Air Live®
Powered by OvisLink Corp.

ES-6000

Email Server Appliance

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.

Table of Contents

Chapter 1 Introduction 5

1.1 Functions and Features 5

1.2 Front Panel 7

1.3 Packing List 7

Chapter 2 System Wizard 8

Chapter 3 System 14

3.1 Admin 14

3.2 Interface 17

3.3 Setting 18

3.4 Storage Device 23

3.5 Date/Time 24

3.6 Software Update 25

Chapter 4 Mail Management 26

4.1 Configure 26

4.1.1 Setting 26

4.1.2 Web Mail Logo 32

4.1.3 Multiple Domains 33

4.1.4 Mail Relay 36

4.1.5 Mail Signatures 38

4.1.6 Mail Routing 40

4.2 Account Management 41

4.2.1 Setting 41

4.2.2 Individual 44

4.2.3 Group 48

4.2.4 Shared Address Book 49

4.3 Queue 61

4.4 Connection Track 63

4.4.1 Outbound SMTP 63

4.4.2 Inbound SMTP 64

4.4.3 POP3 / IMAP 65

Chapter 5 Web Mail 69

5.1 How to use Web Mail 69

5.2 How to configure Web Mail User Preference 72

5.3 Importing Address Book from Outlook Express 74

5.4 Using Web Disk to Transfer Large File 79

5.5 Using White List and Black List to Filter E-Mails 84

5.6 Using Push Mail to Access Instant Messages 86

Chapter 6 Mail Security 88

6.1 Configure 88
6.1.1 Setting 88
6.1.2 Mail Notice 90
6.2 Anti-Spam 97
6.2.1 Setting 97
6.2.2 Personal Rule 100
6.2.3 Global Rule 101
6.2.4 Whitelist 103
6.2.5 Blacklist 104
6.2.6 Auto-Whitelist 105
6.2.7 Training 106
6.3 Anti-Spam Configuration Example 107
6.3.1 Using Whitelist and Blacklist to Filter E-Mails 107
6.3.2 Using Global Rule to Filter E-Mails 111
6.3.3 Raising Bayesian Filtering Accuracy by Spam or Ham Training (Outlook Express) 115
6.3.4 Raising Bayesian Filtering Accuracy by Account Training 125
6.4 Anti-Virus 129
6.4.1 Anti-Virus Setting 129
6.4.2 Anti-Virus Configuration Example 131
6.5 Mail Report 132
6.5.1 Setting 132
6.5.2 Statistics 143
6.5.3 Log 144
Chapter 7 Mail Archie / Audit 151
7.1 Setting 151
7.2 Audit 152
7.3 Archive 153
7.4 Mail Archive / Audit Configuration Example 154
Chapter 8 Push Mail 161
8.1 Push Rule 161
8.2 Push Rule Configuration 163
8.3 Push Mail Example 171
Chapter 9 Remote Backup 174
9.1 Backup Setting 174
9.2 Browse Setting 174
9.3 Browse Mail 175
9.4 Mail Backup Example 176
Chapter 10 HA 181
Chapter 11 DNS Setting 186
11.1 DNS Setting 186

11.2 A (Address) 187
11.3 CNAME (Canonical NAME) 188
11.4 MX (eXchanger) 189
11.5 SPF (Sender policy FrameWork) 191
11.6 Example 192
11.6.1 Setup a host name server 192
11.6.2 Mapping between Servers (Web / FTP / Mail) and Domain Name 196
Chapter 12 Web Server Setting 200
12.1 Setting 200
12.2 Example 201
Chapter 13 Proxy Server Settings 212
Chapter 14 Monitor 213
14.1 System Info 213
14.2 Event Log 215
Chapter 15 Introduction of Mail System 218

Chapter 1 Introduction

Congratulations on your purchase of this outstanding ES-6000 Mail Server Appliance, this product is new generation designed for the SMB or enterprise company that has the need to install an easy maintained and fully function of mail server in office.

AirLive ES-6000 Mail Server Appliance not just supports the basic mail protocol such as ***POP3(s)***, ***SMTP(s)***, ***IMAP(s)***, it also supports the ***Web Mail*** to allow user accessing mail via browser no matter where you are, and the ***Web Disk*** function to offer a solution for delivering large file, so user can download file from ES-6000 directly, and do not need to worry about mail box's limitation. Meanwhile, the ES-6000 ***Push Mail*** function can deliver mail subject to mobile phone, so user can check the mail in anytime and anywhere without carrying laptop.

The more advanced feature of ES-6000 is to provide ***Multiple Domains*** function, so a company or Internet Service Provider can apply two or more mail domains, and configure to one single mail server - ES-6000. Except those advanced feature, ***Anti-Spam*** and ***Anti-Virus*** function are also designed into ES-6000. With complete mail server feature to offer mail service, protect mail security, and backup mail data, AirLive ES-6000 can be your excellent choice for the total solution of mail server.

1.1 Functions and Features

- **Easy installation and useful mail system**
  Just few steps of installation, a useful mail server with POP3(s), SMTP(s), IMAP(s), Push Mail, Web Mail and Web Disk function can be deployed and ready for use.
- **Push Mail**
  System will push email to user's mobile phone, so user can receive and reply mail via mobile phone whenever it is and wherever he goes.
- **Web Mail**
  Sometimes users need to access email in public computer, such as cyber café, and it is not allowed or not properly to download private mail. Web mail function works to provide internet user to check mail via web browser, so users will be able to read or send email everywhere he can connect to Internet.
- **Personal Web Disk**
  Instead of sending mail with attaching large file, user can store the file in Personal web disk and send out the address of hyperlink, and then Internet user will be able to download it without authentication.

- **Multiple Domains**

  Up to 10 mail domains can be created on ES-6000 and work properly simultaneously. Each mail domain can have its own mail account as well.

- **Anti-spam**

  Built-in with Bayesian, fingerprint, verifying sender account, checking sender IP in RBL and else anti-spam system work to filter spam mail automatically.

- **Anti-virus**

  Built-in with Clam AV and Sophos scan engine can filter malicious program in mail content, to prevent mail receiver from virus threat. The virus pattern can be updated regularly, and without any license fee.

- **Mail Audit / Archive**

  User can define rule (such as keyword, sender, receiver, size…) for mail audit, when the incoming or outgoing mail matches the rule, then system will handle the mail based on the rule to pass, delete, inspect, delay, or copy to a specific account.

- **Mail Account Learning**

  Built-in with mail account learning system, such as Automatically Adding, Query Old Mail Server, or LDAP, user can migrate mail account from old mail server, or create new mail account quite facile.

- **Shared Address Book**

  Shared Address Book function not only works for Web Mail users, it can also connect to mail client software with LDAP service, such as Outlook Express, to search the destination address within Shared Address Book.

- **Customize mail account**

  Each mail accounts can be customized quite precisely based on company's policy, such as to enable or disable Mail protocol, Mail size limitation, Mail box Quota, Personal web disk quota, and Push Mail quota.

- **Web Server**

  ES-6000 not only provides mail server function, it also offers web server function to allow user creating company's website on same device. So user will not need to purchase further software or hardware for web service.

- **DNS**

  Built-in with DNS server, administrator can setup the domain name resolution by himself, and will not need to spend money to deposit DNS service at ISP.

- **Remote Backup**

  ES-6000 will record every passing mail as the record, and backup the record to NAS or File Server by schedule. Those mail records can also be retrieved from NAS or File Server via ES-6000.

- **HA**

  Built-in with HA (High Availability) function, the stored data can be synchronized with two ES-6000 devices, to prevent losing mail while mail server is damaged.

1.2 Front Panel

Figure 1-1 Front Panel

LED	Color	Status	Description
POWER	Green	On	Power on the device
Hard Disk	Green	Blinking	Data reading / accessing
Mail Port (Right Led)	Orange	Blinking	Sending / Receiving
Mail Port (Left Led)	Deep Orange	On	1000 Mbps
	Green	On	100 Mbps
		Off	10 Mbps
HA Port (Right Led)	Orange	Blinking	Sending / Receiving
HA Port (Left Led)	Deep Orange	On	1000 Mbps
	Green	On	100 Mbps
		Off	10 Mbps

Ports:

Port	Description
AC Power	Input voltages ranging from 100 ~ 240 VAC, and with a maximum power output of 85 watts.
Mail Port	Use this port to connect to a router, DSL modem, Cable modem, or Switch.
HA Port	Use this port to connect another ES-6000 device for HA function
Console Port	9-pin serial port connector for checking setting and restore to the factory setting

1.3 Packing List

- ES-6000 Mail Server Appliance
- CD-ROM with Quick Installation Guide and User's Manual
- CAT-6 UTP Fast Ethernet cable x 2
- RS-232 cable
- Power code
- Accessories

Chapter 2 System Wizard

When it is first time for user to login ES-6000, system will switch to Wizard page automatically, so user can follow the wizard to configure mail server setting step by step.

Step1. Connect the PC and ES-6000's port 1 to the same Hub / Switch, and launch the browser (IE or Firefox) to link the ES-6000 appliance. The default IP address is http : //192.168.1.1

Step2. Administrator will be requested for **User Name** and **Password** when entering ES-6000 system. (Figure 2-1)

- **User Name** : admin
- **Password** : airlive
- Click **OK**.

Figure 2-1 Login page

Step3. When user first uses the ES-6000 management interface, system will automatically enter **Install Wizard.** It will guide user to make settings. Click **Next**. (Figure 2-2)

Figure 2-2 Enter the setting wizard

Step4. Select the language and character encoding. (Figure 2-3)

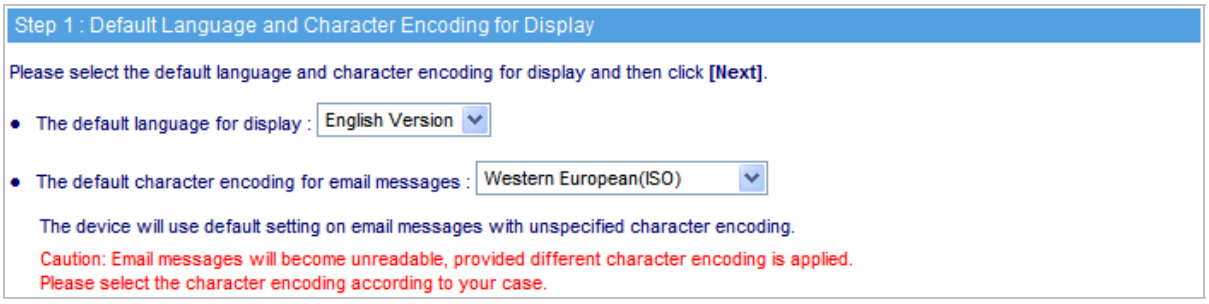


Figure 2-3 Select the language and character encoding

When system can not identify the data character encoding that is going to be saved into database, it will use the default setting.

Step5. Go to System (Interface, enter the following setting: (Figure 2-4)

- Provide a valid IP address of the LAN subnet along with its mask, default gateway and DNS sever address.

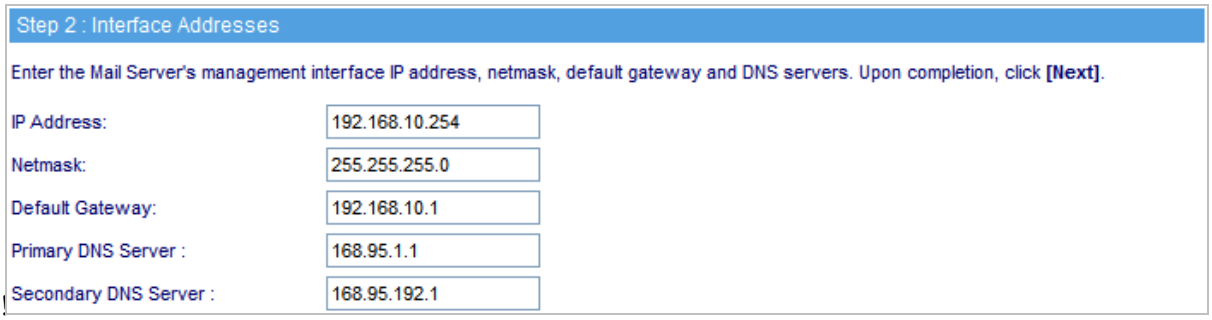


Figure 2-4 Interface setting

Please refer to LAN segment setting to set up interface address. For example, if the LAN segment is 172.16.X.X, then any changes made must be within the same segment in order to take effect.

The following table lists the standard virtual IP range, all external real IPs are forbidden.

10.0.0.0 ~ 10.255.255.255
172.16.0.0 ~ 172.31.255.255
192.168.0.0 ~ 192.168.255.255

Step6. Go to **System → Synchronize System Clock,** enable **Synchronize with an Internet Time Server** and set up offset hours from GMT to assure the correct time. (Figure 2-5)

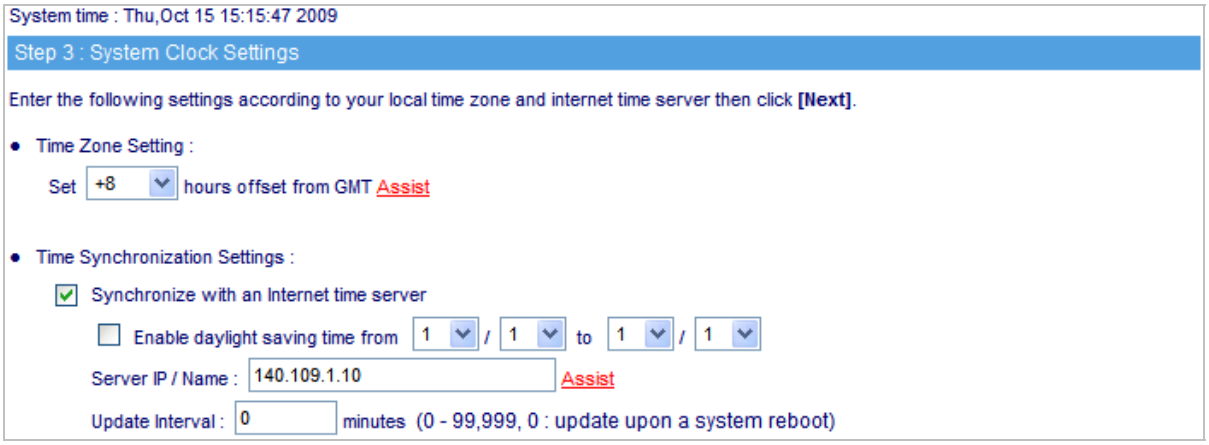


Figure 2-5 Synchronize time setting

If the local area executes the daylight saving time, then enable the **Daylight Saving Time Setting.**

Step7. Enter corresponding domain alias. (Figure 2-6)

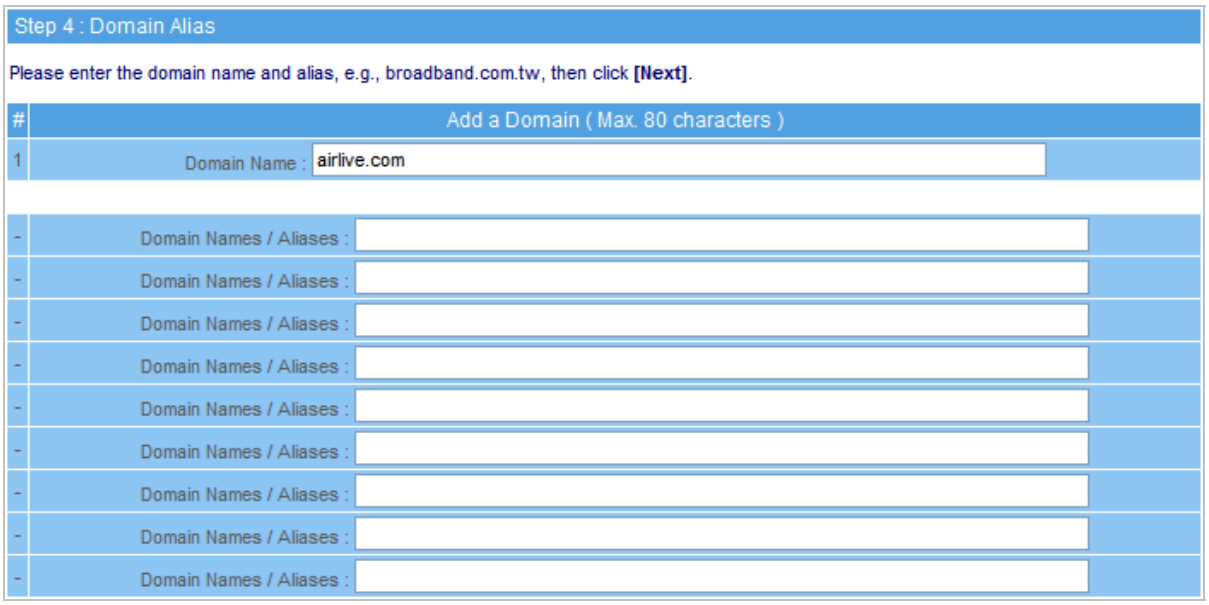


Figure 2-6 Domain alias setting

Step8. Apply permitted mail relay segments and domains. (Figure 2-7)

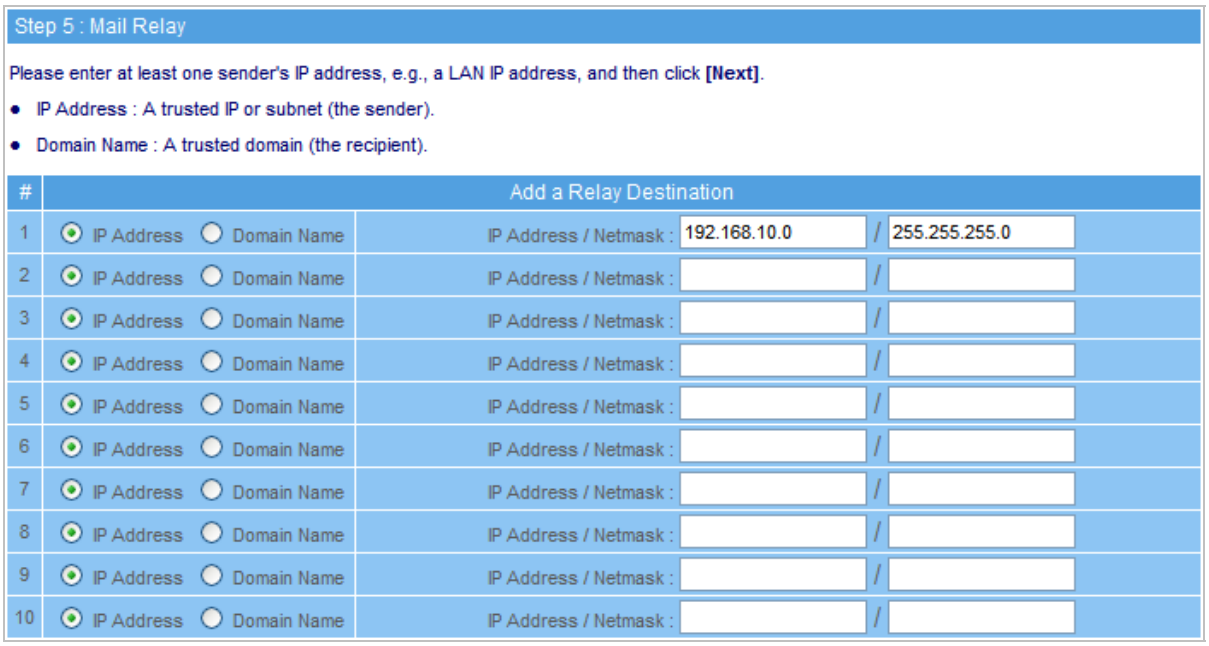


Figure 2-7 Mail relay setting

Step9. If resolving domain name is needed, please enable the **DNS Setting** option. Once the **DNS Setting** is enabled, the install wizard will take you to a further DNS setting after you click **Finish**. (Figure 2-8)

Figure 2-8 Install completed

Step10. Set up account learning approach and default value for new account. (Figure 2-9)

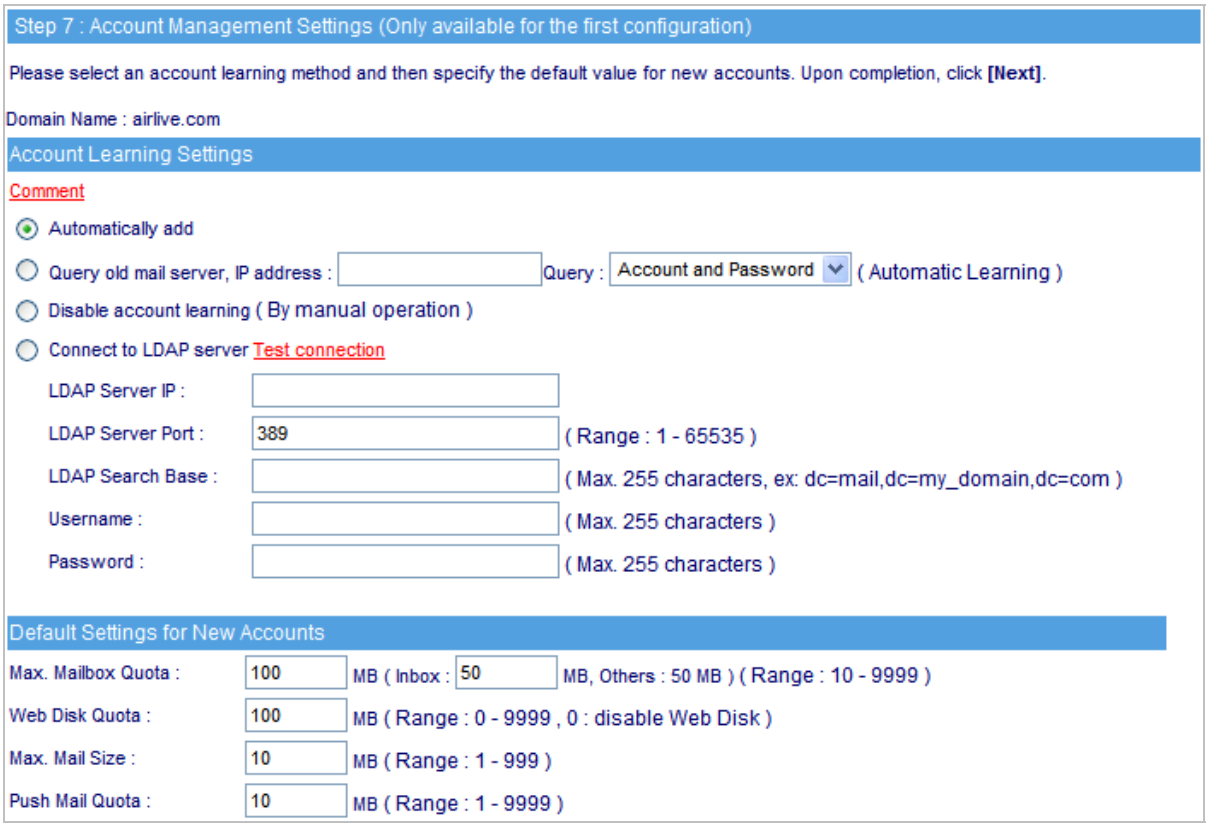


Figure 2-9 Setup account learning approach and default value for new account

Step11. If necessary, select to enable HA feature and configure the IP address of another ES-6000. Both devices will synchronize the database when the connection builds up. (Figure 2-10)

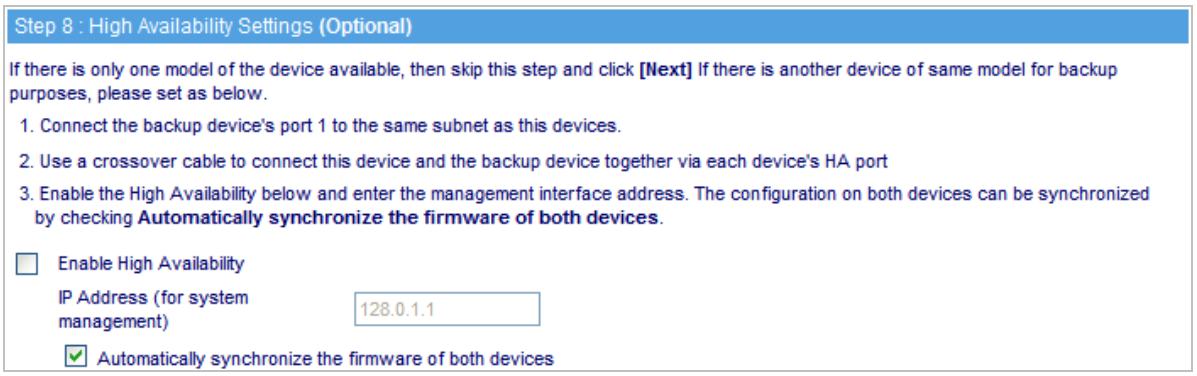
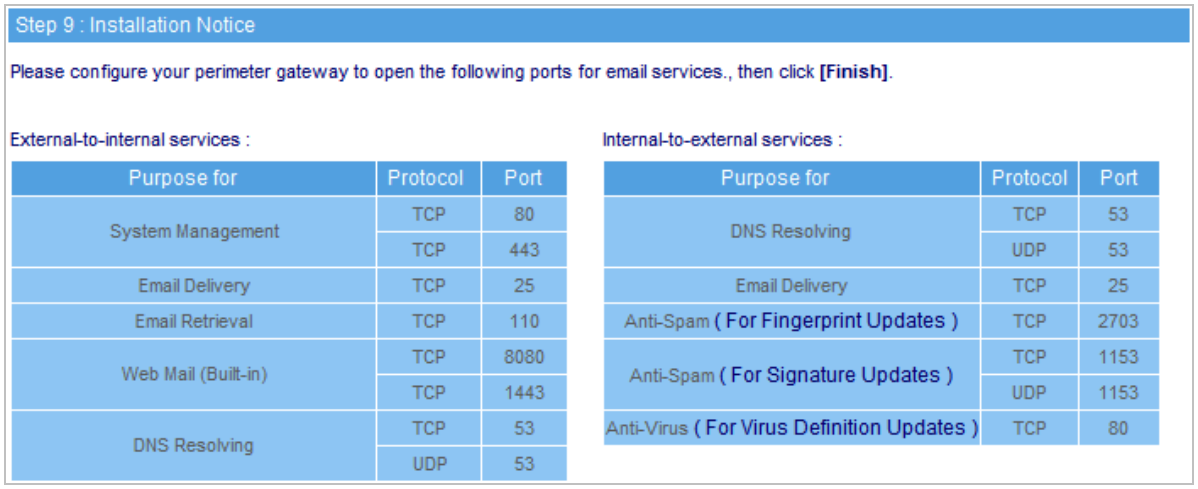


Figure 2-10 High Availability setting

Step12. Prompt users that the listed ports below should be remaining open on Perimeter Gateway while ES-6000 is functioning. (Figure 2-12)



Step 9 : Installation Notice

Please configure your perimeter gateway to open the following ports for email services., then click **[Finish]**.

External-to-internal services :

Purpose for	Protocol	Port
System Management	TCP	80
	TCP	443
Email Delivery	TCP	25
Email Retrieval	TCP	110
Web Mail (Built-in)	TCP	8080
	TCP	1443
DNS Resolving	TCP	53
	UDP	53

Internal-to-external services :

Purpose for	Protocol	Port
DNS Resolving	TCP	53
	UDP	53
Email Delivery	TCP	25
Anti-Spam (For Fingerprint Updates)	TCP	2703
Anti-Spam (For Signature Updates)	TCP	1153
	UDP	1153
Anti-Virus (For Virus Definition Updates)	TCP	80

Figure 2-12 Attention

Step13. Click **Finish.**

Chapter 3 System

The system administration refers to the competency to manage the ES-6000. In this Chapter, it will be defined as the Admin, Interface, Setting, Date/ Time, Logout, Install Wizard, Language, and Software Update.

3.1 Admin

ES-6000 is managed by the main system administrator. The main system administrator can add or delete any system settings and monitor the system status. Other sub administrators have no competency to modify the system settings (sub administrators' names are set by the main system administrator), but only monitor the system status.

Name

- The name of system administrator and sub administrator. **admin** is the default name of system administrator in ES-6000 and it can not be canceled, whereas sub administrators' names can be changed or canceled.
- The default system administrator can add or modify other sub administrators, and also can decide whether a sub administrator has the competency to write into system or not.

The default system administrator account and password is **admin** and **airlive**.

Privilege

- The administrator who has the competency to **read / write,** can change the system settings, monitor the system status, and to add **/** delete other administrators.
- Sub administrators with medium privilege are allowed to modify settings and monitor status, whereas those who are given low privilege can only read.

Password / New Password / Confirm Password

- To add or modify the main /sub administrator password.

Adding a Sub Admin

Step1. In **Admin Setting** window, click the **New Sub Admin**.

Step2. In **Add New Sub Admin** window, enter the following information : (Figure 3-1)

- **Sub Admin :** sub_admin
- **Password :** 12345
- **Confirm Password :** 12345
- **Privilege** set **Low**.

If a new sub admin was given high privilege, which will make him a main admin. Otherwise, else two options represent sub admin.

Step3. Click **OK** to register a new admin, or click **Cancel** to cancel.

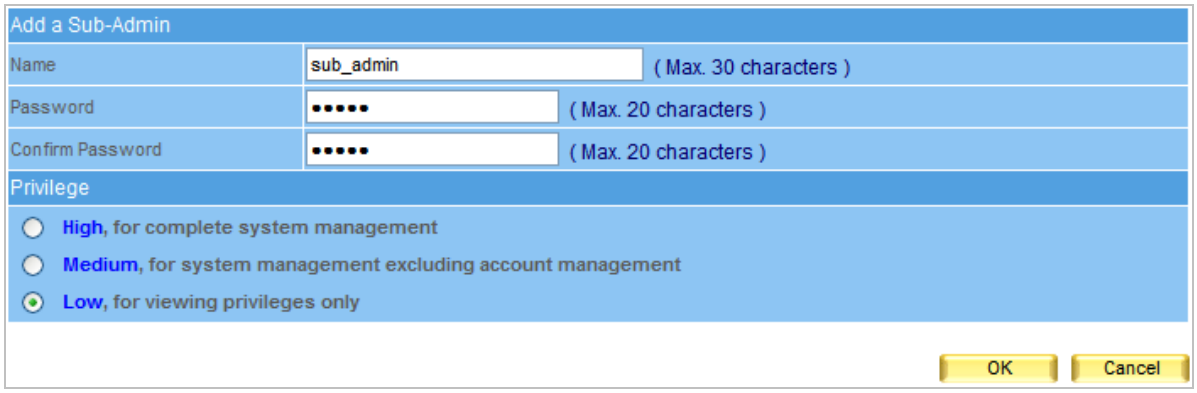


Figure 3-1 Add a sub admin

Modifying Admin's Password

Step1. Select an admin that you want to modify, then click **Modify** in the configure column in cope with that admin.

Step2. In **Modify Admin Password** window, enter the following information :

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

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

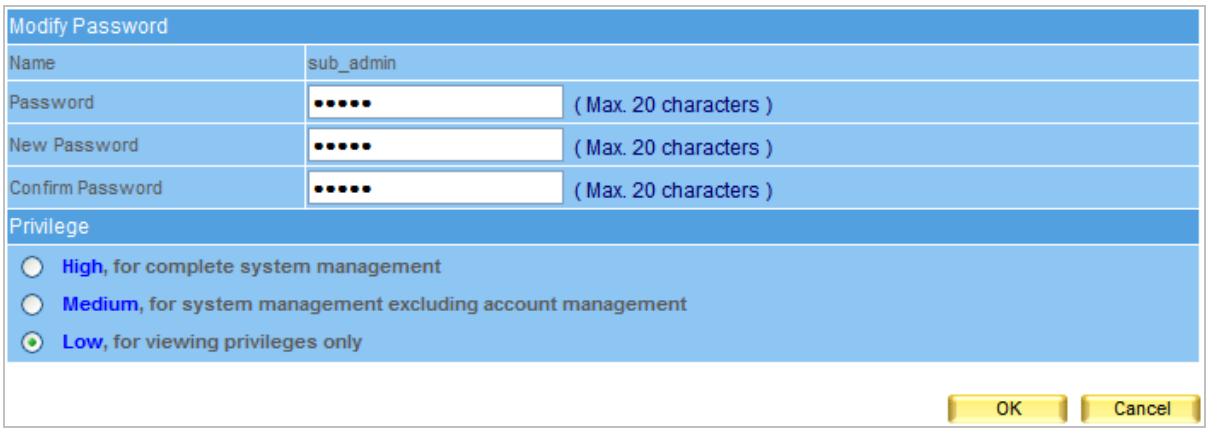


Figure 3-2 To change the admin password

3.2 Interface

Interface → Interface Address

- The administrator can set the IP login information in ES-6000.

Interface Address Setting

Step1. Go to System → Interface, enter the following setting :

- In IP Address, Netmask and Default Gateway fields, enter a valid IP of the LAN subnet.
- Enter DNS server 1 or DNS server 2.
- Click OK. (Figure 3-3)

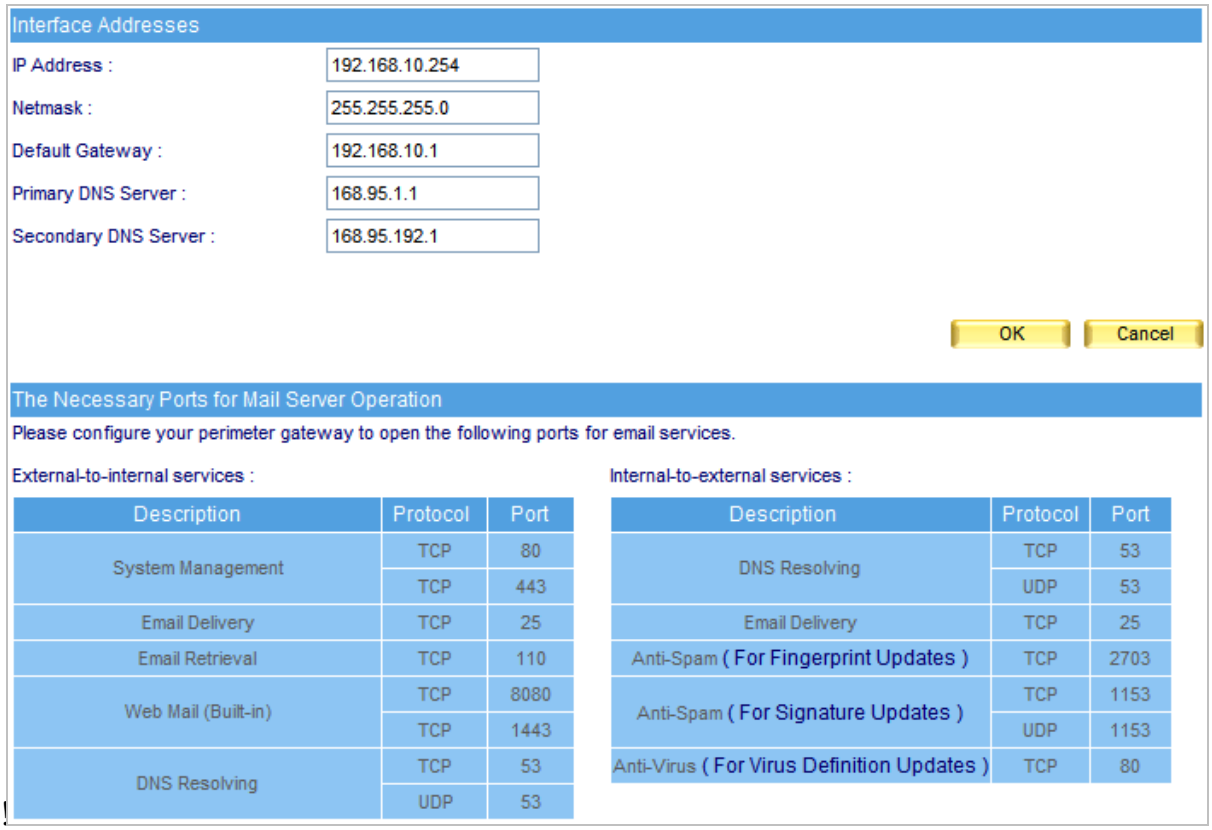


Figure 3-3 The interface address setting

3.3 Setting

- **Configuration**

  Allow system administrator to import / export system settings or reset the factory setting or format the built-in hard disk.

- **Backup System Setting to Hard Disk of Mail Server**

  System settings can backup to the storage section of built-in hard disk automatically or manually. It can be used for restoring the system settings or downloading system settings as a file onto local computer for archive purpose.

- **Format Built-in Hard Disk**

  Allow system administrator to format the built-in hard disk.

- **Name Setting**

  System administrator can enter the name of both company and device.

- **Send Notification / Report**

  When user enables this function, operating log or system error will be timely reported to the system administrator via e-mail.

- **Management Interface Port**

  ES-6000 allows system administrator to perform remote control from everywhere through web browser. The port number for HTTP or HTTPS protocol is alterable.

The port number is required for accessing the management interface from external network. User can choose to select HTTP or HTTPS based on the requirement. The port number has to be appended to the management IP address, such as http:// 172.16.1.254:8080 or https://172.16.1.254:1025.

- **Default Character Encoding for Email Messages**

  The device will use the default character encoding on e-mails with unspecified character encoding.

- **Maximum Number of items Shown per Page**

  It determines the maximum entries shown per page on each kind of list.

- **Data Storage Time**

  It decides the storage time of event log, connection track and quarantined e-mails.

Exporting System Setting to Client

Step1. Go to **System → Setting → System Setting, click** Download next to **Export System Setting to Client**.

Step2. When confirmation dialogue box **File Download** appears, click **Save** button, and it will show where the file will be saved. Click **Save** button again. The system setting file will be copied to the appointed directory. (Figure 3-4)

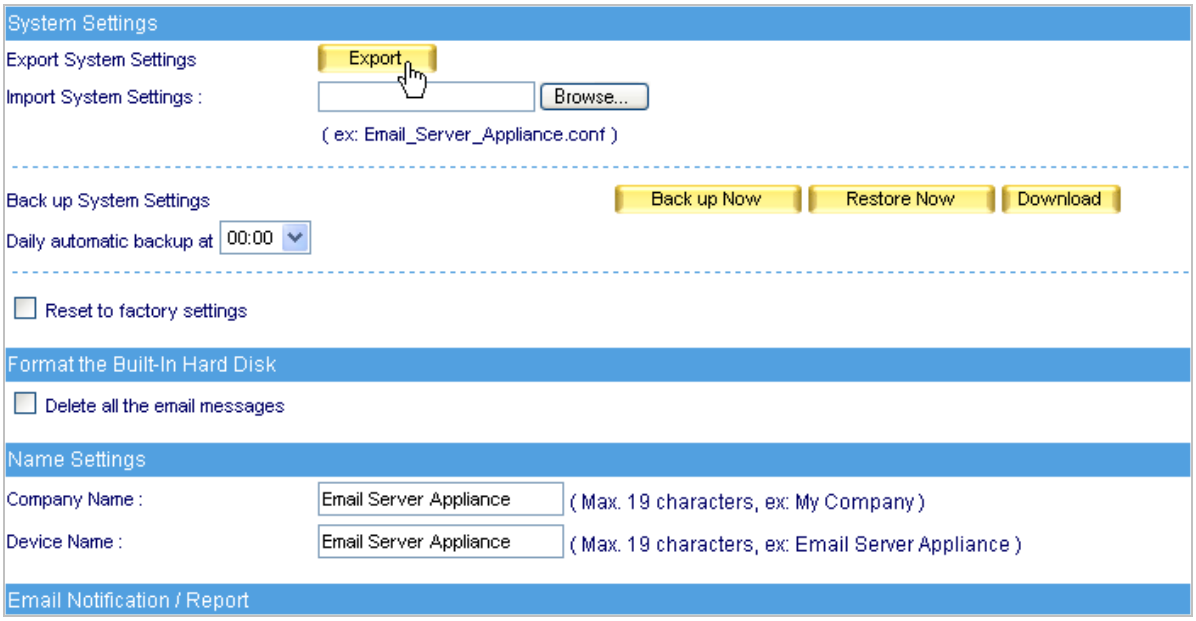


Figure 3-4 Choose a folder to save the export file

Importing System Setting to Client

Step1. Go to **System → Setting → System Setting**; click **Browse** next to **Import System Setting to Client**.

Step2. In **Choose File** window, go to the directory where the ES-6000 system setting file was stored and select the file, then click **Open**. (Figure 3-5)

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

Step4. Click **OK** on the confirmation dialogue box, the setting will be imported to ES-6000. (Figure 3-6)

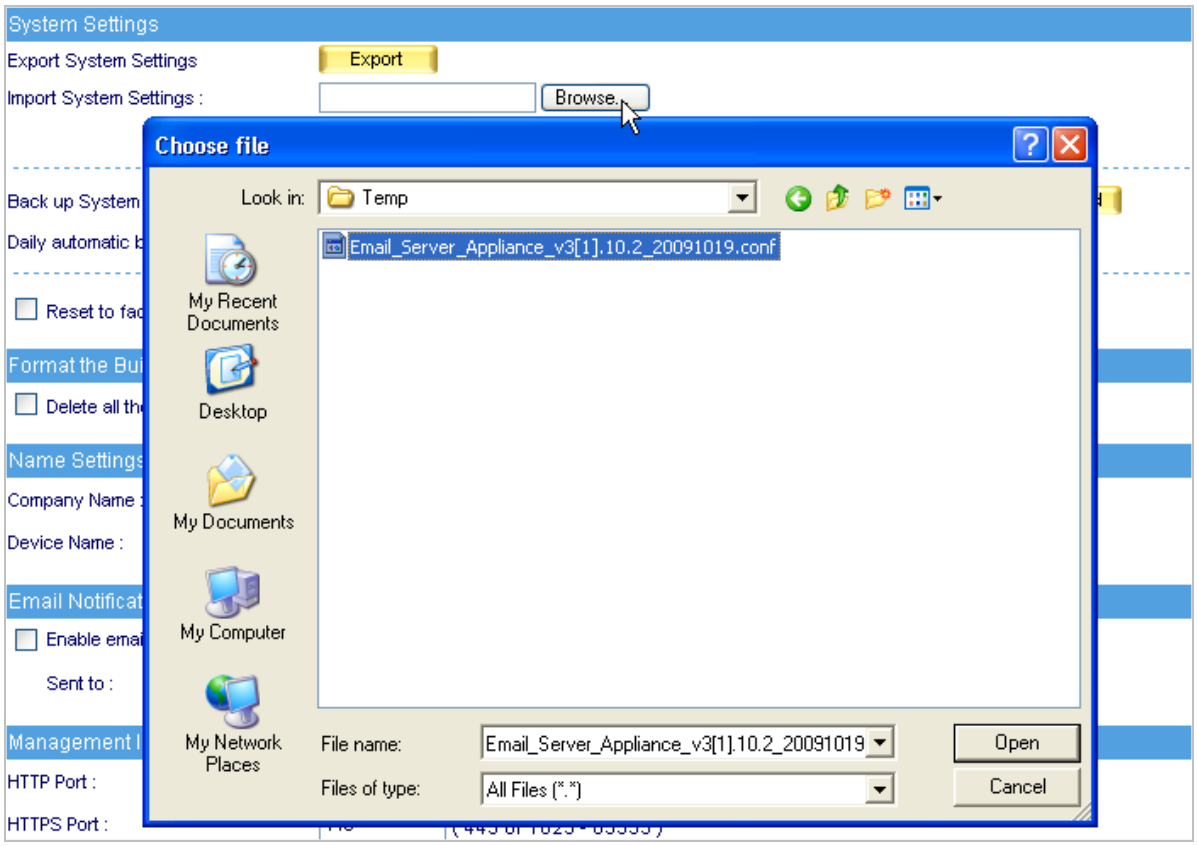


Figure 3-5 Import system setting file

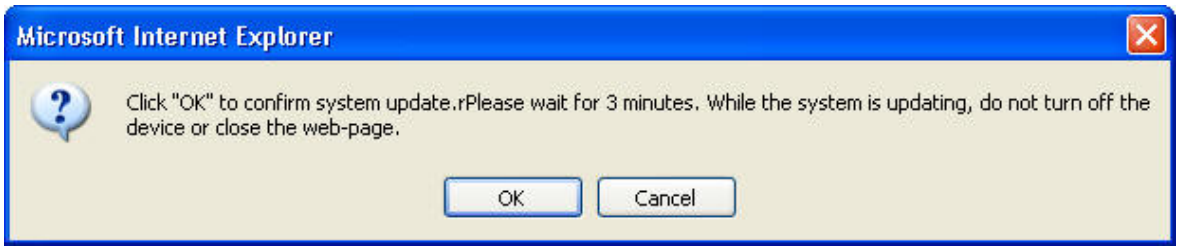


Figure 3-6 Confirm to import system setting

Resetting Factory Setting & Formatting Built-in Hard Disk

Step1. Go to **System → Setting**, select Reset Factory Setting and Format Hard Disk.

Step2. Click **OK** on the lower right, it will start restoring to the factory setting and formatting the built-in hard disk at the same time. (Figure 3-7)

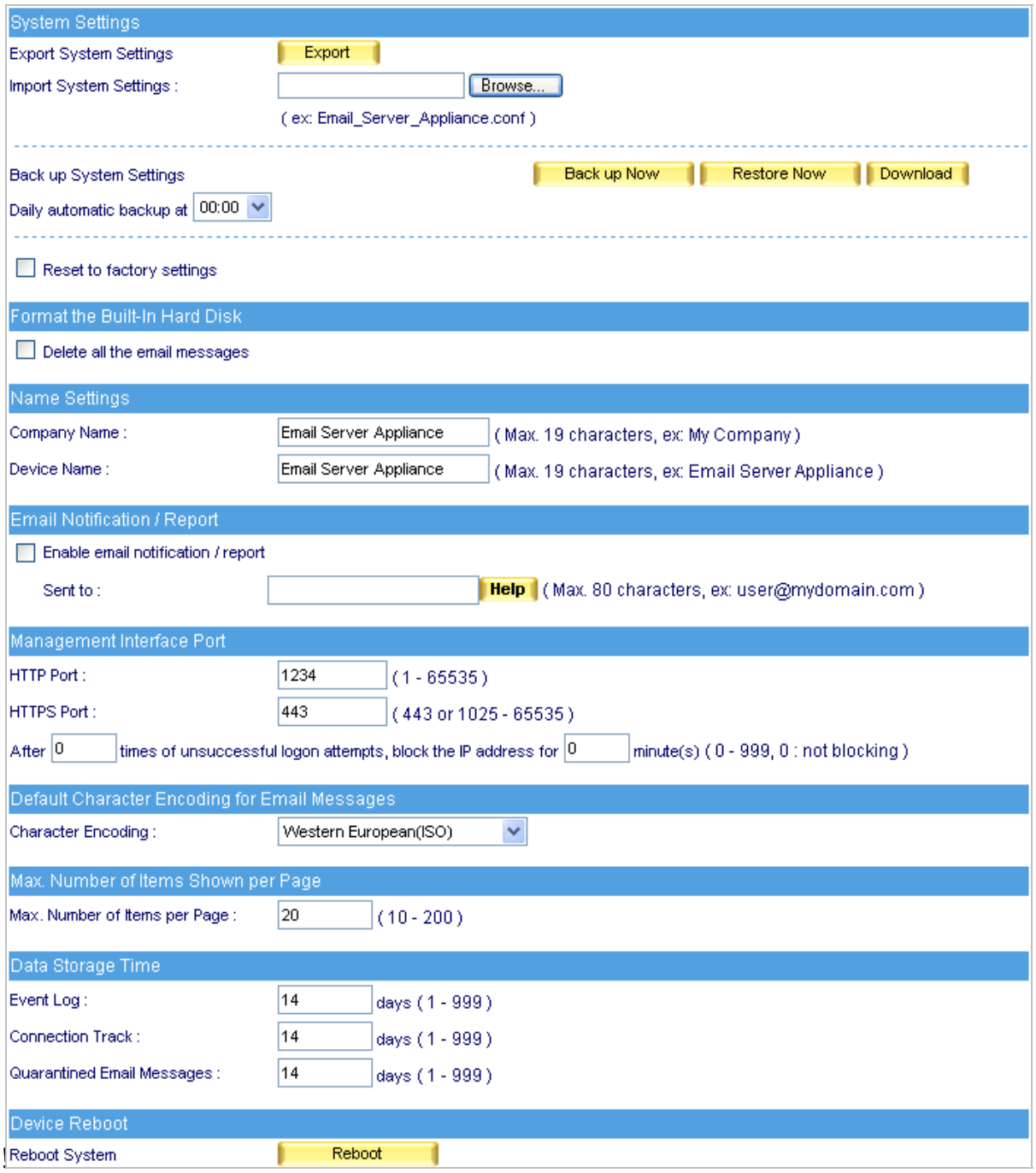


Figure 3-7 Reset factory setting and format hard disk

Mail Notice Setting

Step1. Enter the name of the company in the blank field next to **Company Name**.

Step2. Enter “ES-6000” in the blank field next to **Device Name**.

Step3. Tick **Enable Mail Alert Notification / Report**.

Step4. Enter an internal email address in **Internal E-mail Account** field.

Step5. Click **OK** on the lower right to set the function of message alarm. (Figure 3-8)

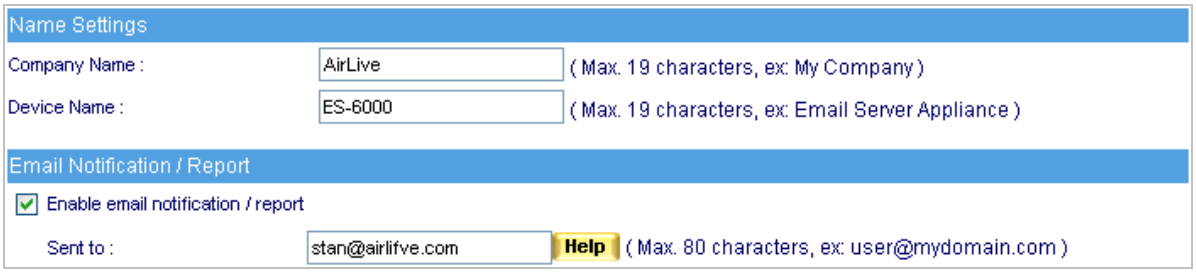


Figure 3-8 Enable the instant message alarm

Rebooting System

Step1. Click **Reboot** on the right of **Reboot Appliance.**

Step2. A confirmation dialogue box saying “**Are you sure to reboot?”** appears.

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

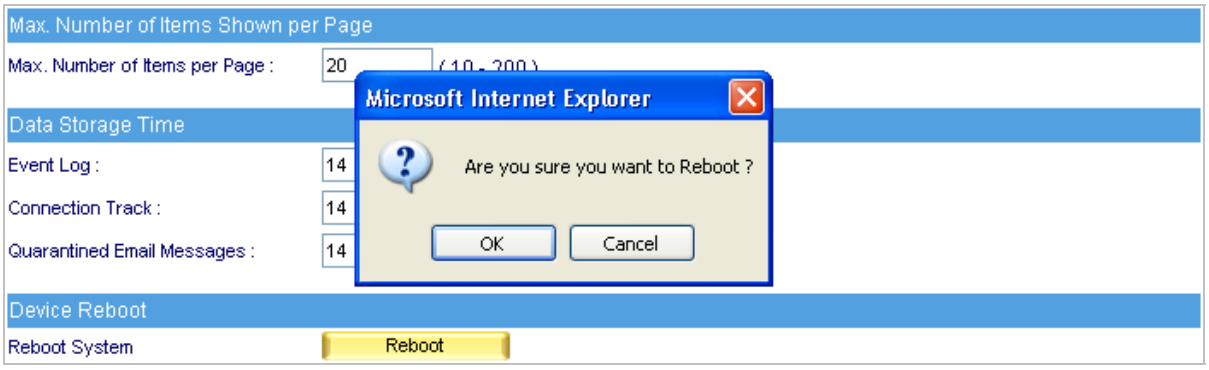


Figure 3-9 Reboot Appliance

3.4 Storage Device

User can define the mail server's storage device to store the mail; by default, the mail will be stored at ES-6000 local hard disk, but its capacity is limited; it can be also stored at remote storage device such as file server or NAS, the capacity is flexible but the performance is less than local hard disk.

Storage Device Information

While the storage device is chosen, the utilization of storage will be displayed, and user may know the hard disk's utilization status.

