7 Searching for a Specific Event

Search Event Logs

File Download

Do you want to open or save this file?

 Name: download.csv
 Type: Microsoft Office Excel Comma Separated Values File
 From: 172.16.3.254

 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. [What's the risk?](#)

: 18
: 14

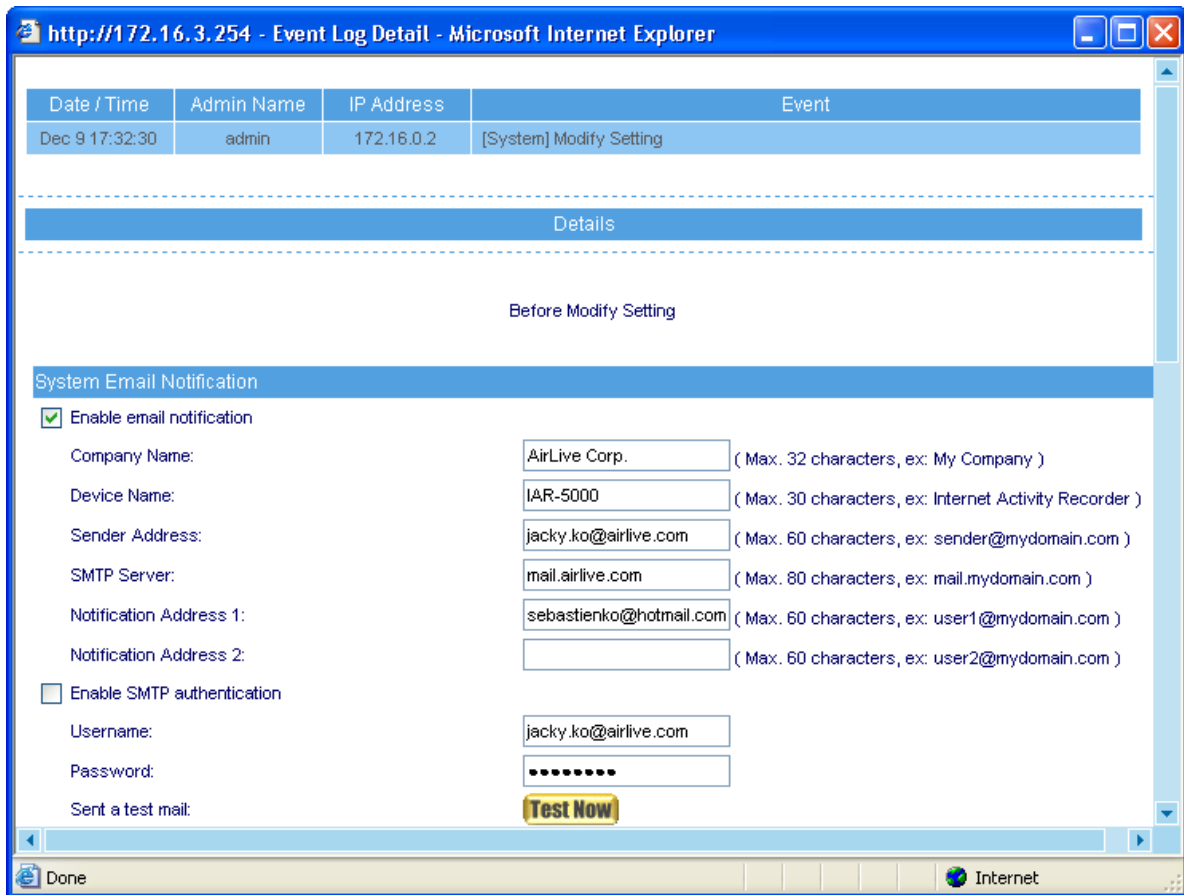
Search

Results

Download ← 1 / 2 →

Date / Time	Admin Name	IP Address	Event	Details
Dec 9 18:14:43	---	172.16.0.2	[Authentication] User 172.16.0.2 Logout success	-
Dec 9 18:11:20	---	172.16.0.2	[Authentication] User stan Login success	-
Dec 9 17:38:28	admin	172.16.0.2	[Report] Send History Report (2009/12/8)	-
Dec 9 17:32:45	admin	172.16.0.2	[Report] Send History Report (2009/12/6)	-
Dec 9 17:32:30	admin	172.16.0.2	[System] Modify Setting	
Dec 9 17:32:17	admin	172.16.0.2	[System] Modify Setting	

17-8 Downloading the Search Result



The screenshot shows a Microsoft Internet Explorer window titled "http://172.16.3.254 - Event Log Detail". The main content area features a table with the following data:

Date / Time	Admin Name	IP Address	Event
Dec 9 17:32:30	admin	172.16.0.2	[System] Modify Setting

Below the table is a "Details" section titled "Before Modify Setting". This section contains a "System Email Notification" form with the following fields and values:

- Enable email notification
- Company Name: AirLive Corp. (Max. 32 characters, ex: My Company)
- Device Name: IAR-5000 (Max. 30 characters, ex: Internet Activity Recorder)
- Sender Address: jacky.ko@airlive.com (Max. 60 characters, ex: sender@mydomain.com)
- SMTP Server: mail.airlive.com (Max. 80 characters, ex: mail.mydomain.com)
- Notification Address 1: sebastienko@hotmail.com (Max. 60 characters, ex: user1@mydomain.com)
- Notification Address 2: (Max. 60 characters, ex: user2@mydomain.com)
- Enable SMTP authentication
- Username: jacky.ko@airlive.com
- Password: (masked with dots)
- Sent a test mail:

17-9 Details of an Event Log

18

Specifications

The specification of IAR-5000 is subject to change without notice. Please use the information with caution.

Category	Configuration Name	Function	Chapter
System	Admin	Used for creating and modifying system administration accounts.	4
	Interface	Used for setting the interface's IP address, subnet mask, etc.	
	Settings	Used for importing/exporting system settings, factory resetting, hard disk formatting, system email notifications, deployment mode, management port, log storage times, device rebooting, etc.	
	Date/Time	Used for setting the system's time.	
	Permitted IPs	Used for specifying IP's permitted to access the management interface.	
	Language	Used for selecting the management interface's language (English, Simplified Chinese and Traditional Chinese)	
	Installation Wizard	Provides a quick method to configure the device.	
	Software Update	Used for upgrading the system's software version.	
User List	Settings	Used for importing /exporting user lists, specifying logged group lists.	5
	Logged	Specifies user's to be logged.	
	Ignored	Specifies user's to be excluded from logging.	
	Settings	Provides settings for the authentication port number, idle time, multiple logins, web site displayed for successful logins, display messages and authentication free table.	

	Auth User		Specifies the authentication name accounts.	
	RADIUS		Used for enabling a Radius server to manage authentication.	
	POP3		Used for enabling a POP3 server to enable authentication.	
	LDAP		Used for enabling an LDAP server to manage authentication.	
Record Analysis	Settings	Settings	Provides settings for: signature definitions, content , username binding, Skype plug-in for AD Server username binding, LAN to LAN activity recording, recording settings, maximum number of logs displayed per page, service logs display, report browsing, default character encoding for recording, etc.	9
	User	Logged	Classifies the services used by each user into SMTP, POP3/IMAP, HTTP, IM, Web SMTP, Web POP3, FTP and Telnet.	10, 11
	Service	SMTP		
		POP3 / IMAP		
		HTTP		
		IM		
		Web SMTP		
		Web POP3		
		FTP		
TELNET				
Behavior Management	IM Management	Login Notice	Provides messages to users upon login to MSN, ICQ/ AIM, Yahoo, etc.	7
		Default Rule	Provides login and file transfer management for MSN Messenger, Skype, Yahoo, ICQ/AIM, QQ, Google Talk , etc.	
		Account Rule		
	Application Management	Default Rule	Manages logins for applications such as eDonkey, BT, Thunder5, etc.	8
		Custom Rule		
	Content Auditing	Settings	Audits the content of services used by users and emails any results matching the criteria to the specified recipient.	12
Anomaly Flow IP	Settings	Provides settings for the management and notification upon detection of anomaly traffic flows.	13	
	Virus-Infected IP			
	Intrusion IP			

Local Disk	Storage Time		Provides individual storage time settings for each of the recorded services based upon their importance.	14
	Disk Space		Provides hard disk utilization statistics based upon the service, user and group.	
Remote Backup	Settings	Backup Settings	Provides settings for the remote backup of the devices records. Records can be backed up periodically or instantly to the specified network path. Access to records stored remotely can also be viewed here.	15
		Browse Settings		
	Browse	SMTP		
		POP3 / IMAP		
		HTTP		
		IM		
		Web SMTP		
		Web POP3		
		FTP		
TELNET				
Reporting	Settings		Charts present statistics based upon traffic, storage and service utilization data.	16
	Storage Report			
Status	System Info		Present statistics of the devices system, e.g. CPU utilization, hard disk utilization, etc.	17
	Current Session		Provides session statistics based upon the services recorded by the device.	
	IM/Application Log		Provides statistics of IM and other applications managed by the device.	
	Event Log		Provides a record of any settings modified and logins made into the device.	