Storage Device Settings

- **Local hard disk**

  It indicates the ES-6000 built-in hard disk. (Figure 3-10)

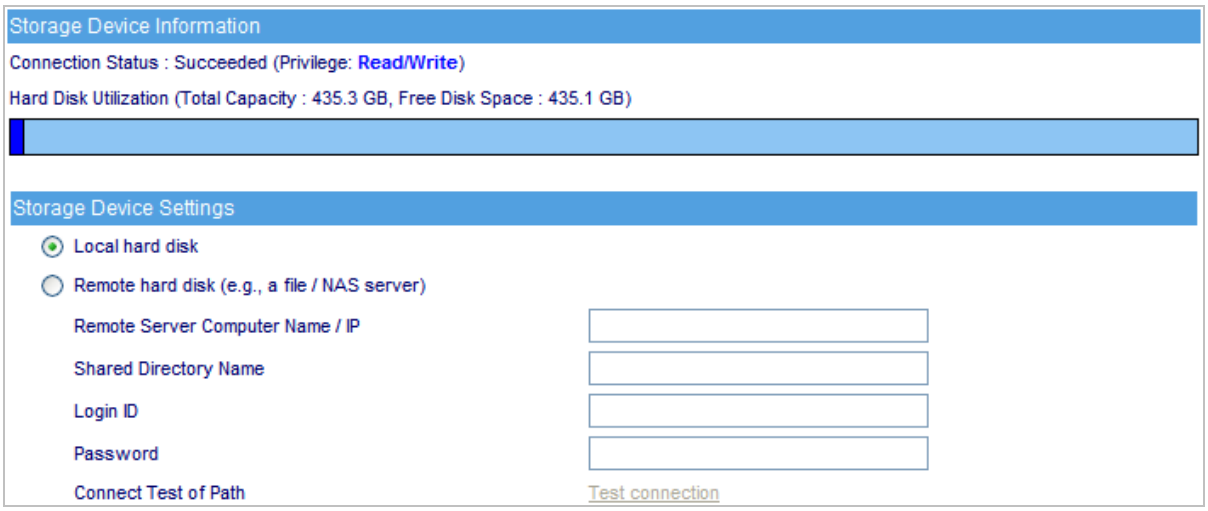


Figure 3-10 Storage Device - Local hard disk

- **Remote hard disk (e.g, a file / NAS server)**

  The ES-6000 will store the mail at remote storage device. You must specify the correct IP address and directory name; it is optional to type in Login ID and password to connect remote storage. (Figure 3-11)

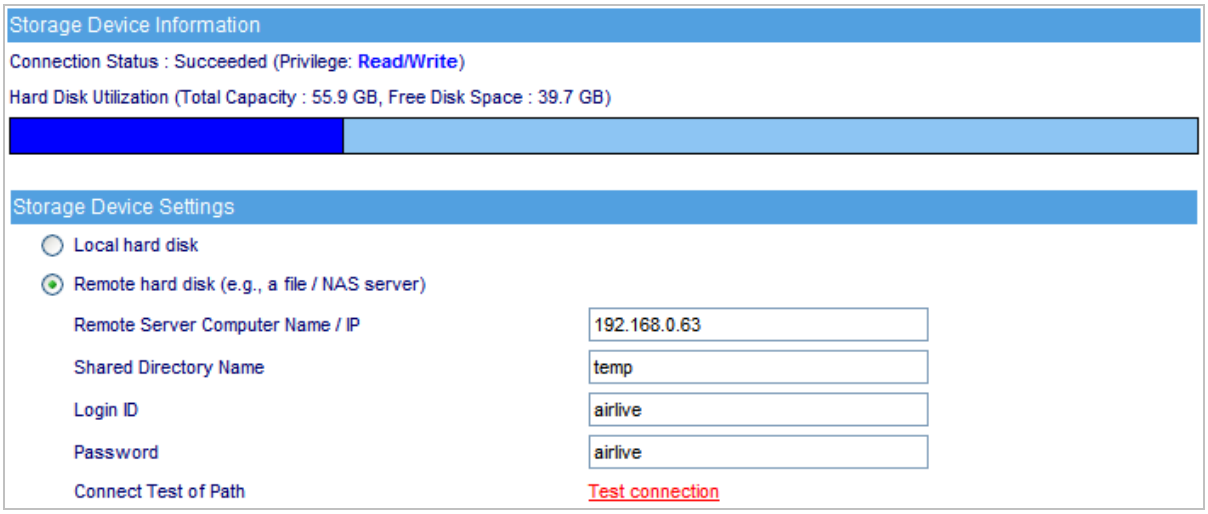


Figure 3-11 Storage Device - Remote hard disk

3.5 Date/Time

Date / Time

- **Synchronize System Clock**

  This option can synchronize system clock with the administrator's PC or the external time server.

- **GMT**

  The international standard time (Greenwich Mean Time: GMT)

- **Daylight Saving Time**

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

Date / Time Setting

Step1. Select **Enable Synchronize with an Internet Time Server.** (Figure 3-12)

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

Step3. Enter the server IP address in **Server IP / Name** field.

Step4. Enter the frequency of updating time in **Update System Clock Every Minutes**.

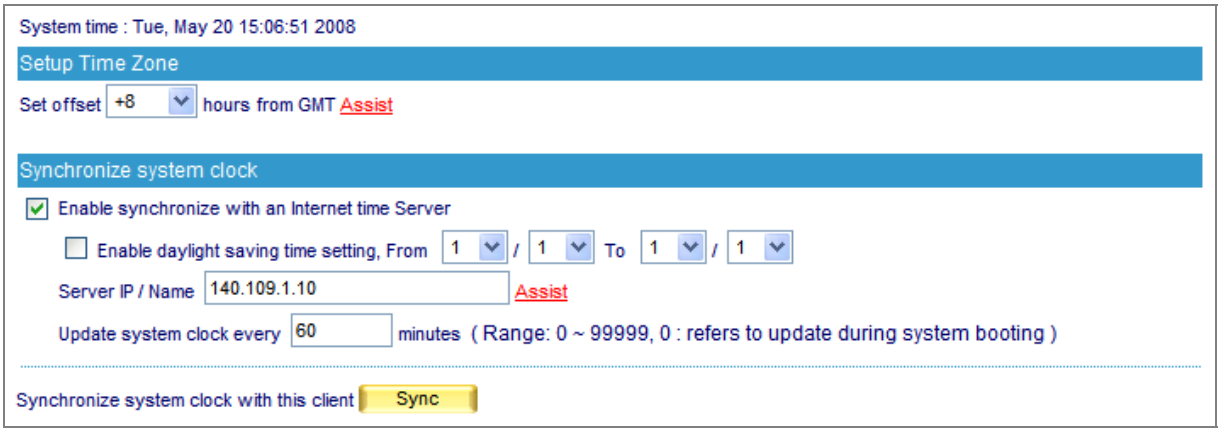


Figure 3-12 Time setting

Click **Sync** button, the system time will synchronize with the administrator's computer.

The reference for setting up the **Set offset hours from GMT** and **Server IP** is available in **Assist.**

If the local area executes the daylight saving time, then **Enable the Daylight Saving Time Setting.**

3.6 Software Update

To update firmware, please go to **System → Software Update** and follow the steps below:

Step1. Version Number indicates the current version that is running. Log onto Internet to obtain the latest version of firmware and download it onto the ES-6000 built-in hard disk.

Step2. Click Browse, then Choose File window pops up, after that, please select the latest firmware from the directory where it was saved earlier.

Step3. Click the lower right **OK**, it will start running the update procedure. (Figure 3-13)

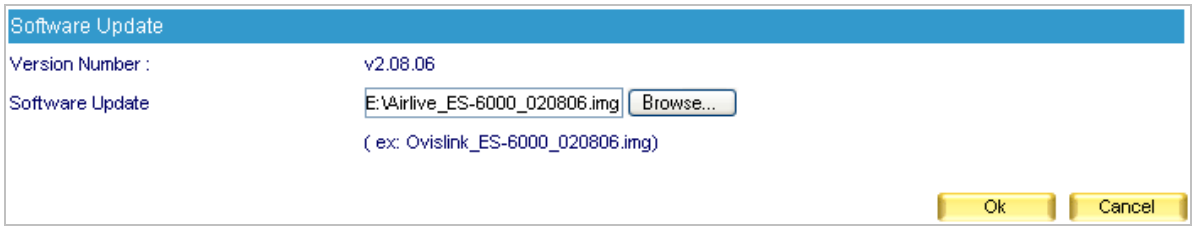


Figure 3-13 Software Update

It takes about 3 minutes to run through the update process, and will automatically reboot after the system is updated. Please do not turn off the power, disconnect the Internet or close the Web UI while running update. These acts might cause an error in the system. (Running the update in the local area network is strongly recommended.)

Chapter 4 Mail Management

4.1 Configure

Mail configure refers to policies of mail services, it is divided into three parts, namely mail management, domain alias and mail relay.

Mail setting:

- Determines of which cryptographic method and port number will be used in each service
- Assigns a port exclusively for logging to web mail interface.
- Allows email account registration from the Web Mail login screen
- Apply the physical IP address for sharing files in web disk.
- Determines the maximum amount of simultaneous connection of sending mail.
- Determines the maximum duration of a mail lifetime in Queue.
- Restricts mail delivery services with local SMTP authentication.
- Auditing outgoing mails for security's sake with mail gateway
- Auto-adjusts the built-in mailbox quota, avoiding insufficient inbox storage space

4.1.1 Setting

Mail Setting Definition:

TLS + SSL:

Transport Layer Security (**TLS**) and its predecessor, **Secure Sockets Layer** (**SSL**), are cryptographic protocols that provide secure communications on the Internet. There are slight differences between SSL and TLS, but the protocol remains substantially the same. However, TLS used to operate at transport layer, which now has changed into alternations between application layer and transport layer. (Figure 4-1)

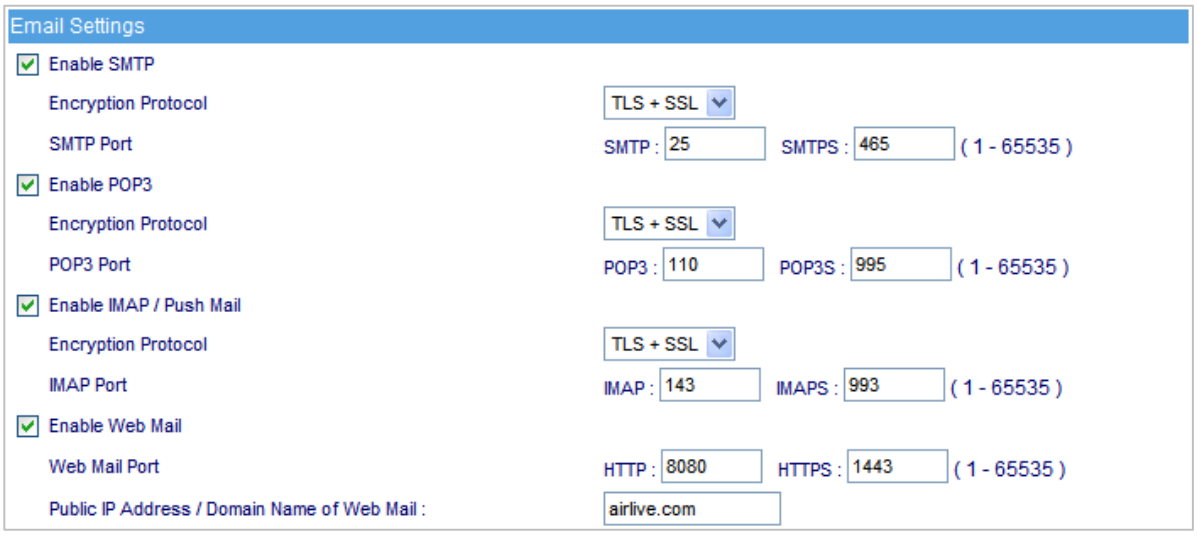


Figure 4-1 Email Setting

Reverse DNS lookup:

Reverse DNS lookup determines whether a domain name is associated with the sender's IP address.

Block Dictionary attacks:

A dictionary attack is an attack which uses a dictionary to randomly generate email addresses that are directed to the same domain.

Account Request Setting:

ES-6000 allows users performing account registration from the Web Mail login screen. If this feature is enabled, it is recommended to set the **Account Request Setting** to **Approval by administrator**; If set to **No approval needed**, then the device might be compromised to send spam.

Max. message queueing time:

What if users' mails failed the delivery, the mail will save in ES-6000 queue and waiting for the next delivery. Users can define the lifetime of mail in queue, when the lifetime is end, the mail will be removed from queue and return a failure notification to sender.

SMTP recipient limit:

The value for **SMTP recipient limit** will affect the system performance. It is not recommended to set a value to more than 100.

Enable Local SMTP Authentication:

When SMTP authentication enabled, users must meet one of the requirements listed below to process mail delivery.

1. Either sender's source IP address or recipient's domain name must exist on the Mail Relay list.
2. Sender has to apply the correct user name and password to SMTP authentication.

Enable Local Delivery Authentication:

Select Enable Local Delivery Authentication function that works to defend mail system against hacker, who delivers spam mail within the same domain. .

Enable Inbox Quota Auto-Adjustment:

When enabled, the device will:

1. Alert both the user and system administrator about the insufficient space upon inbox usage of 80%.
2. Delete older mails until the usage has lowered to 70% as well as alert both the user and system administrator about the insufficient space upon inbox usage of 90%. (Figure 4-2)

Figure 4-2 Mail Configuration setting

Default Value of New Account:

- Allocates the default size of mailbox, Inbox, Web Disk and the maximum size of incoming mails. (The settings here does not apply to those settings made in individual mail management)
  - Below is an example for your reference :
    1. Tick **Enable SMTP**
    2. Select **TLS+SSL** from the pull-down menu for **Security Session**
    3. Enter “25” for **SMTP** and “465” for **SMTPS**
    4. Tick **Enable POP3**
    5. Select **TLS+SSL** from the pull-down menu for **Security Session**
    6. Enter “110” for **POP3** and “995” for **POPS**
    7. Tick **IMAP**
    8. Select **TLS+SSL** from the pull-down menu for **Security Session**
    9. Enter “143” for **IMAP** and “993” for **IMAPS**
    10. Tick **Enable Web Mail**
    11. **Web Mail Port: HTTP** set as “8080**”** and **HTTPS** set as “1443”
    12. Configure **Public IP Address / Domain Name of Web Mail** accordingly
    13. Tick **Enable reverse DNS lookup**
    14. Tick **Block dictionary attacks**
    15. Select **Approval by administrator** from the drop-down list for **Account Request Setting**
    16. Enter “10” for **The number of sessions allowed per IP address per minute**
    17. Enter “50” for **The number of maximum concurrent sessions per IP address**
    18. Configure **Max. message queueing time** as “4 Hours”
    19. Enter a desired value (recommended less than 100) for **SMTP recipient limit**
    20. Tick **Enable Local SMTP Authentication**
    21. Tick **Enable Local Delivery Authentication**
    22. Tick **Enable Inbox Quota Auto-Adjustment**.
    23. Click **OK**. (Figure 4-3)

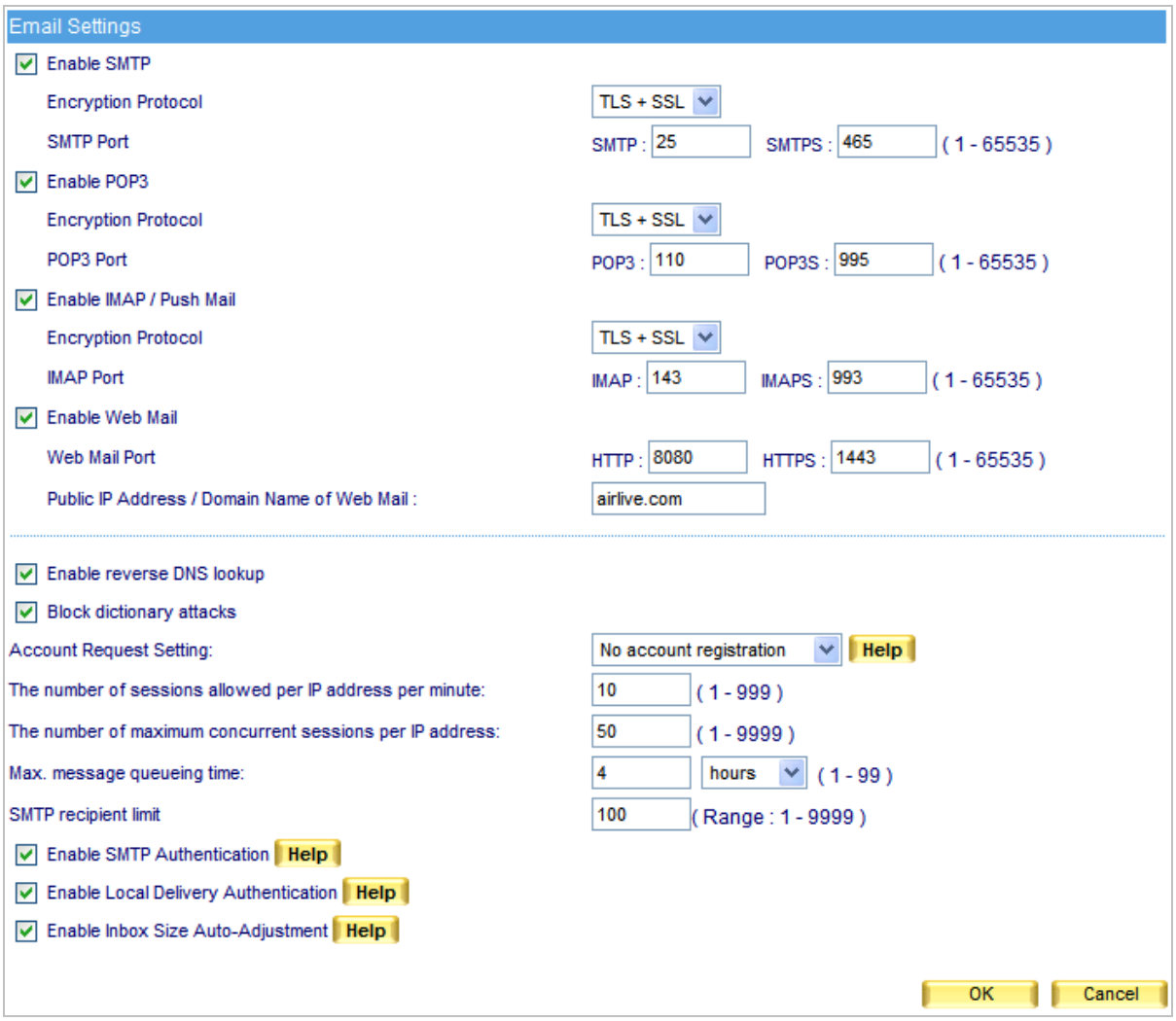


Figure 4-3 Mail management configuration

Once **Inbox Quota Auto-Adjustment** is enabled, ES-6000 will check each built-in mail account for available inbox storage. Both the account user and the system administrator will receive an e-mail notification about inbox usage reaching 80%; when inbox usage reaches 90%, the device will send out an e-mail notification as well as delete the older e-mail messages until the usage has lowered to 70%.

For client users using e-mail program, ES-6000 device requires the configuration of e-mail protocols and port numbers. Below is an example on how to configure the port numbers in Outlook Express:

1. On the menu bar, click **Tools** and then **Accounts…**. (Figure 4-4)

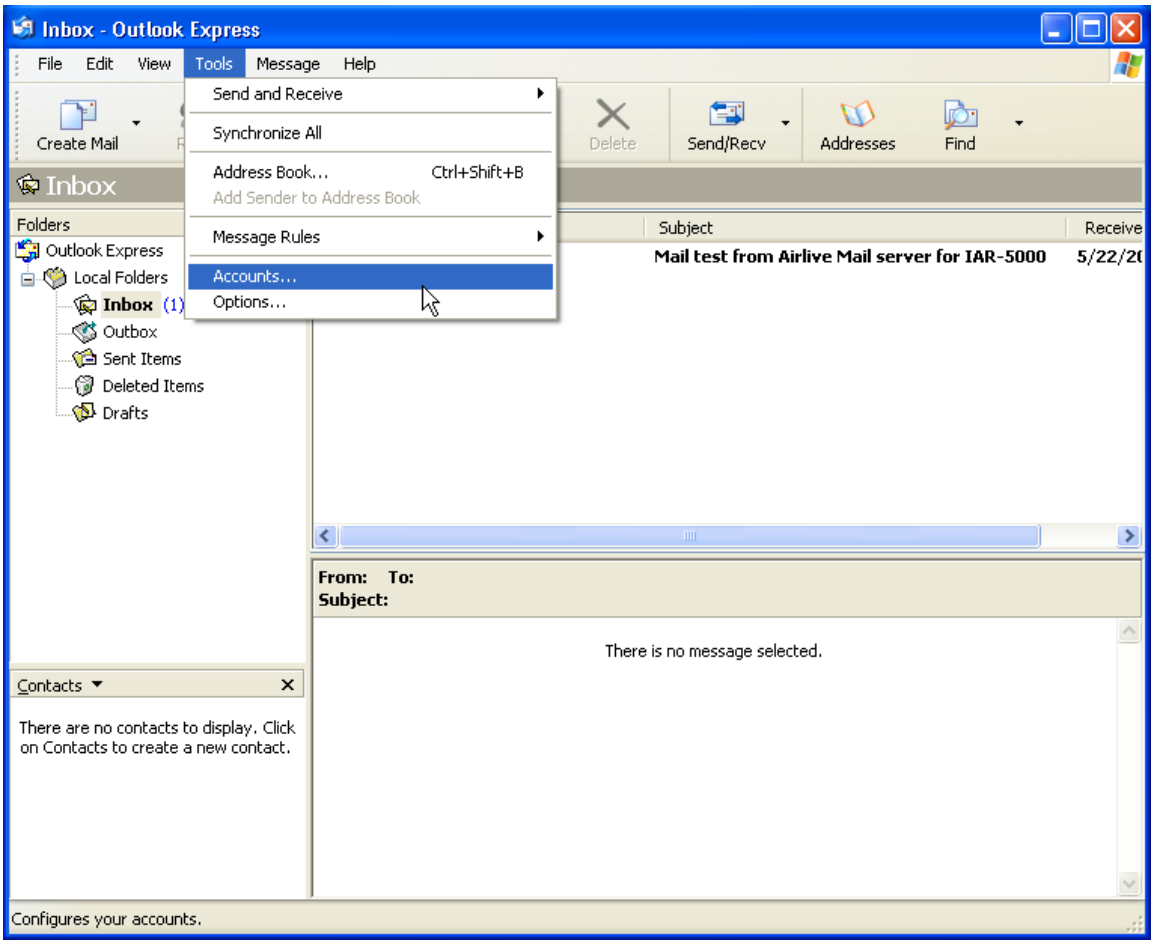


Figure 4-4 Opening Internet Accounts

2. Click **Mail** tab and then the desired account to change. Next, click **Properties** on the right. (Figure 4-5)

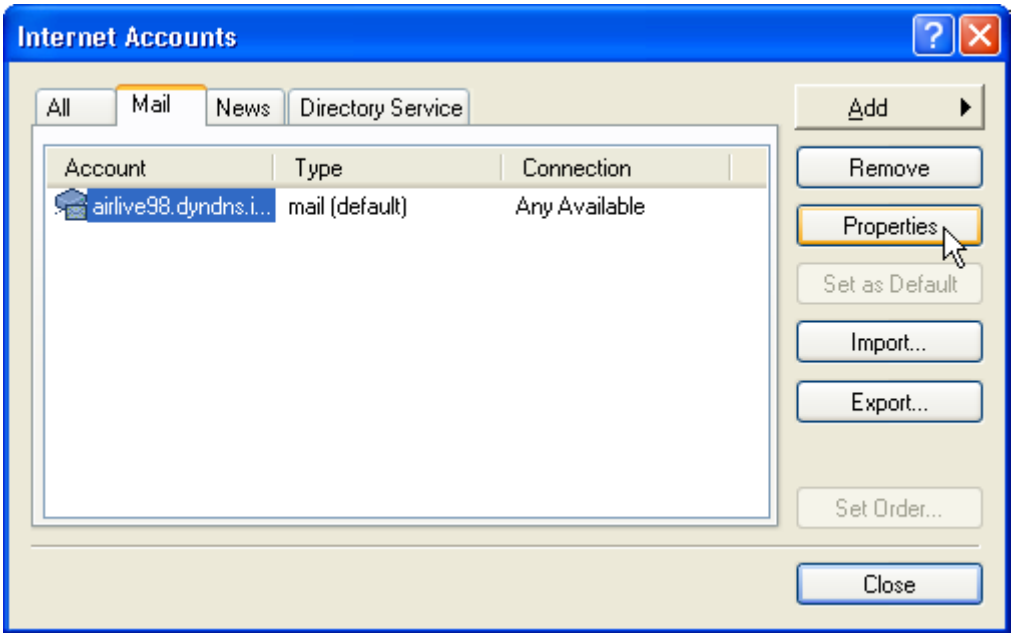


Figure 4-5 Opening Internet Accounts

3. In the **Properties** window, click **Advanced** tab to adjust the port numbers for SMTP and POP3 protocols. When finished, click **OK**. (Figure 4-6)

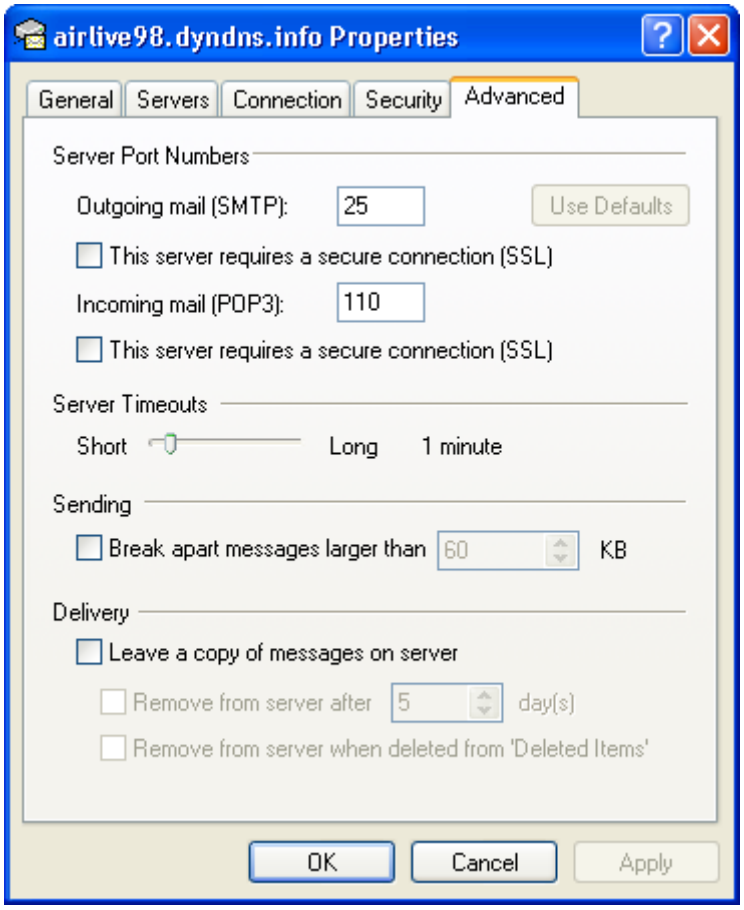


Figure 4-6 Server Port Number Settings

4. Close **Internet Accounts** window. (Figure 4-7)

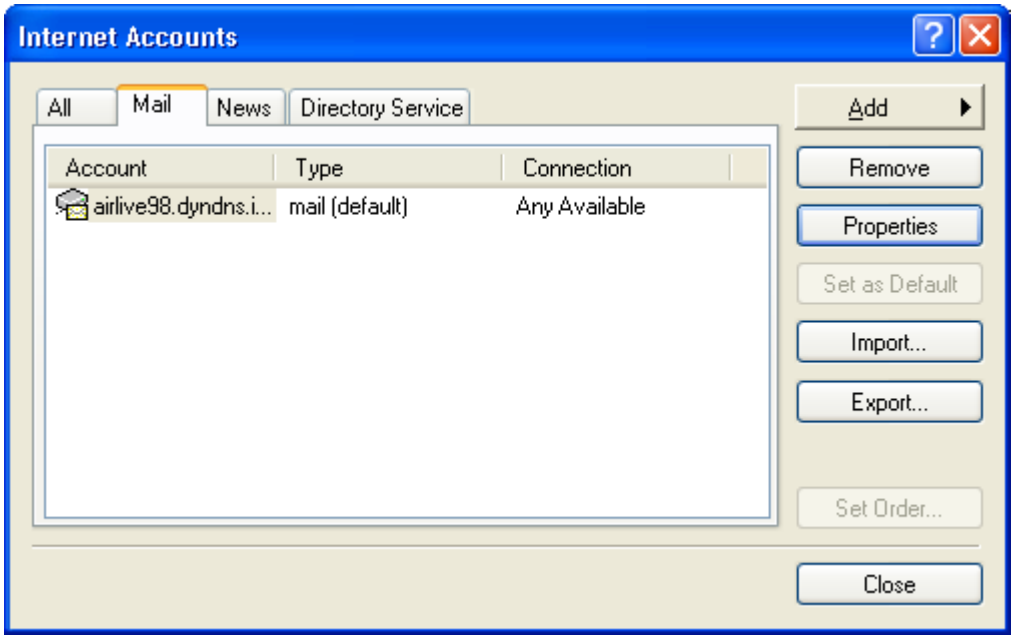


Figure 4-7 Closing Internet Accounts

4.1.2 Web Mail Logo

ES-6000 allows user to upload a background picture as web mail wallpaper. The image file should be limited as:

Max. File Size: 1 Mbytes

Resolution: 1022 x 622 pixels

File Types: jpg, jpeg, jpe, gif, bmp, png... (Figure 4-8)

Figure 4-8 Upload picture as wallpaper

If user would like to check the display, click “Preview” and verify the image. (Figure 4-9)

Figure 4-9 Homepage of Web Mail

4.1.3 Multiple Domains

Definition:

- **Multiple Domains**

  The function is allowed to configure several domains on a single device, and each domain has its own mail accounts. When user send mails to the accounts of different mail domain, the accounts will receive their own mail.

- **Domain Alias**

  On ES-6000, each mail domain can also create Domain Alias. The difference between Multiple Domain and Domain Alias is that Multiple Domains have their own mail accounts, but the account of Domain Alias is the same one of Mail Domain. So, when user sends mail to an account of Mail Domain and Domain Alias, actually the mails will be sent to the same mail box.

Using Multiple Domains to Provide Mail Service

Step1. Apply to local ISP for several domain names, “airlive.com”, “ovilink.com.tw”, “airlive-info.com” and “airlive-sales.com” for instance, to provide mail service.

- The Alias Domain of “**airlive.com**” is “**ovislink.com.tw**”.
- The Alias Domain of “**airlive-info.com**” is “**airlive-sales.com**”

Step2. Under **Mail Management → Configure → Multiple Domains**, set as below:

- Click **New Entry**
- Type “test.com” in the **Domain Name** field.
- Click OK. (Figure 4-10)
- Click **New Entry**.
- Type “test1.com.tw” as its alias. (Figure 4-11)
- Click **OK** to complete the first entry. (Figure 4-12)
- Click submenu item “**Multiple Domains**” on the left panel.
- Click **New Entry**.
- Type “test-info.com” in the **Domain Name** field.
- Click **OK**. (Figure 4-13)
- Click **New Entry**.
- Type “test-sales.com” as its alias. (Figure 4-14)
- Click **OK** to complete the second entry. (Figure 4-15, 4-16)

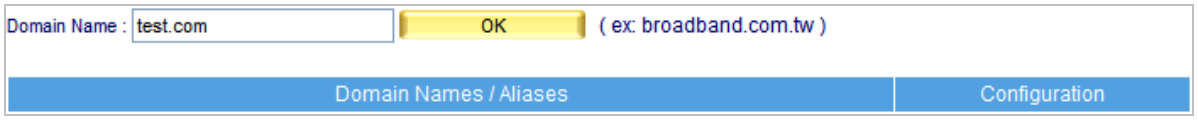


Figure 4-10 Typing the First Domain Name

Figure 4-11 Typing the Domain Alias

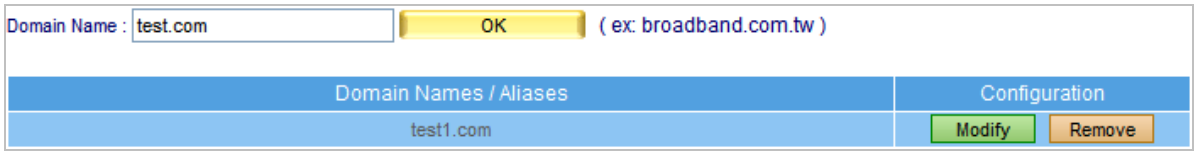


Figure 4-12 Alias Added

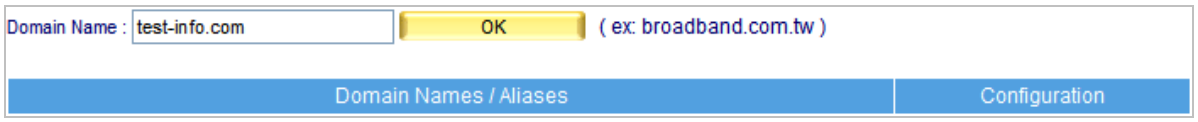


Figure 4-13 Typing the Second Domain Name

Figure 4-14 Typing the Domain Alias

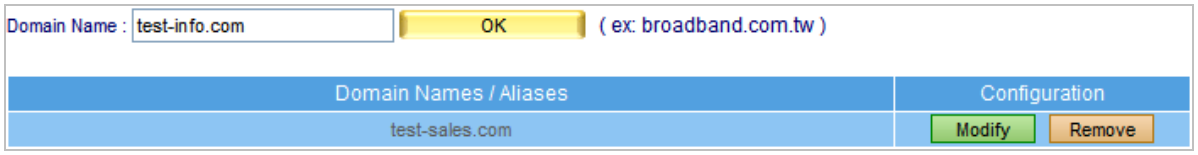


Figure 4-15 Alias Added

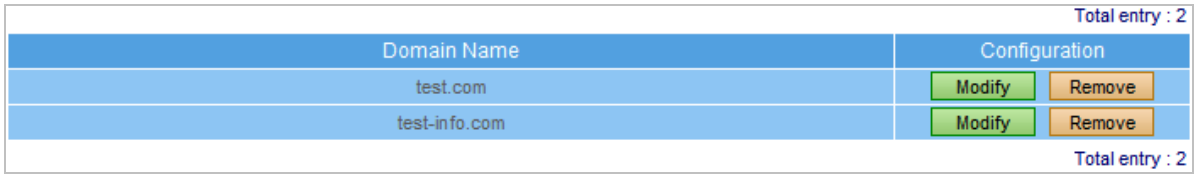


Figure 4-16 Second Entry Completed

Step3. E-mails that go to stan@test.com or its alias stan@test1.com will be stored in the same storage location, the internal account “stan” will be able to retrieve them by logging in to either account.

Step4. E-mails that go to stan@test-info.com or its alias stan@test-sales.com will be stored in the same storage location, the internal account “stan” will be able to retrieve them by logging in to either account.

Step5. It can be concluded from **Step 3** and **4** no matter how many aliases a domain has, whether e-mails go to the domain itself or any of the aliases, the recipient will be able to retrieve them anyhow.

4.1.4 Mail Relay

Mail Relay works to define the available IP subnet or domain to allow replaying mail via the mail server.

Enabling Replay to an IP subnet or Domain Name

Preparation

Perimeter Firewall set as **192.168.0.0 / 24**

ES-6000 Virtual IP Address set as **192.168.0.248**

ES-6000 Physical IP Address set as **60.250.158.64**

Map registered domain name “airlive.com” to DNS IP address which is assigned mail server IP to MX record.

Step1. Enable internal senders to send mails, please go to **Mail Management → Configure → Mail Relay** for settings :

- Click **New Entry** to enter the first entry.
- Check **IP Address**. (This enables relay to this IP address)
- **IP address** set as 192.168.0.0
- **Netmask** set as 255.255.255.0
- Click **OK** to complete the first entry. (Figure 4-17, 4-18)
- Click **New Entry** to enter the second entry.
- **IP address** set as 60.64.125.55
- **Netmask** set as 255.255.255.255
- Click **OK** to complete the second entry. (Figure 4-19, 4-20)

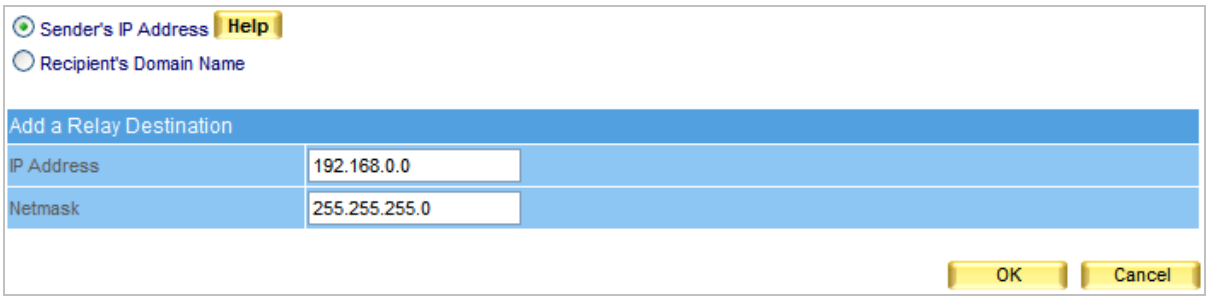


Figure 4-17 Enter the first entry to enable relay

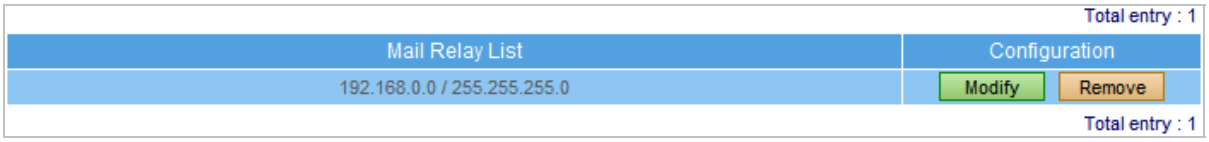


Figure 4-18 Complete the first entry

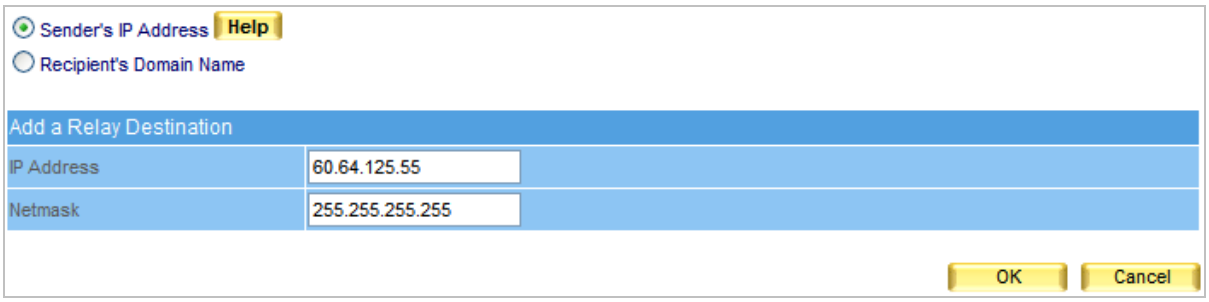


Figure 4-19 Enter the second entry to enable relay

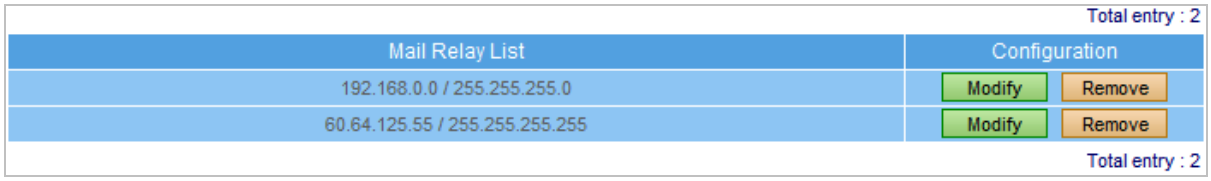


Figure 4-20 Complete the second entry

Step2. Enable external senders to send mails via relay, please go to **Mail Management → Configure → Mail Relay** for settings:

- Click **New Entry**.
- Check **Domain Name**. (This enables relay to this Domain name)
- **Domain Name** set as airlive.com
- Click **OK** to complete the setup process. (Figure 4-21, 4-22)

Figure 4-21 Enter an domain name to enable relay

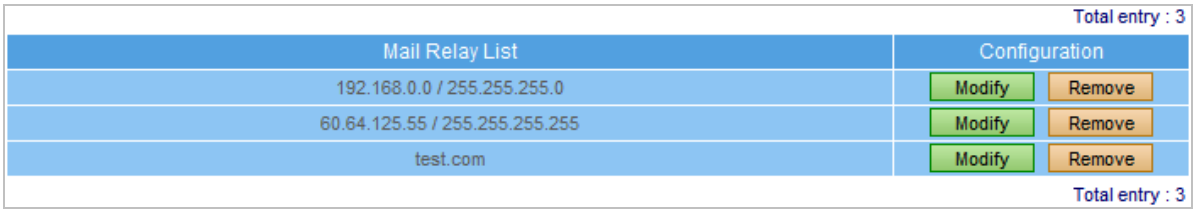


Figure 4-22 Domain name setup completed

When **Local SMTP Authentication** is activated, internal accounts sending mails off-site does not required setting up the **Relay**.

4.1.5 Mail Signatures

Enable Mail Signature function will add the signature on all outgoing mails.

Step1. On **Mail Management → Configure → Mail Signature** setting, add a new entry.

- Click **Add signatures to all outgoing messages**.
- Fill in the content you want to publish on the message.
- Press OK to finish the setting. (Figure 4-23)

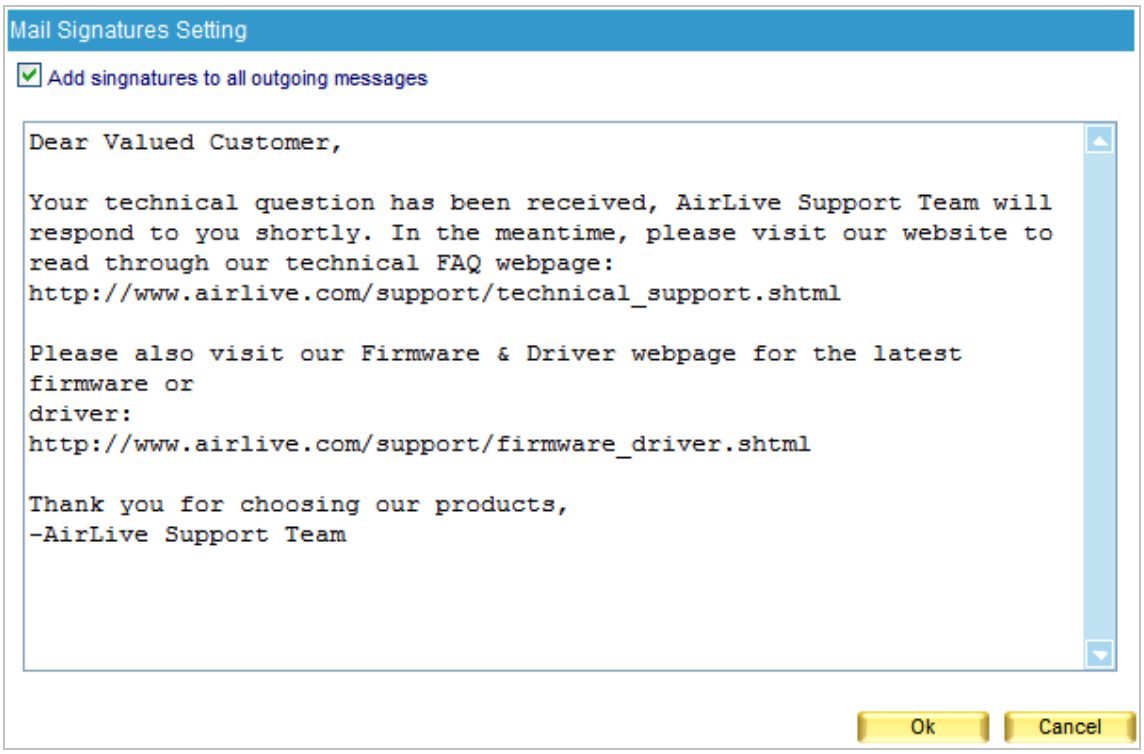


Figure 4-23 Mail Signature setting

Step2. User will fine the message on the bottom of mail content for all outgoing mails. (Figure 4-24)

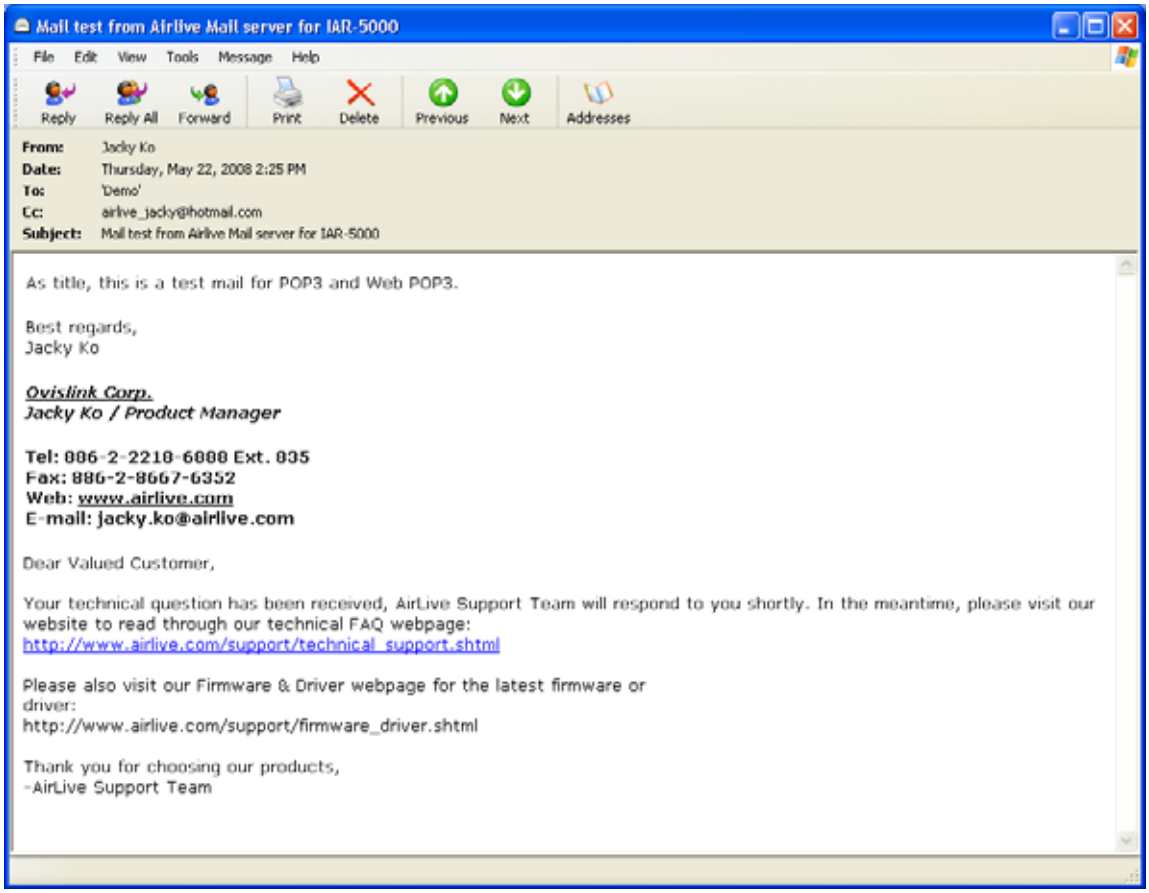


Figure 4-24 Recipient receives mail with signature

4.1.6 Mail Routing

IP Address of Mail Gateway

Enter the mail gateway IP address in this column, all outgoing mails will pass to mail gateway, and send to recipient. Mail Routing also allows administrator arranging some mail services, such as mail backup or auditing, to construct more completely mail services.

Assigning a Mail Server to Process E-Mails from Specific Domains or E-Mail Addresses

Step1. Decides using which mail server to relay e-mail messages.

Step2. Under **Mail Management → Configure → Mail Routing**, refer to the steps below to make settings:

- Click **New Entry**.
- Specify of which **Relayed Domain Name / Mail Address** is to be relayed.
- Specify a mail server in the **Mail Relay Server IP / Domain Name** field.
- Specify a port number for creating a SMTP connection with the mail server.
- Determine whether to employ SMTP authentication accordingly. (Figure 4-25)
- Click **OK** to complete settings. (Figure 4-26)

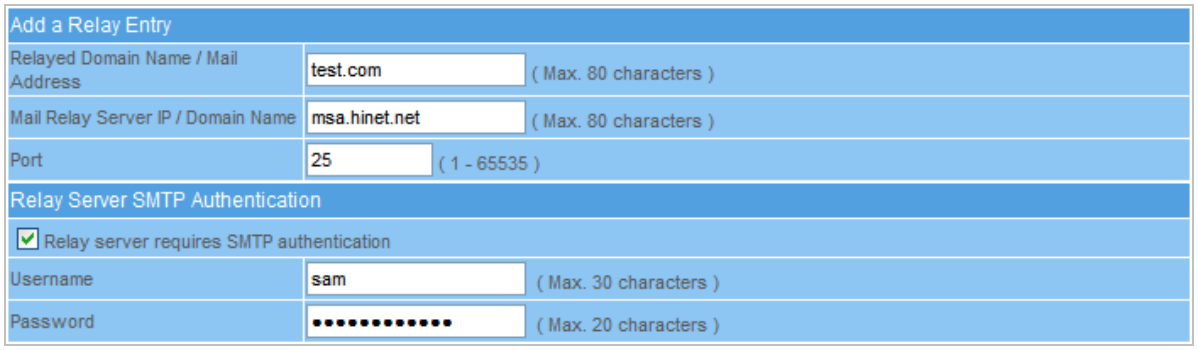


Figure 4-25 Mail Routing Settings

Figure 4-26 Mail Routing Setting Completed

Step3. E-mails sent from the ES-6000's mail accounts to the domain name / mail address you specified will be relayed by the mail server you designated

Supposed the **Relayed Domain Name / Mail Address** setting is given an asterisk (*), then e-mail delivery to the mail accounts, except for those of ES-6000, will be processed by the relay server you designated.

4.2 Account Management

The most troublesome step of setting up a mail server is creating e-mail accounts. With approaching like ***Automatically Adding***, ***Query Old / LDAP mail server***, and ***Import*** function, e-mail accounts can be created or transferred in just no time.

4.2.1 Setting

Learning Account Setting

Once recipient has logged in ES-6000, mail account will automatically be created on ES-6000 according to the account and password that has logged in; Or via communicating with the old mail server or the LDAP server, mail account will be imported as an internal account when the authentication is specified.

- **Automatically Add:**
  - Check **Automatically Add**.
  - Click **OK**. (Figure 4-27)
  - Once recipient has logged in ES-6000, an internal account will be immediately created on ES-6000 according to recipient's account and password.

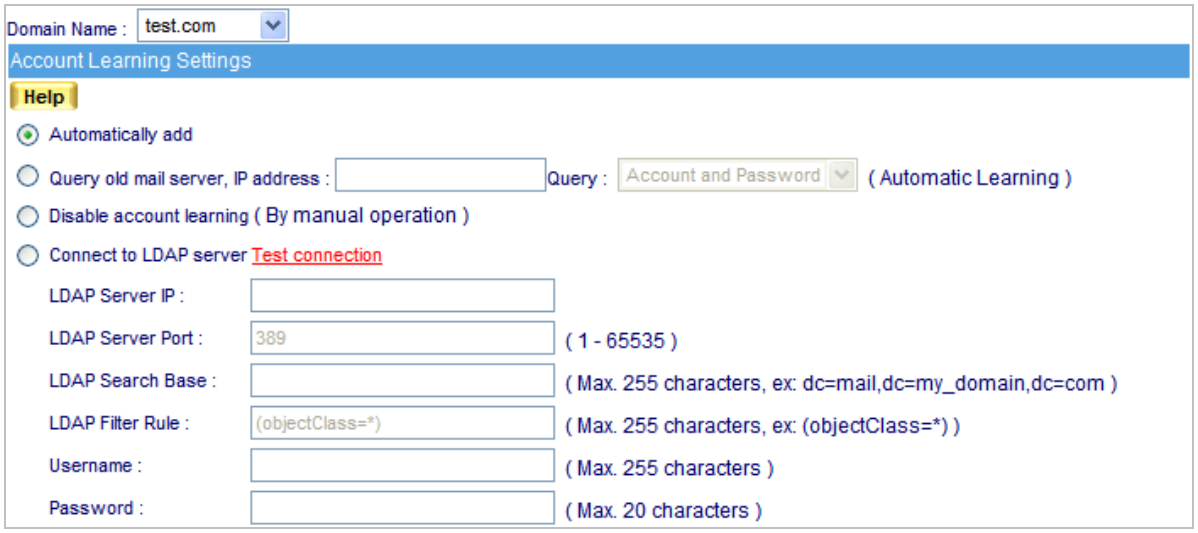


Figure 4-27 Automatically Add

◆ **Query Old Mail Server:**

- Check **Query Old Mail Server** and fill in old mail server's IP address to the blank field.
- Click **OK**. (Figure 4-28)
- When recipient has logged in ES-6000, **with the old mail server's authentication**, mail account will automatically be created on ES-6000 according to recipient's account and password. Meanwhile, ES-6000 will start to retrieve mails on the old mail server until all mails are all being transferred.

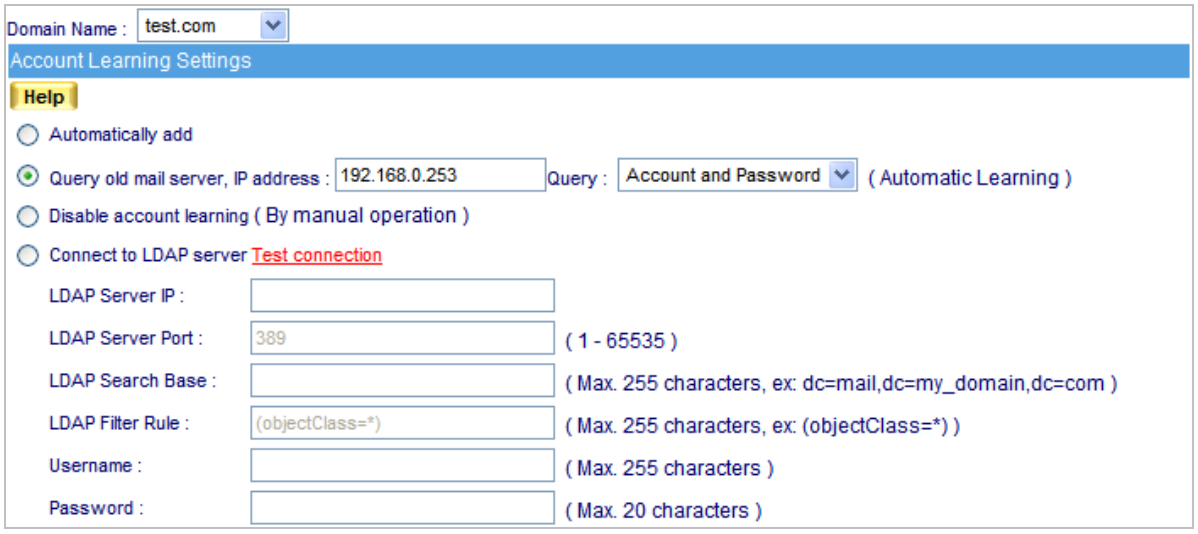


Figure 4-28 Transfer accounts and mails from old mail server

◆ **Disable Account Learning (By manual operation):**

- Check **Disable Account Learning**
- Click **OK**. (Figure 4-29)
- ES-6000 will not create any account automatically; the mail account must be created by manually.

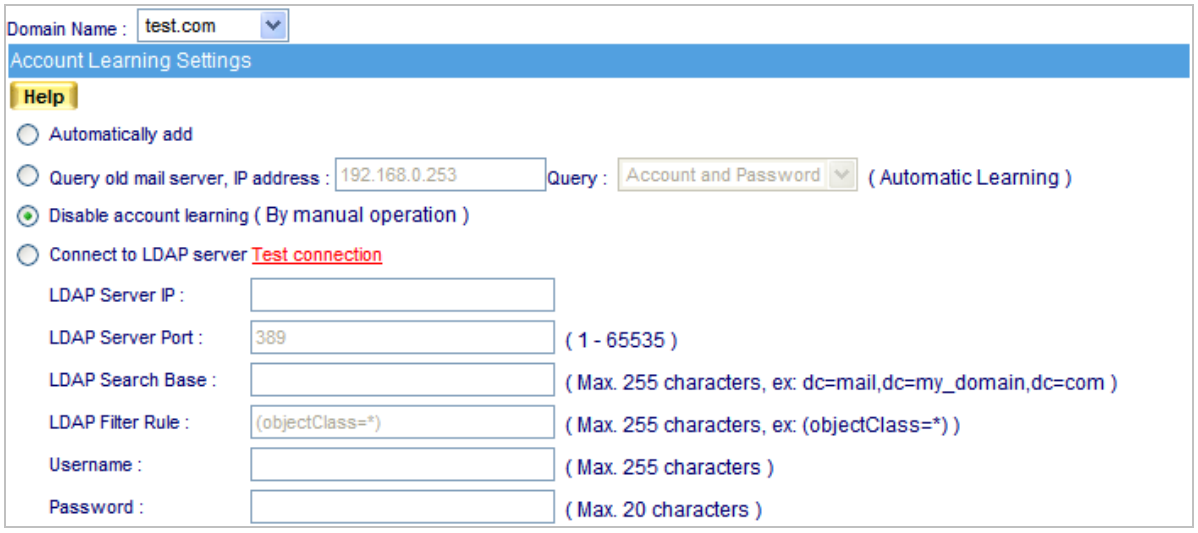


Figure 4-29 Disable Account Learning

◆ **Import Account from LDAP server:**

- Check **Connect to LDAP Server** and apply correlative addresses and settings.
- Click **OK**. (Figure 4-30)
- When recipient has logged in ES-6000, **with the LDAP mail server's authentication**, mail account will automatically be created on ES-6000 according to recipient's account and password.

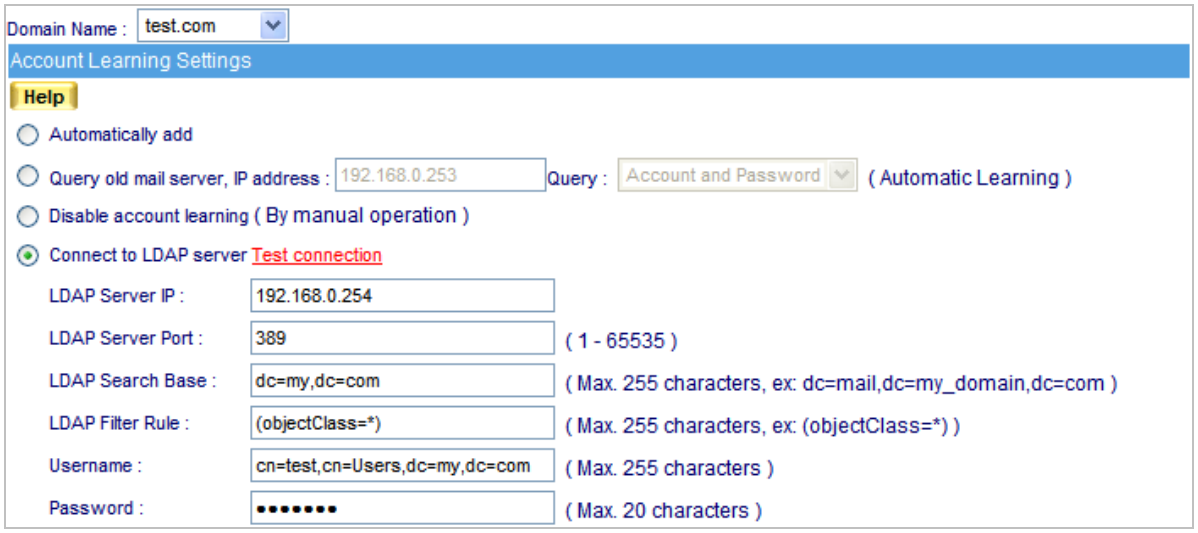


Figure 4-30 Using LDAP authentication to create new account

Default Settings for New Account

Configure **Default Settings of New Account** to define the default setting for each new account. (Figure 4-31)

- **Web Mail**, **POP3**, **IMAP**, **SMTP Inbound**, **SMTP Outbound:** Enable
- **Maximum Mail Box Quota:** 100MB (Inbox set as 50 MB)
- **Maximum Web Disk Quota:** 100MB
- **Maximum Message Size of a Mail:** 10MB
- **Push Mail Quota:** 10MB

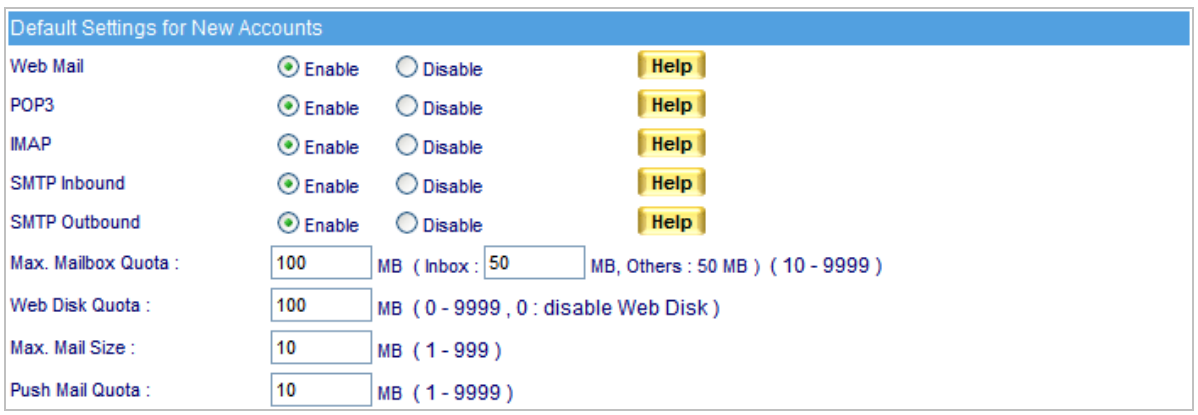


Figure 4-31 Configure Default Settings of New Account

4.2.2 Individual

Definition

◆ **Export Account:**

To export exist accounts for backup and rearrangement, please go to **Mail Management → Account Management → Individual**:

- Click **Export** next to **Export Account**.
- Click **Save** in the confirmation dialogue box, then select folder for storage, after that, click **Save**. (Figure 4-32)

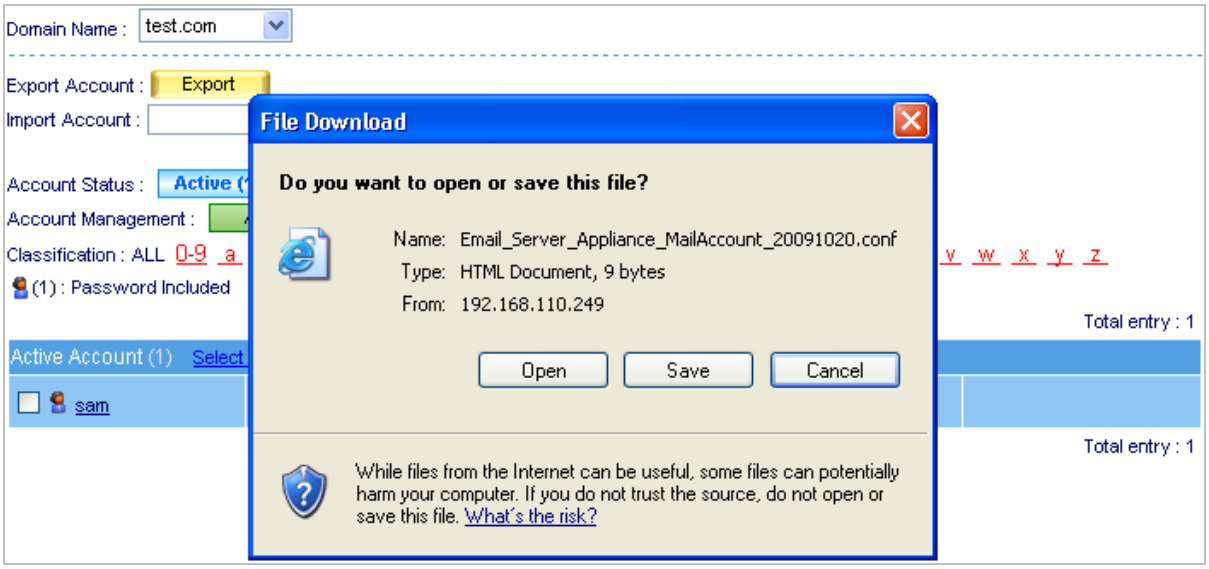


Figure 4-32 Export existed accounts

◆ **Import Account:**

To use arranged account list, go to **Mail Management → Account Management → Individual**:

- Click **Browse** to select the folder where the account list file is saved, then click **Upload**. (Figure 4-33)
- Choose file type in the **Import File Type** window, and then click **Upload**. (Figure 4-34)
- Click **OK** in the confirmation dialogue box to complete import. (Figure 4-35)

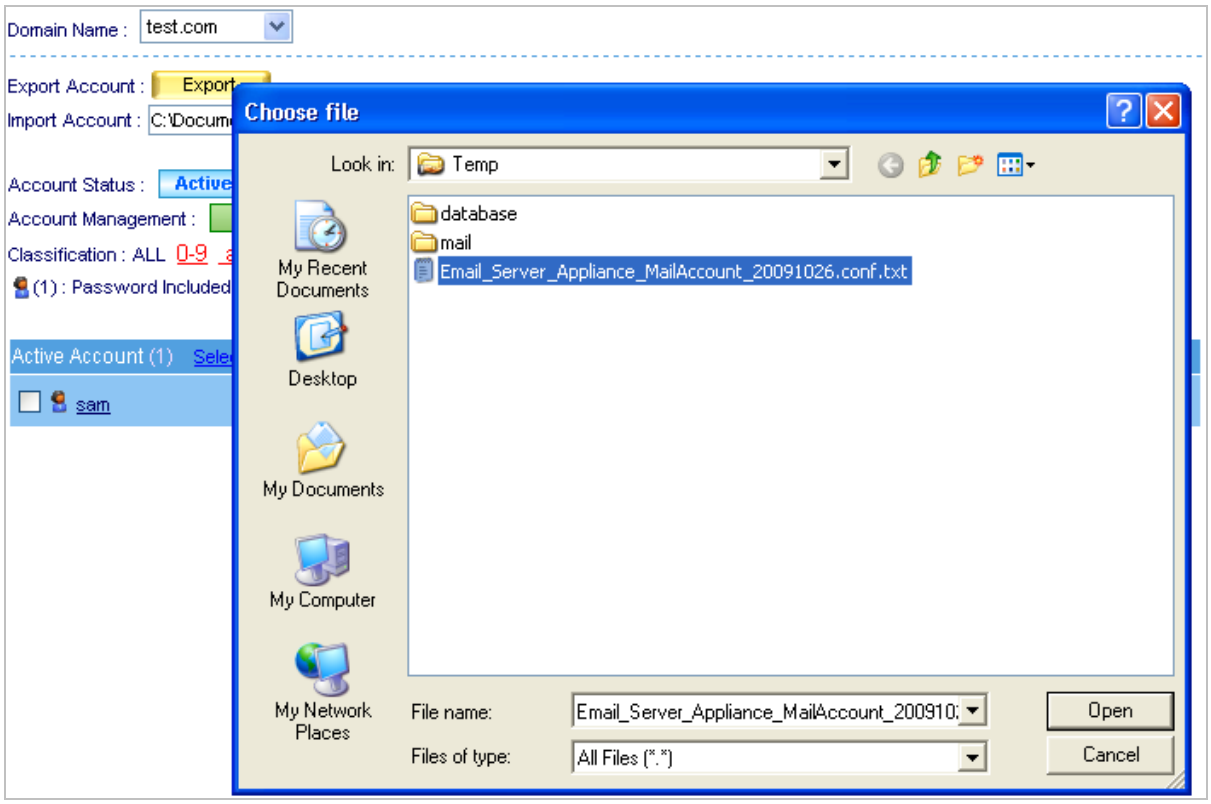


Figure 4-33 Choose account list file to import

Figure 4-34 Choose import file type

Figure 4-35 Confirm to import accounts

◆ **Individual Setting:**

To adjust individual setting, please go to **Mail Management → Account Management → Individual**:

- Click Add to Individual Setting.
- Enter account information in the Add New Account window. (Figure 4-36)
- Click OK to complete adding new account. (Figure 4-37)
- Check unwanted account, and then click **Remove** next to **Individual Setting.**
- Click **OK** in the confirmation dialogue box. (Figure 4-38)

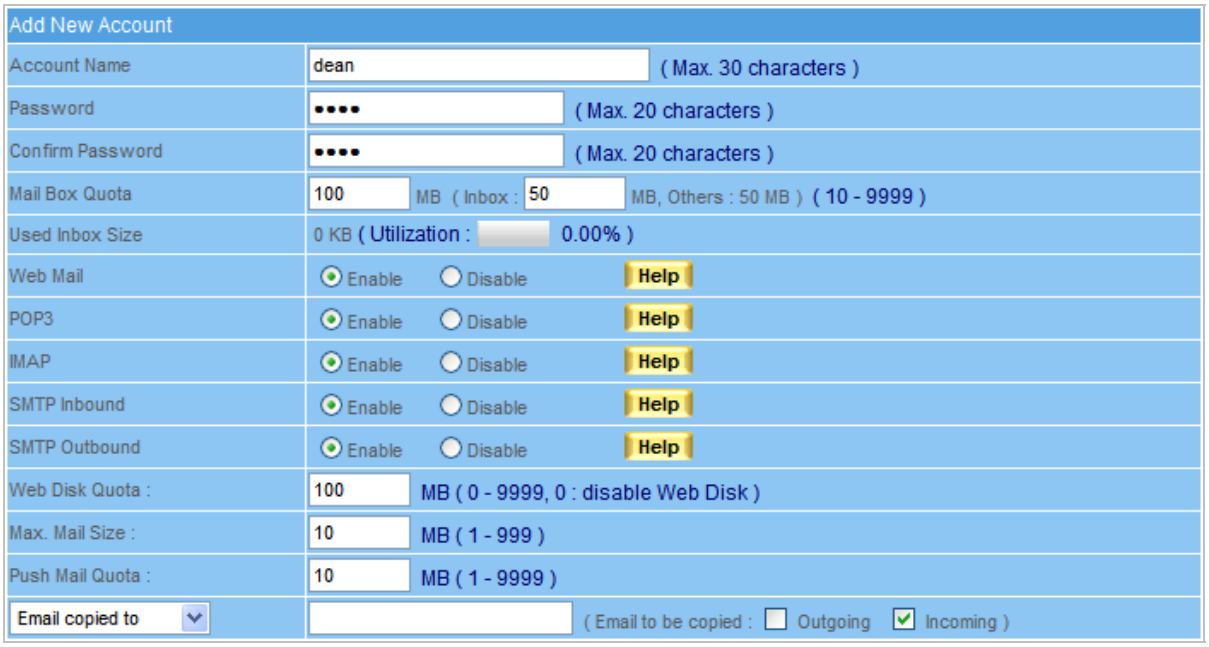


Figure 4-36 Add a new account

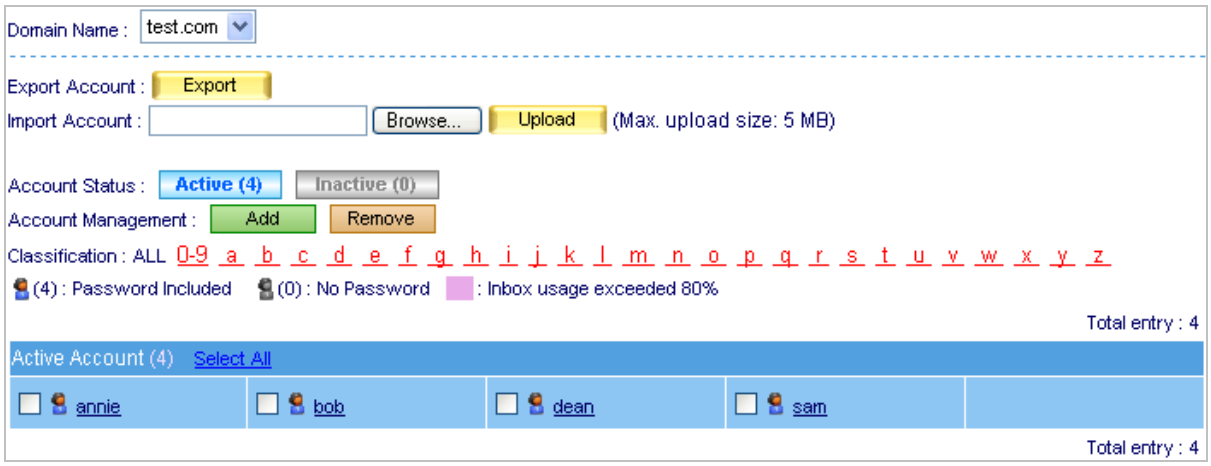


Figure 4-37 New account is added

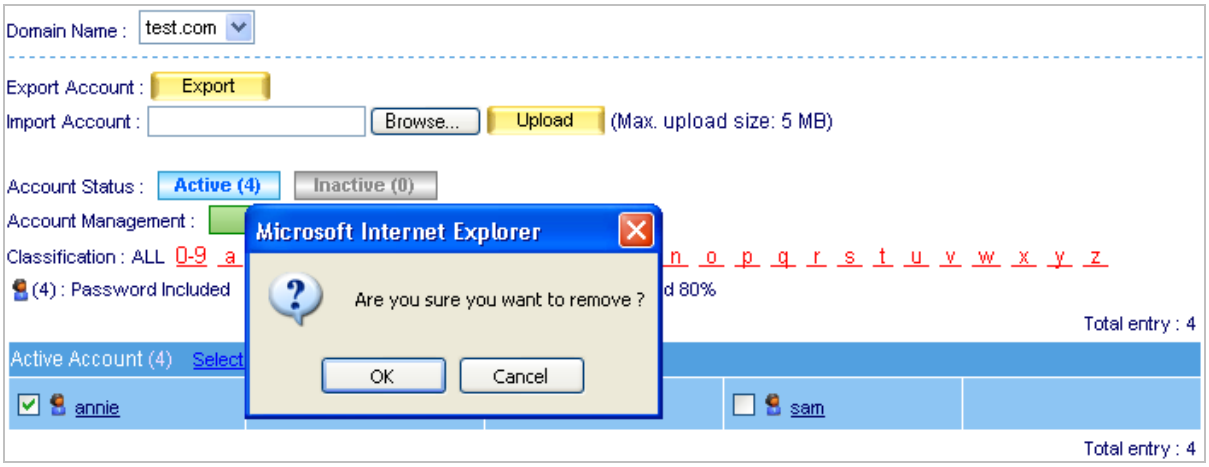


Figure 4-38 Remove an account

Auditing specific account can be achieved by forwarding or duplicating every mail into an assigned mailbox.

User can find the user quickly with Classification function. Just click the first letter of name and it will display the account list started with specific letter.

4.2.3 Group

In the path of **Mail Management → Account Management → Group**, set as followed:

- Click **Add** next to **Group Setting**.
- Name the group and select group member, then click the lower right **OK** in the **Add New Group** screen. (Figure 4-39, 4-40)
- Mails that go to a group account will be distributed to each group member.

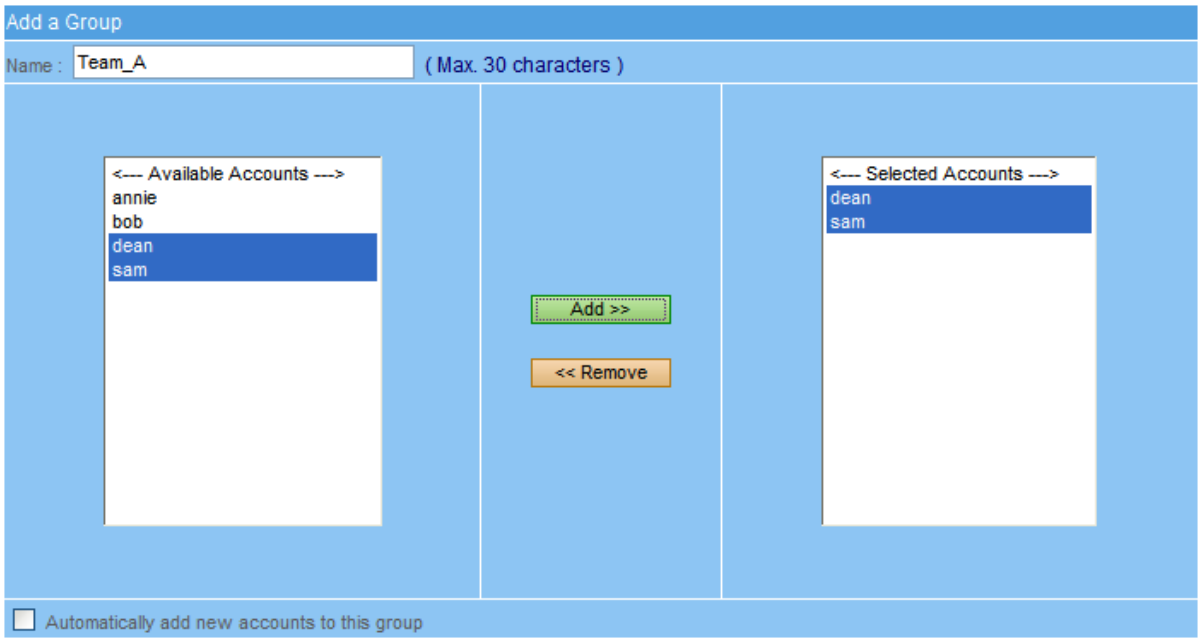


Figure 4-39 Add new group

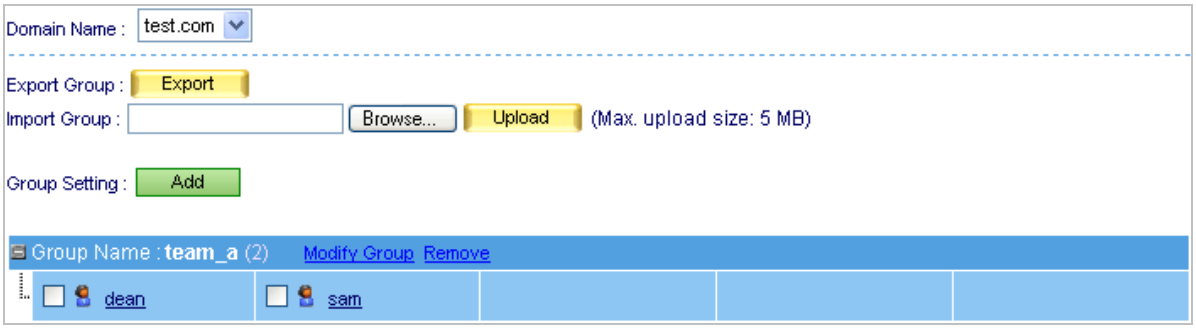


Figure 4-40 Complete forming a group

4.2.4 Shared Address Book

User can search the target via Name, E-mail Address, Company Name, Office Name, and Job Title, and find out the matched one in ES-6000 Shared Address Book records.

◆ **Export Address Book:**

To export the address book, go to **Mail Management → Account Management → Shared Address Book**:

- Click **Export** next to Export Account Book.
- Click **Save** in the confirmation dialogue box, then select folder for storage, after that, click **Save**. (Figure 4-41)

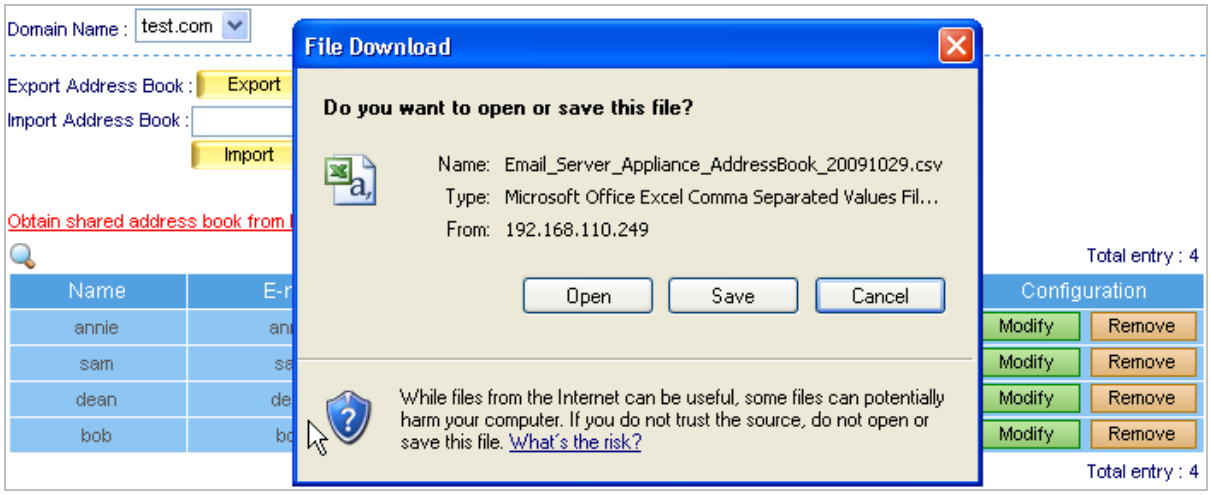


Figure 4-41 Export Address Book

System administrator may add detailed information to each contact in **Shared Address Book**.

◆ **Import Address Book:**

To import Address book, go to **Mail Management → Account Management → Shared Address Book**:

- Click **Browse** to select the folder where the account list file is saved, then click **Open**. (Figure 4-42)
- Choose file type in the **Import File Type** window, and then click **Import**.
- Click **OK** in the confirmation dialogue box to complete import. (Figure 4-43)

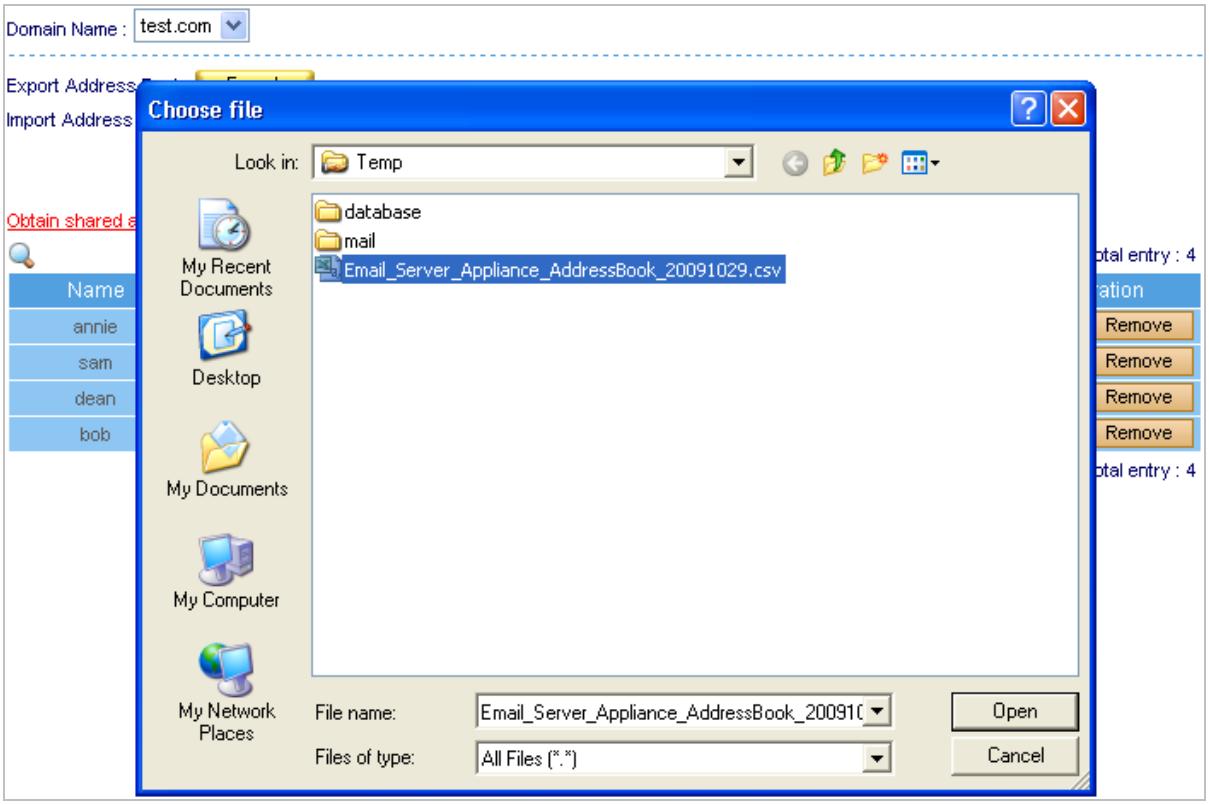


Figure 4-42 Choose file to import Address Book

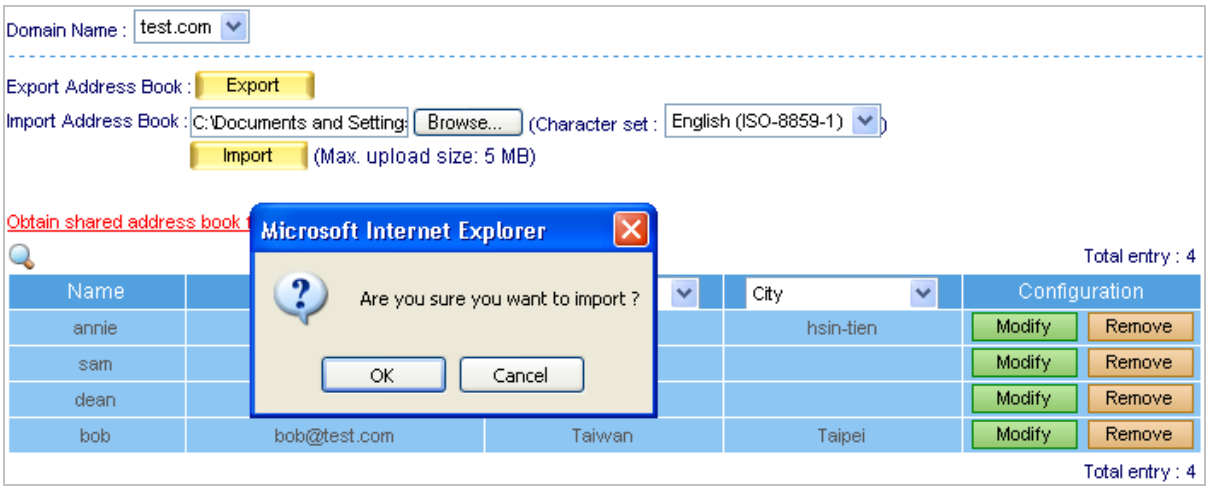


Figure 4-43 Confirm to import Address Book

◆ **Import Address Book from LDAP Server:**

To add contacts from a LDAP server, select **Mail Management → Account Management → Shared Address Book** and then set as below:

- Click on the hyperlink **Add Addresses from LDAP**, then enter all the necessary information in the pop-up window. (Figure 4-44)
- After finishing filling in each field, click **OK** to complete importing addresses from a LDAP server. (Figure 4-45)

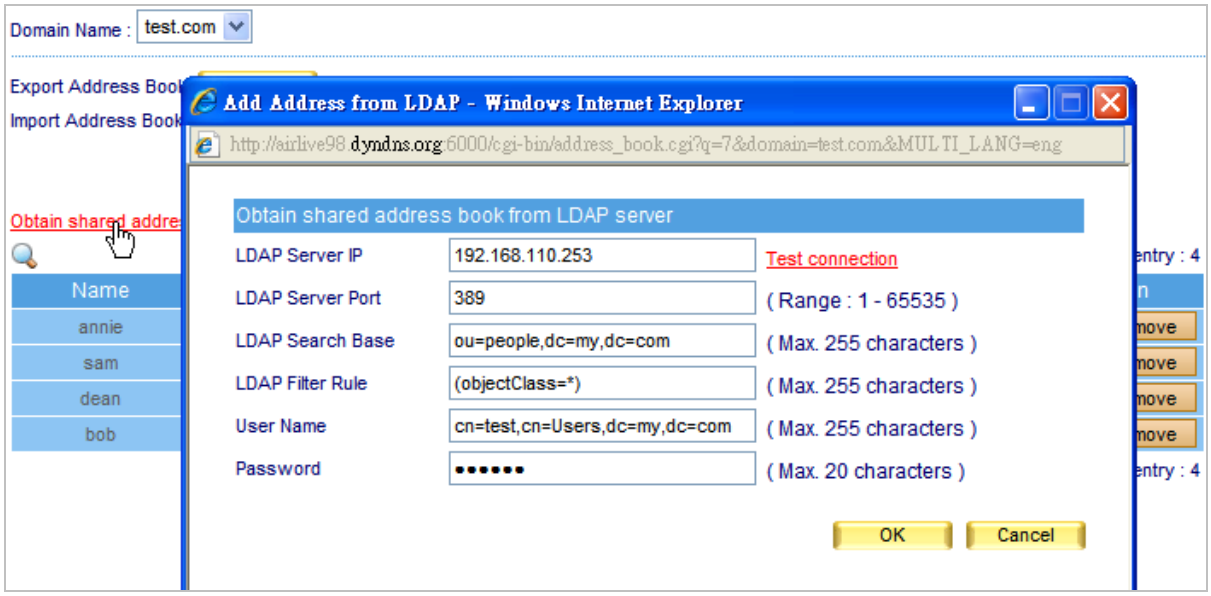


Figure 4-44 Importing Contacts from a LDAP Server

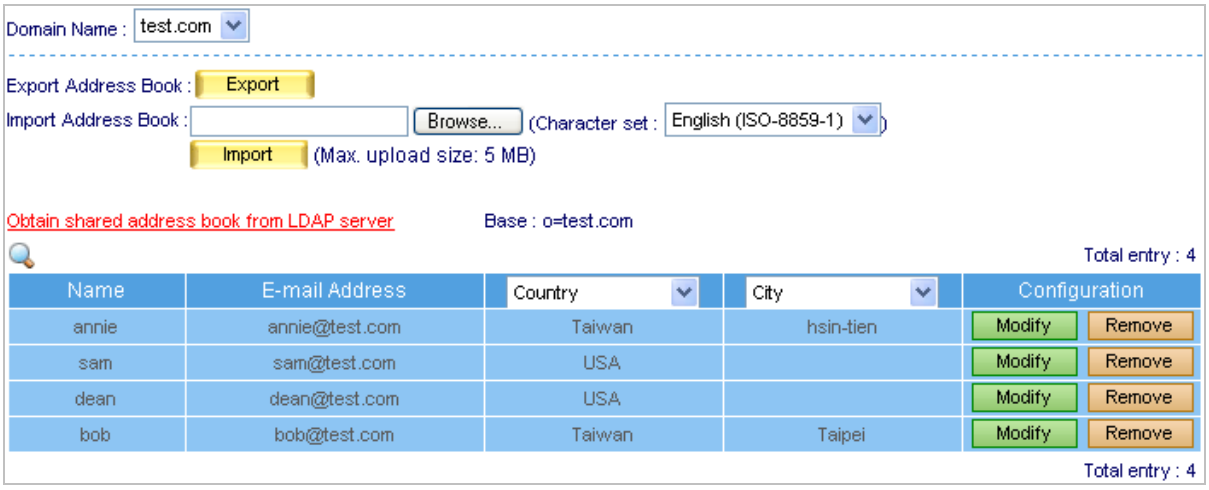


Figure 4-45 Contacts Imported from LDAP server

◆ **Modify Address Book from LDAP Server:**

To add or modify Address books information:

- Click on **New Entry** on the bottom.
- In the **Add Contact** screen, fill out the contact's information. (Figure 4-46)
- Click **OK** to complete adding new contact. (Figure 4-47)
- Remove the unwanted contact by clicking **Remove** button.
- Click **OK** in the dialogue box to confirm deletion. (Figure 4-48)

Modify Contact		
Name	annie	(Max. 30 characters, ex: Rob)
First Name	Lui	(Max. 30 characters, ex: Robert)
Middle Name		(Max. 30 characters)
Last Name	annie	(Max. 30 characters, ex: Wang)
E-mail Address	annie@test.com	(Max. 80 characters)
Home Street		(Max. 128 characters)
Home Phone		(Max. 20 characters, ex: 886-02-20168168)
Home Fax		(Max. 20 characters, ex: 886-02-20168168)
Mobile Phone		(Max. 20 characters, ex: 886-02-20168168)
Company Name		(Max. 30 characters)
Country	Taiwan	(Max. 30 characters)
State	Taipei	(Max. 30 characters)
City	hsin-tien	(Max. 30 characters)
Postal Code	231	(Max. 10 characters)
Company Street	Min Chung Rd.	(Max. 128 characters)
Company Phone	886-2-2218-6888	(Max. 20 characters, ex: 886-02-20168168)
Company Fax	886-2-8667-6352	(Max. 20 characters, ex: 886-02-20168168)
Company Website		(Max. 128 characters)
Office Name		(Max. 30 characters)
Department Name		(Max. 30 characters)
Job Title		(Max. 30 characters)
Pager		(Max. 20 characters)
IP Phone		(Max. 15 characters)
Netmeeting		(Max. 80 characters)
Comment		(Max. 1024 characters)

Figure 4-46 Adding a Contact

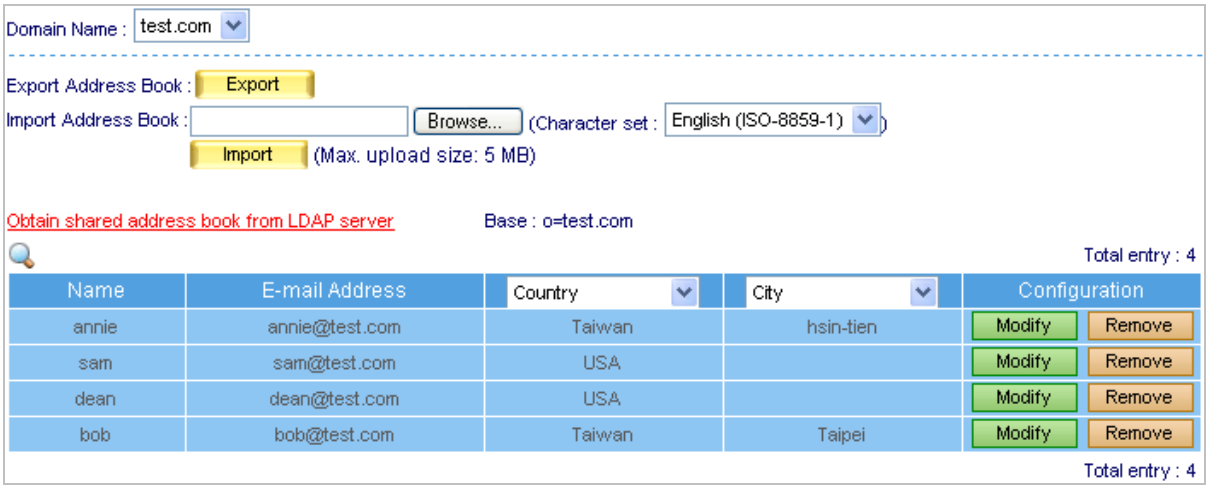


Figure 4-47 New Contact Added

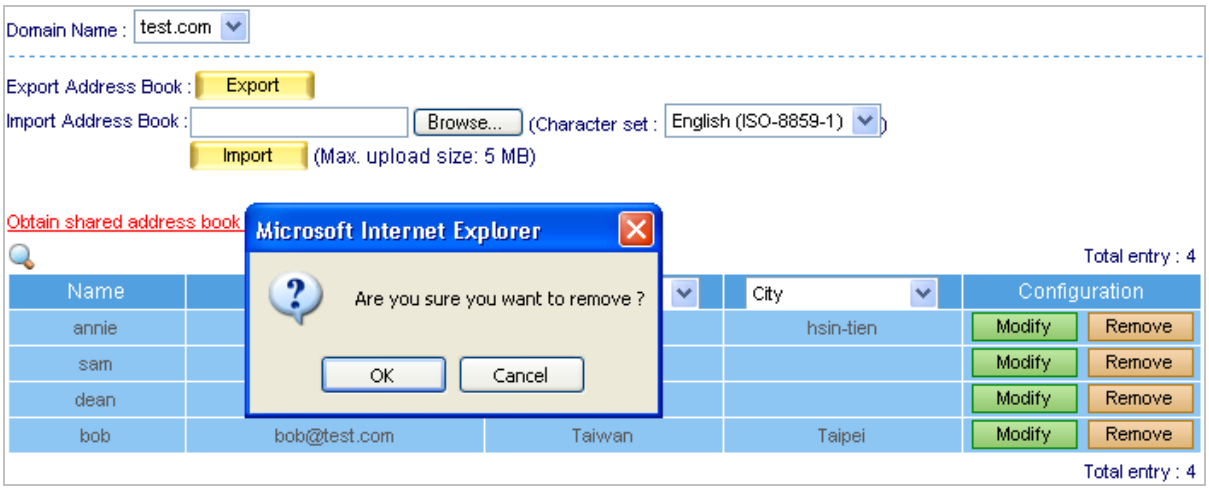


Figure 4-48 Removing a Contact

◆ **Search Address Book:**

- Go to **Mail Management → Account Management → Shared Address Book**
- Click the search icon
- Type keyword in the column of **"E-Mail Address**".
- Press Search button
- Display the searching result. (Figure 4-49)

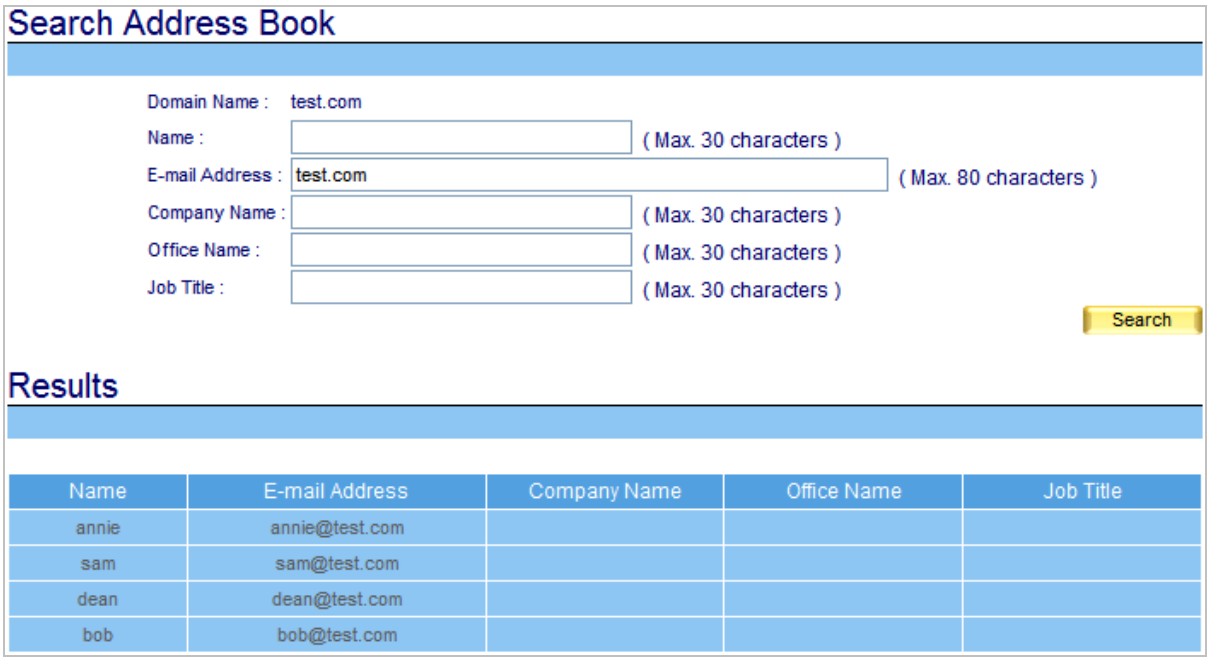


Figure 4-49 Address Book searching result

When you create ES-6000 mail account, it will also create a copy in Shared Address Book.

User can choose two displayed item in Shared Address Book list, the items include First Name, Middle Name, Last Name, Home Street, Home Phone, Home Fax, Mobile Phone, Company Name, Country, State, City, Postal Code, Company Street, Company Phone, Company Fax, Company Website, Office Name, Department Name, Job Title, Pager, IP Phone, and Netmeeting.

◆ **Search user mail address via Outlook Express:**

Shared Address Book is not only co-worked with ES-6000 Web Mail, user's mail address also can be searched by Mail client software. We take Outlook Express as example to demonstrate how to search:

- Open Outlook Express **Address Book**. (Figure 4-50)
- Select **Main Identity's Contacts** → **Tools** → **Accounts…** function. (Figure 4-51)
- Press **Add…** button and follow the wizard to configure setting. (Figure 4-52, 4-53, 4-54, 4-55)
- Select the new created Internet account and press **Properties…** button. (Figure 4-56)
- Highlight and copy ES-6000 Shared Address Book LDAP directory. (Figure 4-57)
- Paste ES-6000 LDAP directory to Advanced setting, click OK and close the setting (Figure 4-58)
- Press Find People button and the windows will show up to allow user searching target. User can also specify the condition to search the specific target. (Figure 4-59, 4-60)

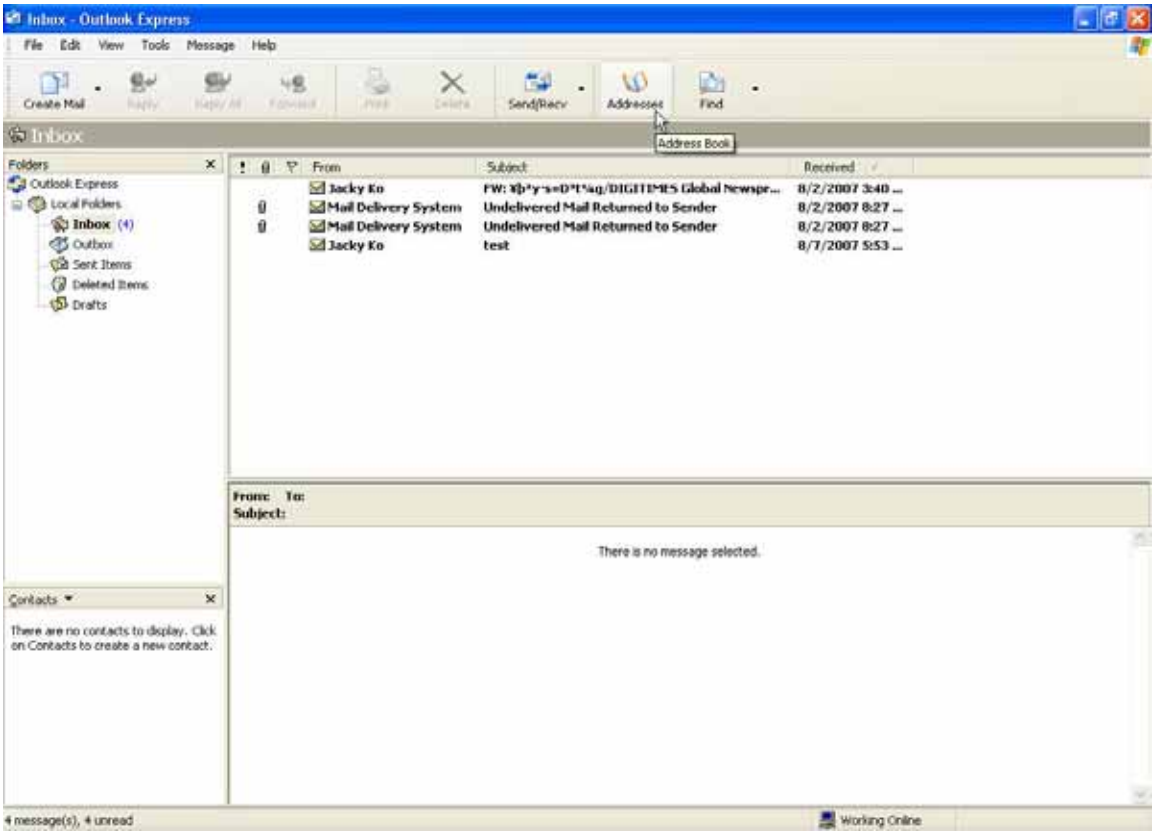


Figure 4-50 Open Outlook Express Address Book

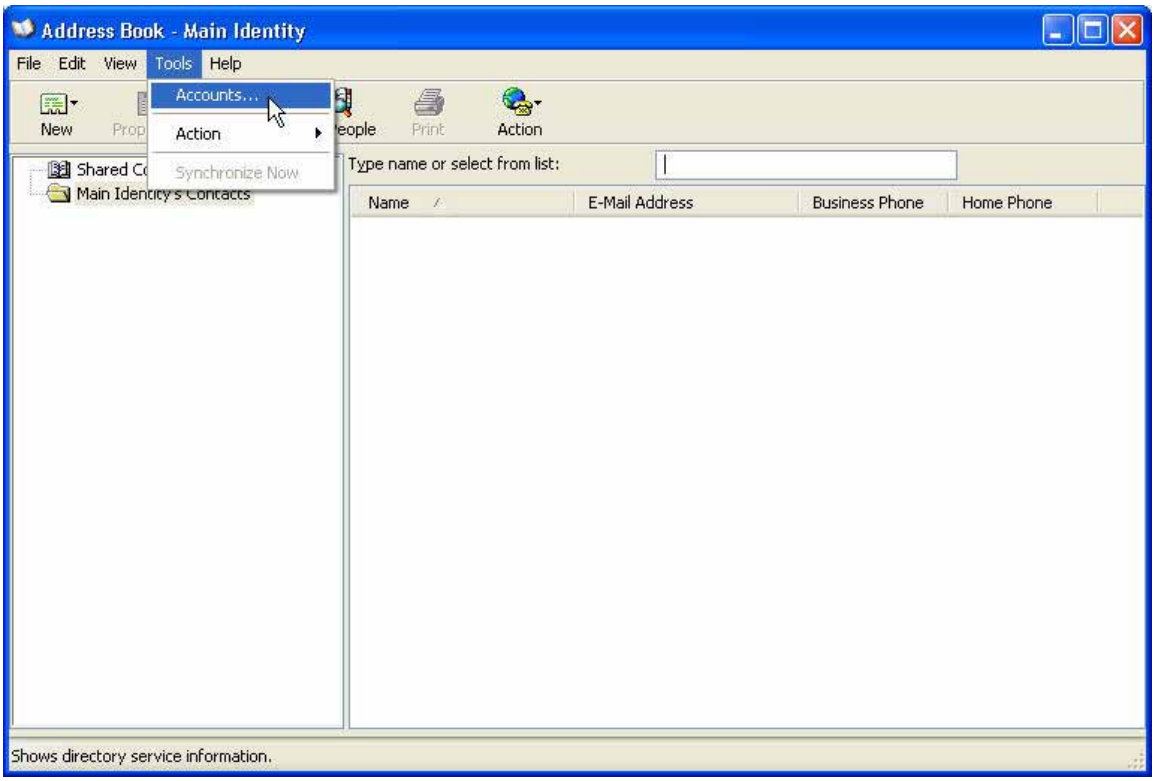


Figure 4-51 Open Internet Accounts managed windows

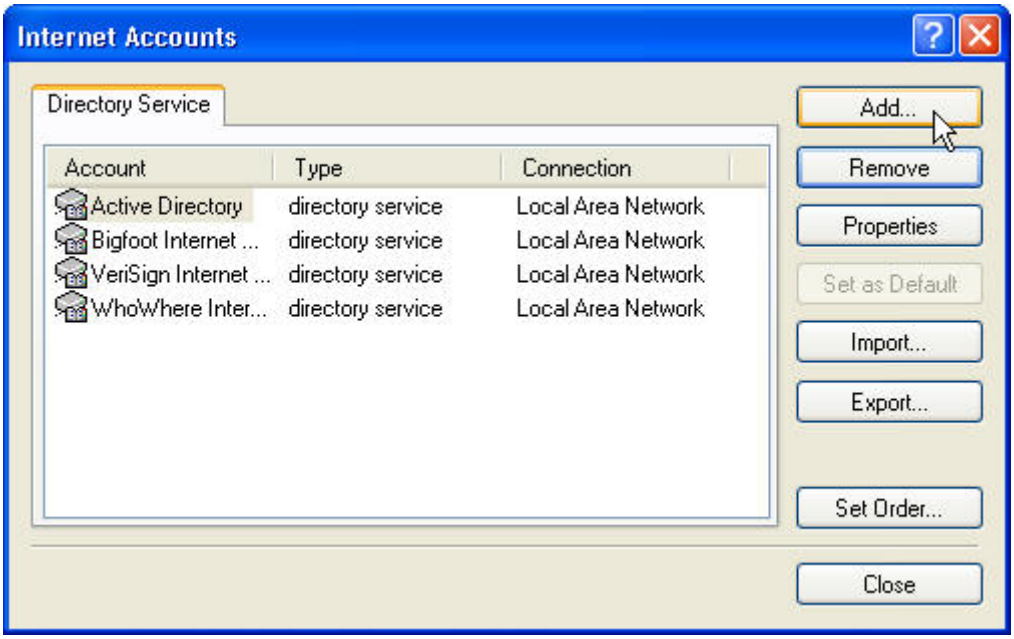


Figure 4-52 Create new Internet Account

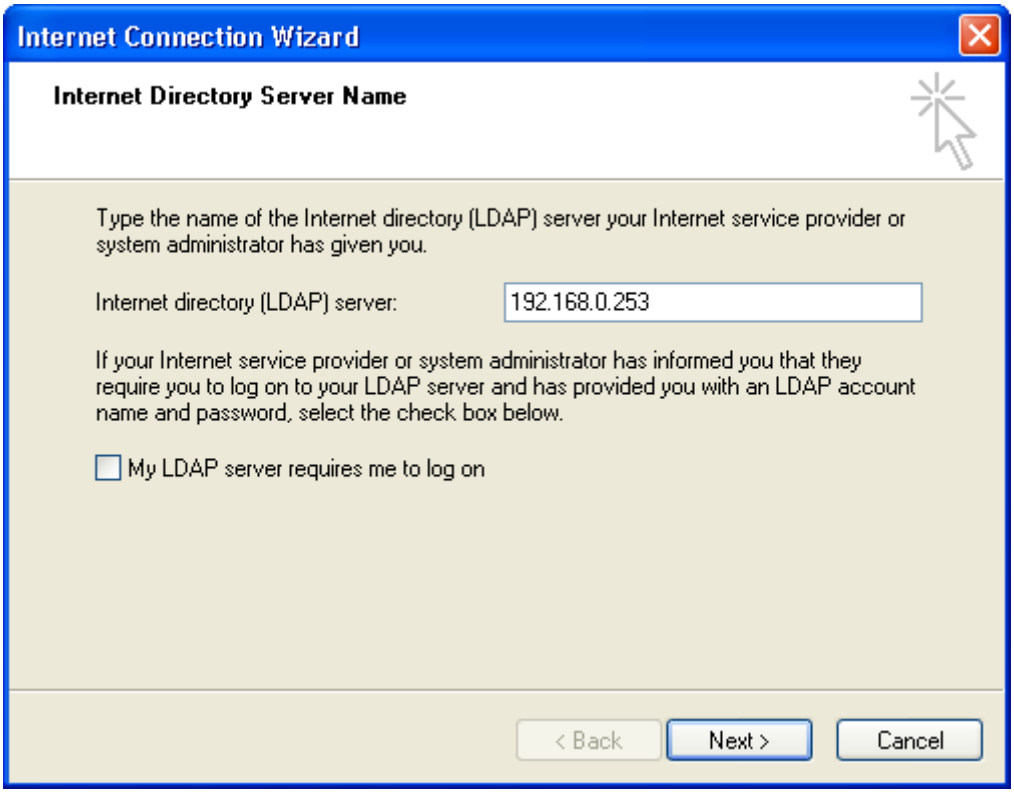


Figure 4-53 Define LDAP server IP address

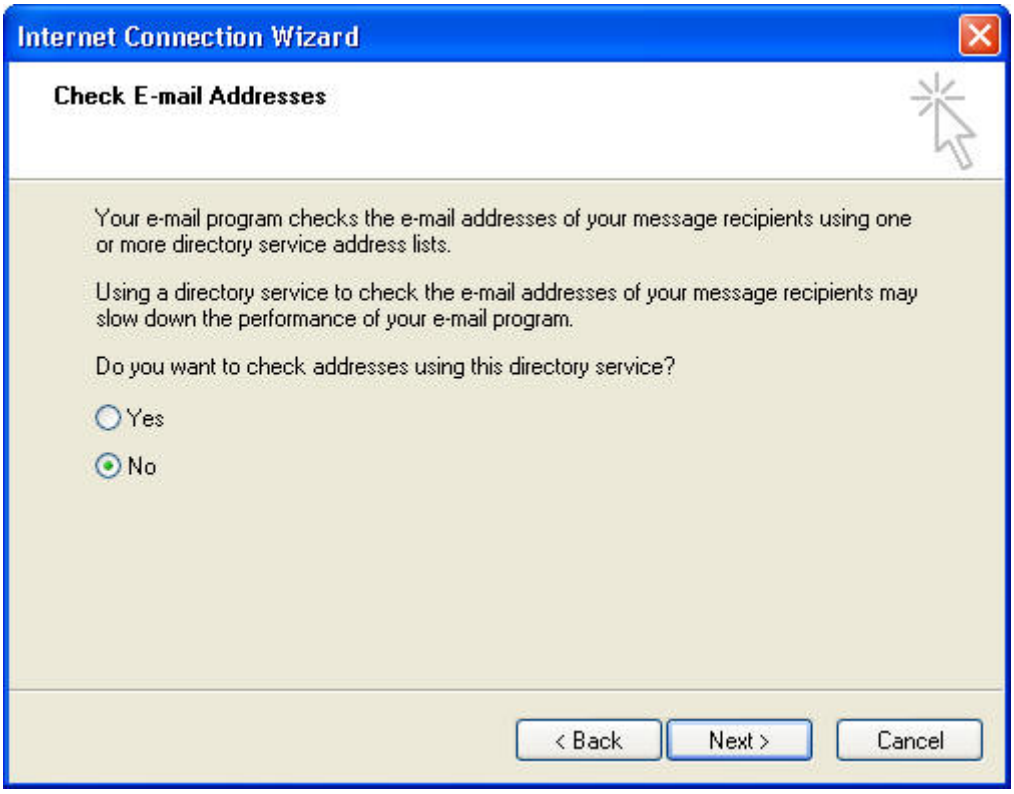


Figure 4-54 Do not check Email Address due to the setting is incomplete

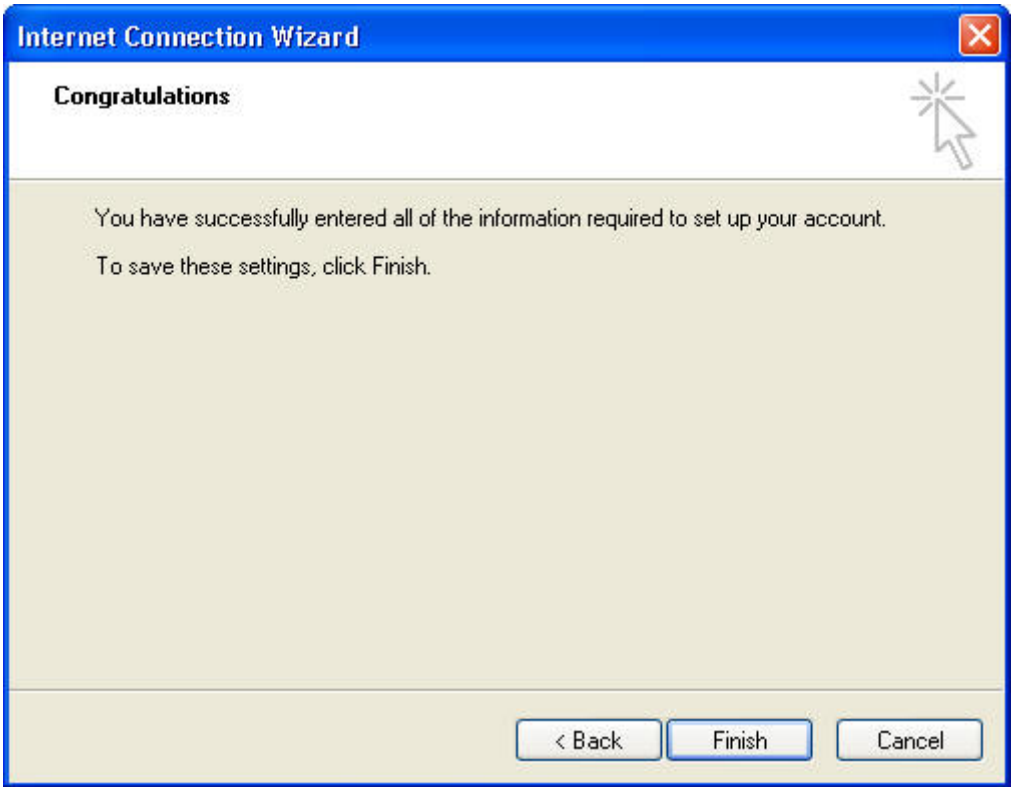


Figure 4-55 Click Finish to complete the setting

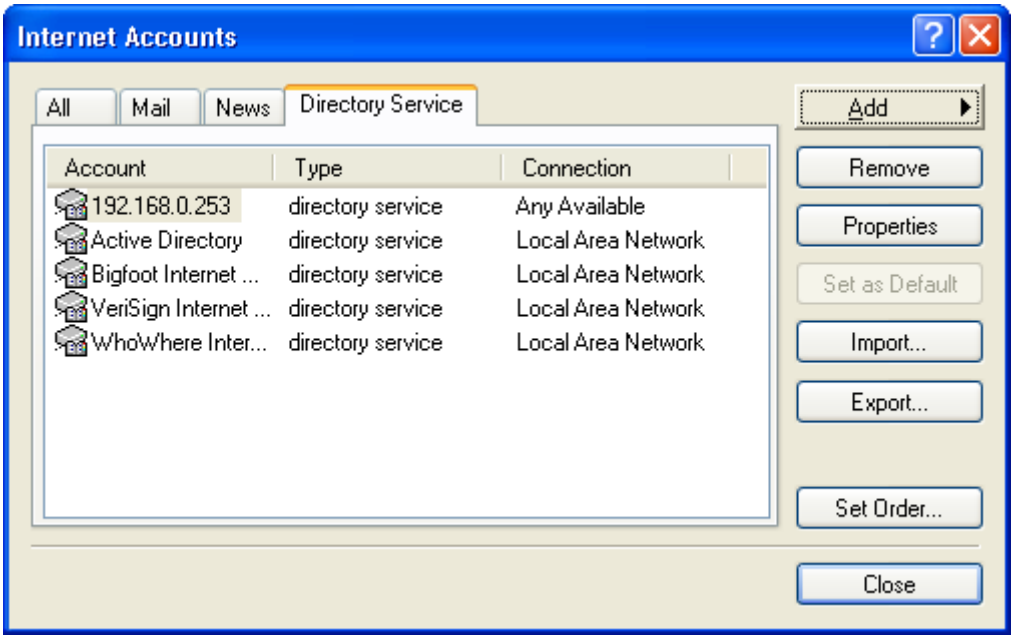


Figure 4-56 Select new created Internet Account and Click Properties for more setting

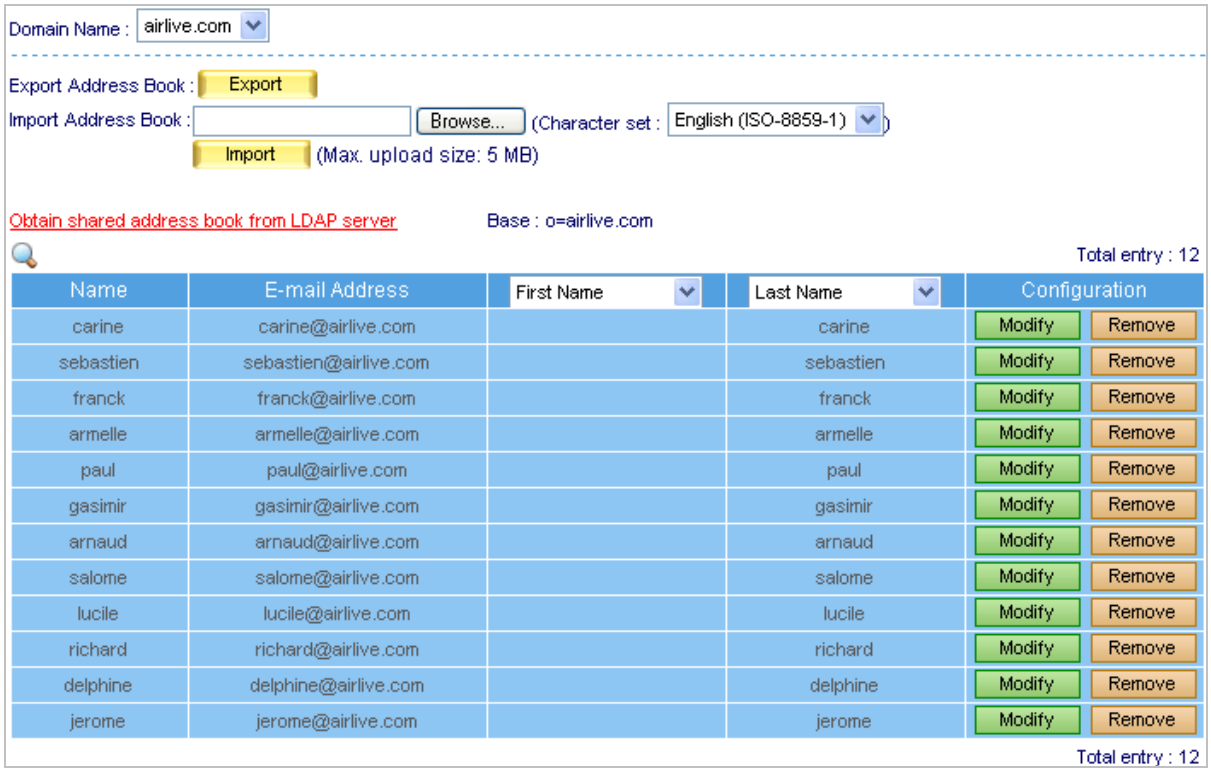


Figure 4-57 Highlight and copy ES-6000Shared Address Book LDAP directory

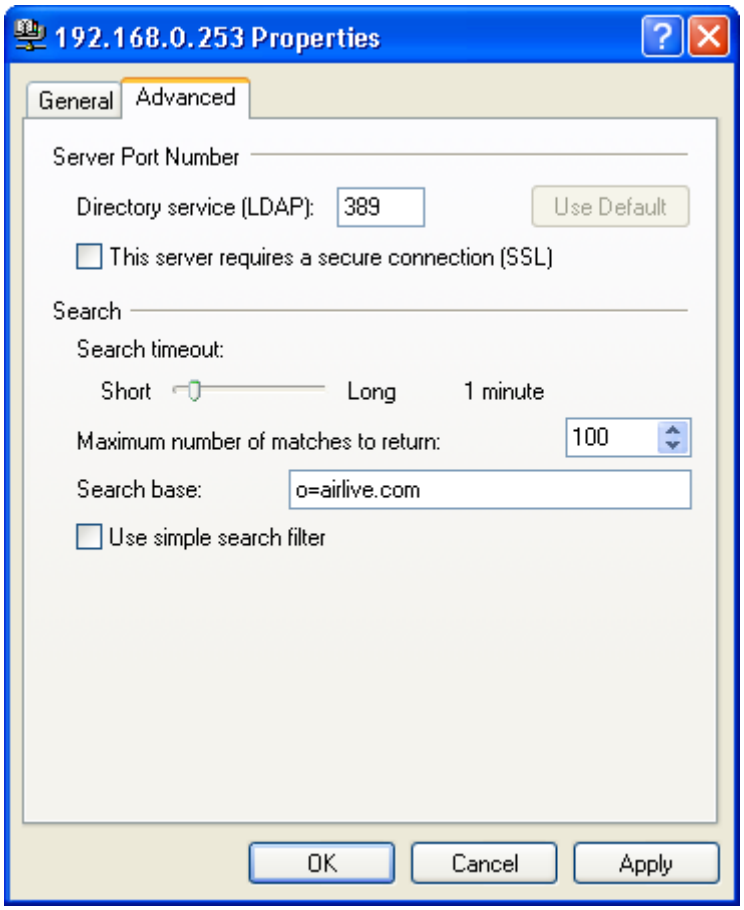


Figure 4-58 Configure LDAP server Advanced setting

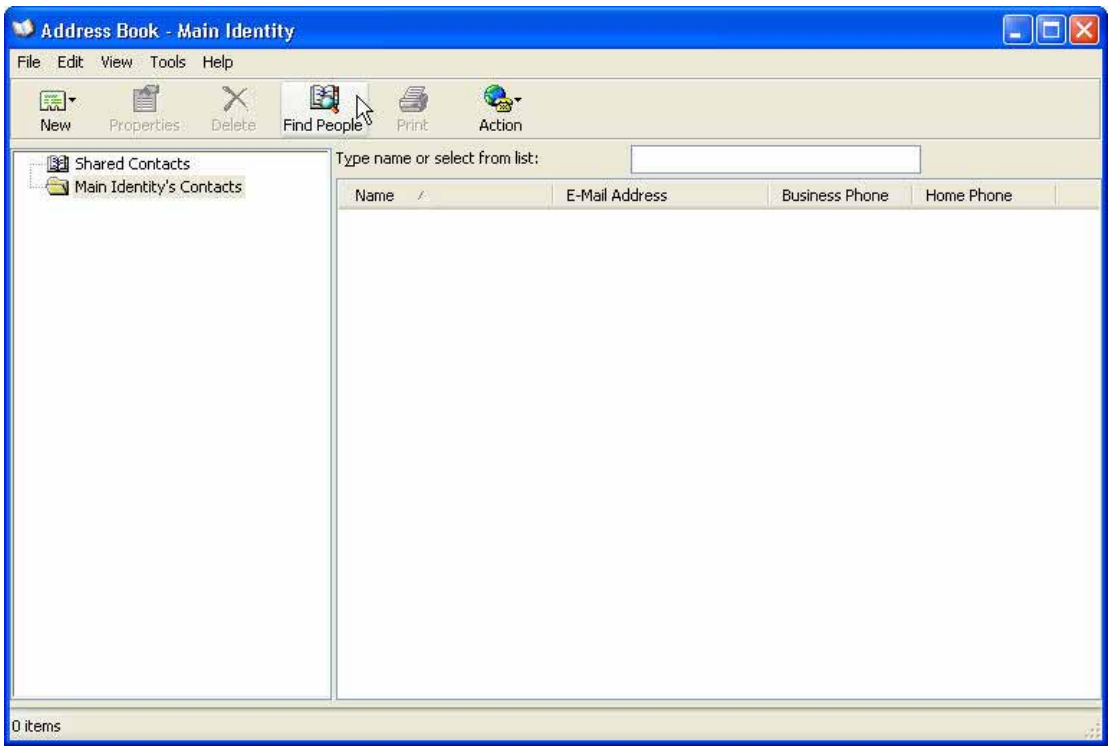


Figure 4-59 Press Find People button to search target

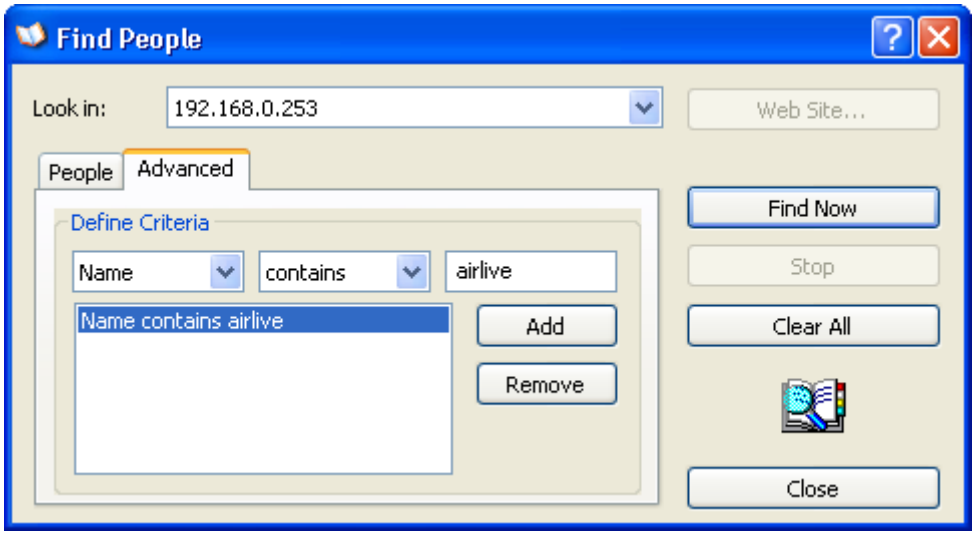


Figure 4-60 Select Advanced to define the searching condition and find the target

4.3 Queue

Detailed delivery status is available for MIS engineer to have a better understanding and be able to react to it on the spot.

Monitoring Mail Delivery Status, Responding on the Spot

Step1. Go to **Mail Management → Configure → Setting → Mail Setting**, set as followed:

- Set **Max. Lifetime of a Mail in Queue** as 4 hours. (Figure 4-61)
- When delivery is failed, system will keep trying to resend the mail to recipient periodically in the storage time.

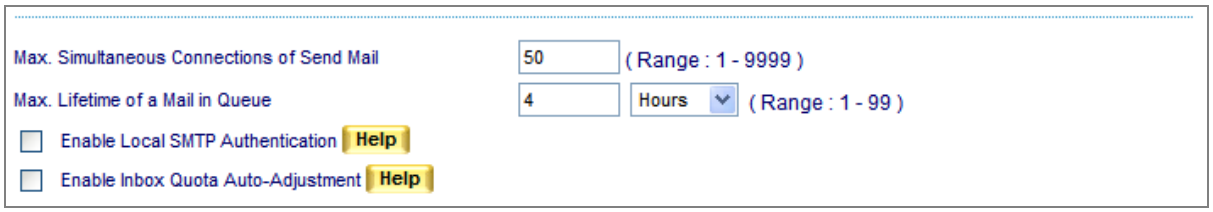


Figure 4-61 Maximum lifetime of a mail in queue

Step2. Go to **Mail Management → Queue → Unsent Mail**, mail status is always obtainable:

- When delivering a mail, it shows its processing procedure. (Figure 4-62)
- Factor caused failed delivery is at hand and by clicking **Resend Now** to resume sending. (Figure 4-63, Figure 4-64)
- System will keep on resending mail to recipient until mail is successfully delivered in the storage time.
- A specific mail or all mails in Queue may be removed to terminate the delivery. (Figure 4-65, Figure 4-66)

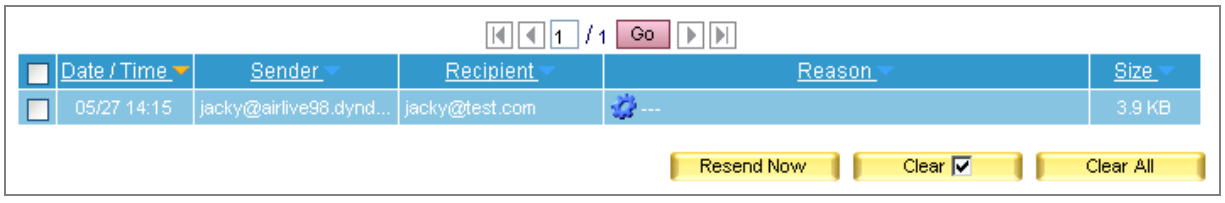


Figure 4-62 E-Mails under Process

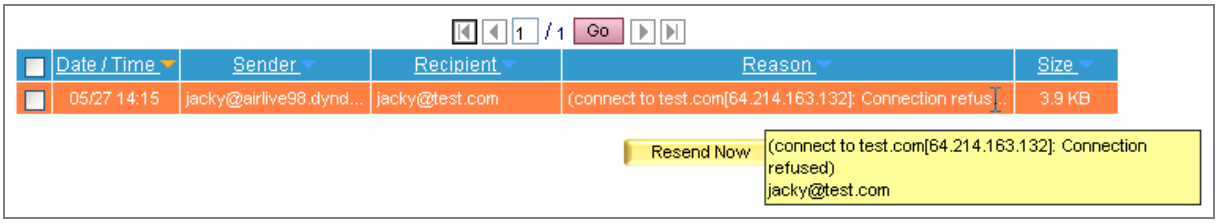


Figure 4-63 Failed Delivery

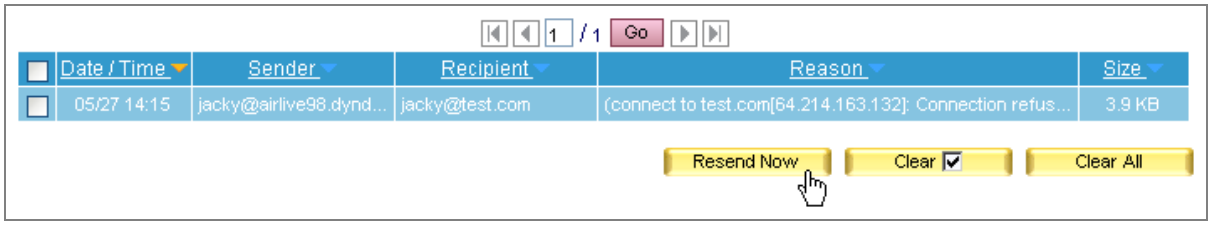


Figure 4-64 Resuming a Failed Delivery

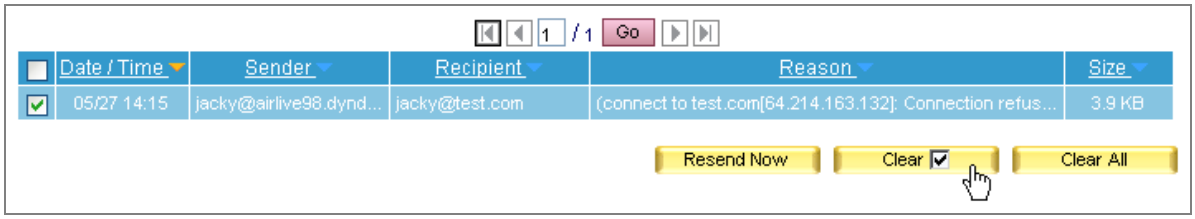


Figure 4-65 Erasing an E-Mail Delivery

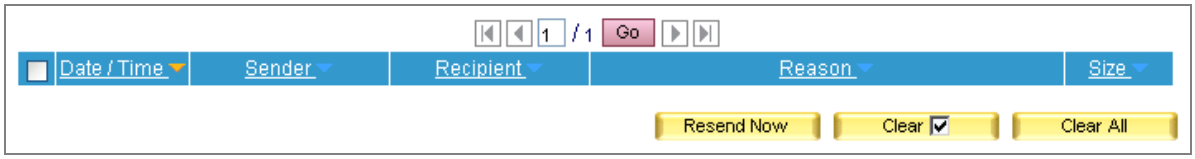


Figure 4-66 Queue Emptied

4.4 Connection Track

Whether it is receiving, sending, or retrieving e-mails from mail server, ***Connection Track*** has the detailed log corresponding to each e-mail process. By which system administrator may use the log as reference to manage and adjust e-mail service.

4.4.1 Outbound SMTP

- User can use date, IP address, sender, recipient and content as keyword to search matched records.
  - To use this feature, please follow the steps below:

1. Press icon to enter the web page for searching mail log. (Figure 4-67)

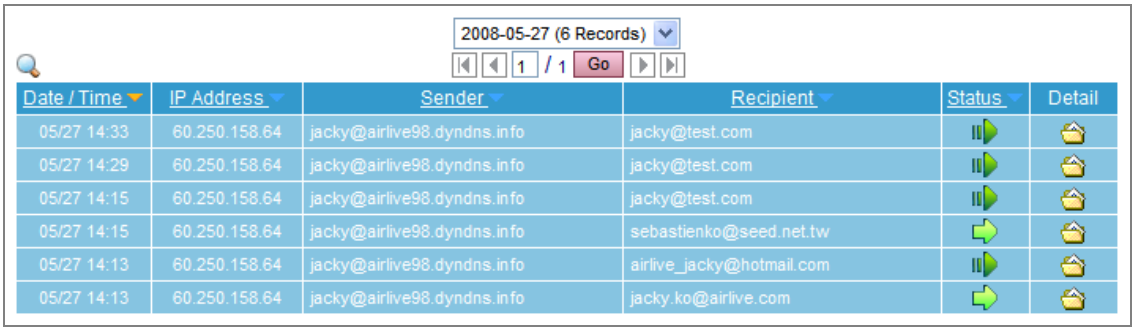


Figure 4-67 Outbound SMTP

2. Enable searching duration and assign a period of time.
3. Input a sender as keyword.
4. Select **All Types** for status and click **Search**.
5. Shows results. (Figure 4-68)

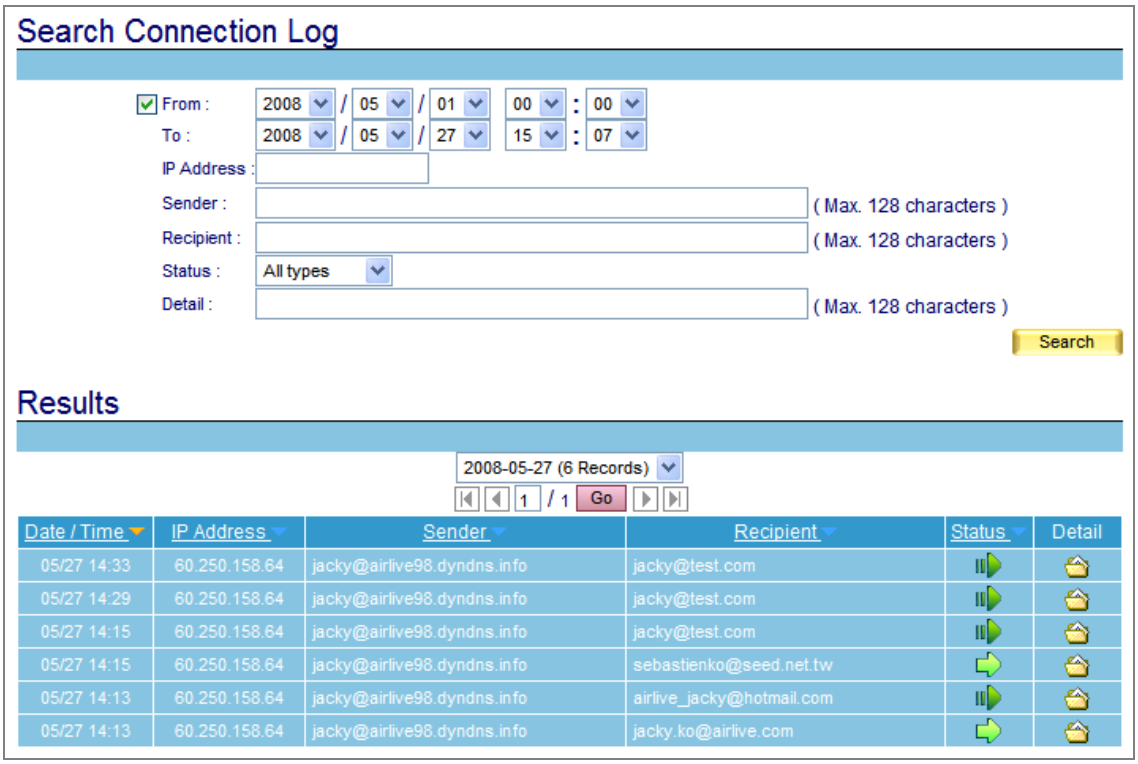


Figure 4-68 Search for specific record

4.4.2 Inbound SMTP

- User can use date, IP address, sender, recipient and content as keyword to search matched records stored in ES-6000.
  - To use this feature, please follow the steps below:

    1. Press icon to enter the web page for searching mail log. (Figure 4-69)

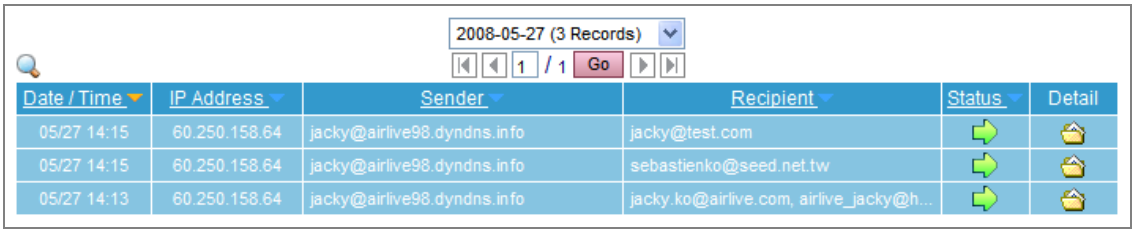


Figure 4-69 Inbound SMTP

    2. Enable searching duration and assign a period of time.
    3. Input a sender as keyword.
    4. Select **All Types** for status.
    5. Click **Search.**
    6. Shows results. (Figure 4-70)

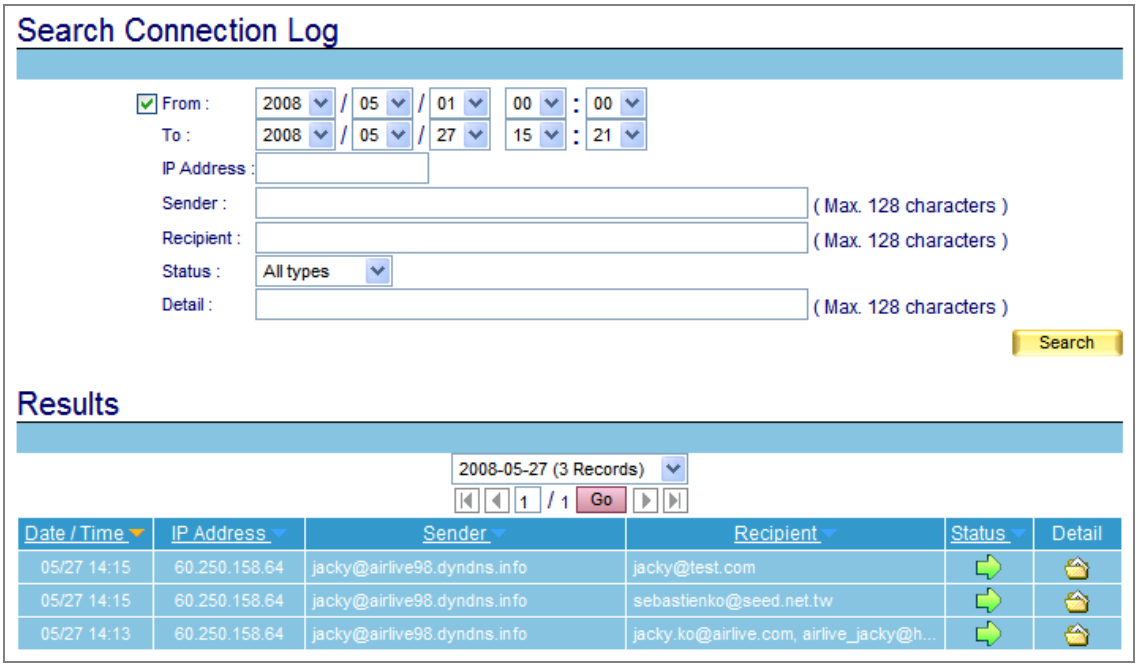


Figure 4-70 Search for specific record

4.4.3 POP3 / IMAP

- User can use date, IP address, sender, recipient and content as keyword to search matched records stored in ES-6000.
  - To use this feature, please follow the steps below:

    1. Press icon to enter the web page for searching mail log. (Figure 4-71)

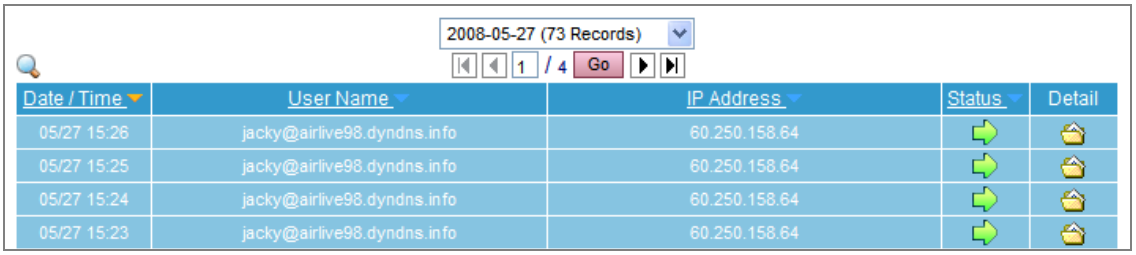


Figure 4-71 POP3 / IMAP

    2. Enable searching duration and assign a period of time.
    3. Select **All Types** for status.
    4. Click **Search**.
    5. Shows results. (Figure 4-72)

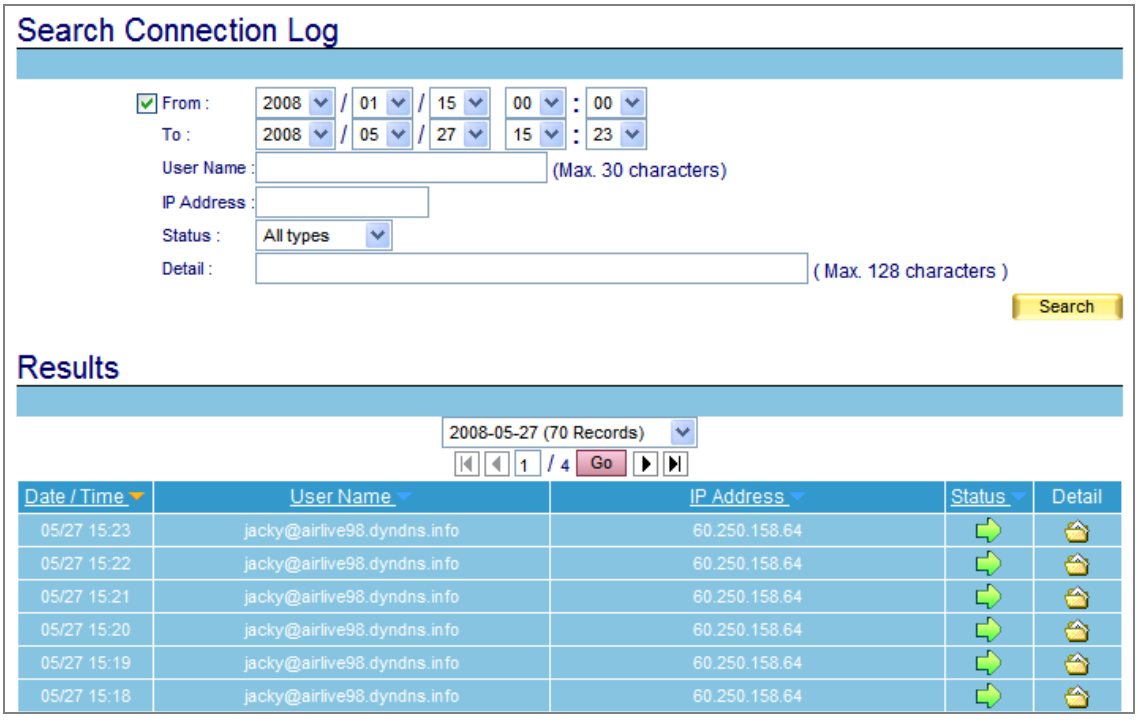


Figure 4-72 Search for specific record

Search results will be sorted by day, MIS engineer can use pull-down menu to choose records of specific day.

Ex. Viewing Mail Log of Outgoing Mail

Step1. Go to **Mail Management → Connection Track → Outbound SMTP**, there it shows mail log of outgoing mails. (Figure 4-73)

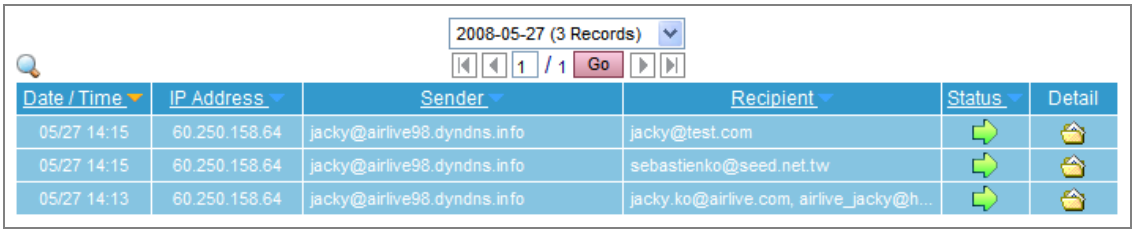


Figure 4-73 Mail log of Outbound SMTP

Step2. Click **Detail** for detail information. (Figure 4-74)

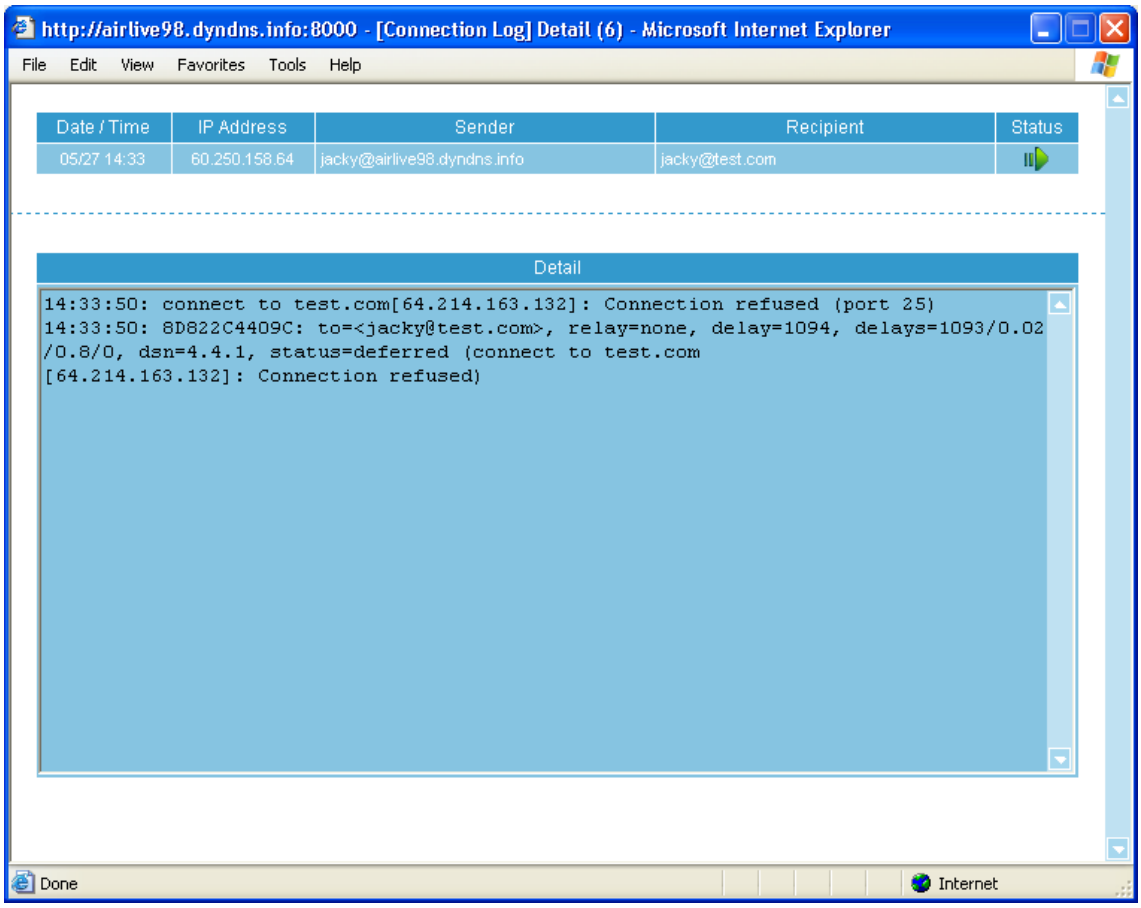


Figure 4-74 Details of mail log

Ex. Viewing Mail Log of Incoming Mail

Step1. Go to **Mail Management → Connection Track → Inbound SMTP**, there it shows mail log of incoming mails. (Figure 4-75)

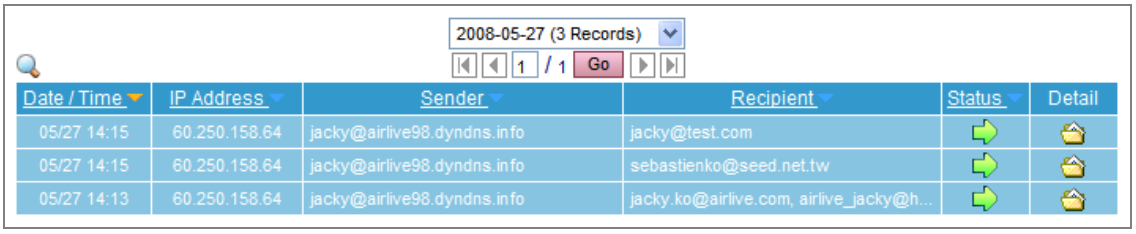


Figure 4-75 Mail log of Inbound SMTP

Step2. Click **Detail** for detail information. (Figure 4-76)

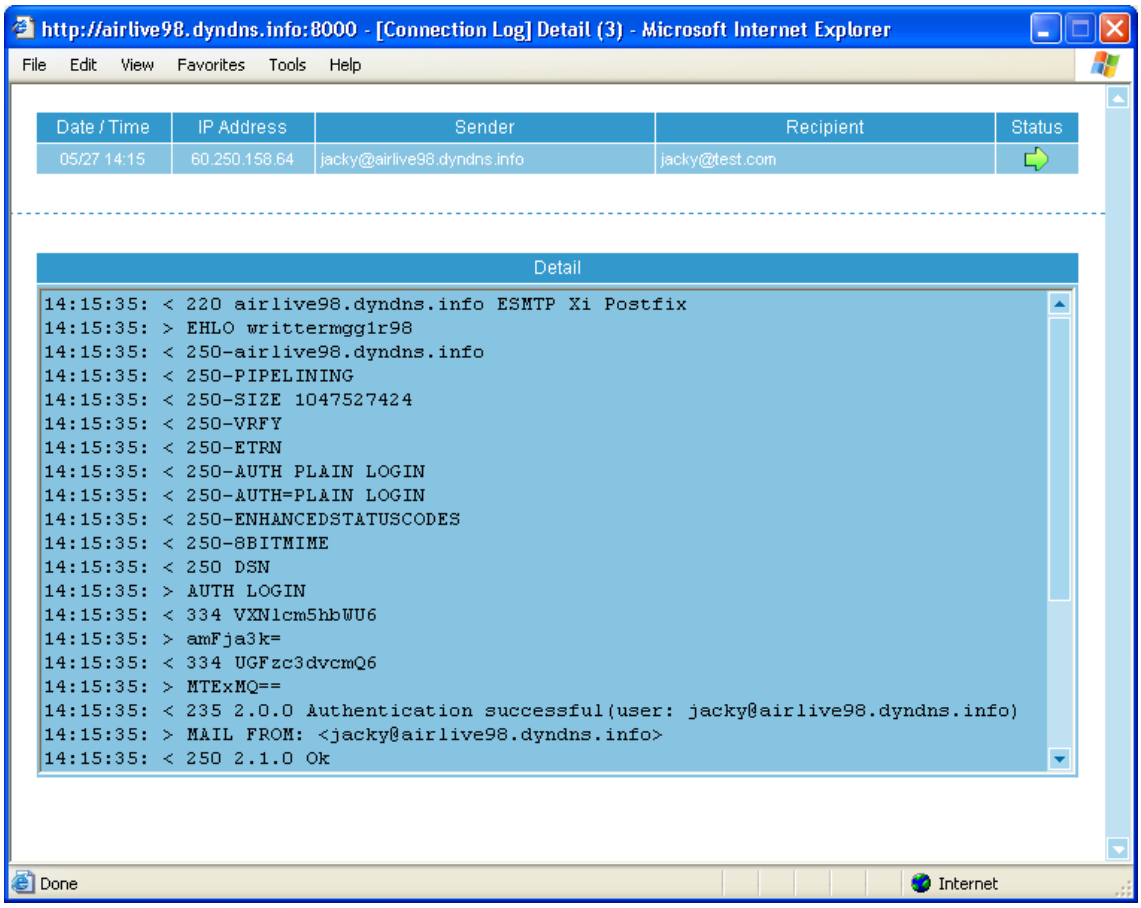


Figure 4-76 Details of mail log

Ex. Viewing Mail Log of Retrieved Mails from ES-6000

Step1. Go to **Mail Management → Connection Track → POP3 / IMAP**, there it shows mail log of retrieved mails from ES-6000. (Figure 4-77)

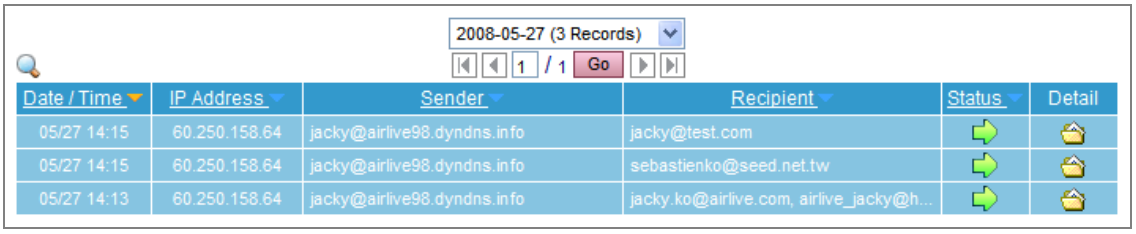


Figure 4-77 Mail log of POP3

Step2. Click **Detail** for detail information. (Figure 4-78)

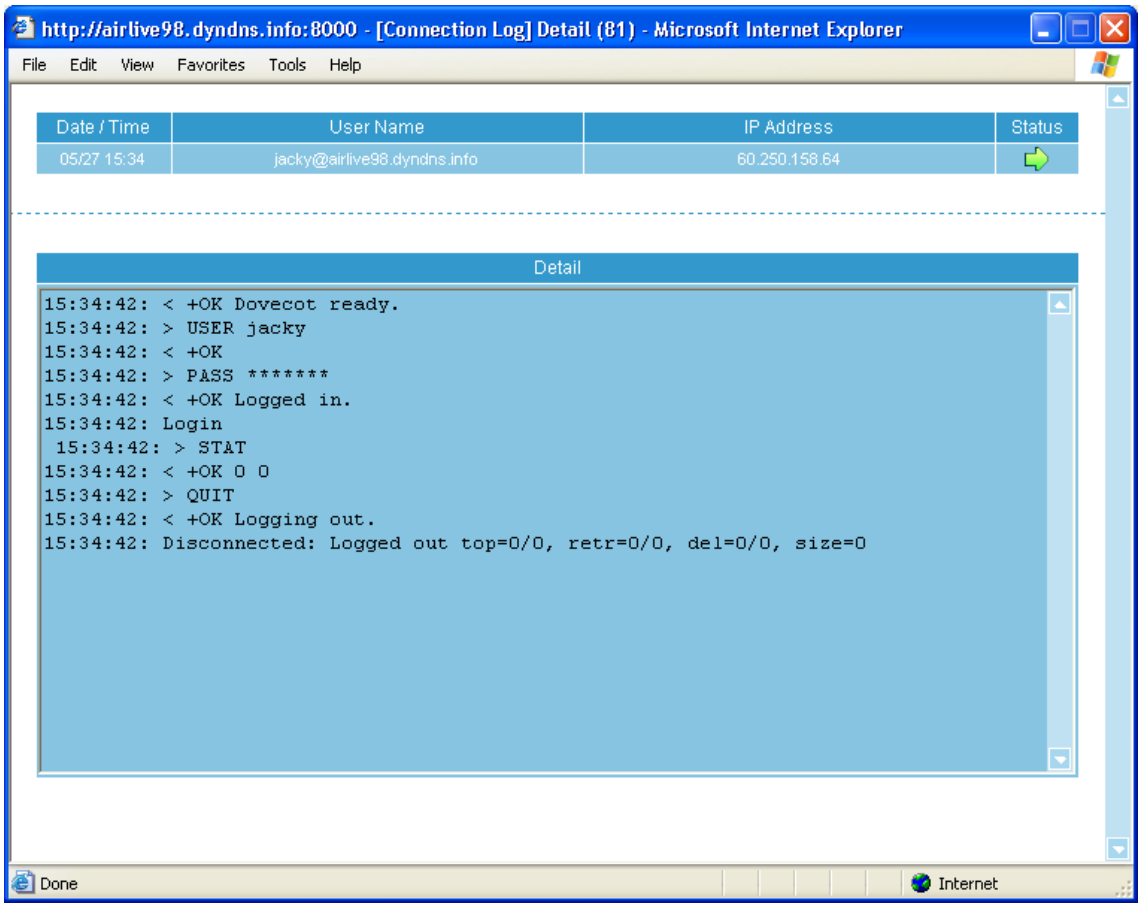


Figure 4-78 Details of mail log

Chapter 5 Web Mail

5.1 How to use Web Mail

The example shows you how to use web mail:

Step1. To use the web mail service, please type the default IP address 192.168.1.1 with the HTTP port (8080) or HTTPS port (1443) in the address of web browser.

For example, http://192.168.1.1:8080 or https://192.168.1.1:1443 (Using 8080 or 1443 depends on protocol type.) (Figure 5-1)

- Enter user account and password.
- Click **Login**.

Figure 5-1 Log in web mail

Step2. When user first uses web mail service, system will require user to enter basic information.

- Click **Continue**. (Figure 5-2)
- Select **language**, **timezone offset**, **sender address** and edit your **signature** below **User Preference**. (Figure 5-3)
- Click **Save**.
- Display preferences successfully saved. (Figure 5-4)
- Click **Continue**.

Figure 5-2 First use of web mail service

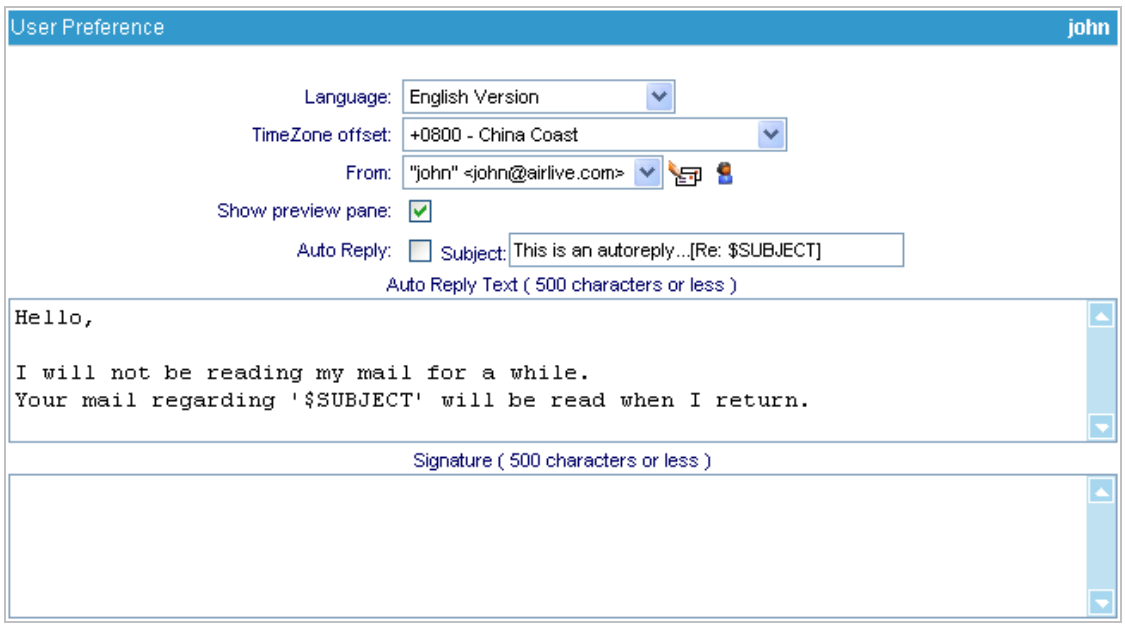


Figure 5-3 User Preference

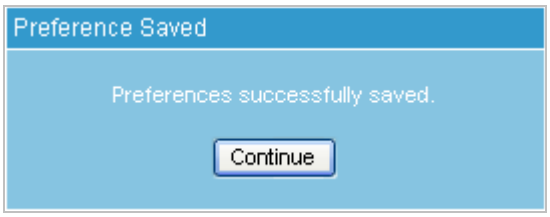


Figure 5-4 Preferences successfully saved

Step3. Web based mail for easy mail access. (Figure 5-5)

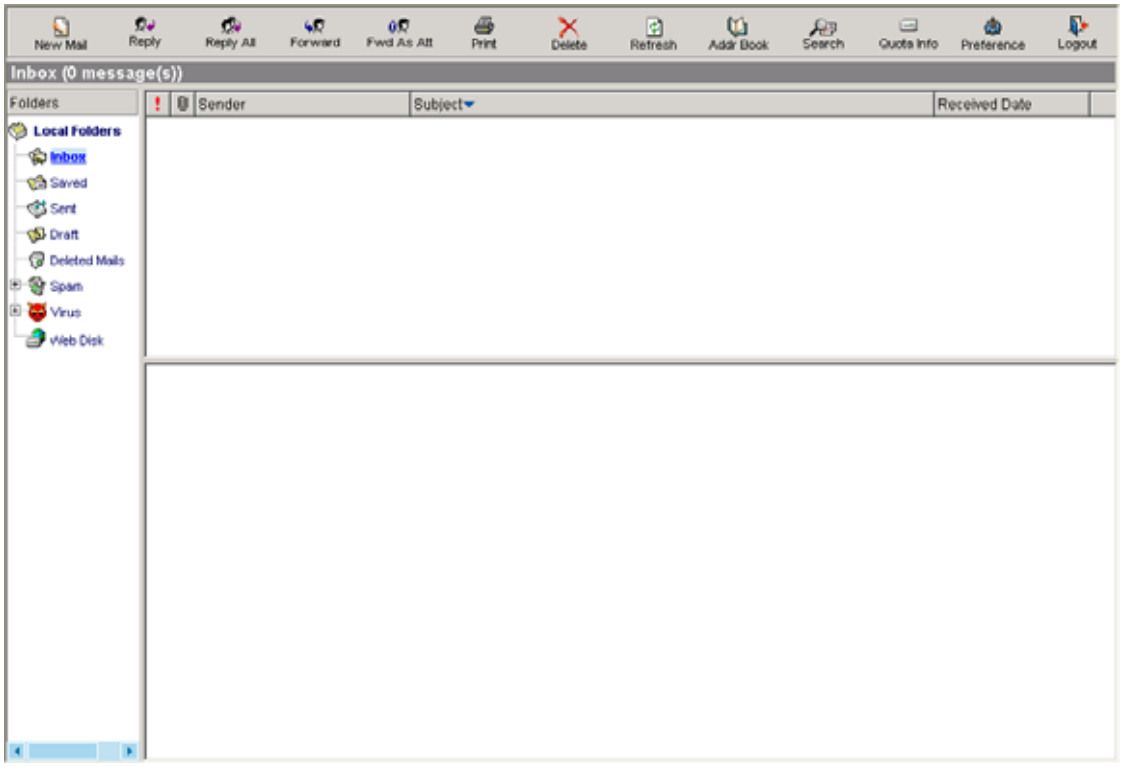


Figure 5-5 Web Mail Interface

5.2 How to configure Web Mail User Preference

Click **Preference** in the web-based mailbox main screen, and then set as below: (Figure 5-6)

- Click to edit sender name.
- Click sender name and the original name and mail address will be shown at the column.
- Rename the original name in **Name** field. (Figure 5-7)
- Click **Modify** to complete modification. (Figure 5-8)
- Click to edit personal information.
- After finished, click **Save**.
- Click **Save** in the **User Preference** screen to complete settings. (Figure 5-9)

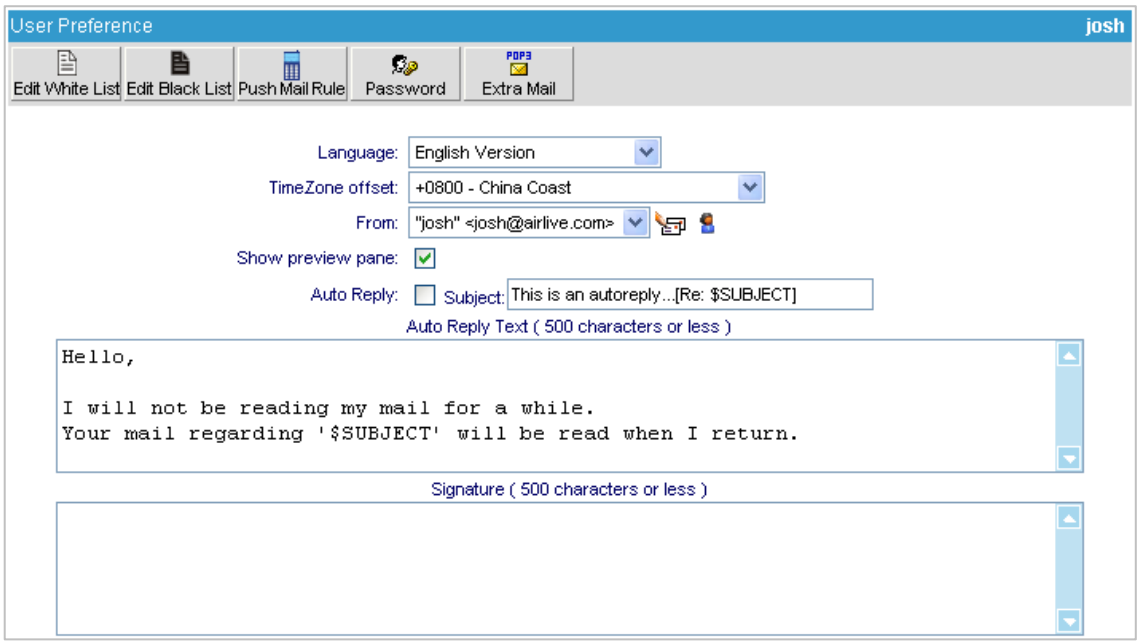


Figure 5-6 User Preference

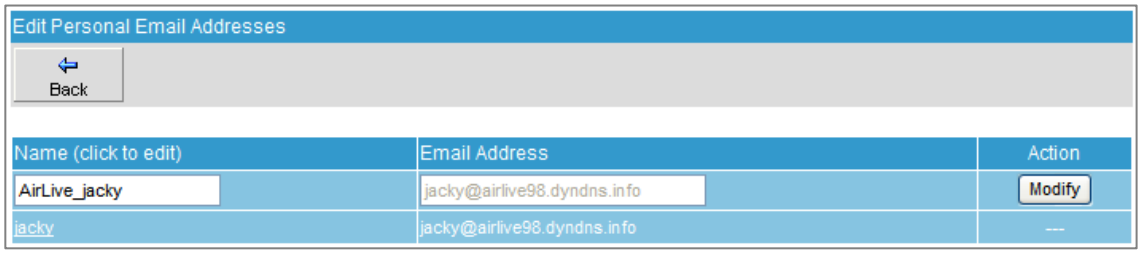


Figure 5-7 Modifying the Sender Name

Figure 5-8 Sender Name Successfully Modified

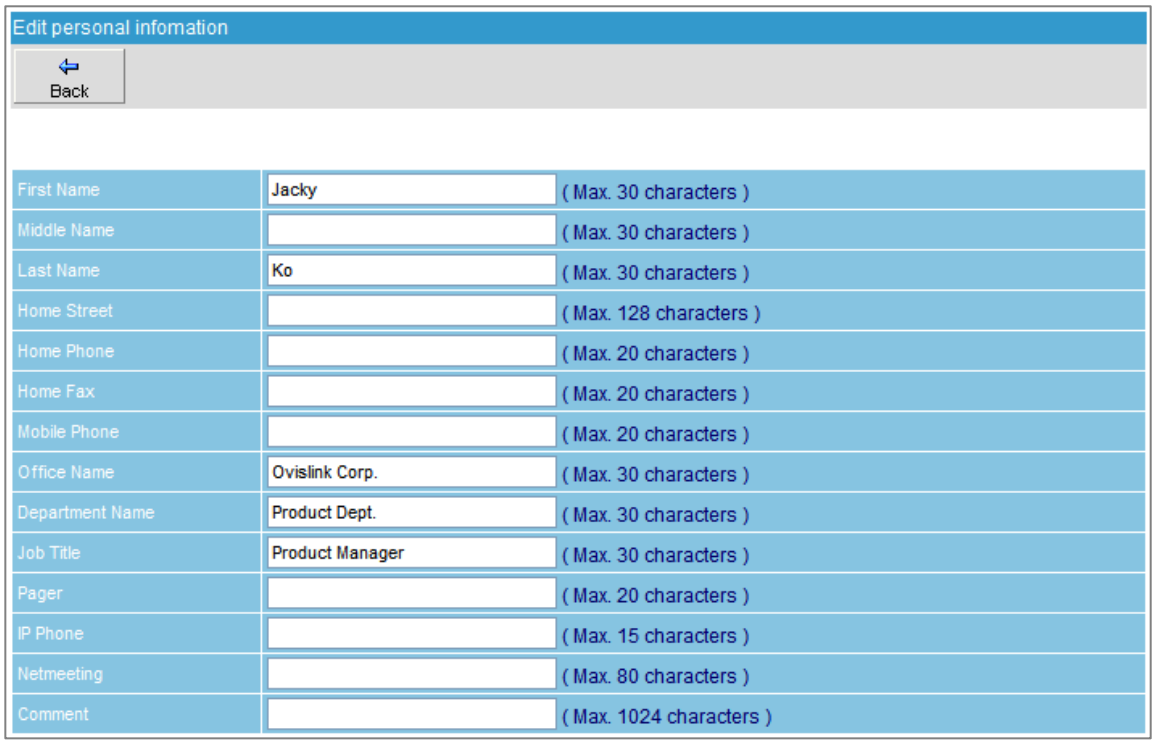


Figure 5-9 Editing Personal Information

5.3 Importing Address Book from Outlook Express

Step1. To export the address book from Outlook Express, follow these steps:

- On the **File** menu, point to **Export**, and then click **Address Book**. (Figure 5-10)
- In the **Address Book Export Tool** dialog box, click **Text File (Comma Separated Values)**, and then click **Export**. (Figure 5-11)
- In the **CSV Export** dialog box, specify the storage path and the file name, and then click **Next**. (Figure 5-12)
- Tick the desired fields to export and then click **Finish**. (Figure 5-13)
- A dialog box says, “Address book export progress has completed.” Then, click OK. (Figure 5-14)

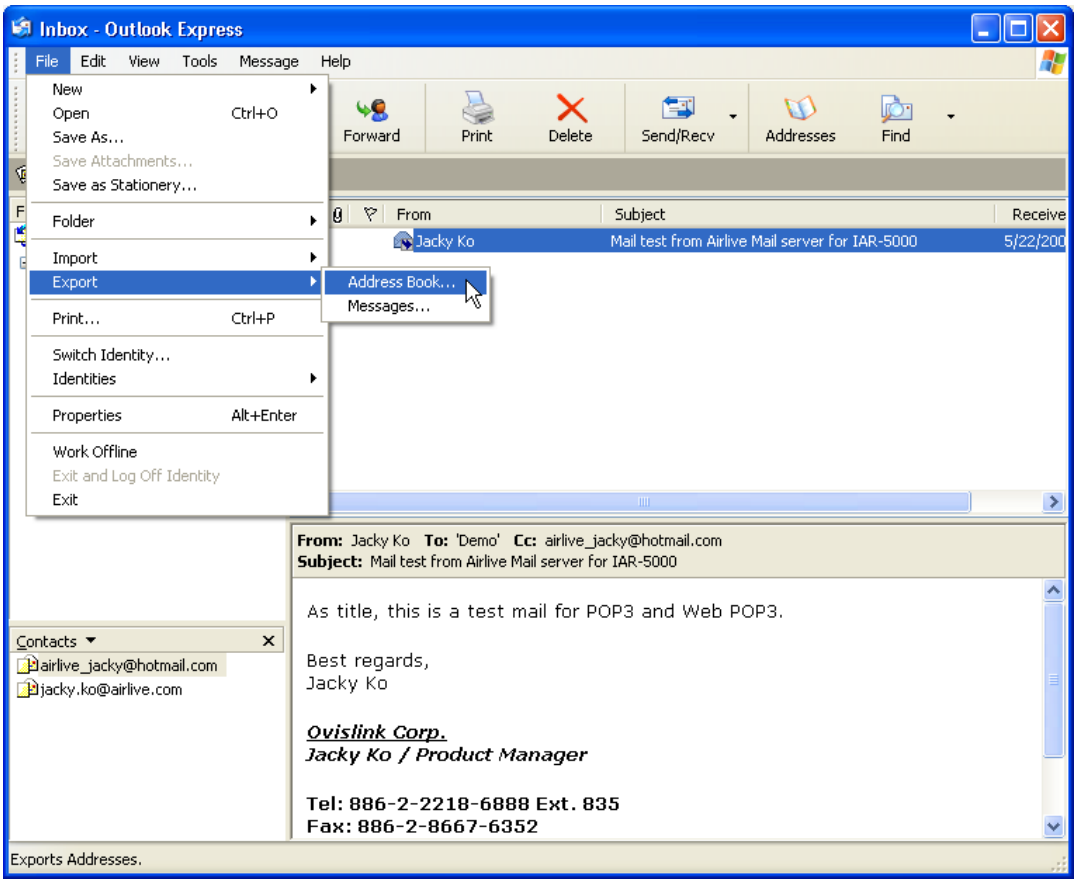


Figure 5-10 Selecting Address Book on the File Menu

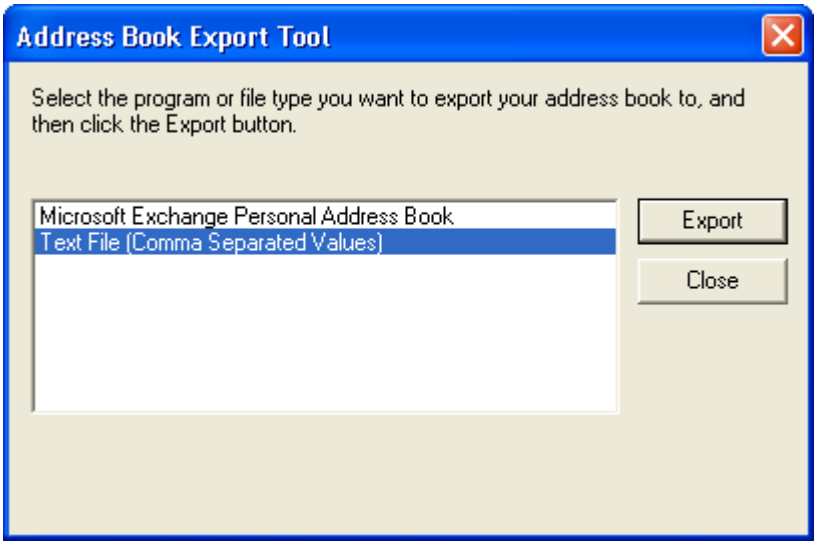


Figure 5-11 Selecting a File Type to Export

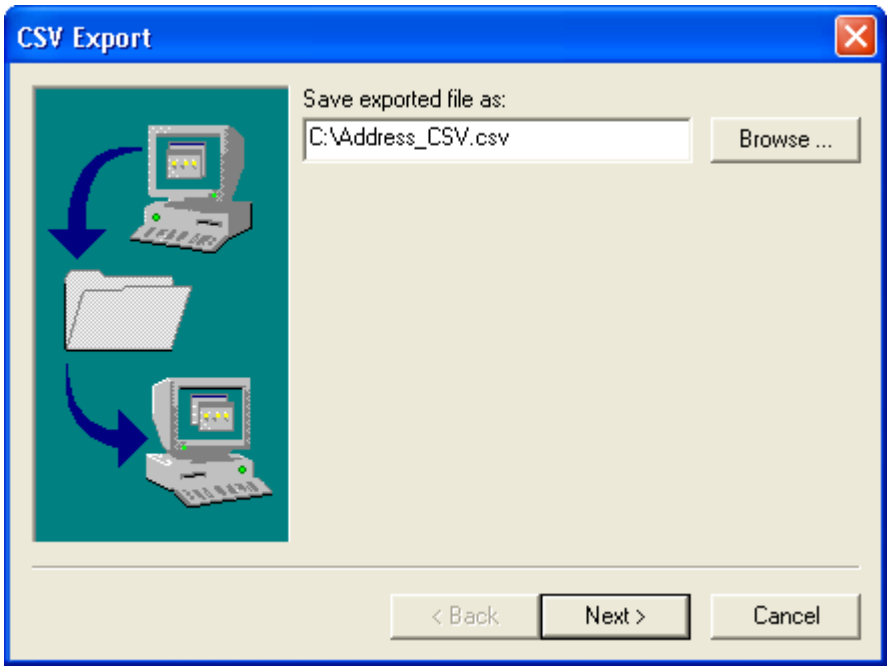


Figure 5-12 Specifying the Storage Path and File Name

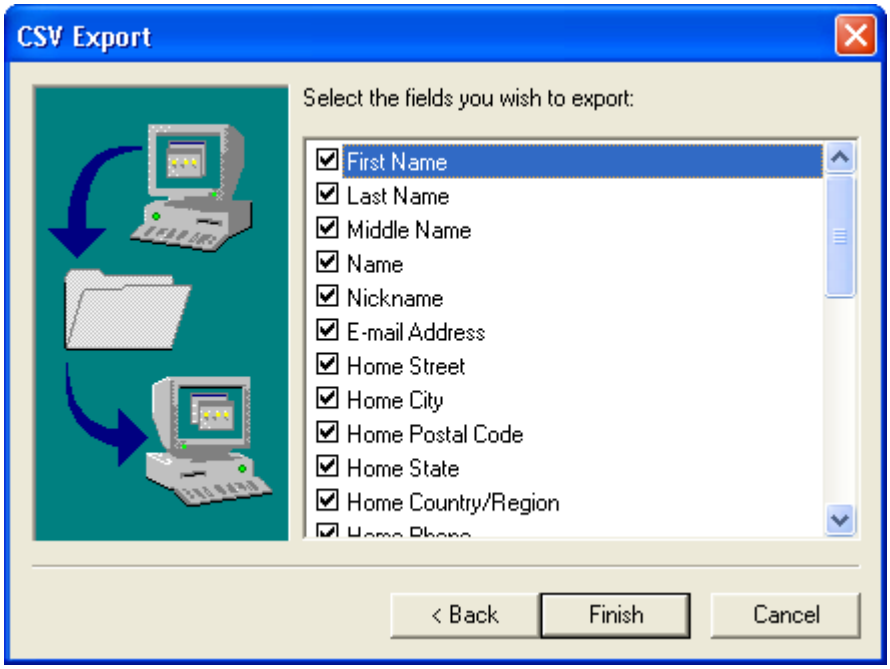


Figure 5-13 Selecting the Desired Fields to Export

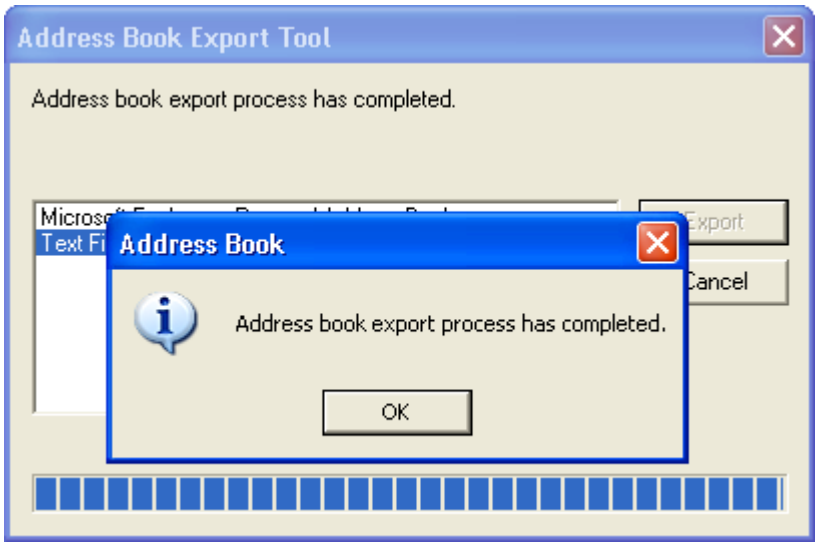


Figure 5-14 Export Process Completed

Step2. To import the address book, follow these steps:

- Click Address Book. (Figure 5-15)
- Click **Import**. (Figure 5-16)
- Locate the file by clicking **Browse**.
- Select “CSV (first line contains field names.csv)” as file format.
- Select “English Version” for **Charset**.
- Click **Import**. (Figure 5-17, 5-18)

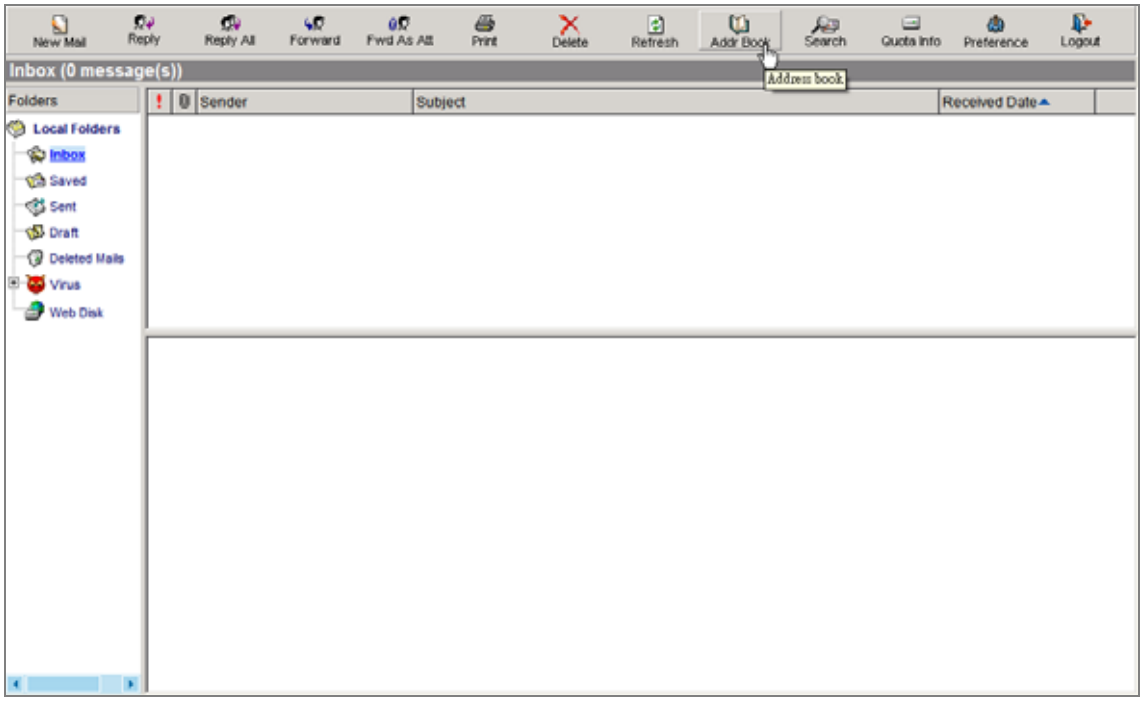


Figure 5-15 Clicking into Address Book

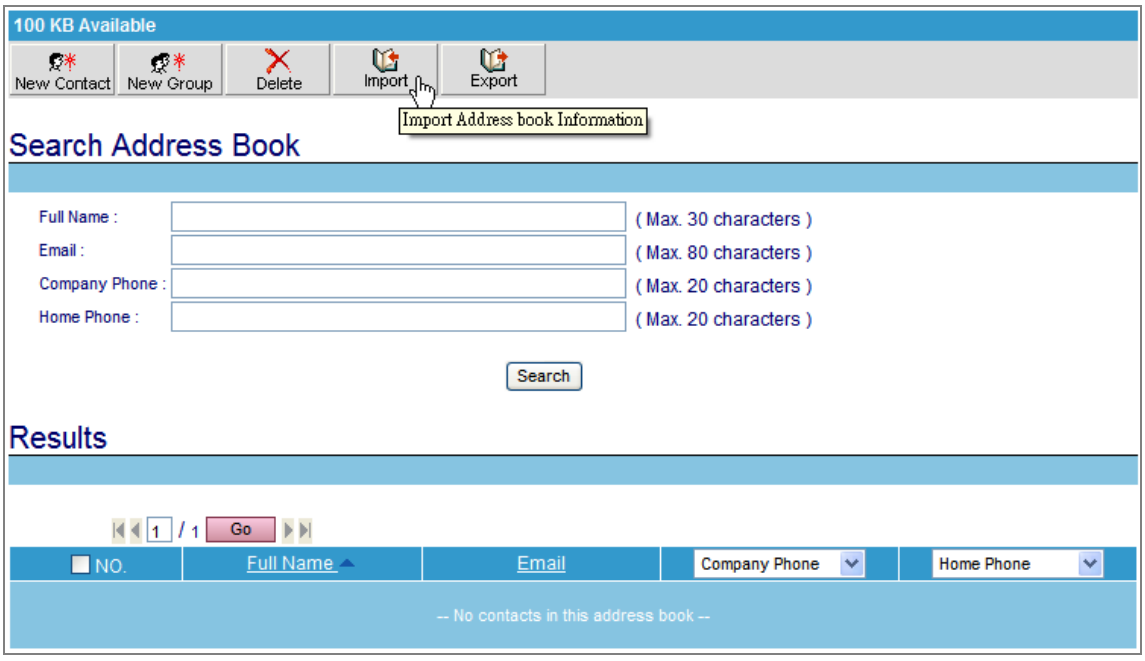


Figure 5-16 Clicking into Import Screen

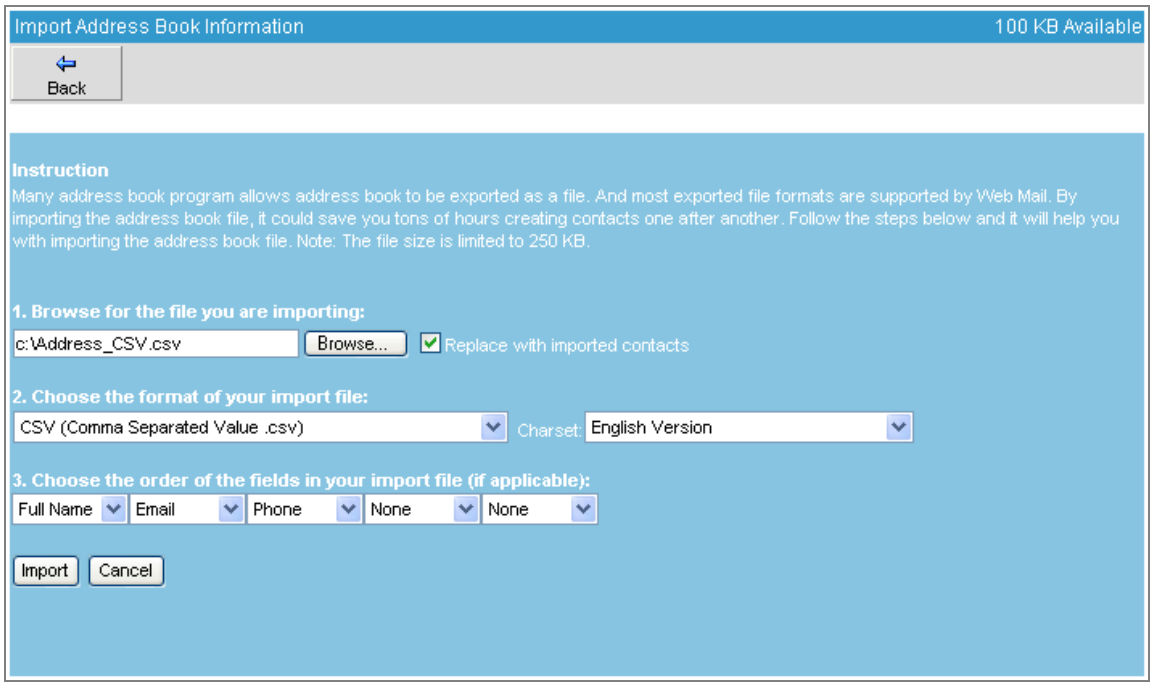


Figure 5-17 Clicking into Import Screen

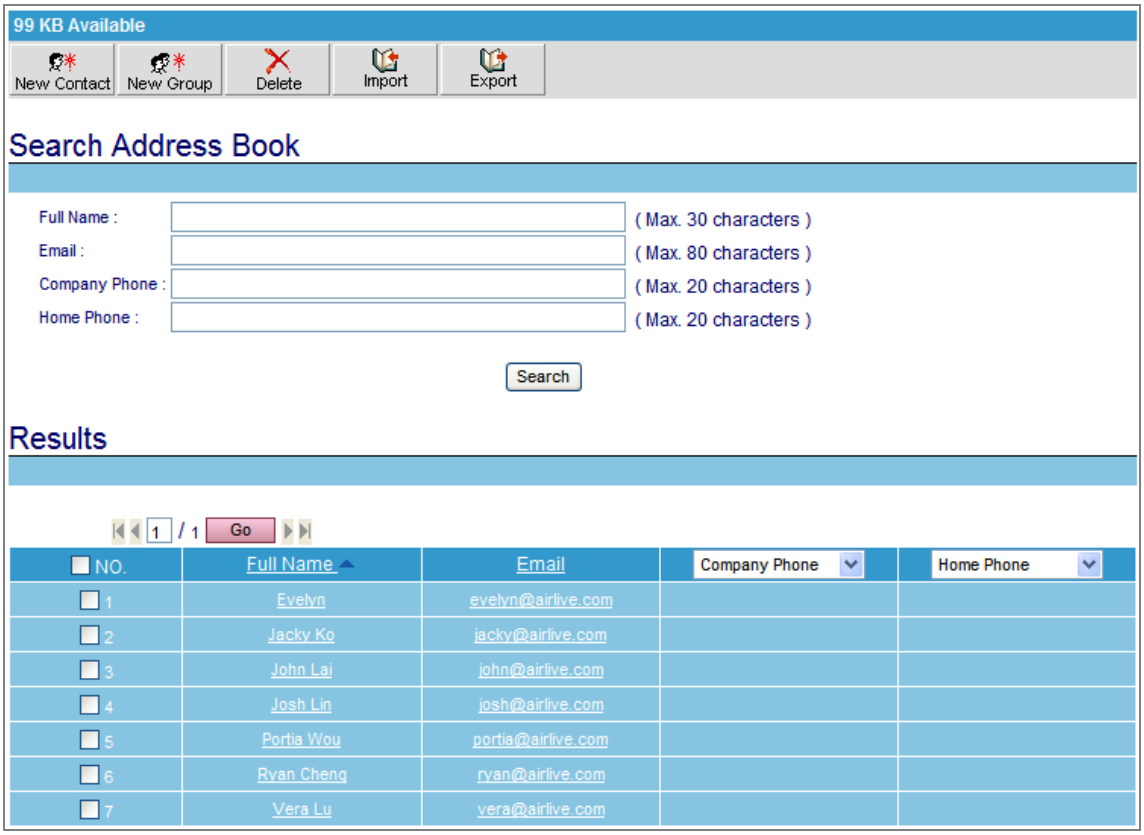


Figure 5-18 Address Book Successfully Imported

5.4 Using Web Disk to Transfer Large File

Step1. Click **Web Disk** tab in the web-based mailbox main screen, and then: (Figure 5-19)

- Locate the file by clicking **Browse** under the **Upload File to Web Disk** bar.
- Click **Upload** button. (Figure 5-20, Figure 5-21)

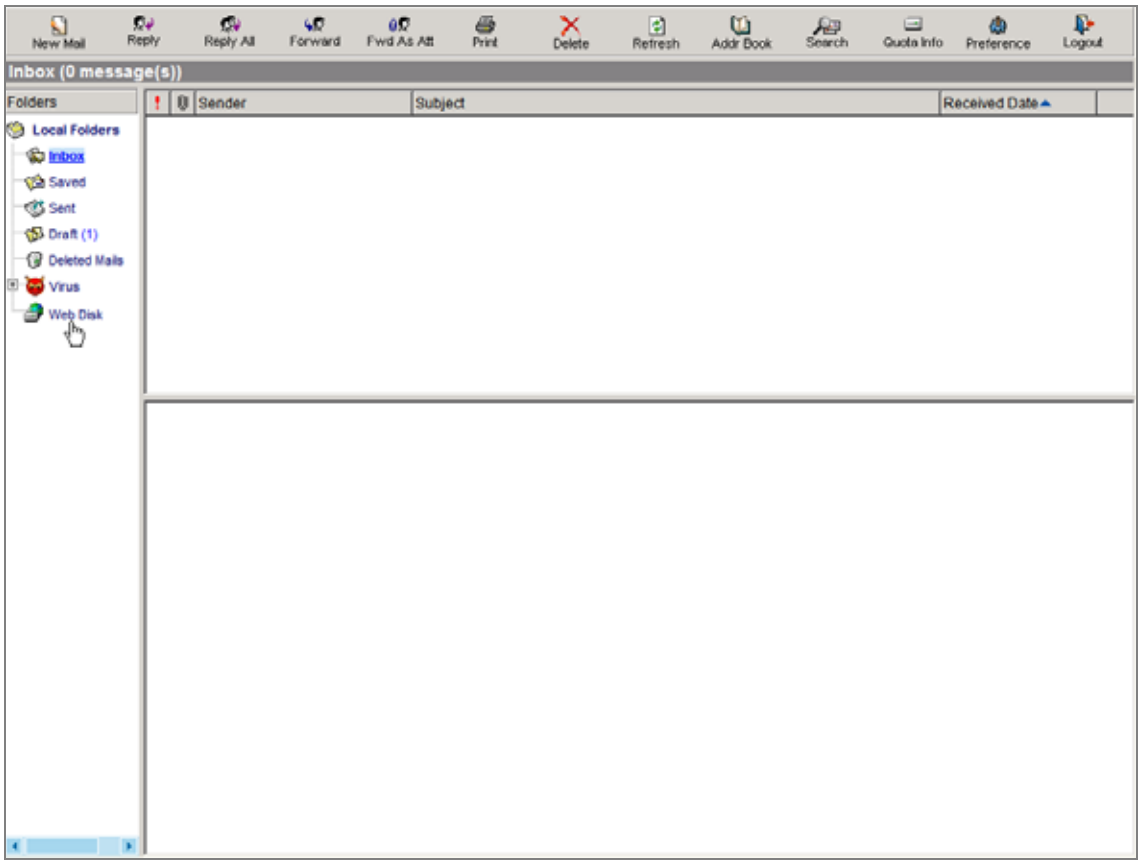


Figure 5-19 Select Web Disk on the web-based mailbox main screen

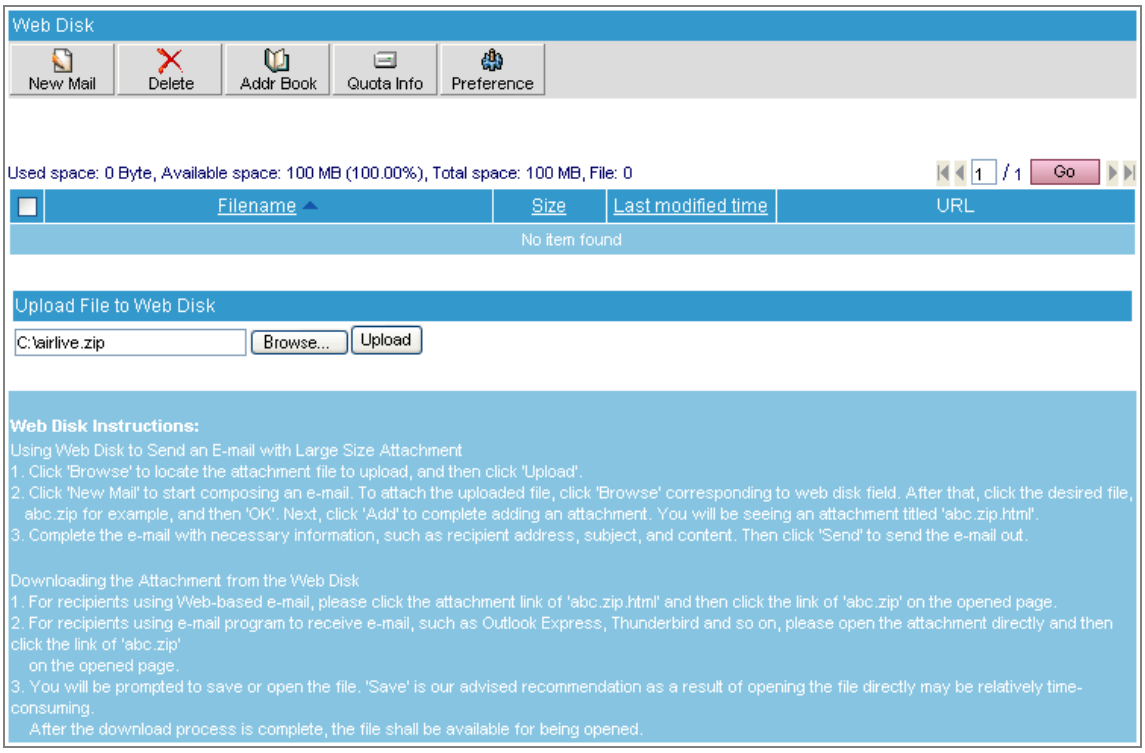


Figure 5-20 Uploading a File to ES-6000's Built-in Web Disk

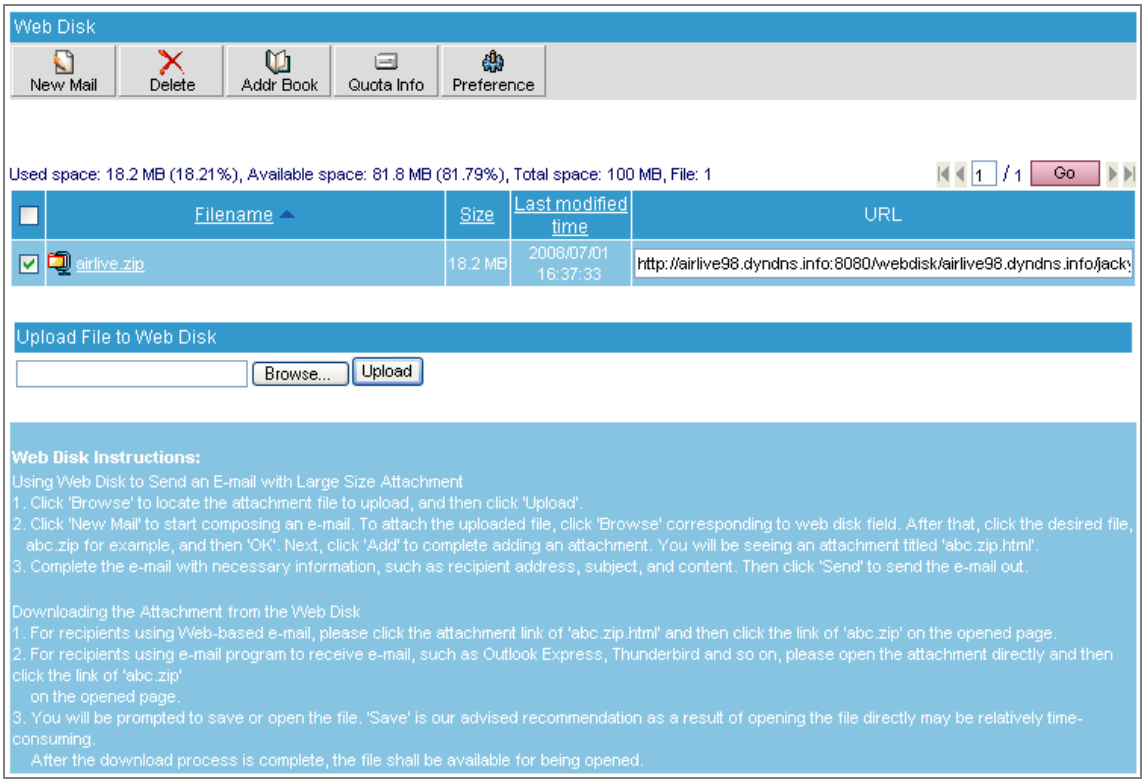


Figure 5-21 File Uploaded

Step2. Click **New Mail** in the web-based mailbox main screen, and then: (Figure 5-22)

- In the **Attachment** column, click **Browse** corresponding to **Web Disk** field.
- Click the desired file and then click **OK**. (Figure 5-23)
- Click **Add** corresponding to **Web Disk** field. (Figure 5-24)
- Complete this e-mail with necessary information, such as subject, content and recipient address.
- Click **Send**. (Figure 5-25)

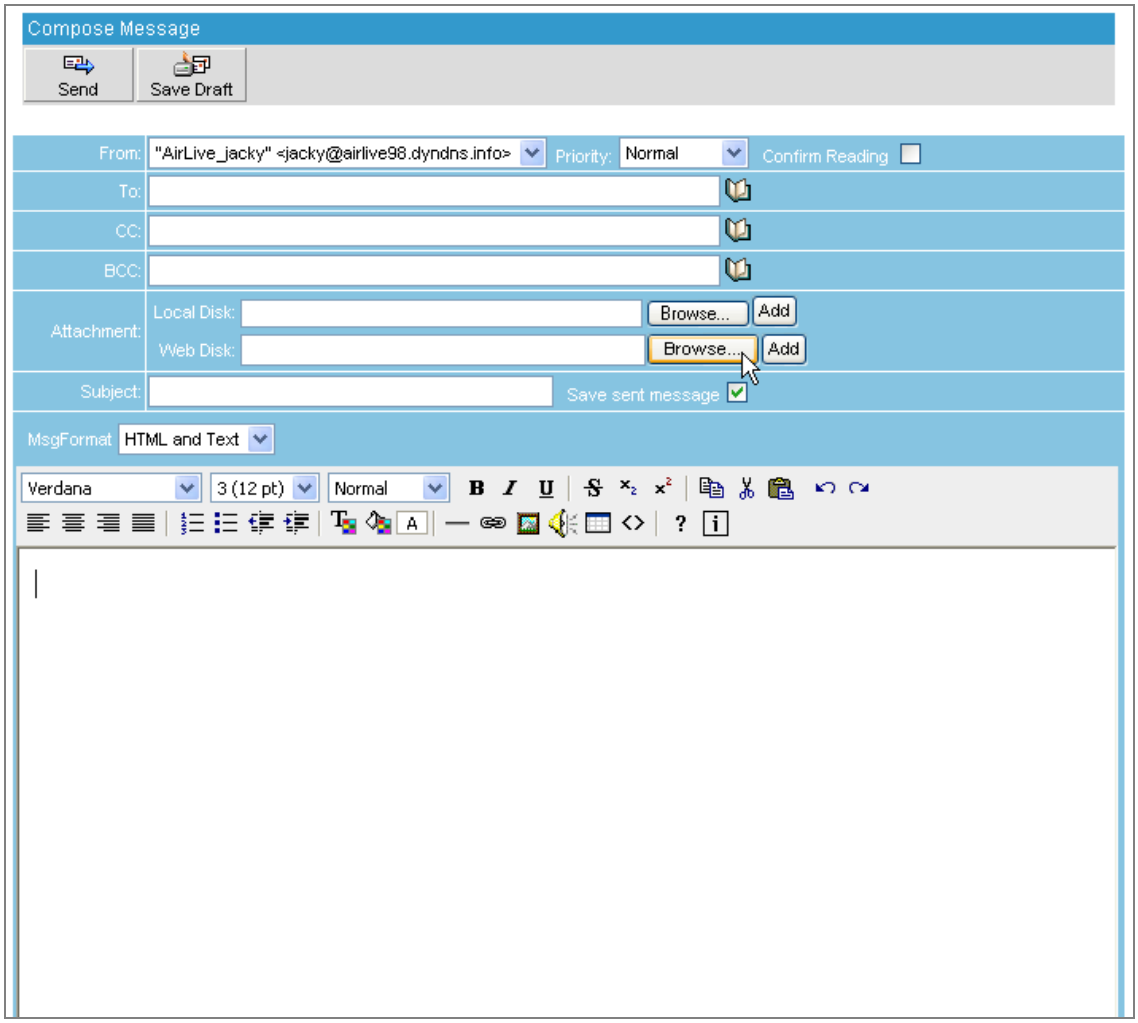


Figure 5-22 Click Brows on Web Mail main screen

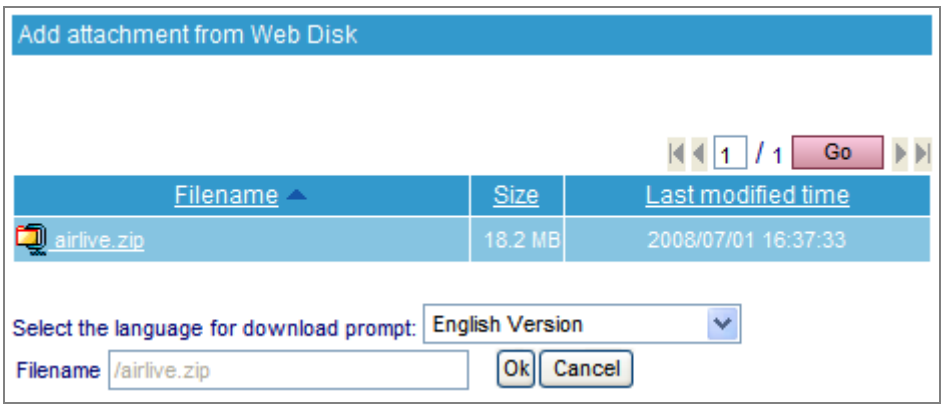


Figure 5-23 Adding an Attachment from Web Disk

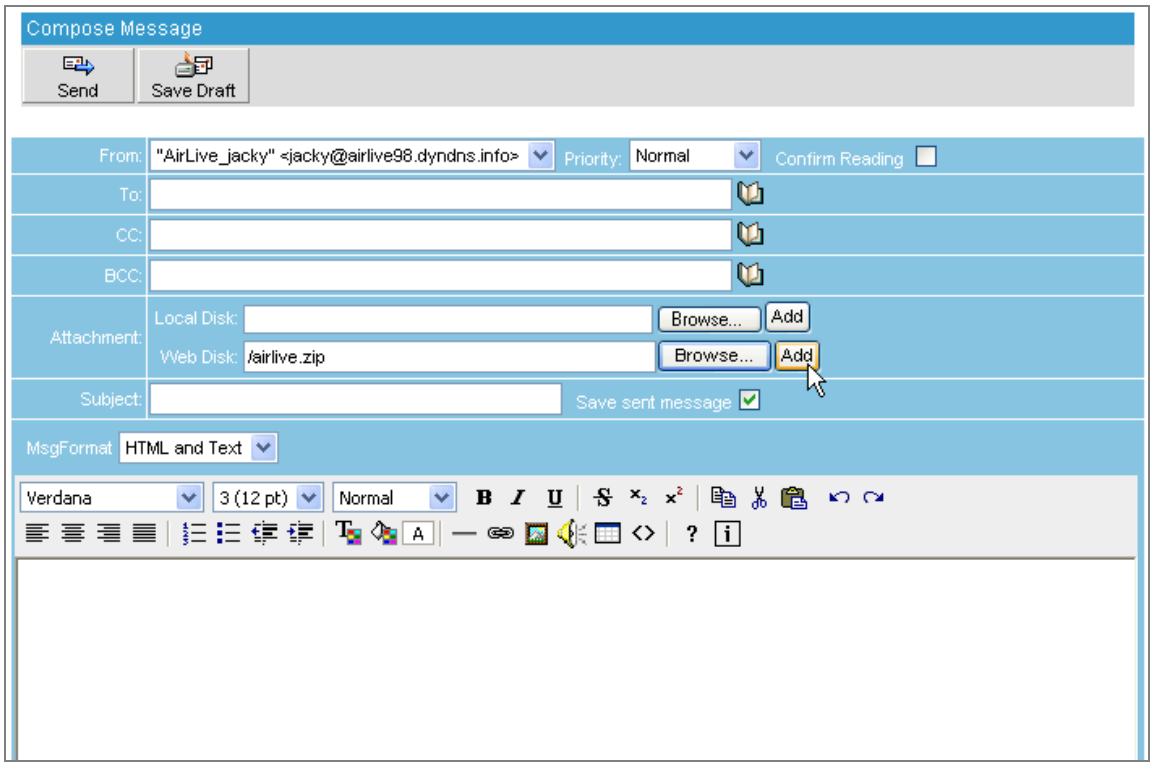


Figure 5-24 Click Add to add hyperlink file to receiver

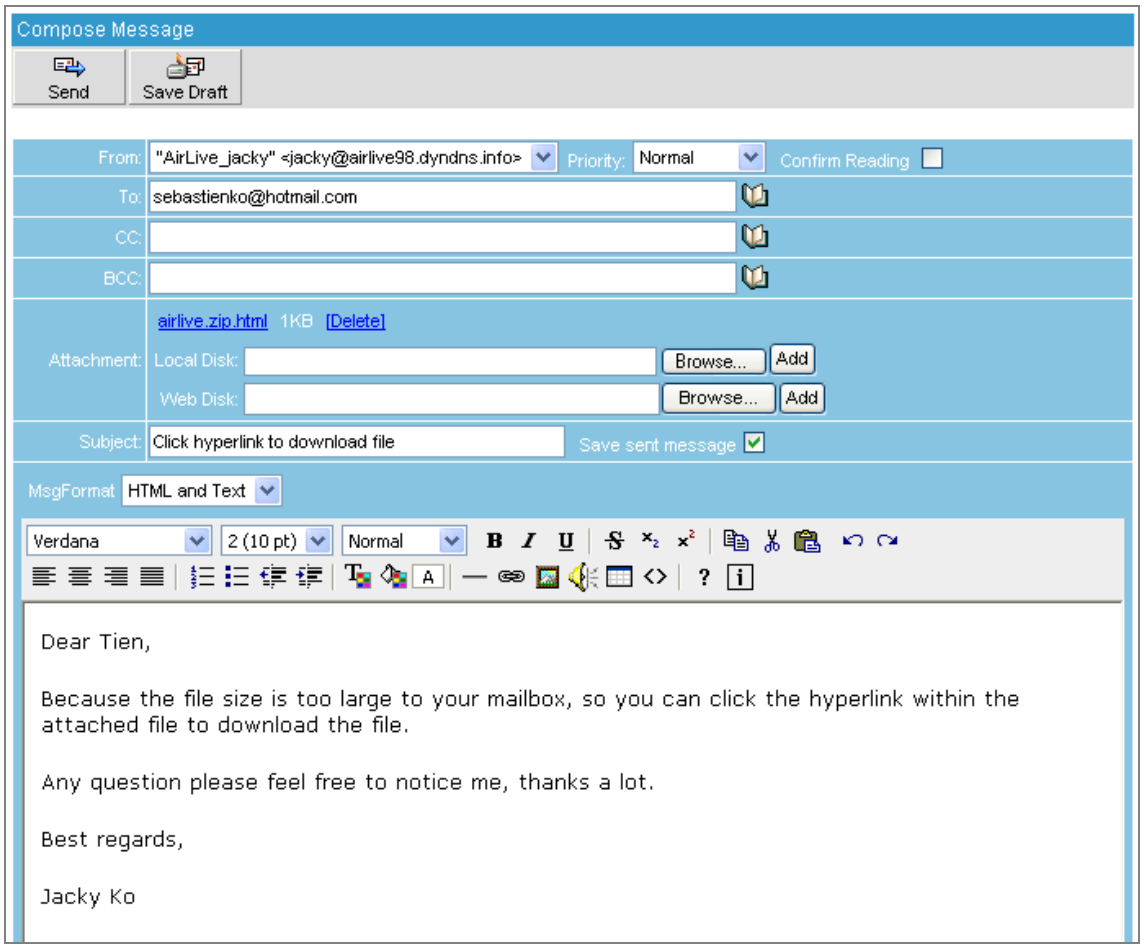


Figure 5-25 Sending out the Message

Step3. The recipient opens the attachment and then download the attachment file through a HTML page provided by ES-6000 device: (Figure 5-26, Figure 5-27)

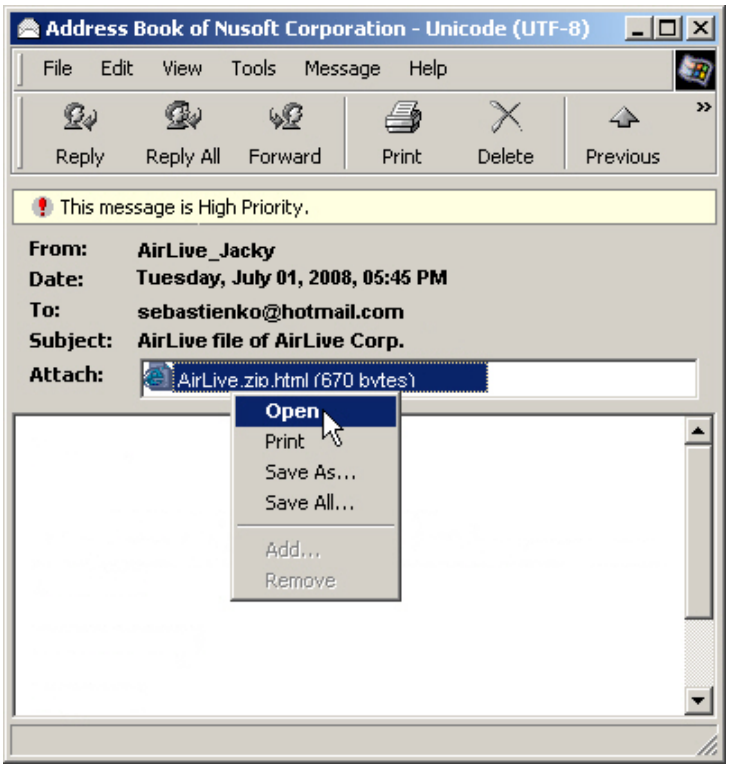


Figure 5-26 Opening the Attachment

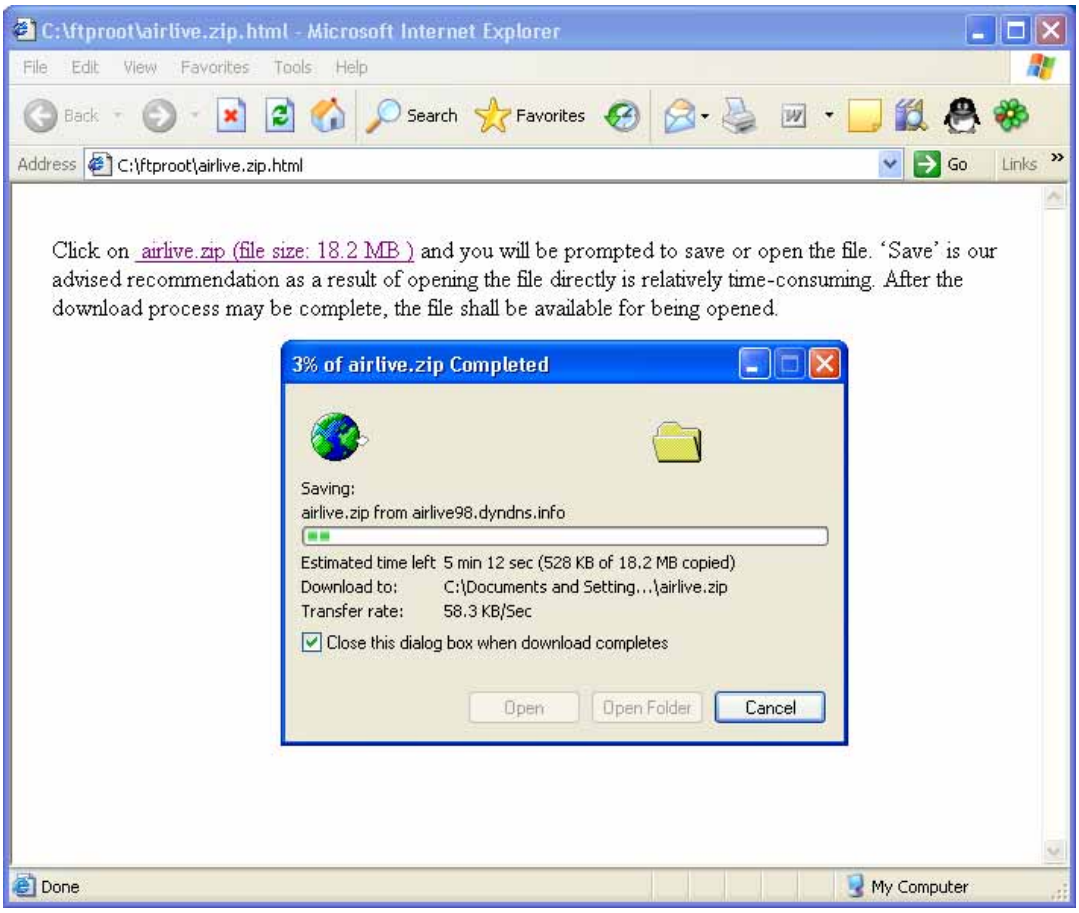


Figure 5-27 Opening the Attachment

5.5 Using White List and Black List to Filter E-Mails

Supposed the domain name “airlive.com” is registered to your organization; and you are using the account “josh” to log onto Web Mail, then:

Step1. Click **Preference** in the Web Mail main screen, and then set as below:

- Click **Edit White List**.
- Click **New**
- Create a new entry of 123xyz@hotmail.com
- Select “From” for **Direction**.
- Click **OK**. (Figure 5-28)
- Click **New** again.
- Create another entry of 123xyz@hotmail.com.
- Select “To” for **Direction**.
- Click **OK**. (Figure 5-29)
- Setting is completed. (Figure 5-30)

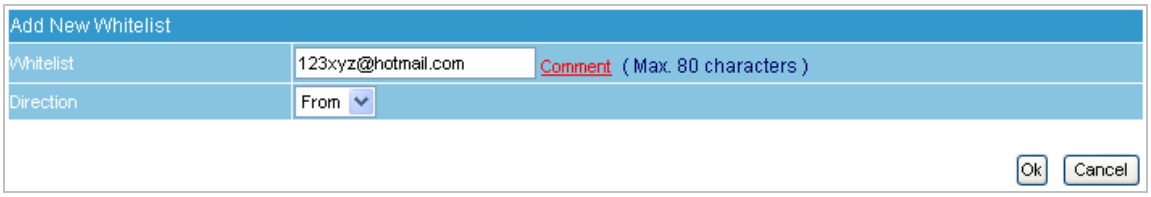


Figure 5-28 Creating the First Entry of White List

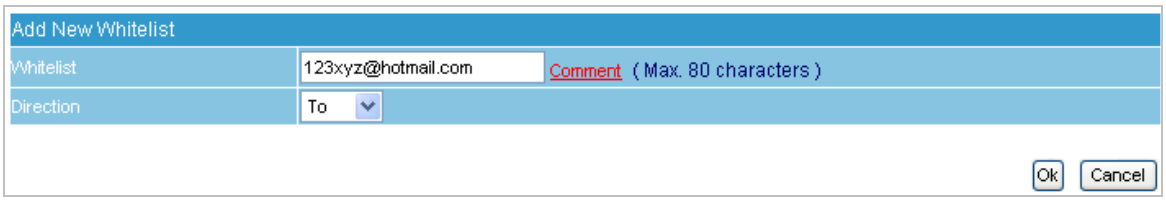


Figure 5-29 Creating the Second Entry of White List

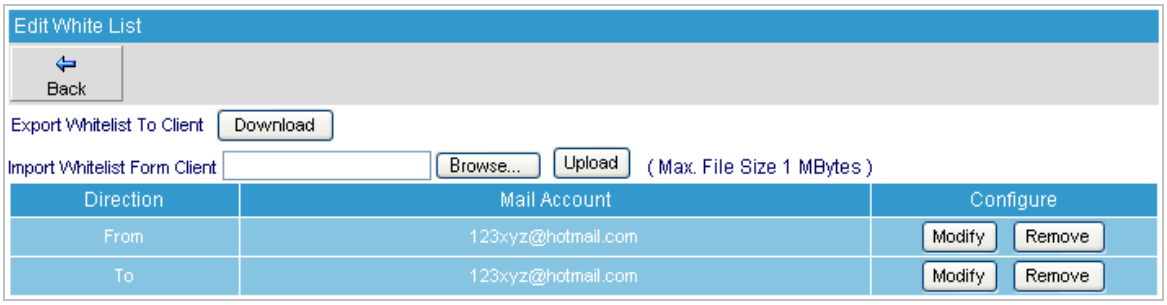


Figure 5-30 White List Completed

Step2. Click **Preference** in the Web Mail main screen, and then set as below:

- Click **Edit Black List**.
- Click **New**
- Create a new entry of *hotmail*.
- Select “From” for **Direction**.
- Click **OK**. (Figure 5-31)
- Click **New** again.
- Create another entry of *hotmail*.
- Select “To” for **Direction**.
- Click **OK**. (Figure 5-32)
- Setting is completed. (Figure 5-33)

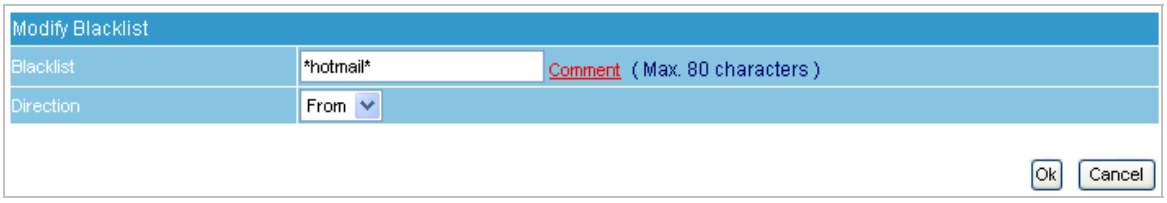


Figure 5-31 Creating the First Entry of Black List

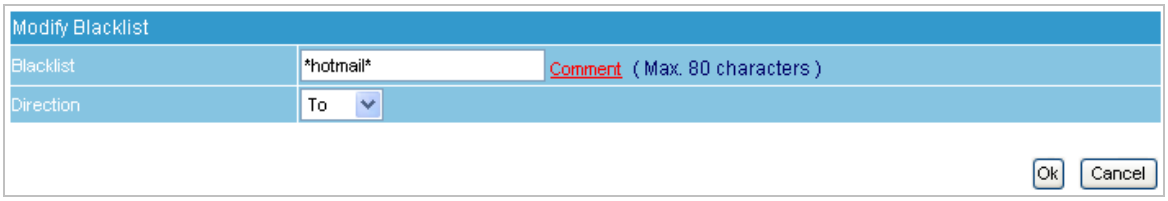


Figure 5-32 Creating the Second Entry of Black List

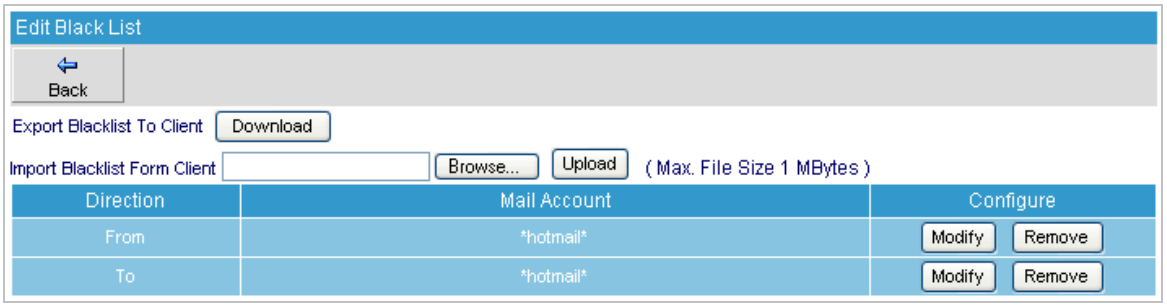


Figure 5-33 Black List Completed

Step3. When josh@airlive.com receives an e-mail from a Hotmail account:

- If the address is 123xyz@hotmail.com, then Josh will receive it.
- But if it is 456xyz@hotmail.com, then e-mails from this account will be rated as spam.

Step4. When josh@airlive.com tries to send e-mails to both 123xyz@hotmail.com and 456xyz@hotmail.com:

- Only 123xyz@hotmail.com will receive e-mails from Josh, whereas 456xyz@hotmail.com receives none as a result of e-mails sent to it are rated as spam.

5.6 Using Push Mail to Access Instant Messages

Supposed the domain name “airlive15.dyndns.org” is registered to your organization; and you are using the account “jacky” to log onto Web Mail, then:

Step1. Click **Preference** in the Web Mail main screen, and then set as below:

- Click **Push Mail Rule**.
- Click **New Entry**.
- Type “Not_Push” in the **Rule Name** field.
- Type “Not Push Mail” in the **Comments** field.
- Select “Or” for **Combination**.
- Select “Not Push” for **Action**.
- Select “From” for **Item**, “Contains” for **Condition** and then type “hotmail” as **Pattern**. (Figure 5-34)
- Click **OK**.
- Tick **When e-mail does not meet the User-defined Rule, then: Push mail to this account** for **Default Rule**.
- Click **OK**. (Figure 5-35)

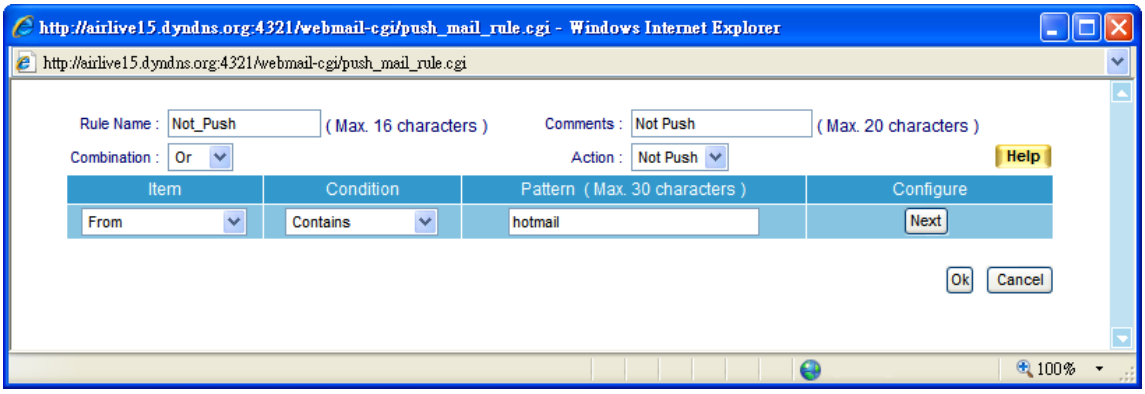


Figure 5-34 Setting Completed

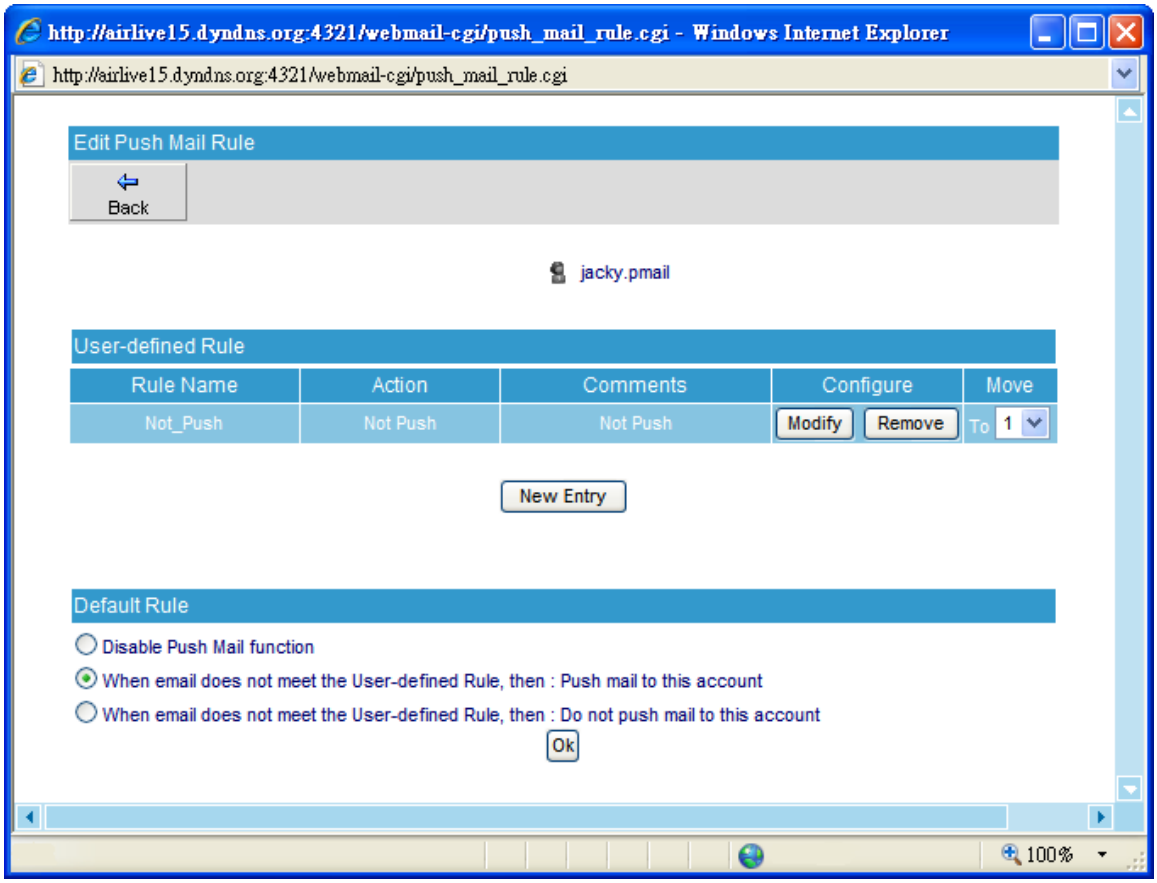


Figure 5-35 User-defined Rule Settings

Step2. When Jacky receives e-mails from any account except the hotmail account, then:

- He will be able to receive them on his mobile device immediately on condition that his mobile device supports push mail.
- He will not be able to receive mail from hotmail account on his mobile phone.

Chapter 6 Mail Security

6.1 Configure

Mail Security Configure item is the foundation of ES-6000 Anti-Spam and Anti-Virus engine to filter email; the feature is divided as **Setting** and **Mail Notice**.

6.1.1 Setting

Definition

Mail Scanned Settings:

- To define spam and virus mail size as the standard, if virus mail size exceeds the definition, the mail will not be scanned.

Unscanned Mail Setting:

- Those mails that skip the scan can be added the message to the subject.

The Subject and Content of the Notice:

- Administrator can define the subject and message contents of Mail notice. If leave both column a blank, the notice message will be sent as default contents.

Quarantine Setting:

- Check to disallow user to retrieve mail from quarantine.

1. **Only scan spam mail with a size less than:** 128K bytes.
2. **Only scan virus mail with a size is less than:** 512K bytes.
3. Unscanned e-mails will be marked as "**---Unscanned---**" in front of the subject.
4. Customize the subject and message of the mail notice.
5. Click **OK**. (Figure 6-1)

Figure 6-1 Scanned Mail Setting

- A mail notice with the customized subject and message: (Figure 6-2)

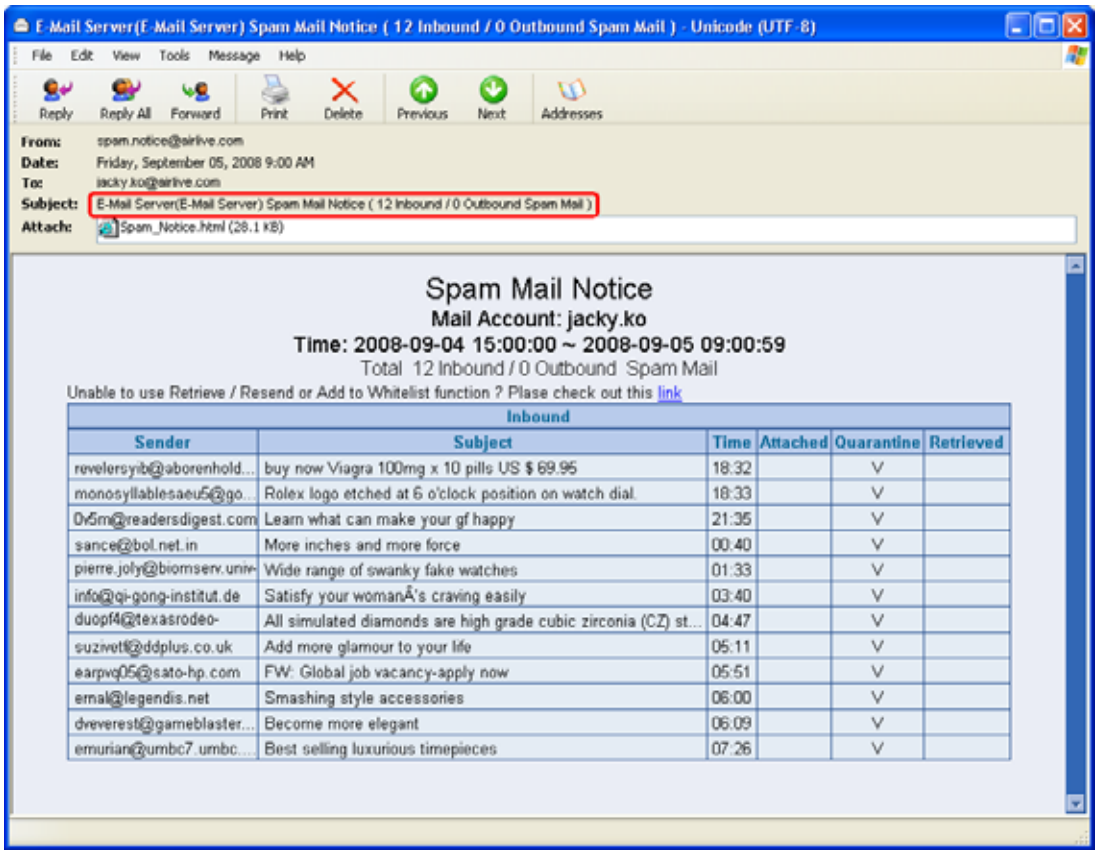


Figure 6-2 A Mail Notice with Customized Subject and Message

- Unscanned e-mails will be marked as "**---Unscanned---**" in front of the subject. (Figure 6-3)

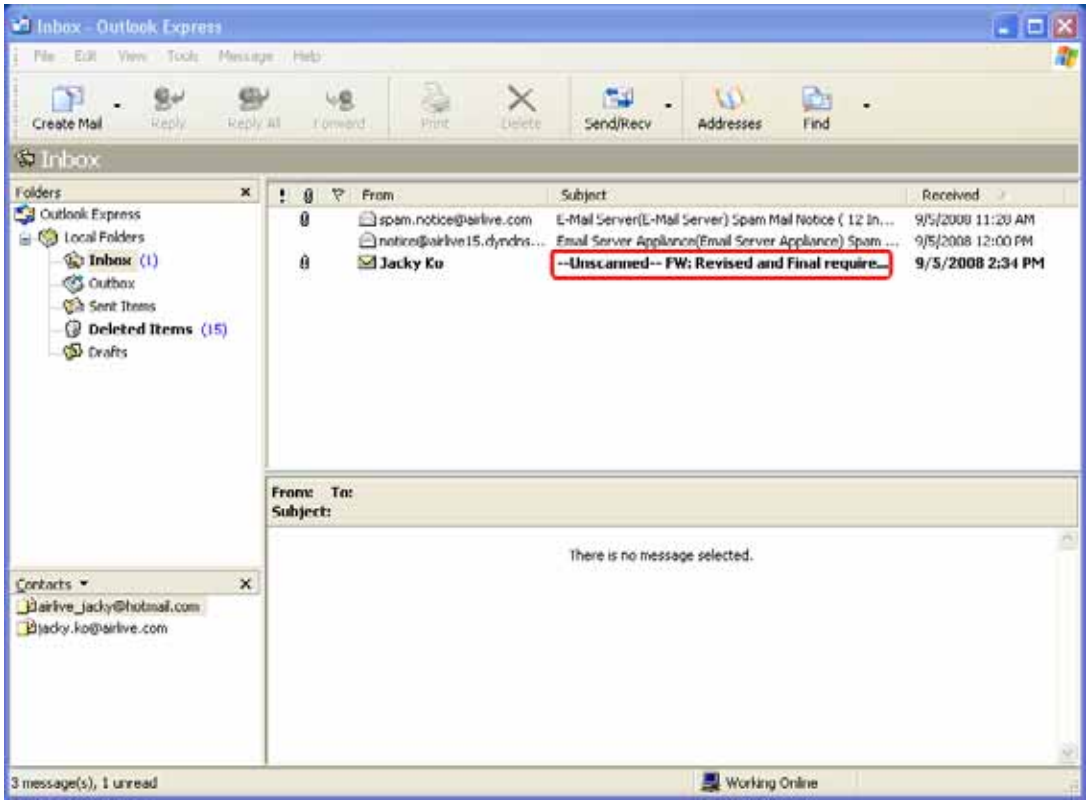


Figure 6-3 An E-Mail Marked as "Unscanned"

6.1.2 Mail Notice

Mail Notice feature is not just to inform the mail report, administrator can also retrieve the mail from Mail Notice.

The example will show you the procedure and demonstrate how to retrieve the mail.

Step1. In the path of **Mail Security → Configure → Mail Notice**, there you can select notice accounts: (Figure 6-4)

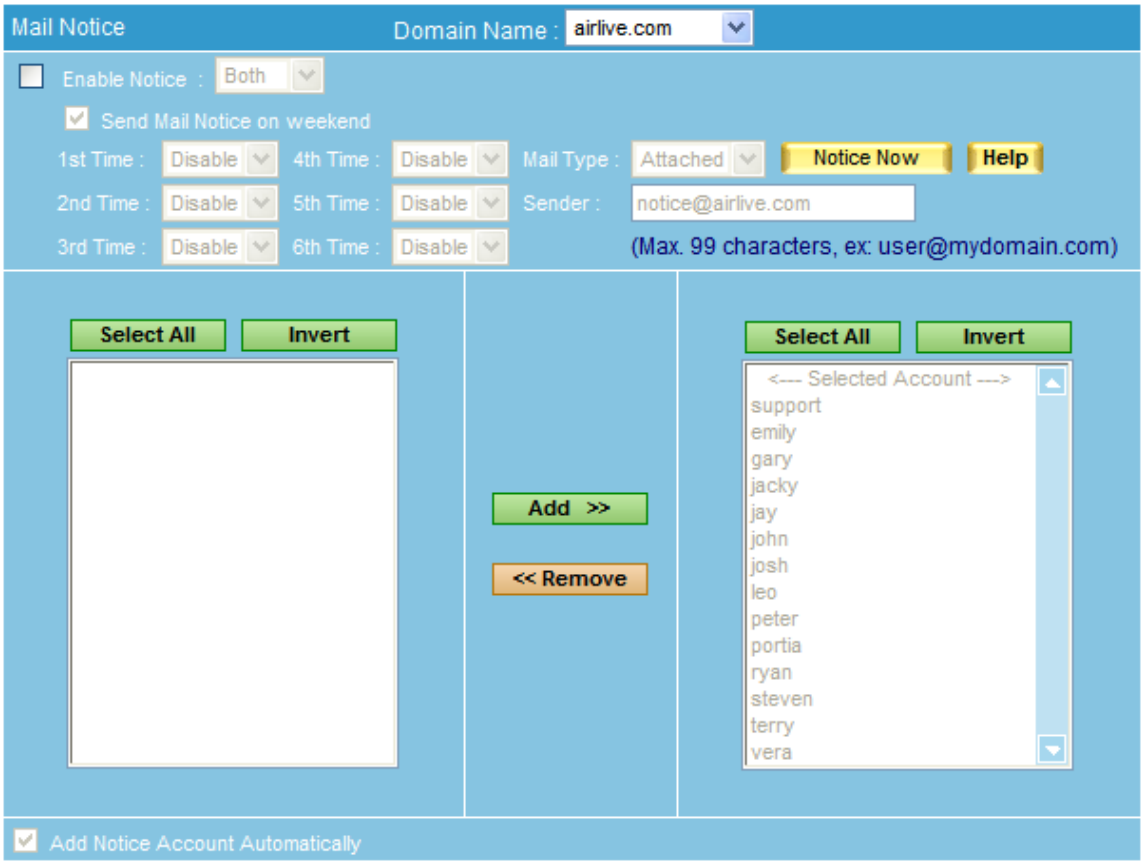


Figure 6-4 Notice account list

Step2. In the path of **Mail Security → Configure → Mail Notice**, select or input setting as below:

- Check **Enable Notice**
- Check **Send Mail Notice on Weekend**
- Select **00:00** for **1st time**
- Select **04:00** for **2nd time**
- Select **08:00** for **3rd time**
- Select **12:00** for **4th time**
- Select **16:00** for **5th time**
- Select **20:00** for **6th time**
- Select **HTML** for **Mail Type**
- **Sender** sets as **notice@aitlive.com** (Default)

- Choose accounts for mail notice and click **Add**. The selected accounts list on the right shows result.
- Enable **Add Notice Account Automatically**
- Click **OK**
- When a new account is created on ES-6000, this account will be automatically created in **Selected Accounts** and receiving mail notice periodically. (Figure 6-5)

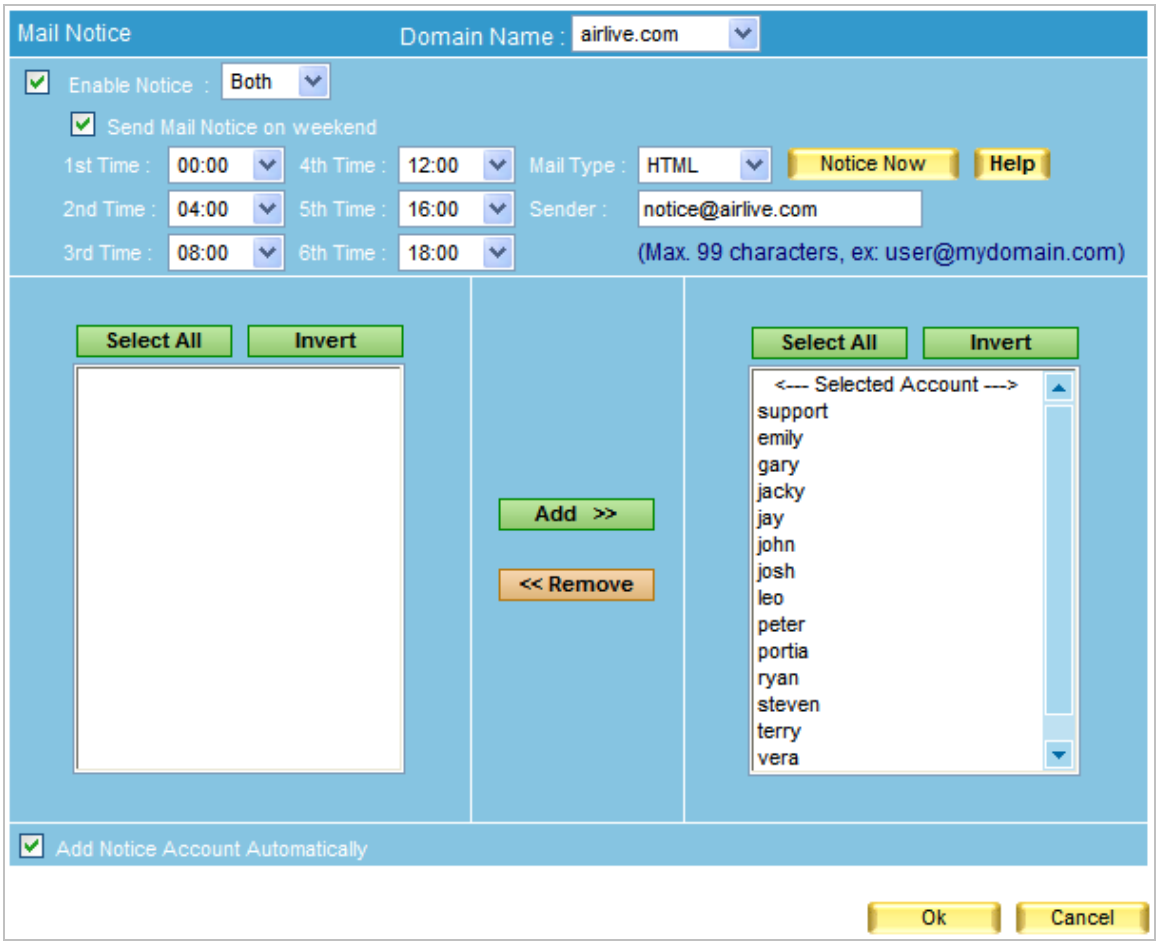


Figure 6-5 Mail notice settings

1. When inbound or outbound mails are inspected as spam or virus mails, and those mails happen to be the mails of **Selected Account**, system will send mail notice to those accounts. Account user can decide whether to retrieve quarantined mails or not.
2. Mail notice issues on schedules and choose the nearest time to issue.
3. Recipient will not receive any mail notice if there is not any spam or virus mails exist.
4. Administrator can use **Select All** or **Invert** to remove accounts from **Selected Account**, so as to cancel mail notice.
5. If **Send Mail Notice on Weekend** is disabled, mail notice will be issuing according to the 1st time setting on Monday.
6. If **Add Notice Account Automatically** is disabled, new created account will not be receiving mail notice.

Step3. When receiving mail notice, recipient can:

- Retrieve incoming mail by clicking **Retrieve** in the **Inbound List**. (Figure 6-6)
- After system resend mail, it shows completed. (Figure 6-7)
- Resend outgoing mail by clicking **Resend** in the **Outbound List**. (Figure 6-8)
- After system resend mail, it shows completed. (Figure 6-9)

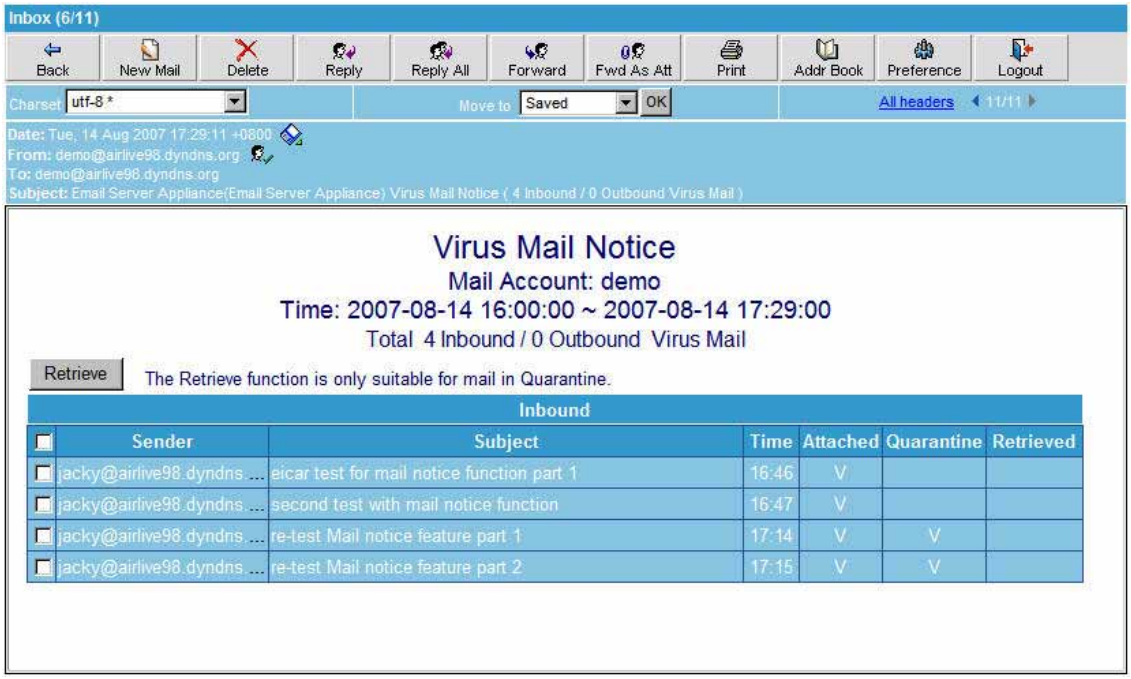


Figure 6-6 Check mails to retrieve

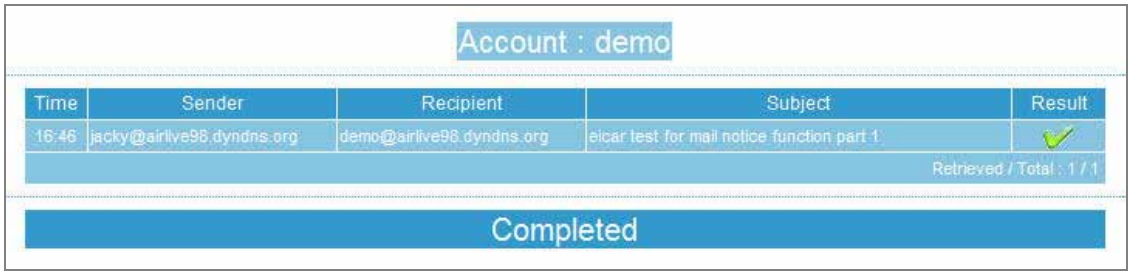


Figure 6-7 Retrieve completed

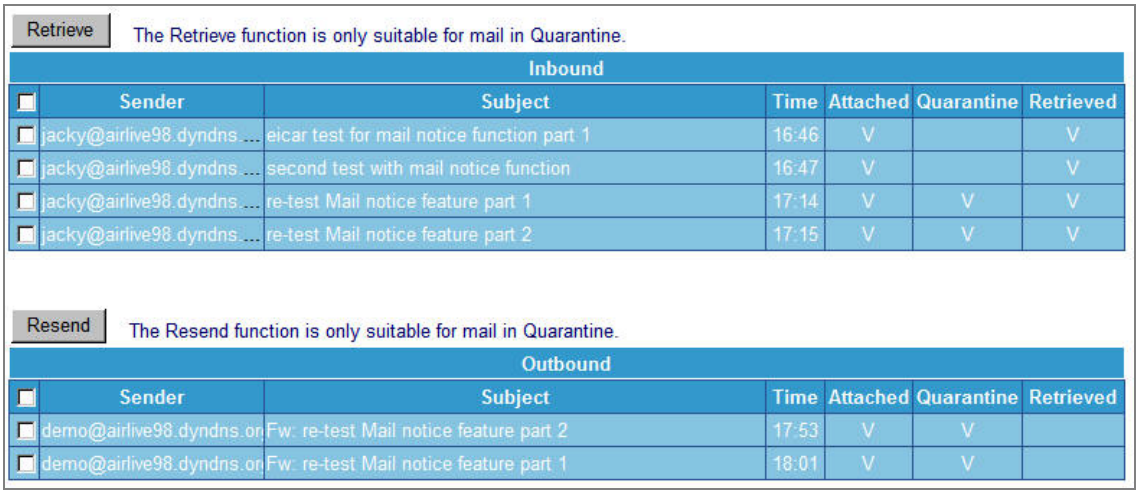


Figure 6-8 Check mails to resend

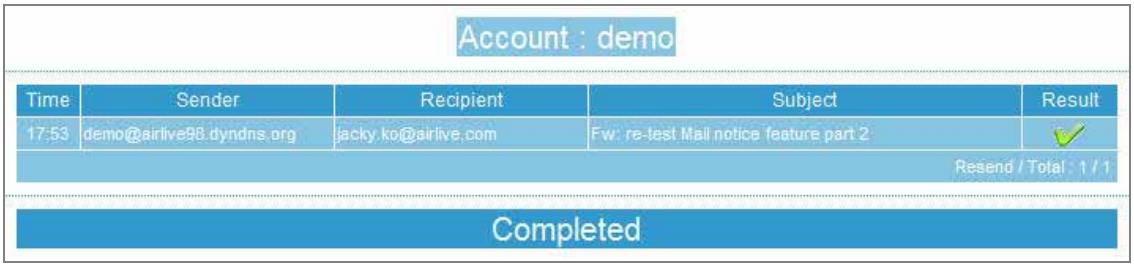


Figure 6-9 Resend completed

To retrieve or resend mails that inspected as spam or virus mail:

Method 1:

- Open the attachment (Spam_Notice.html or Virus_Notice.html) of mail notice. (Figure 6-10)
- Check **Open it** and click **OK** in the **Open Attachment Warning** window. (Figure 6-11)
- Check the box next to **Sender** under the **Retrieve** button, and click **Retrieve** to retrieve all mails. (Figure 6-12)
- Check the box next to **Sender** under the **Resend** button, and click **Resend** to resend all mails. (Figure 6-13)

Method 2:

- When receiving a HTML Mail Notice :
  - By reason of the Java Script feature is set as **Restricted Sites Zone** by the default setting in Outlook Express, which limits the function of Java Script, thus, user has to :
    1. Check boxes one at a time and click **Retrieve** in the inbound list to retrieve mails. (Figure 6-14)
    2. Check boxes one at a time and click **Resend** in the outbound list to resend mails. (Figure 6-15)

- To modify Java Script feature setting in Outlook Express, please go to **Tools → Options → Security → Virus Protection**, check **Internet Zone**. After doing so, user will be able to check all boxes at once by checking the box next to the **Sender** under the **Retrieve** or **Resend** button

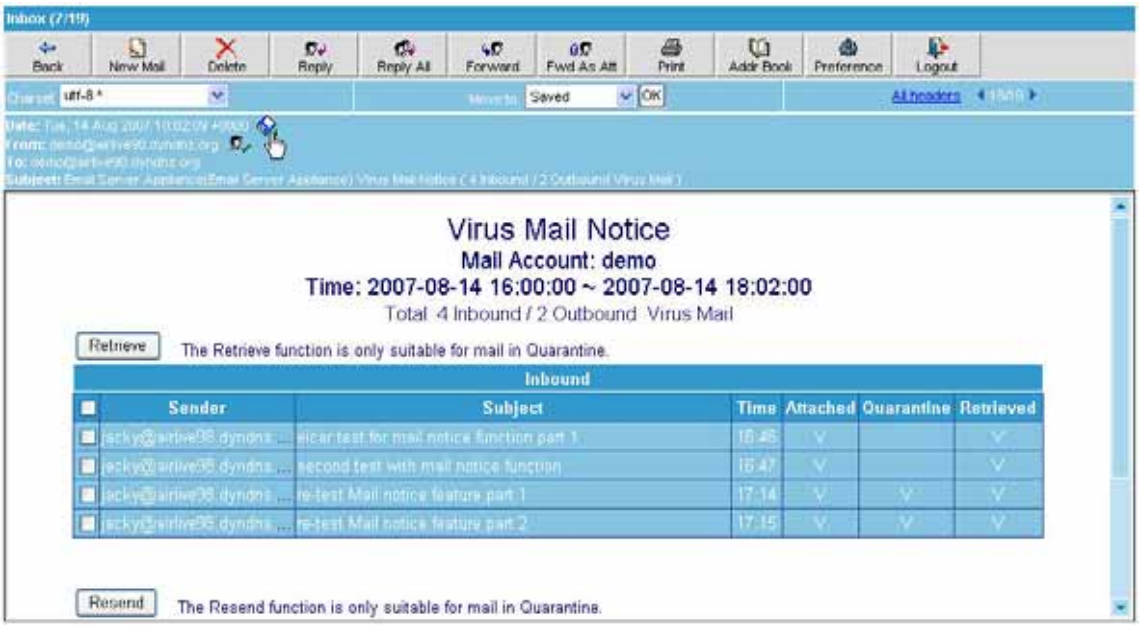


Figure 6-10 Open the attachment of notice mail

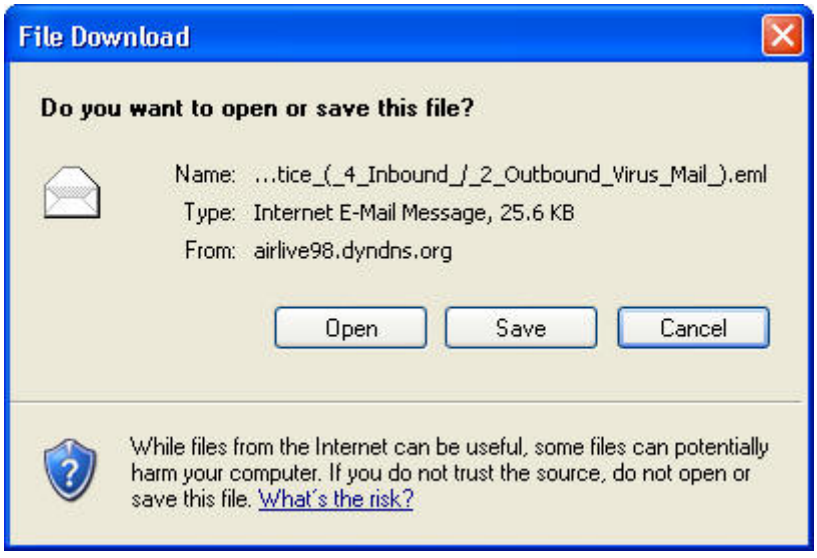


Figure 6-11 Confirm to open attachment

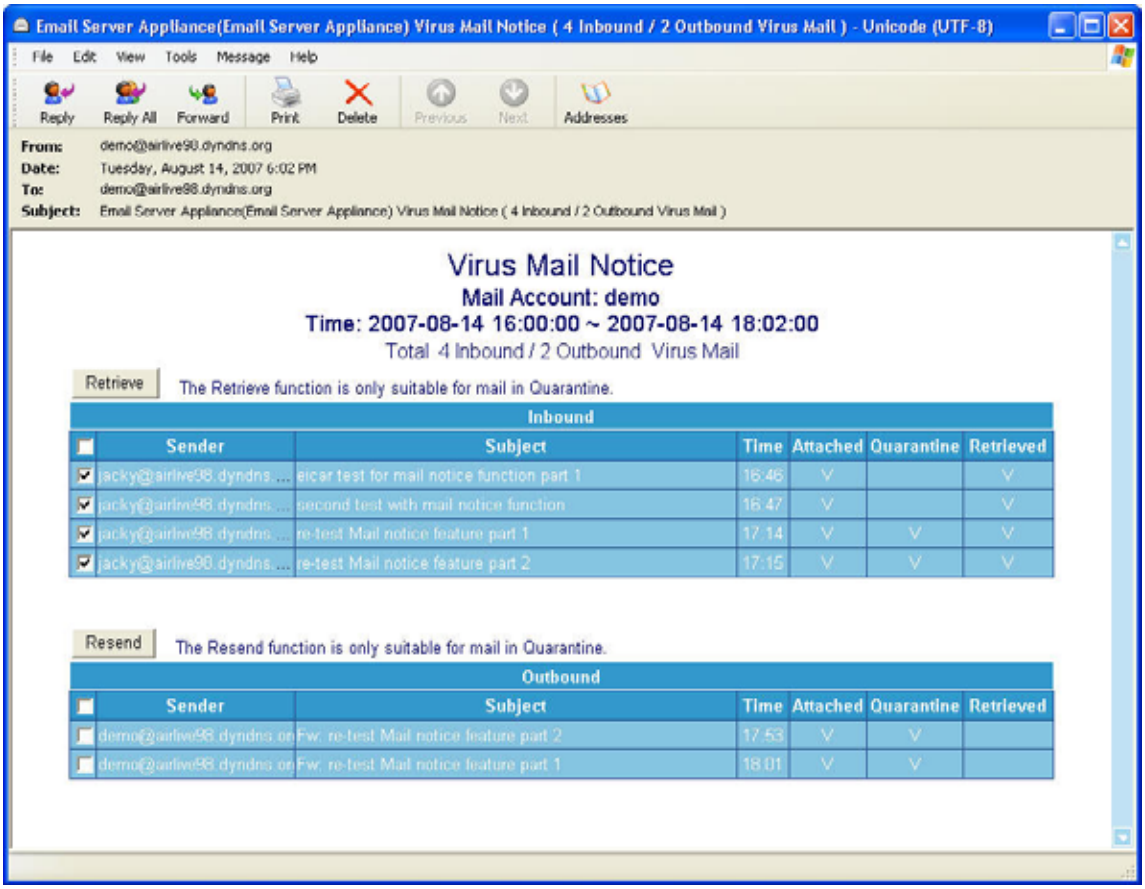


Figure 6-12 Check all mails to retrieve

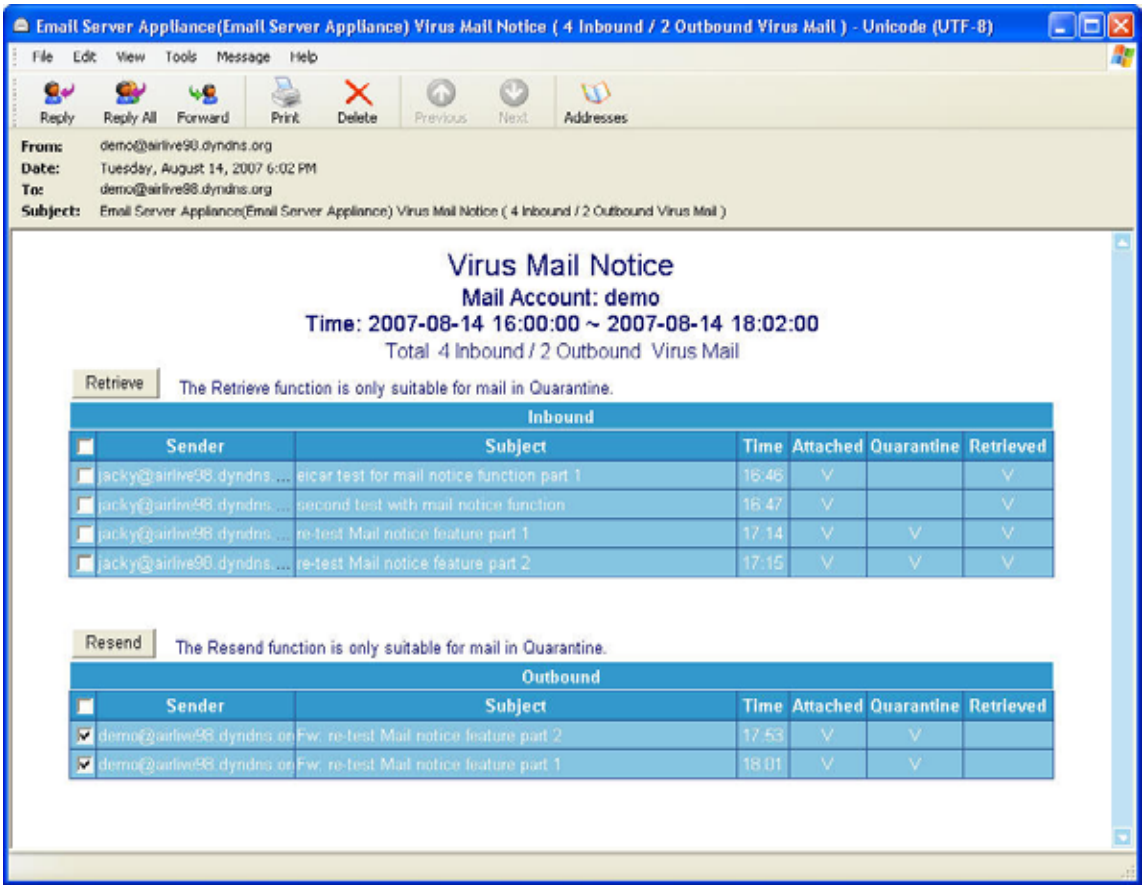


Figure 6-13 Check all mails to resend

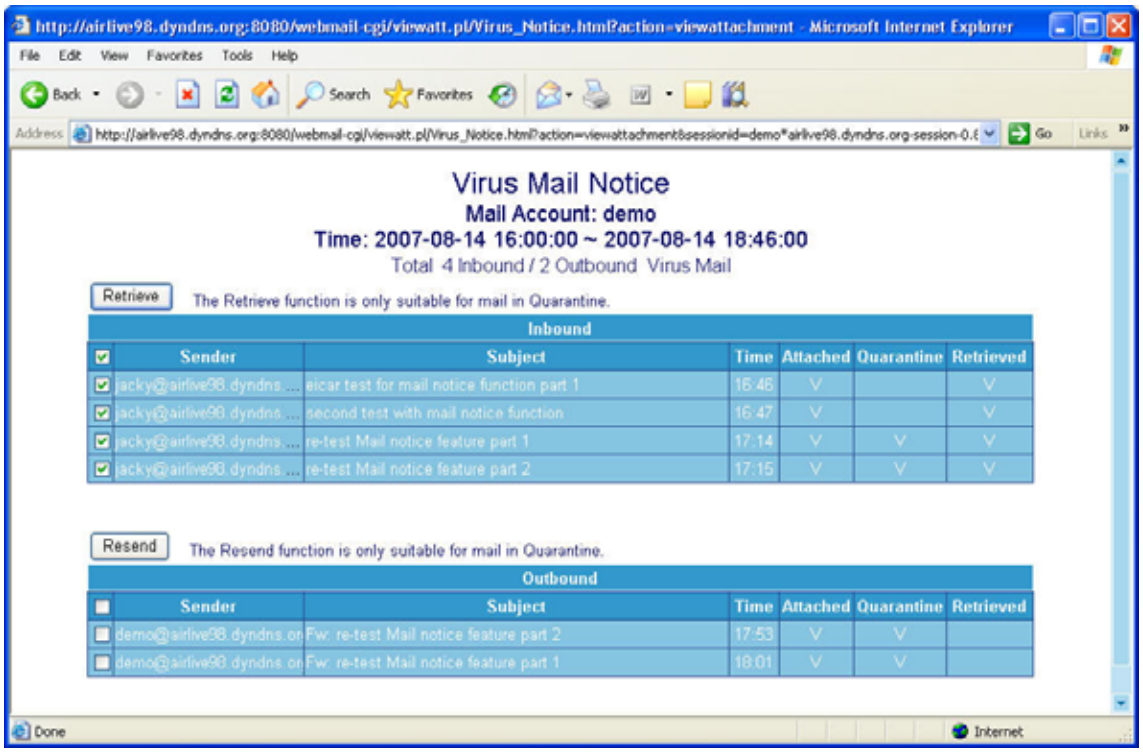


Figure 6-14 Check all mails to retrieve in a HTML Mail Notice

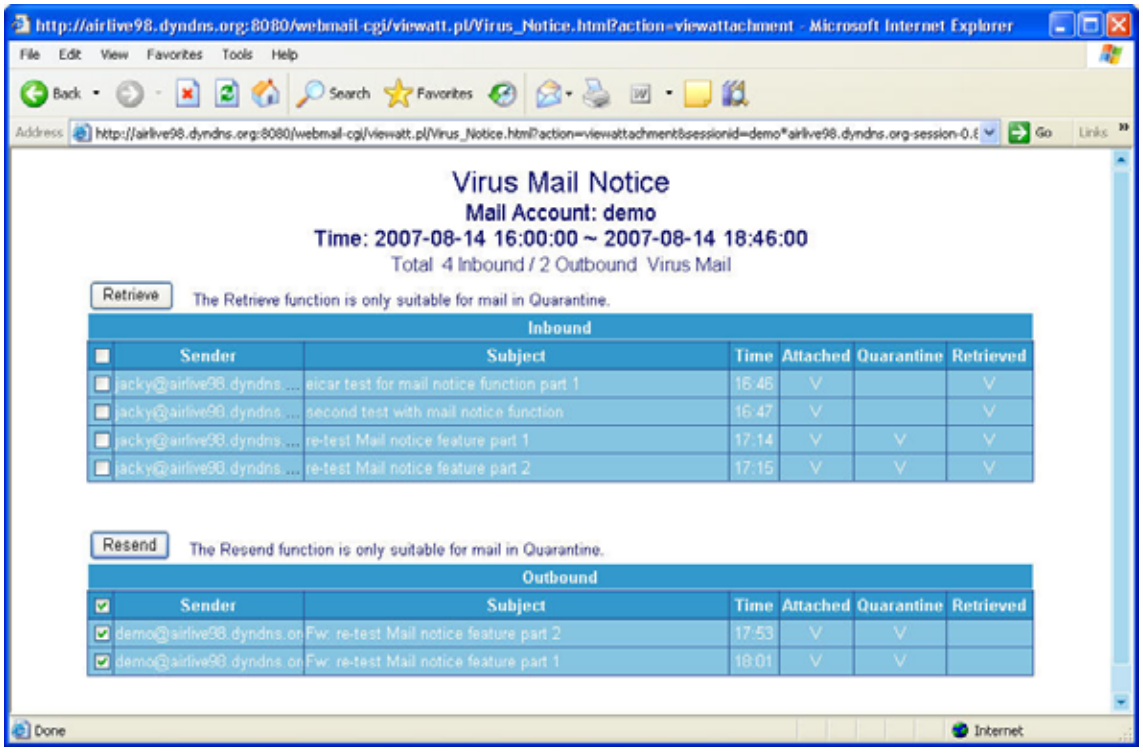


Figure 6-15 Check all mails to resend in a HTML Mail Notice

6.2 Anti-Spam

ES-6000 can filter every incoming and outgoing e-mail. Users will no longer receive plenty of spam which saves your precious time for work rather than waste your time on taking the business e-mails out of spam. It also lowers the risk of deleting the business e-mails when deleting spam.

6.2.1 Setting

Anti-Spam Setting

- You may view or configure the settings of e-mail inspection.
- E-mails exceeding the threshold score can be added a warning message and a score tag to the subject, whereas others below the threshold score can only be added a score tag in the subject line.
- The approaches of inspection:
  - **Check spam fingerprint**: Generates an ID number by analyzing the e-mail with algorithms, and then compare it to the spam ID list on server.
  - **Enable Bayesian filtering**: Compares the e-mail header to the Bayesian database.
  - **Enable spam signature push update**: Generates a value by analyzing the e-mail with algorithms, and then compare it to the spam signatures on database.
  - **Greylist Filtering**: Drops the session created by the first incoming e-mail.
  - **Check if the sender's IP address is on Real-Time Block List**: Compares the sender IP address to the blacklist on server.
  - **Enable email spoofing detection**: Checks whether the domain engaged in the execution of SMTP HELO / ESMTP EHLO commands is identical with that of the sender's address.
  - **Check the validity of each sender's account**: Uses probing packets to detect the validity of a sender's account.
  - **Auto-Whitelist**: Automatically whitelists the subnet belonging to senders based upon a mean spam weighting accumulated from previously sent email.
  - **Enable Sender Policy Framework (SPF)**: Checks whether the sender's IP address is identical with the one specified in the DNS SPF record.
  - **Enable DomainKeys**: Verifies the domain of an email sender and the message integrity.

ES-6000 uses default settings to filter spam upon no approach being taken.

Bayesian filtering works not until database has accumulated 200 spams and 200 hams.

Inspection Direction

- Action to inbound spam e-mails can be deleted, or delivered, or quarantined.
- Action to outbound spam e-mails can be deleted, or delivered, or quarantined.

◆ Refer to the steps below to make settings:

1. Under **Inspection Direction** bar, tick both **Action of Inbound Spam Mail** and **Action of Outbound Spam Mail**, then tick **Deliver to the recipient** for both.
2. Select “5” for **The threshold score of spam mail**.
3. Type “**---spam---**” in the **Add the spam string to the subject line** field.
4. Check **Add score tag to the subject line**.
5. Click **OK**. (Figure 6-16)

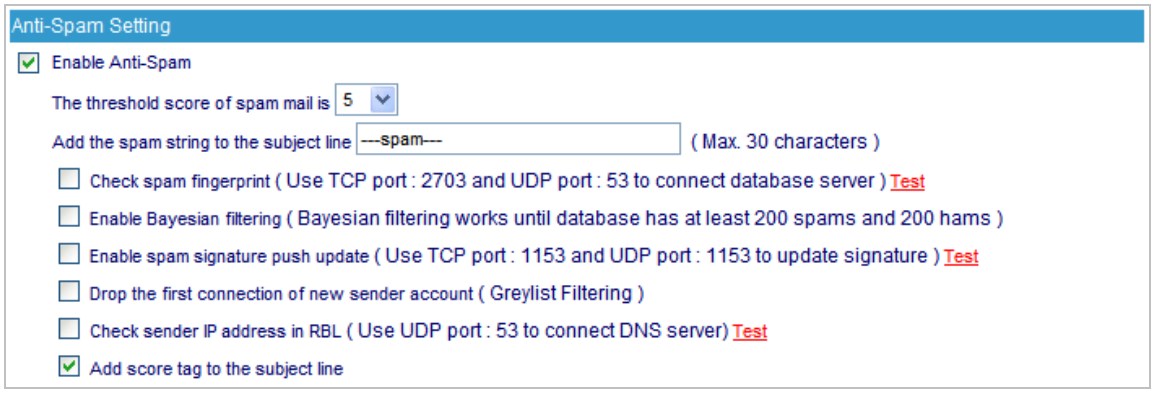


Figure 6-16 Anti-Spam Settings

◆ The figure below shows an e-mail is marked as “---spam---” along with a score tag (optional) in the subject. (Figure 6-17)

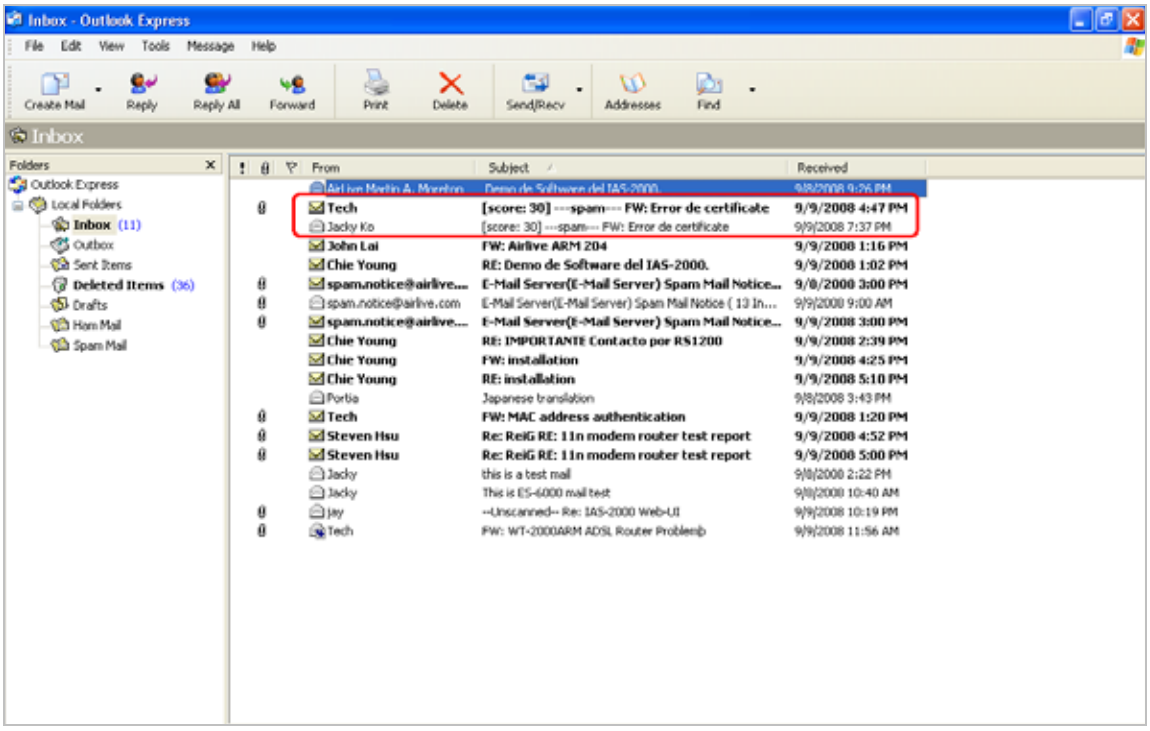


Figure 6-17 An E-Mail Marked as “---spam---” in the Subject

◆ The figure below shows a normal e-mail merely has a score tag (optional) in the subject. (Figure 6-18)

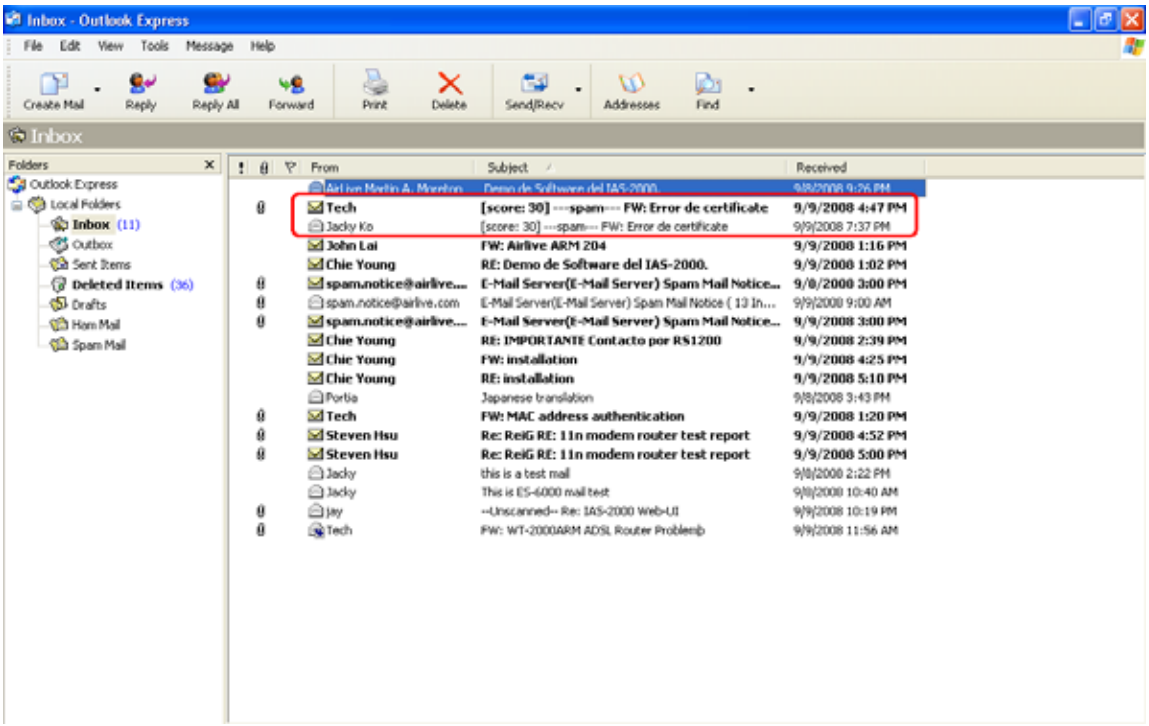


Figure 6-18 Normal E-Mail with a Score Tag in the Subject

6.2.2 Personal Rule

The Mail server administrator can help user to search the target mail, and verify if the target mail was delivered successfully or not. It can also retrieve mail from quarantine.

For the further feature of personal rule, administrator can manage user's personal whitelist or blacklist as well. (Figure 6-19)

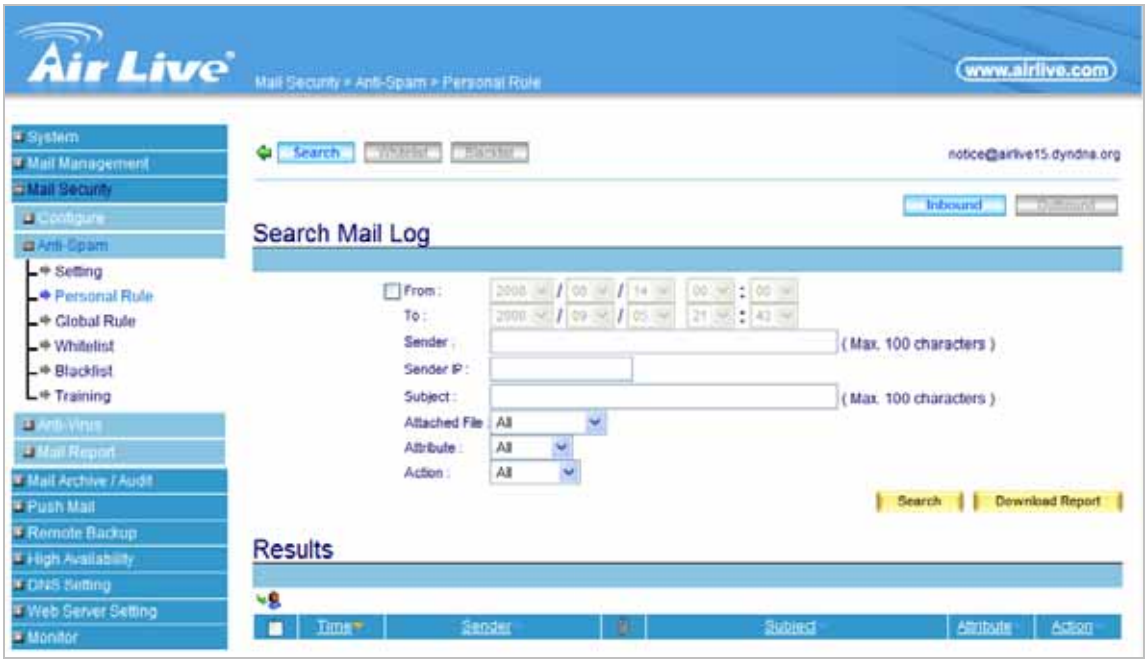


Figure 6-19 Personal Rule

Definition:

- **Search**
  - Used for searching for individual e-mails
  - Used for retrieving quarantined e-mails

- **Whitelist**
  - Specifies permitted e-mail addresses

- **Blacklist**
  - Specifies prohibited e-mail addresses

6.2.3 Global Rule

Global rule works to identify mail rule to filter all incoming or outgoing mails, once the mail matches the rule, it will be processed based on configuration. (Figure 6-20)

Figure 6-20 Global Rule

Definition:

- **Rule Name**
  - The name of the custom spam mail determination rule

- **Comment**
  - To explain the meaning of the custom rule

- **Combination**
  - **Add:** It must be fit in with all of the custom rule mails that would be considered as spam mail or ham mail.
  - **Or:** Only be fit in with one of the custom rule mails that would be considered as spam mail or ham mail.

- **Classification**
  - When setting as **Spam**, it will classify the mails that correspond to the rule as spam mail.
  - When setting as **Ham (Non-Spam)**, it will classify the mails that correspond to the rule as ham mail.

- **Action**
  - Only when **Classification** is set as **Spam** that will enable this function. Because only spam mail needs to be handled.

- You can choose **Store in quarantine**, **Delete spam mail**, **Deliver to the recipient**, or **Same as Spam Setting** to process the spam mail.

- **Item**
  - To judge if it is spam mail according to the Header, Body, Size or else content of the mail.
  - The item includes **Received**, **Envelope-To**, **From**, **To**, **Cc**, **Bcc**, **Subject**, **Sender**, **Reply-To**, **Errors-To**, **Message-ID**, **Date**, **Header**, **Body**, **Attach File Name**, **Size (Kbytes)**, **mailcommand-From**, and **mailcommand-To**. Each item also has its own **Condition** and **Pattern** settings.

- **Condition**
  - When **Item** is selected except **Size** item, the available conditions are: **Contains**, **Does Not Contain**, **Is Equal To**, **Is Not Equal To**, **Starts With**, **Ends With**, **Exists** and **Does Not Exists**.
  - When **Item** is selected as **Size**, the available conditions are: **More Than**, **Is Equal To**, **Is Not Equal To** and **Less Than**.

- **Pattern**
  - Enter the relevant value in **Item** and **Condition** field. For example: **From** Item and use **Contains** Condition, and enter josh as a characteristics. Afterward when the sender and receiver's mail account has josh inside and then it will be considered as spam mail or ham mail.

6.2.4 Whitelist

When the mail matches ES-6000 Whitelist, it will forward to recipient directly without passing the examination of Anti-Spam. (Figure 6-21)

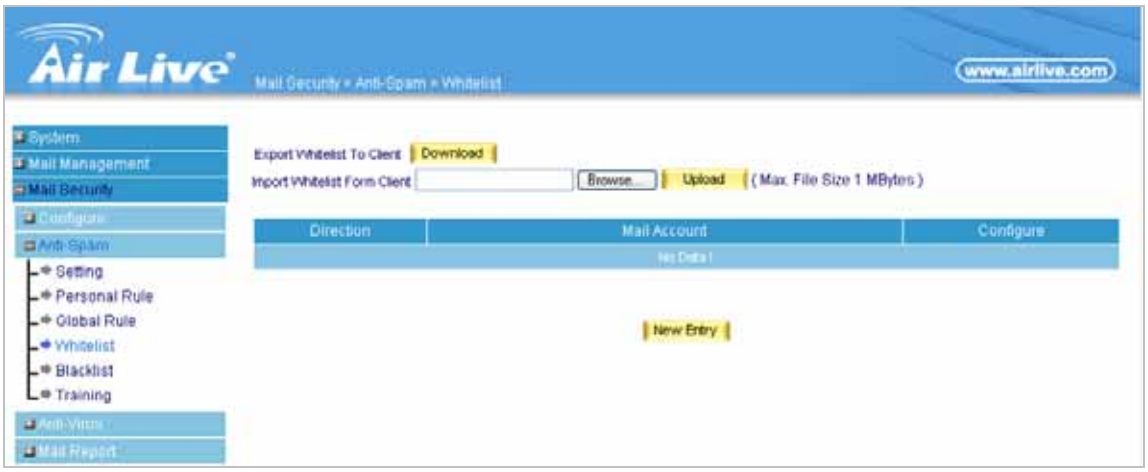


Figure 6-21 Whitelist

Definition:

- **Mail Account**
  - Used as a reference for inspecting ham e-mails.

- **Direction**
  - **From:** Inspects e-mails sent from a specific sender address
  - **To:** Inspects e-mails sent to a specific recipient address

6.2.5 Blacklist

When the mail matches ES-6000 Blacklist, it will be defined as spam mail and be arranged based on Spam Setting. (Figure 6-22)

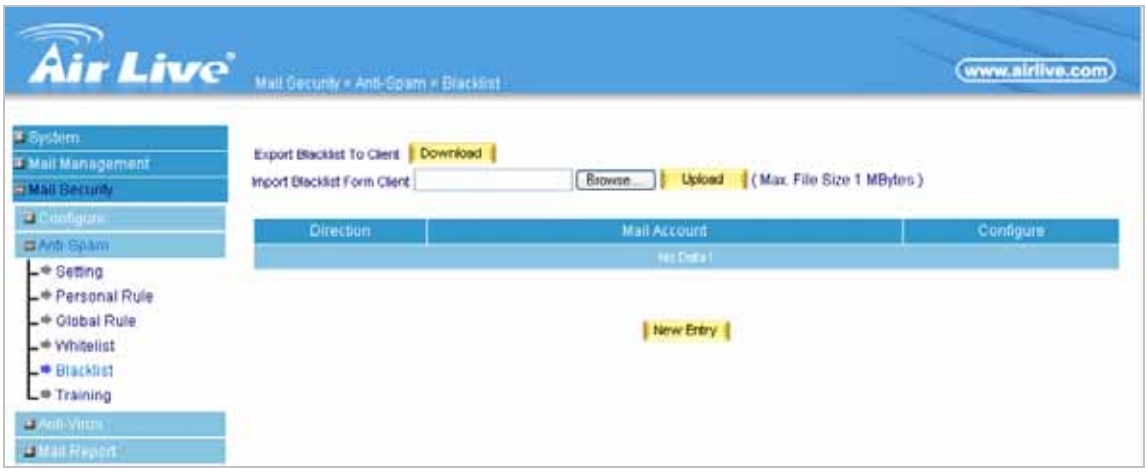


Figure 6-22 Blacklist

Definition:

- **Mail Account**
  - Used as a reference for inspecting ham e-mails.

- **Direction**
  - **From:** Inspects e-mails sent from a specific sender address
  - **To:** Inspects e-mails sent to a specific recipient address

6.2.6 Auto-Whitelist

Definition:

- **Auto-Whitelist Factor**
  - Obtained by dividing the **Total Score** (the amount of spam emails sent) by **Count** (the amount of emails sent). It directly affects the **Mean Score** and also is the major factor that decides whether an email is to be identified as spam.
- **Source IP**
  - The subnet belonging to the sender(s) of email
- **Count**
  - The total amount of emails sent from a specific subnet.
- **Total Score**
  - The total amount of spam emails sent from a specific subnet
- **Mean Score**
  - The value derived from the division of **Total Score** by **Count**
- **Details**
  - Displays all the email senders and their related statistics.

1. The Auto-Whitelist mechanism can evaluate whether an email is spam by assigning each email a score based upon the current email's spam score and the mean score history of the sender's subnet. Higher scores represent emails that are more likely to be spam.

2. Considering a sender may have sent an email from a different IP within the same subnet, thus they are identified using both their address and the most significant two octets of their IP address by which effectively helps avoid IP or email forgery.

3. The mean score of a sender is calculated by the sender's subnet's total score divided by the total number of emails previously sent from the subnet. It is in direct ratio to **Auto-Whitelist Factor**, that is to say, provided the factor is set with a high value then the mean score will be increased proportionately as well.

4. Under such a mechanism, a sender who had never previously sent spam but sends an email with a high spam score could have the score reduced. For example, if a sender sent an email that scored 10, and the factor was set to 0.4, then the mean score (-5 for instance) will push the score down to 4 (operation: ((-5)×0.4)+(10×0.6)) on the email sent.

5. On the contrary, even if an email is rated with a low score, it still has a possibility of being rated as spam if the user's subnet had previously sent emails with high spam ratings. For example, if a sender sent an email that scored 2, and the factor was set to 0.4, then the mean score (20 for instance) will push the score up to 9.2 (operation: (20×0.4)+(2×0.6)) on the email sent.

6.2.7 Training

ES-6000 provides an advanced function to improve spam detection system more precisely. The training can be processed by manually or automatically. (Figure 6-23)

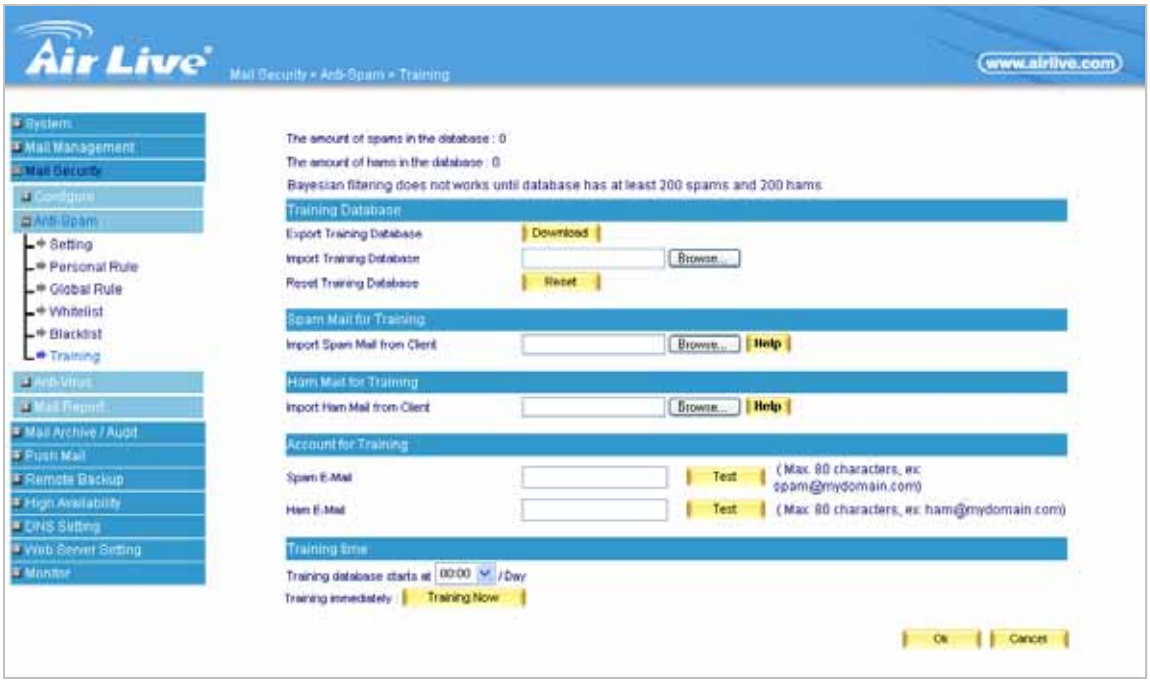


Figure 6-23 Training

Definition:

- **Training Database**
  - Enables the system administrator to import, export or reset the training database.

- **Spam Mail for Training**
  - Spam e-mails can be imported onto the device for training to lift up the inspection accuracy

- **Ham Mail for Training**
  - Ham e-mails can be imported onto the device for training to lift up the inspection accuracy.

- **Account for Training**
  - Spam and ham will be sent to the assigned e-mail accounts respectively and retrieved by ES-6000 periodically for training so as to raise the inspection accuracy

- **Training Time**
  - ES-6000 can be scheduled a daily time for spam or ham training.
  - Forces the training to take place at once.

6.3 Anti-Spam Configuration Example

Here are four application examples of Anti-Spam

1. *Using Whitelist and Blacklist to Filter E-Mails*
2. *Using Global Rule to Filter E-Mails*
3. *Raising Bayesian Filtering Accuracy by Spam or Ham Training (Outlook Express)*
4. *Raising Bayesian Filtering Accuracy by Account Training*

6.3.1 Using Whitelist and Blacklist to Filter E-Mails

Step1. Select **Mail Security → Anti-Spam → Setting**, and then set as below: (Figure 6-24)

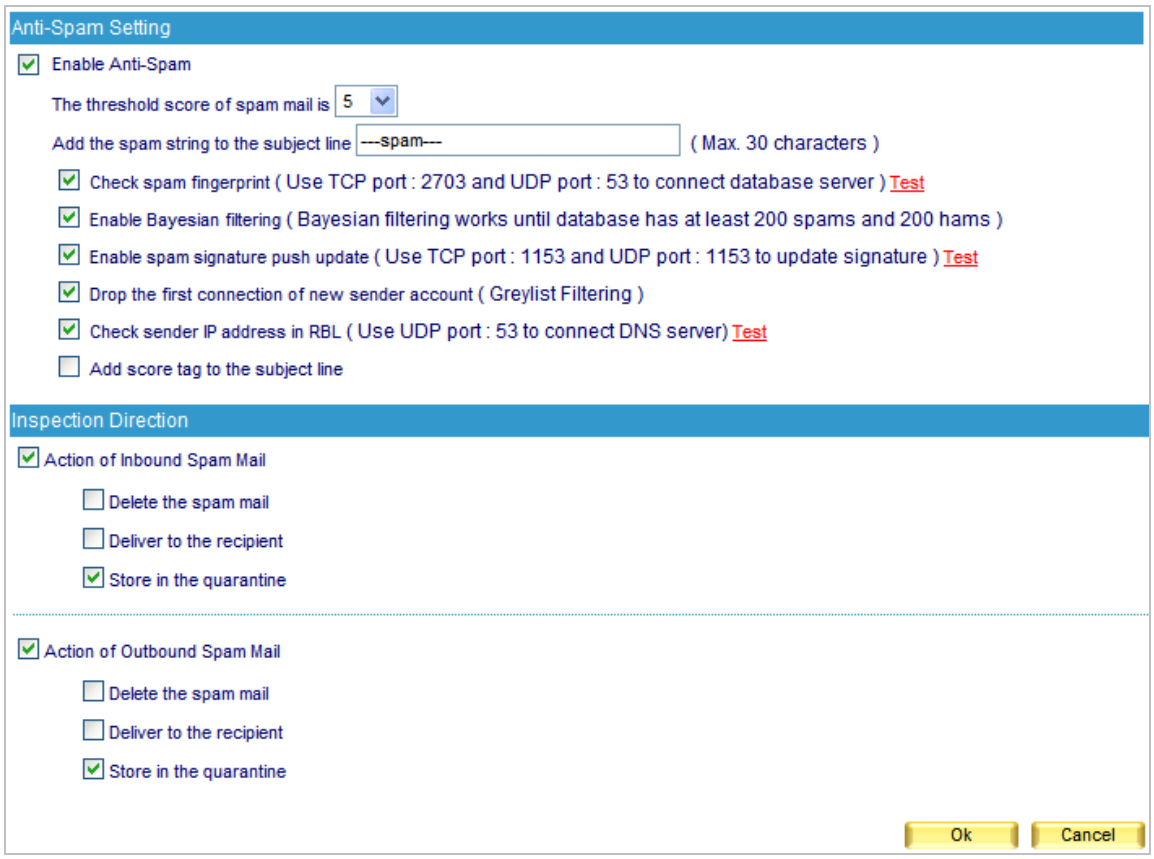


Figure 6-24 Configuring the Inspection and Action of Spam E-Mails

When the action of spam e-mails set as **Delete the spam mail**, the rest two options will not be available for selection. Spam e-mails will be deleted right away when detected, and then a corresponding log will be created under **Mail Security → Mail Report → Log**.

Step2. Select **Mail Security → Anti-Spam → Whitelist**, and then set as below:

- Click **New Entry**.
- Type an e-mail address in the **Mail Account** field. For example, jacky@hotmail.com
- Select “From” for **Direction**
- Click **OK** (Figure 6-25)
- Click **New Entry** again
- Type an e-mail address in the **Mail Account** field. For example, jacky@hotmail.com
- Select “To” for **Direction**
- Click **OK** (Figure 6-26)
- Click **New Entry** again
- Type an e-mail address in the **Mail Account** field. For example, josh@airlive.com
- Select “From” for **Direction**
- Click **OK** (Figure 6-27)
- Click **New Entry** again
- Type an e-mail address in the **Mail Account** field. For example, josh@airlive.com
- Select “To” for **Direction**
- Click **OK** (Figure 6-28)
- Setup is completed. (Figure 6-29)

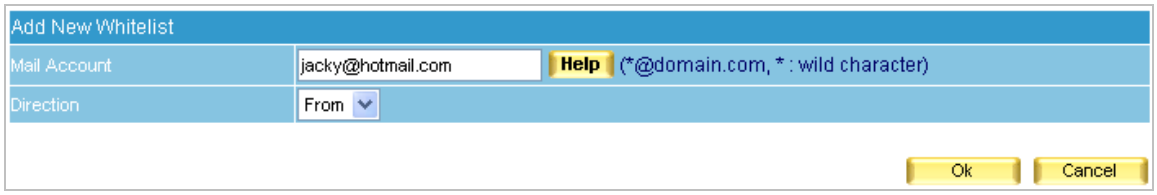


Figure 6-25 First Entry of Whitelist

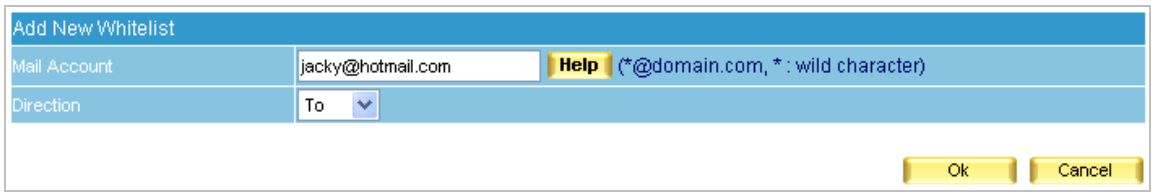


Figure 6-26 Second Entry of Whitelist

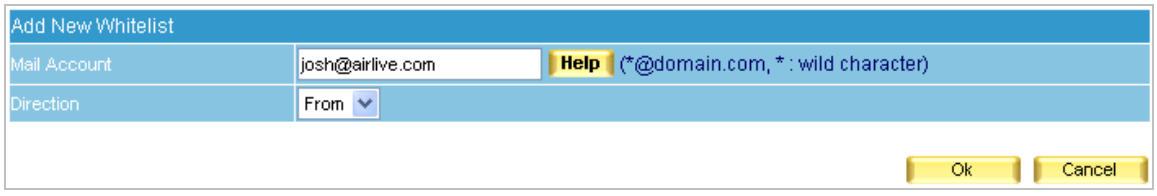


Figure 6-27 Third Entry of Whitelist

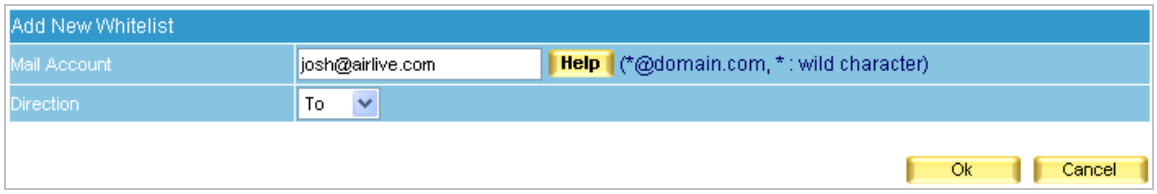


Figure 6-28 Fourth Entry of Whitelist

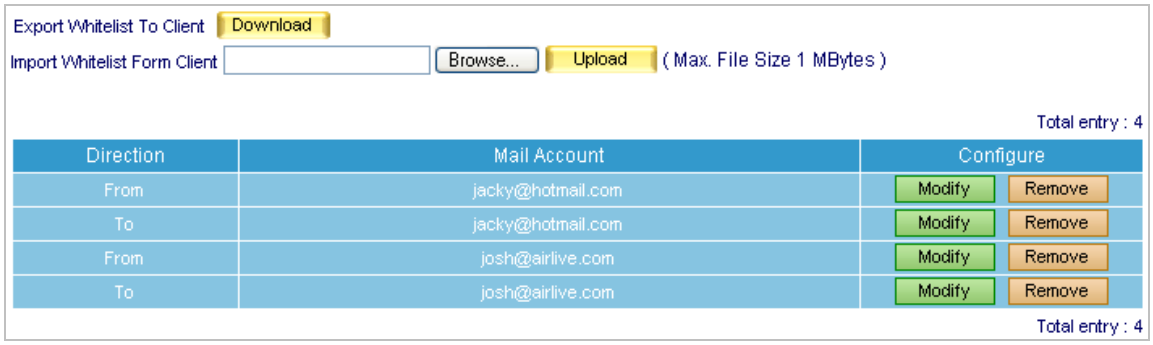


Figure 6-29 Setup Completed

Whitelist can be exported as a file for archive and editing purpose, which can be used for restoring the list later on.

Ham training takes place on the scheduled time which is configured at **Training time**.

Step3. Select **Mail Security → Anti-Spam → Blacklist**, and then set as below:

- Click **New Entry**.
- Type "***hotmail***" as a keyword in the **Mail Account** field
- Select "From" for **Direction**
- Click **OK** (Figure 6-30)
- Click **New Entry** again
- Type "***hotmail***" as a keyword in the **Mail Account** field
- Select "To" for **Direction**
- Click **OK** (Figure 6-31)
- Setup is completed. (Figure 6-32)

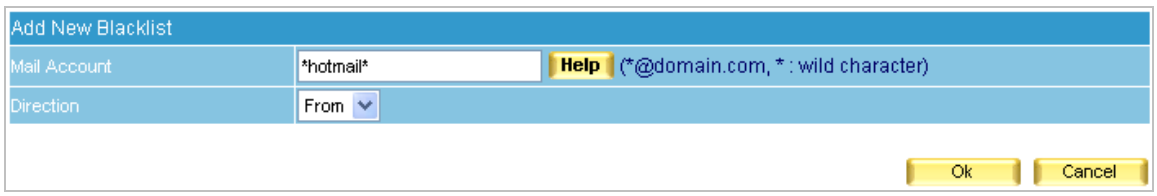


Figure 6-30 First Entry of Blacklist

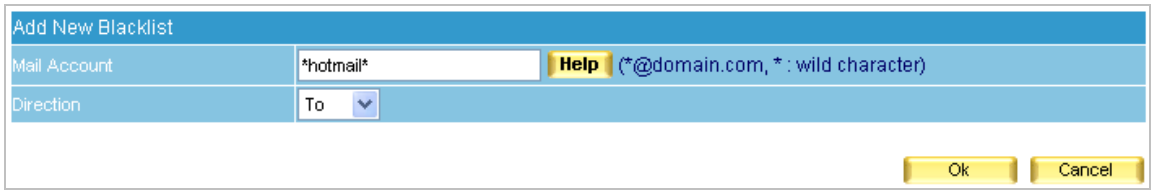


Figure 6-31 Second Entry of Blacklist

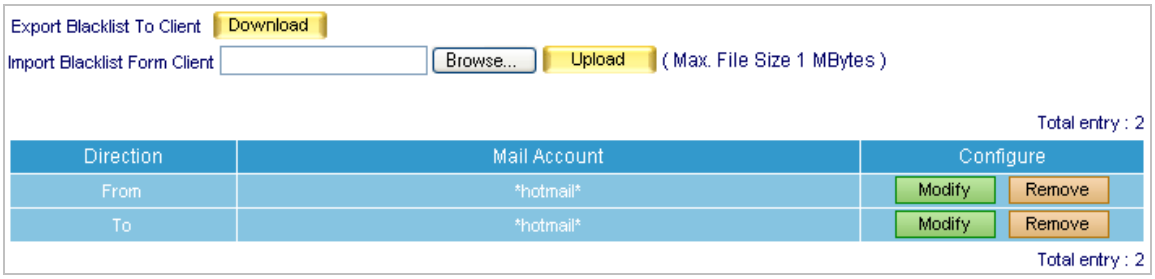


Figure 6-32 Setup Completed

Blacklist can be exported as a file for archive and editing purpose, which can be used for restoring the list later on.

Spam training takes place on the scheduled time which is configured at **Training time**.

The **Mail Account** field of **Whitelist** or **Blacklist** can be a complete e-mail address or a word string containing wildcard characters (＊). For example, "*hotmail*" means e-mail address that contains "hotmail".

Whitelist overrides **Blacklist**, thus, e-mail inspection will firstly act on **Whitelist** and then **Blacklist**.

Step4. Provided that josh@airlive.com and ryan@airlive.com both receive an e-mail from a Hotmail account:

- If the sender's address is jacky@hotmail.com, then both Josh and Ryan will receive it.
- But if the sender's address is portia@hotmail.com, only Josh will receive it. E-mails that sent to Ryan will be rated as spam and quarantined.

Step5. When an internal account from **airlive.com** sends an e-mail to both jacky@hotmail.com and portia@hotmail.com:

- If the sender's address is josh@airlive.com, then both of them will be receiving the e-mail from Josh.

- But if the sender is someone other than Josh, for instance vera@airlive.com, then only Jacky will receive the e-mail from Vera. E-mails that sent to Portia will be rated as spam and quarantined..

6.3.2 Using Global Rule to Filter E-Mails

Step1. Select **Mail Security → Anti-Spam → Setting**, and then set as below: (Figure 6-33)

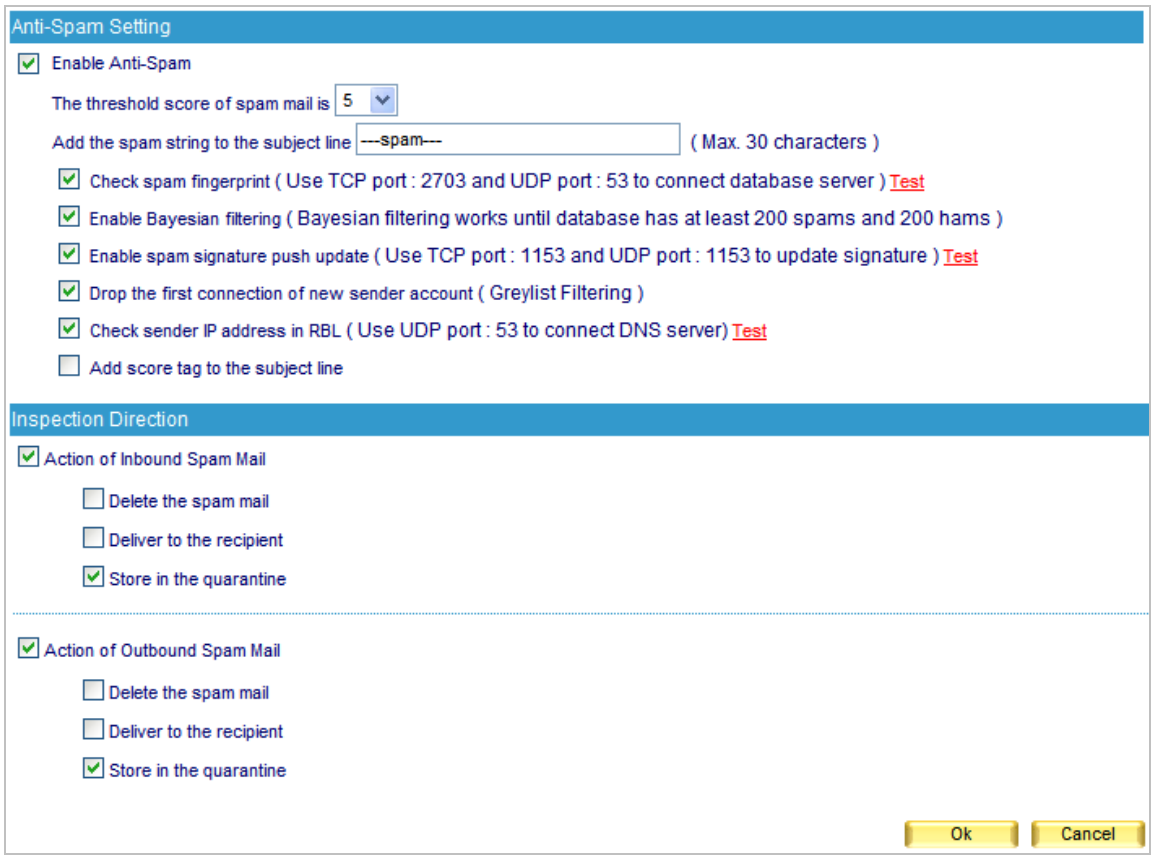


Figure 6-33 Configuring the Inspection and Action of Spam E-Mails

E-mails that meet the criteria of **Global Rule** will be processed by the action setting.

Step2. Select **Mail Security → Anti-Spam → Global Rule**, and then set as below:

- Click **New Entry**.
- Type “HamMail” in the **Rule Name** field.
- Type “Ham Mail” in the **Comments** field.
- Select “Or” for **Combination**.
- Select “Ham(Non-Spam)” for **Classification**.
- Select “From” for **Item**, “Contains” for **Condition** and then type “jacky” as **Pattern**.

- Click **Next**.
- In the second row, select “To” for **Item**, “Contains” for **Condition** and then type “jacky” as **Pattern**.
- Click **Next**.
- In the third row, select “From” for **Item**, “Contains” for **Condition** and then type “Josh” as **Pattern**.
- Click **Next**.
- In the fourth row, select “To” for **Item**, “Contains” for **Condition**, and then type “Josh” as **Pattern**. (Figure 6-34)
- Click **OK**. (Figure 6-35)

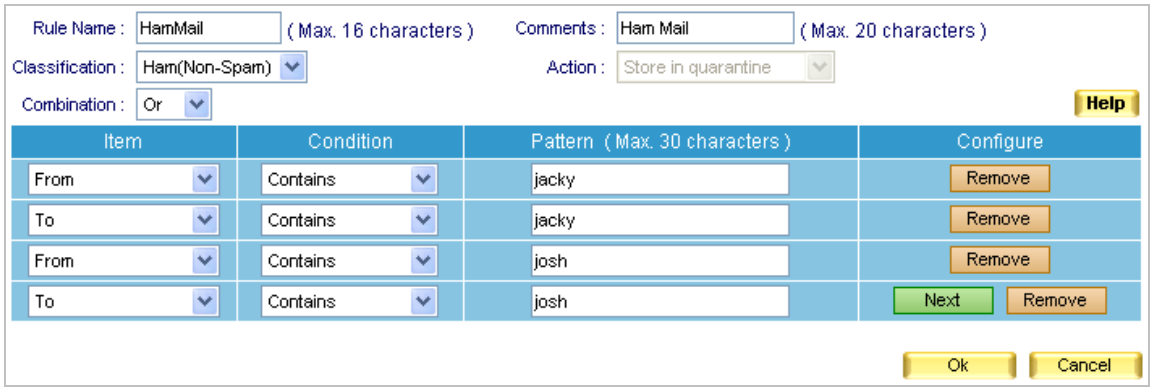


Figure 6-34 First Global Rule

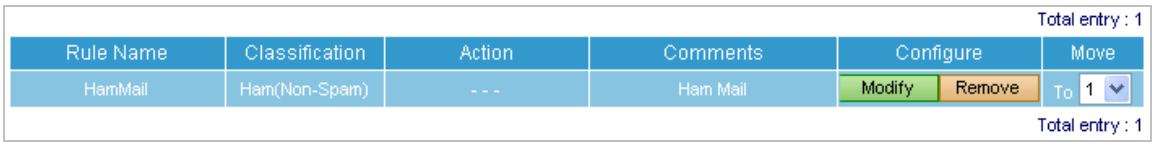


Figure 6-35 First Global Rule Completed

Action will not be available for selection when **Classification** set as **Ham(Non-Spam)**. Ham e-mails will be sent to the recipients directly.

Step3. Select **Mail Security → Anti-Spam → Global Rule**, and then set as below:

- Click **New Entry**.
- Type “SpamMail” in the **Rule Name** field.
- Type “Spam Mail” in the **Comments** field.
- Select “Or” for **Combination**.
- Select “Store in quarantine” for **Action.**
- Select “Spam” for **Classification**.
- In the first row, select “From” for **Item**, “Contains” for **Condition**, and then type “hotmail” as **Pattern**.

- Click **Next**.
- In the second row, select “To” for **Item**, “Contains” for **Condition**, and then type “hotmail” as **Pattern**. (Figure 6-36)
- Click **OK**. (Figure 6-37)

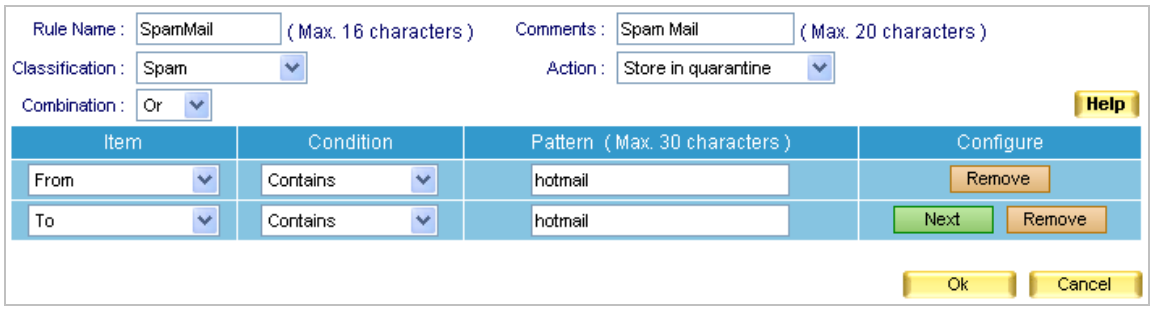


Figure 6-36 Second Global Rule Completed

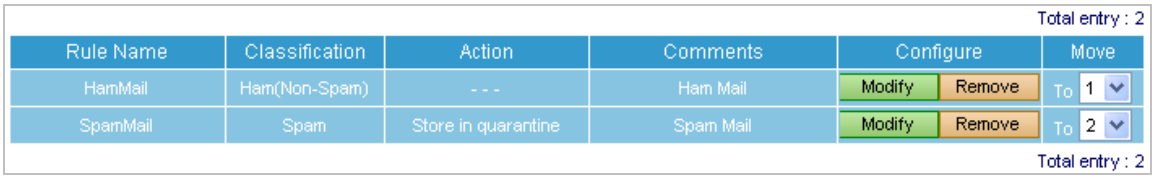


Figure 6-37 Second Global Rule Completed

The **Action** of a spam e-mail can be deleted, or forwarded, or quarantined, or delivered, or using the same setting of spam when **Classification** set as “**Spam**”.

The filtering priority from high to low is **Greylist → Whitelist in User Preference → Blacklist in User Preference → Global Rule → Whitelist → Blacklist → Default Filtering Rules → Spam Fingerprint Database → Bayesian Filtering → Spam Signature → Checking Sender IP Address in RBL**.

Note: For filtering using Global Rule, it acts on the order of settings within.

E-mail header can be used as a reference when configuring **Condition** and **Item** of Global Rule. Figure 6-38 shows the header of an e-mail. To view header, click to select any e-mail in your Outlook Express, then right-click it and move to **Properties** on the pop-up menu. After that, click the **Details** tab for header information. (Figure 6-38)

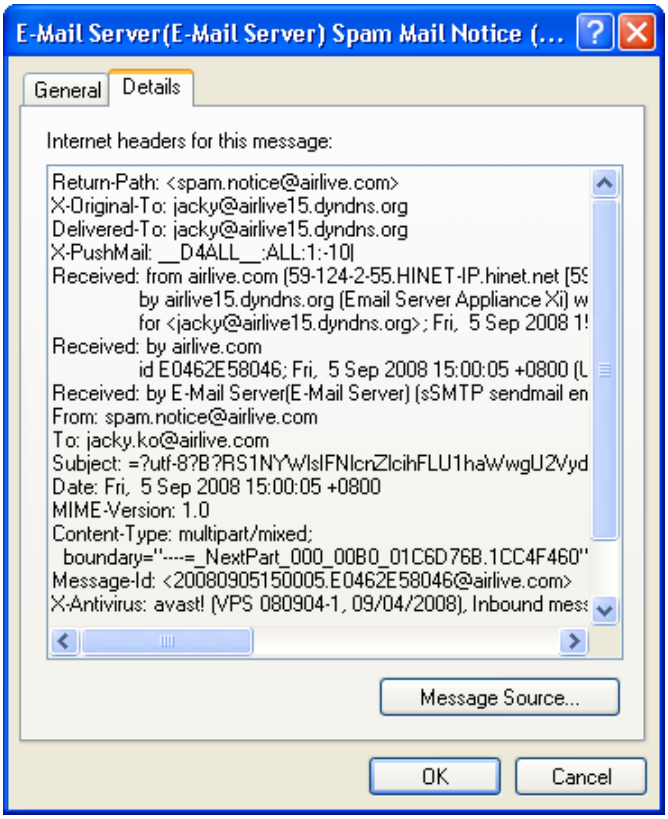


Figure 6-38 Detailed Information of an E-Mail

Step4. Provided that josh@airlive.com and ryan@airlive.com both receive an e-mail from a hotmail account :

- If the sender's address is jacky@hotmail.com, then both Josh and Ryan will receive it.
- But if the sender's address is portia@hotmail.com, only Josh will receive it. E-mails that sent to Ryan will be rated as spam and quarantined.

Step5. When an internal account from **airlive.com** sends an e-mail to both jacky@hotmail.com and prtia@hotmail.com:

- If the sender's address is josh@airlive.com, then both of them will be receiving mail from Josh.
- But if the sender's address is someone else than Josh, for instance vera@airlive.com, then only Jacky will receive the e-mail from Vera. E-mails that sent to Portia will be rated as spam and quarantined.

6.3.3 Raising Bayesian Filtering Accuracy by Spam or Ham Training (Outlook Express)

Training to Filter Spam E-Mails

Step1. Create a new folder named “Spam Mail” in Outlook Express.

- Right-click **Local Folders** and move to **New folder**, then click it. (Figure 6-39)
- In the **Create Folder** window, type “Spam Mail” as **Folder name**, then click **OK**. (Figure 6-40)

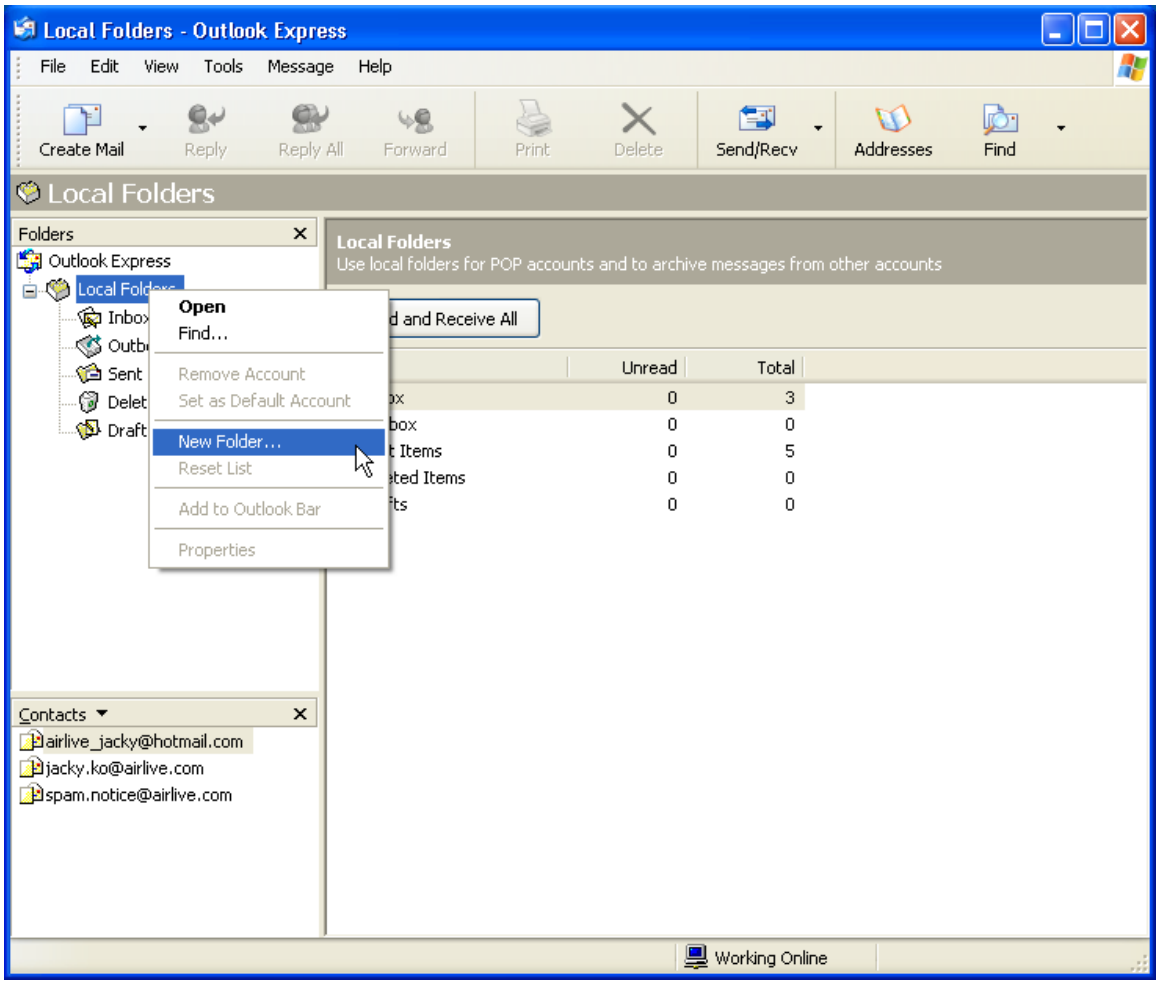


Figure 6-39 Creating a New Folder

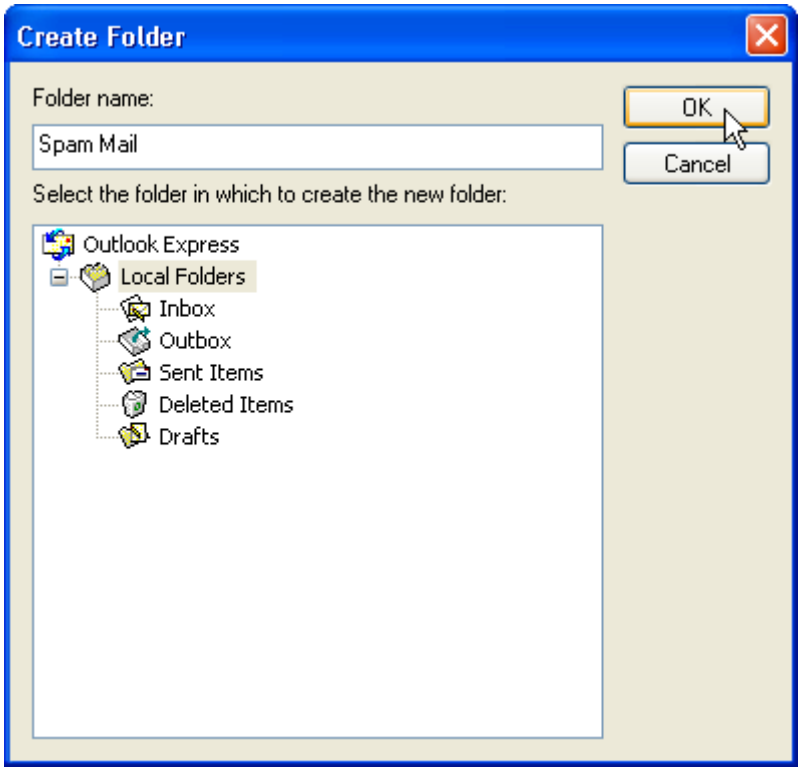


Figure 6-40 Specifying the Folder Name

Step2. Move spam e-mails from inbox to “Spam Mail” folder:

- In inbox, select all spam e-mails and right-click them. Next, move to **Move to folder** on the pop-up menu, and then to click it. (Figure 6-41)
- In the **Move** window, select “Spam Mail” folder, then click **OK**. (Figure 6-42)

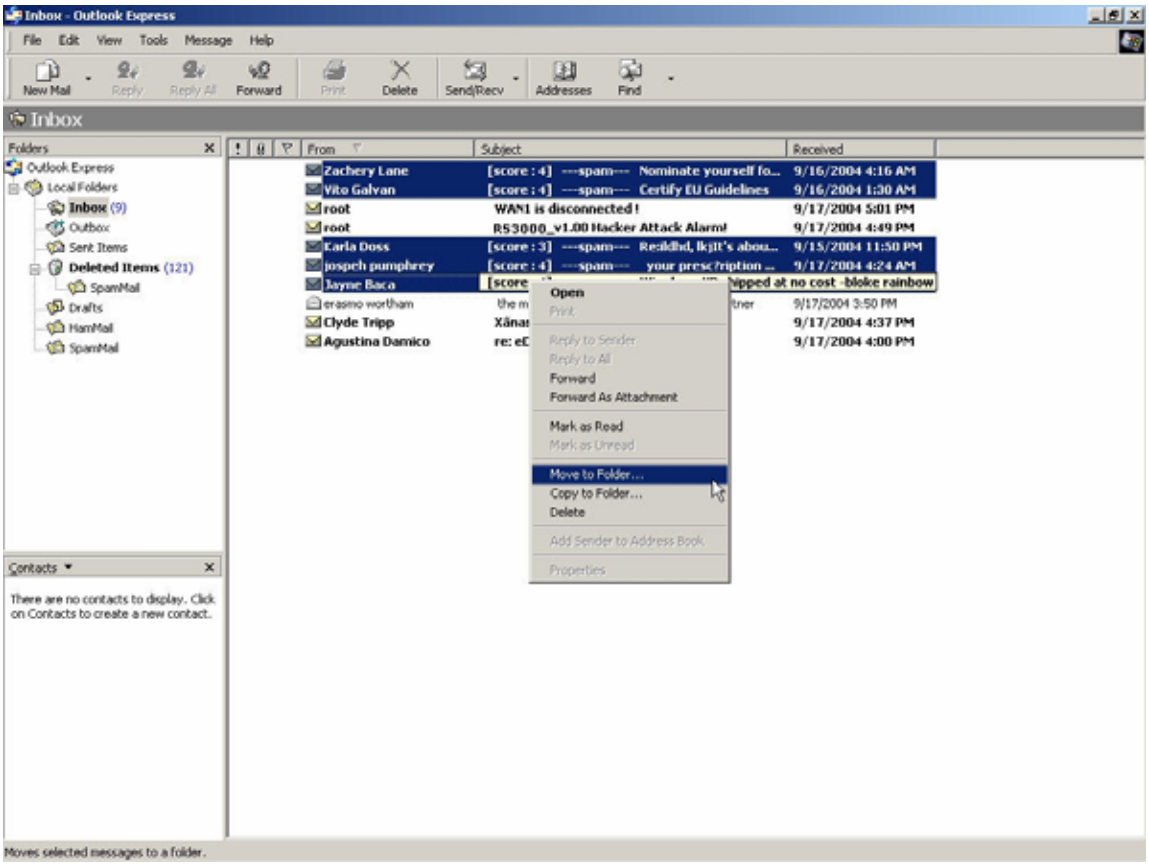


Figure 6-41 Selecting All Spam E-Mails

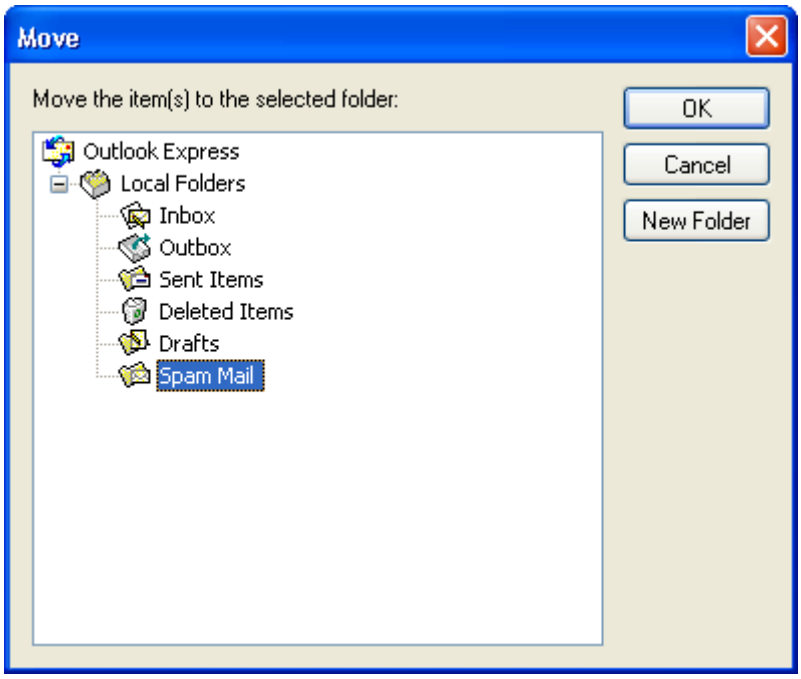


Figure 6-42 Moving Spam E-Mails to "Spam Mail" Folder

Step3. Compress "Spam Mail" folder in order to upload to ES-6000 for training:

- Click "Spam Mail" folder.
- On the **Menu Bar**, go to **File → Folder → Compact** (Figure 6-43)

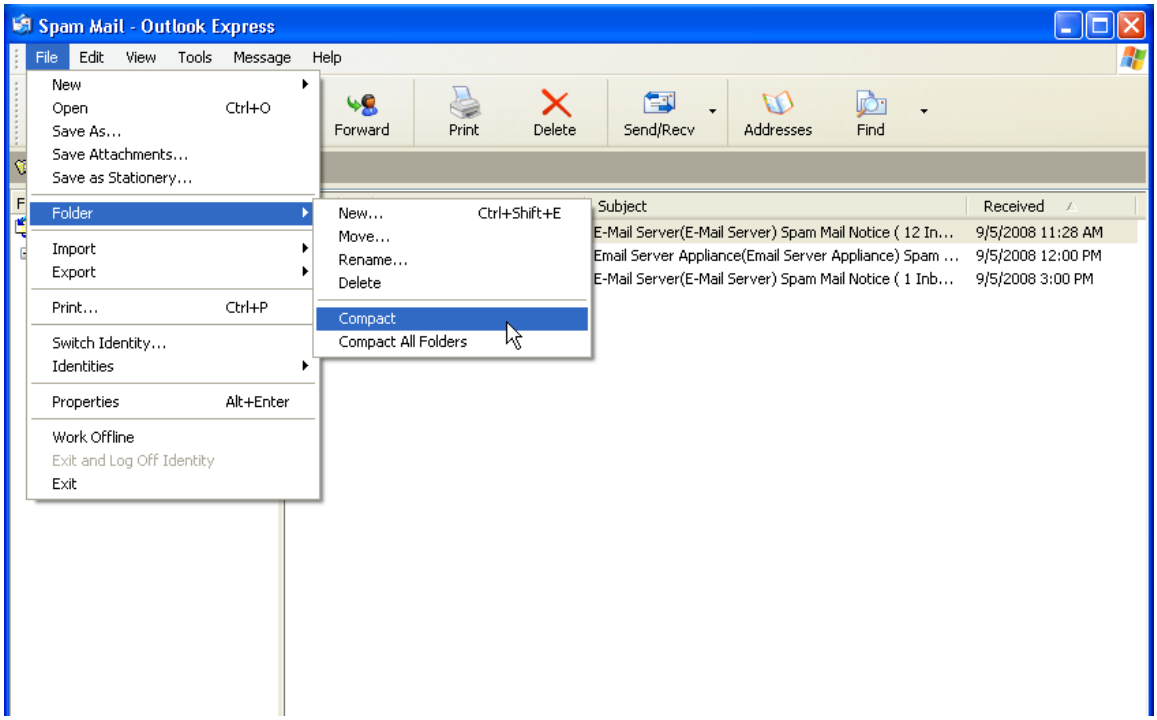


Figure 6-43 Compressing "Spam Mail" Folder

Step4. Copy the storage path of “Spam Mail” folder:

- Right-click the “Spam Mail” folder and move to **Properties** on the pop-up menu, then click it. (Figure 6-44)
- In the **Spam Mail Properties** window, copy the storage path. (Figure 6-45)

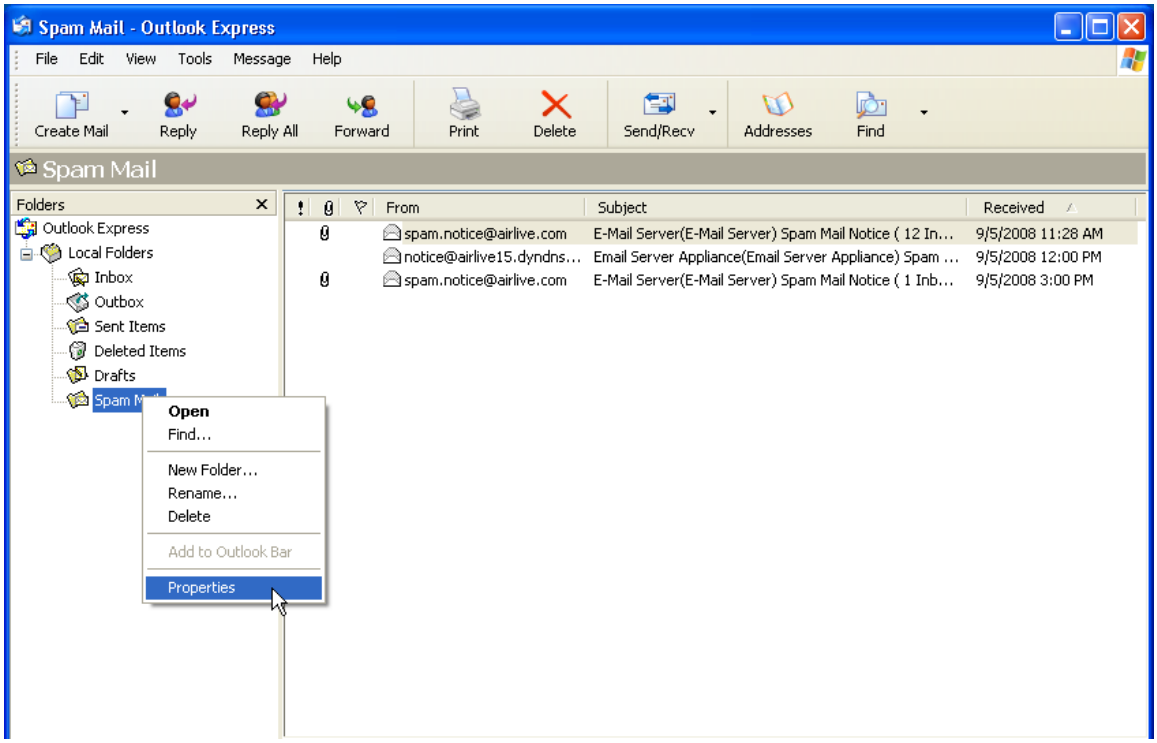


Figure 6-44 Right-Clicking “Spam Mail” Folder and Moving to Properties

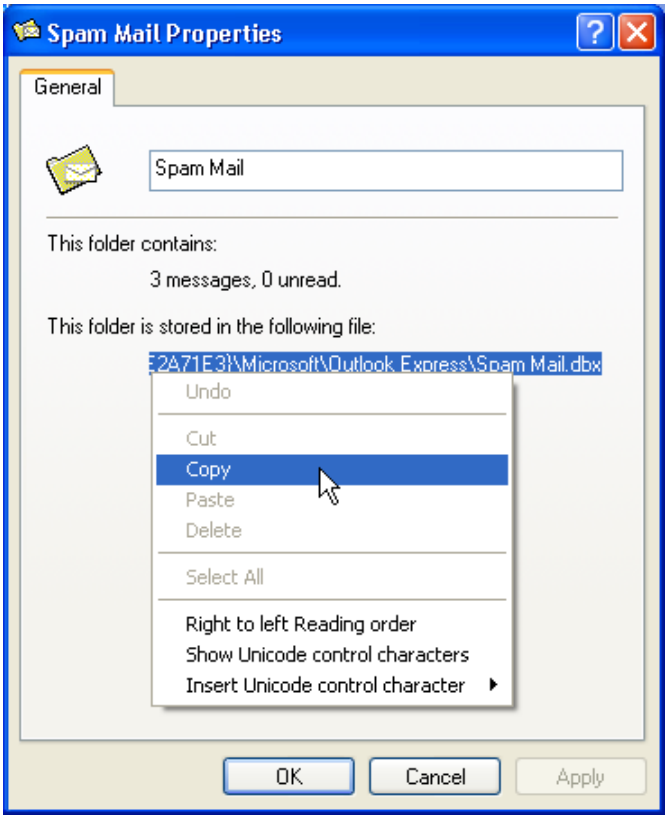


Figure 6-45 Copying the Storage Path

Step5. Select **Mail Security → Anti-Spam → Training**, and then set as below:

- Paste the storage path of “Spam Mail” folder in the **Import Spam Mail from Client** field.
- Click **OK** to start importing. ES-6000 will start training on scheduled time. (Figure 6-46)

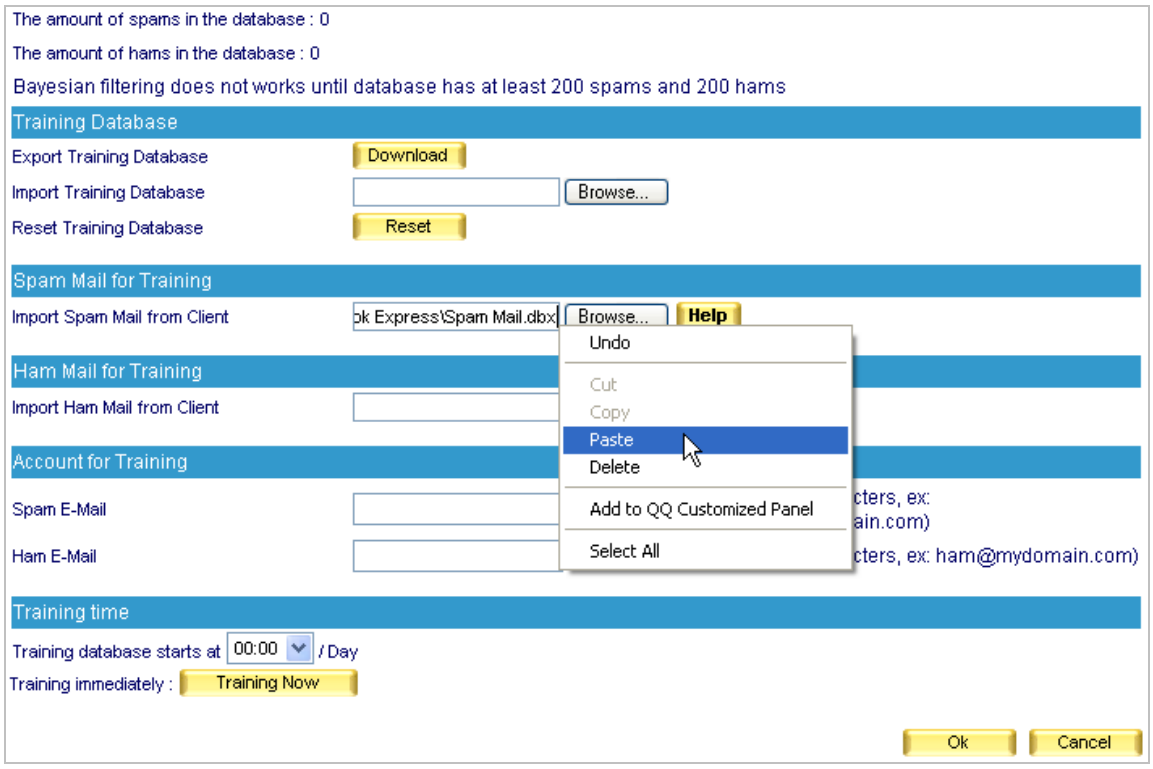


Figure 6-46 Pasting the Storage Path of Compressed Spam E-Mails

The file for training can be any database file. However, it has to be in ASCII format.

If the file for training has an extension file name of “.pst” (generated by Microsoft Office Outlook), then Outlook must be closed before starting import.

Step6. Since current spam e-mails have been compressed and uploaded to ES-6000, e-mails in this folder are of no use any longer. Therefore, delete all spam e-mails so that no old spam e-mails will be imported onto ES-6000 next time.

- Select all e-mails in “Spam Mail” folder, then right-click them and move to **Delete** on the pop-up menu and click it.

Training to Filter Ham E-Mails

Step1. Create a new folder named “Ham Mail” in Outlook Express.

- Right-click **Local Folders** and move to **New folder**, then click it. (Figure 6-47)
- In the **Creat Folder** window, type “Ham Mail” as **Folder name**, then click **OK**. (Figure 6-48)

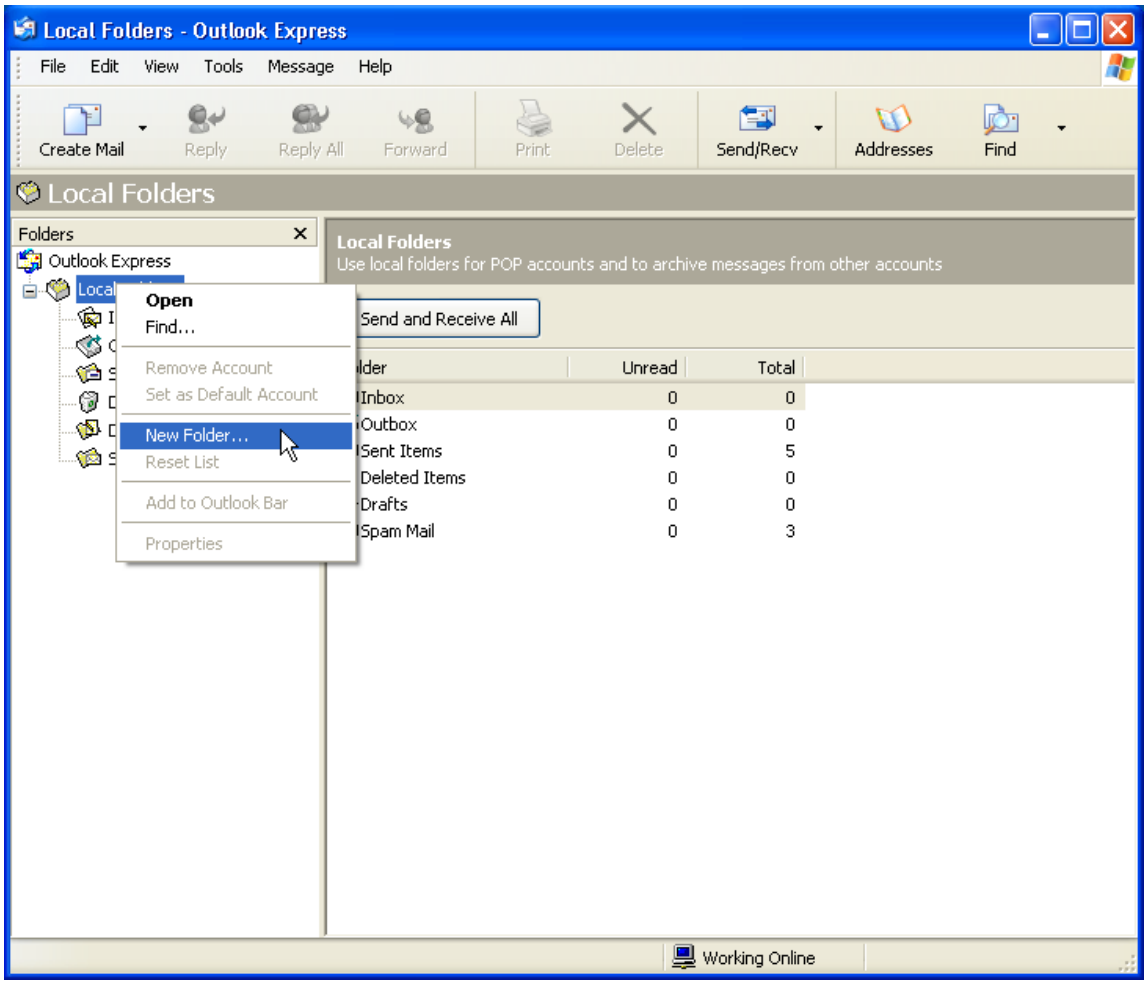


Figure 6-47 Creating a New Folder

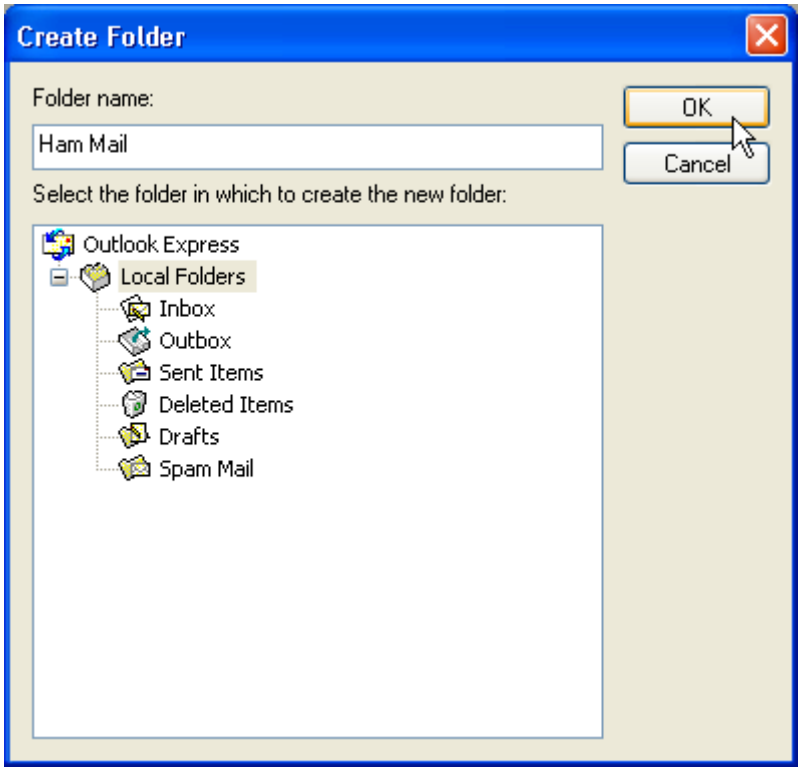


Figure 6-48 Specifying the Folder Name

Step2. Move ham e-mails from inbox to “Ham Mail” folder:

- In inbox, select all ham e-mails and right-click them. Next, move to **Move to folder** on the pop-up menu, and then to click it. (Figure 6-49)
- In the **Move** window, select “Ham Mail” folder, then click **OK**. (Figure 6-50)

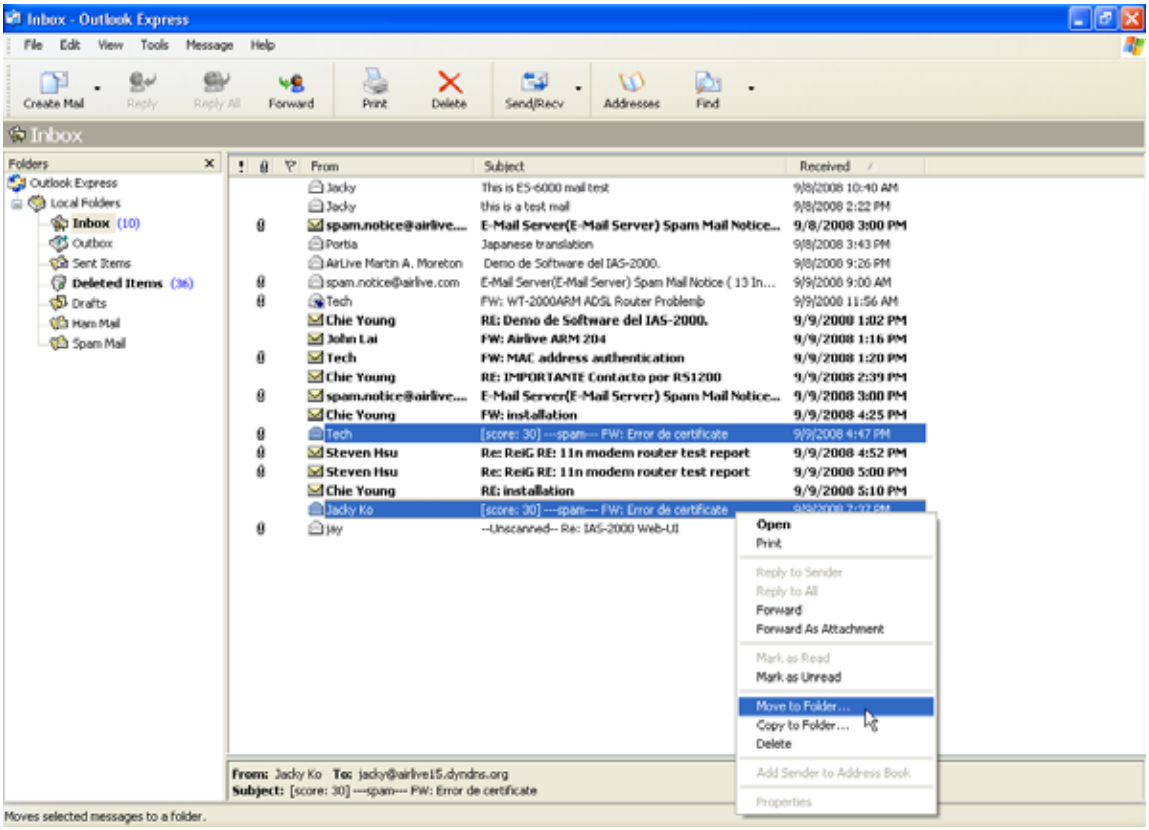


Figure 6-49 Selecting All Ham E-Mails

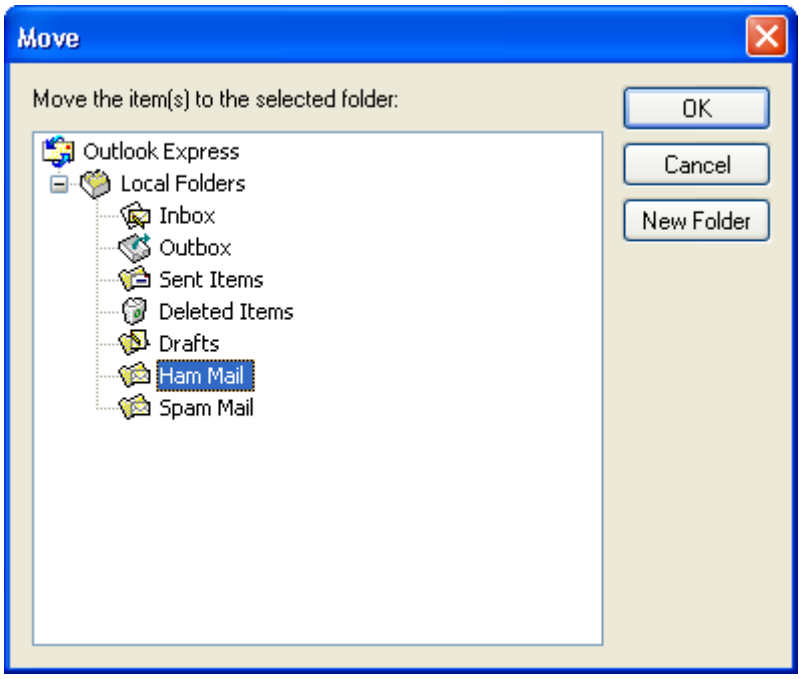


Figure 6-50 Moving Ham E-Mails to "Ham Mail" Folder

Step3. Compress "Ham Mail" folder in order to upload to ES-6000 for training:

- Click "Ham Mail" folder.
- On the **Menu Bar**, go to **File → Folder → Compact** (Figure 6-51)

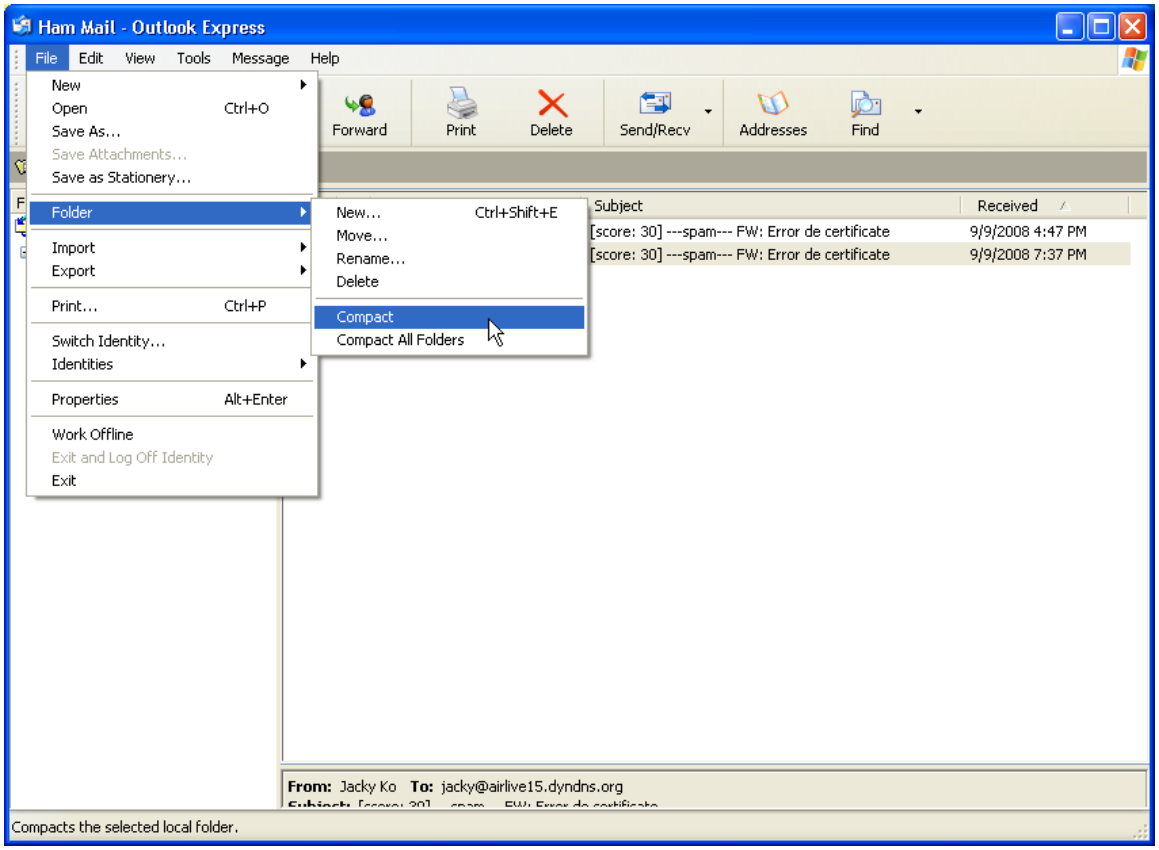


Figure 6-51 Compressing "Ham Mail" Folder

Step4. Copy the storage path of “Ham Mail” folder:

- Right-click the “Ham Mail” folder and move to **Properties** on the pop-up menu, then click it. (Figure 6-52)
- In the **Ham Mail Properties** window, copy the storage path. (Figure 6-53)

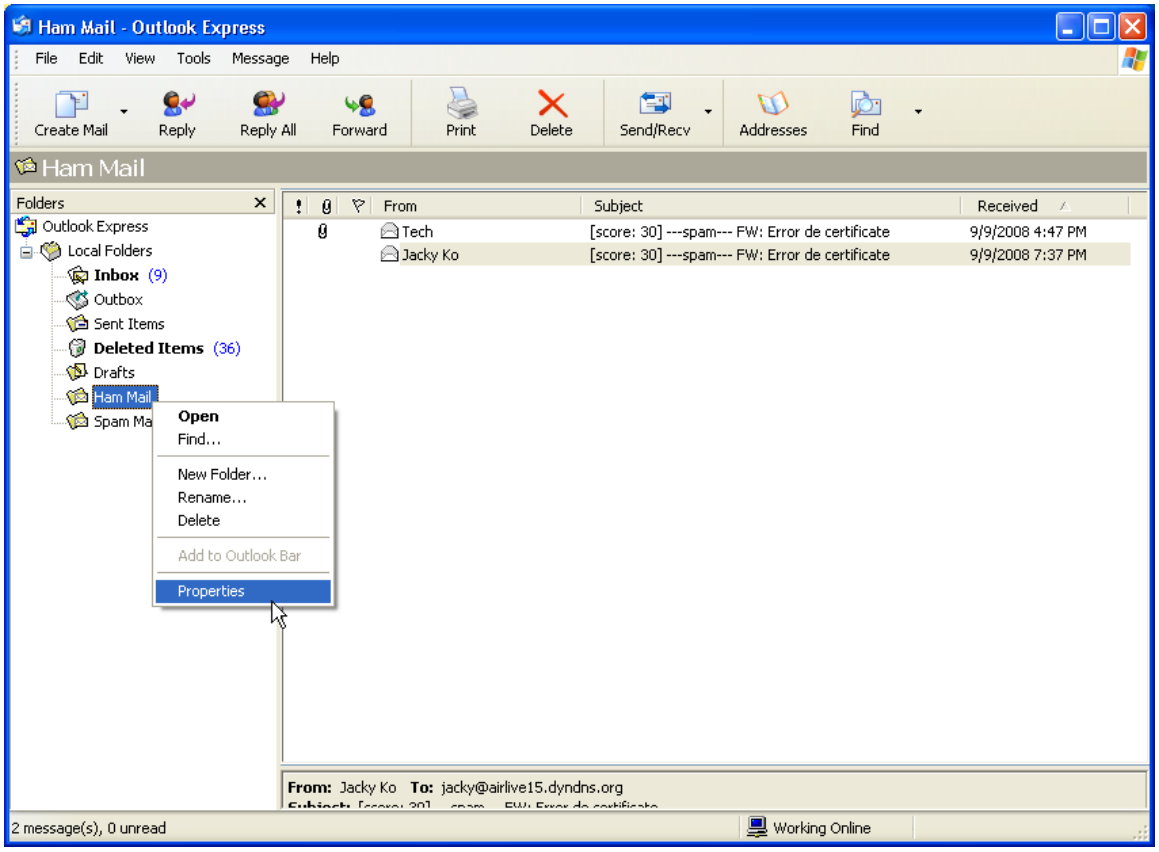


Figure 6-52 Right-Clicking “Ham Mail” Folder and Moving to Properties

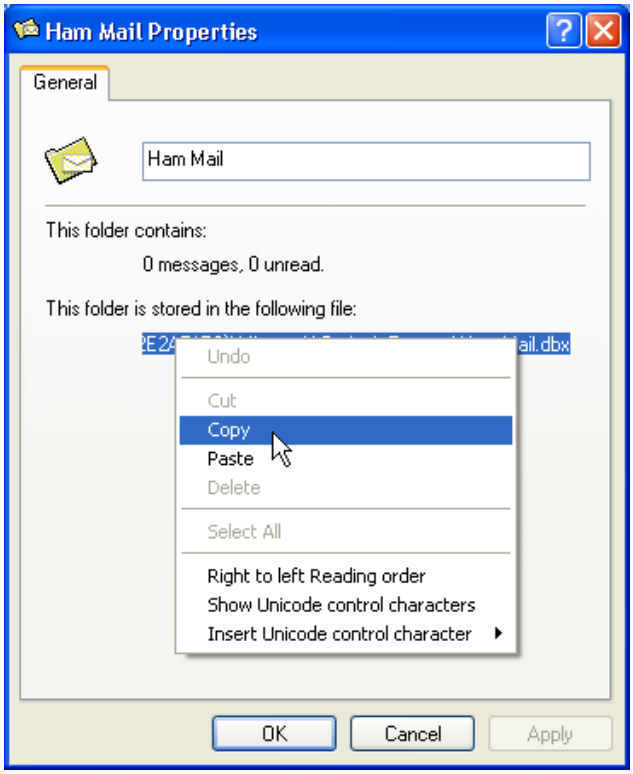


Figure 6-53 Copying the Storage Path

Step5. Select **Mail Security → Anti-Spam → Training**, and then set as below:

- Paste the storage path of “Ham Mail” folder in the **Import Ham Mail from Client** field.
- Click **OK** to start importing. ES-6000 will start training on scheduled time. (Figure 6-54)

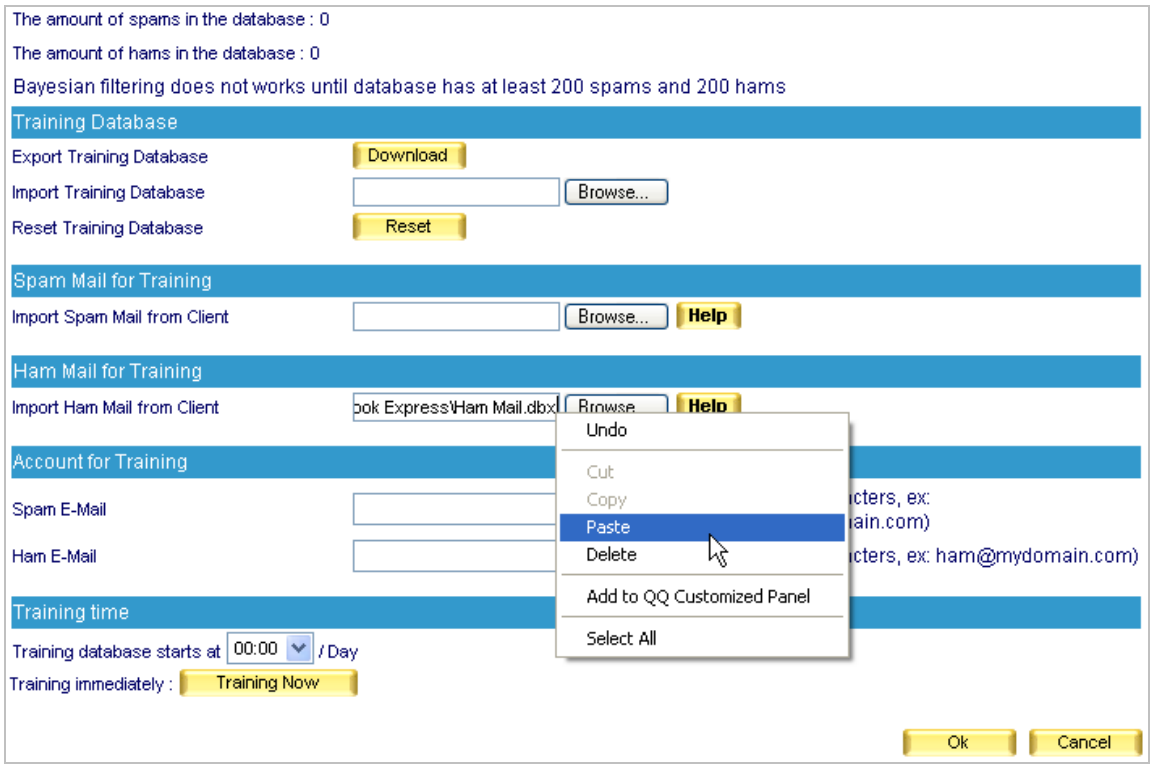


Figure 6-54 Pasting the Storage Path of Compressed Ham E-Mails

Step6. Since current Ham e-mails have been compressed and uploaded to ES-6000, e-mails in this folder are of no use any longer. Therefore, delete all Ham e-mails so that no old Ham e-mails will be imported onto ES-6000 next time.

- Select all e-mails in “Ham Mail” folder, then right-click them and move to **Delete** on the pop-up menu and click it.
- Make sure this folder has been emptied.

6.3.4 Raising Bayesian Filtering Accuracy by Account Training

Step1. Create a spam account for training. (e.g., spam@airlive.com)

Step2. Create a ham account for training. (e.g., ham@airlive.com)

Step3. Select **Mail Security** → **Anti-Spam** → **Training**, and then configure **Account for Training** as below:

- Type “spam” in the **SPAM Account** field.
- Type “ham” in the **HAM Account** field.
- Click **OK**. (Figure 6-55)

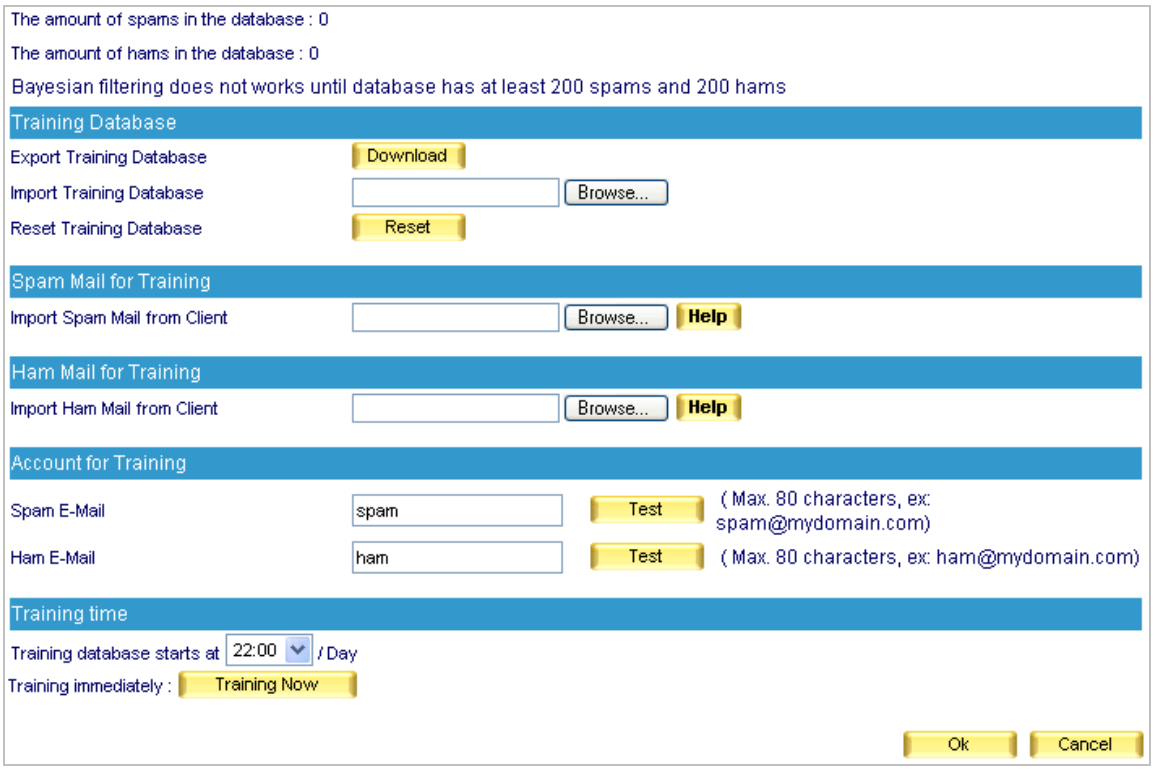


Figure 6-55 The Accounts Used for Training

Step4. Training to filter Spam e-mails.

- Run Outlook Express and forward all spam e-mails in inbox as attachment.
- Select all spam e-mails and right-click them, then move to **Forward as attachment** and click it. (Figure 6-56)
- In the **New Message** window, type **spam@airlive.com** in the **To** field, **Spam** in the **Subject** field and leave **Body** blank, and then click **Send**. (Figure 6-57)

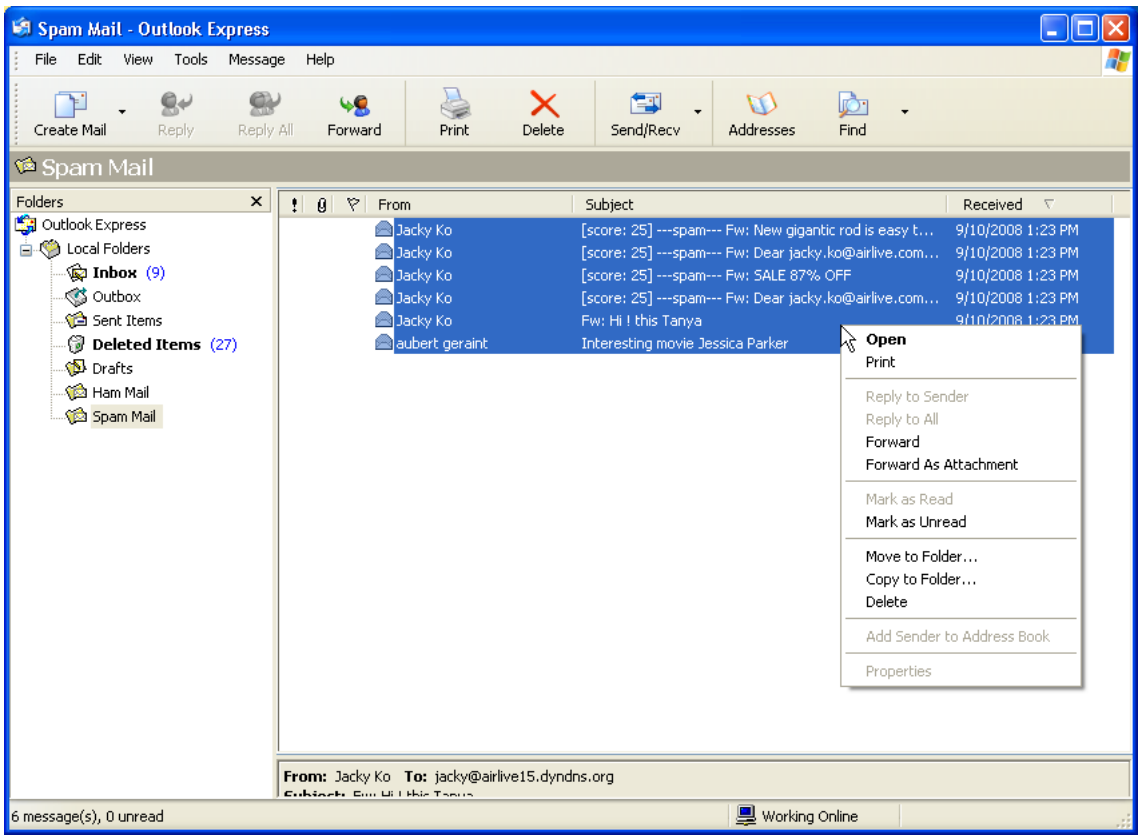


Figure 6-56 Selecting Spam E-Mails

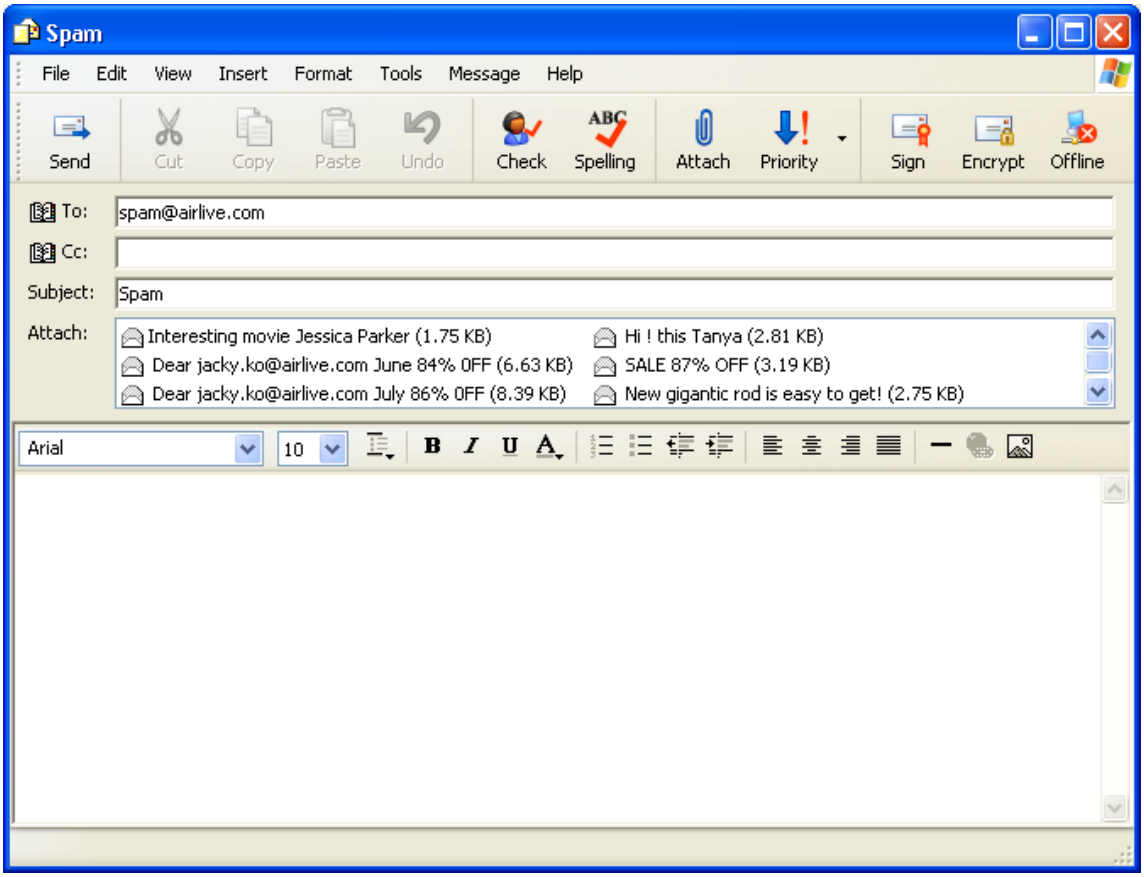


Figure 6-57 Forwarding Spam E-Mails as Attachment

Step5. Training to filter Ham e-mails.

- Forward all ham e-mails in inbox as attachment.
- Select all ham e-mails and right-click them, then move to **Forward as attachment** and click it. (Figure 6-58)
- In the **New Message** window, type **ham@airlive.com** in the **To** field, **Ham** in the **Subject** field and leave **Body** blank, and then click **Send**. (Figure 6-59)

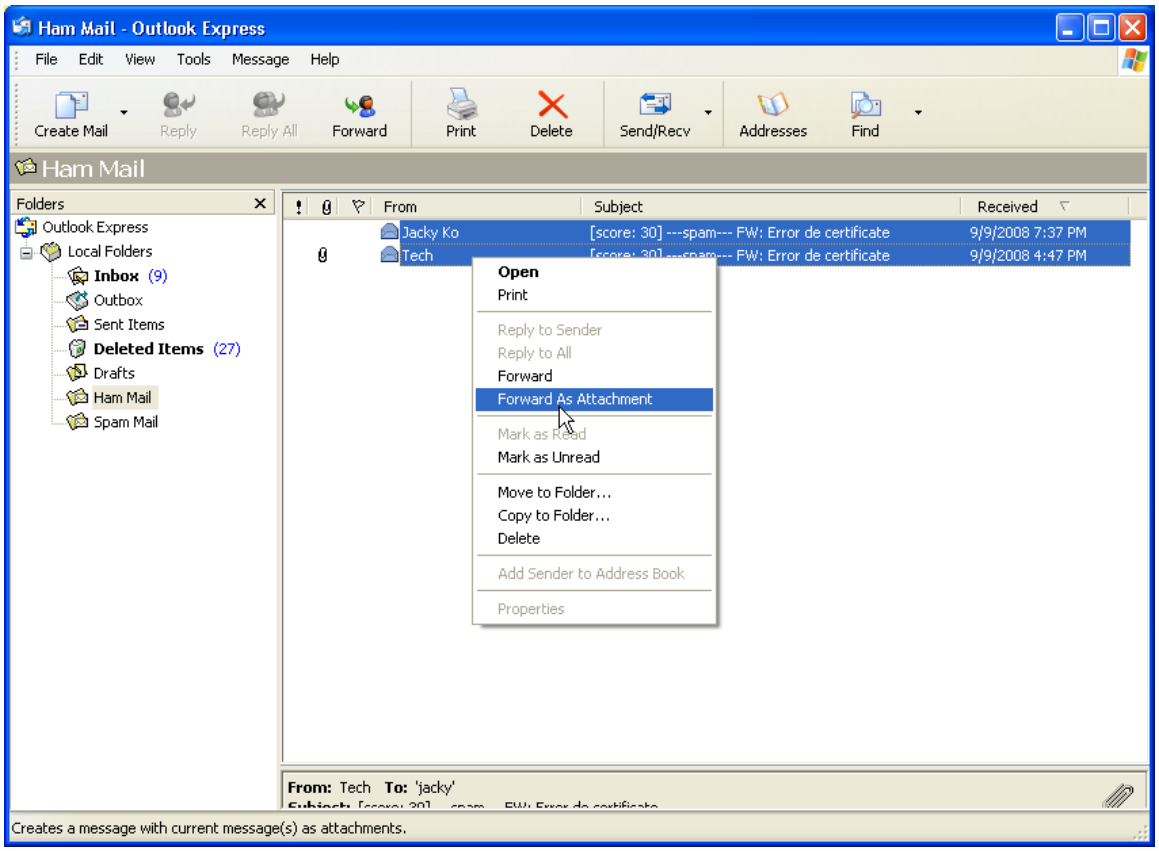


Figure 6-58 Selecting Ham E-Mails

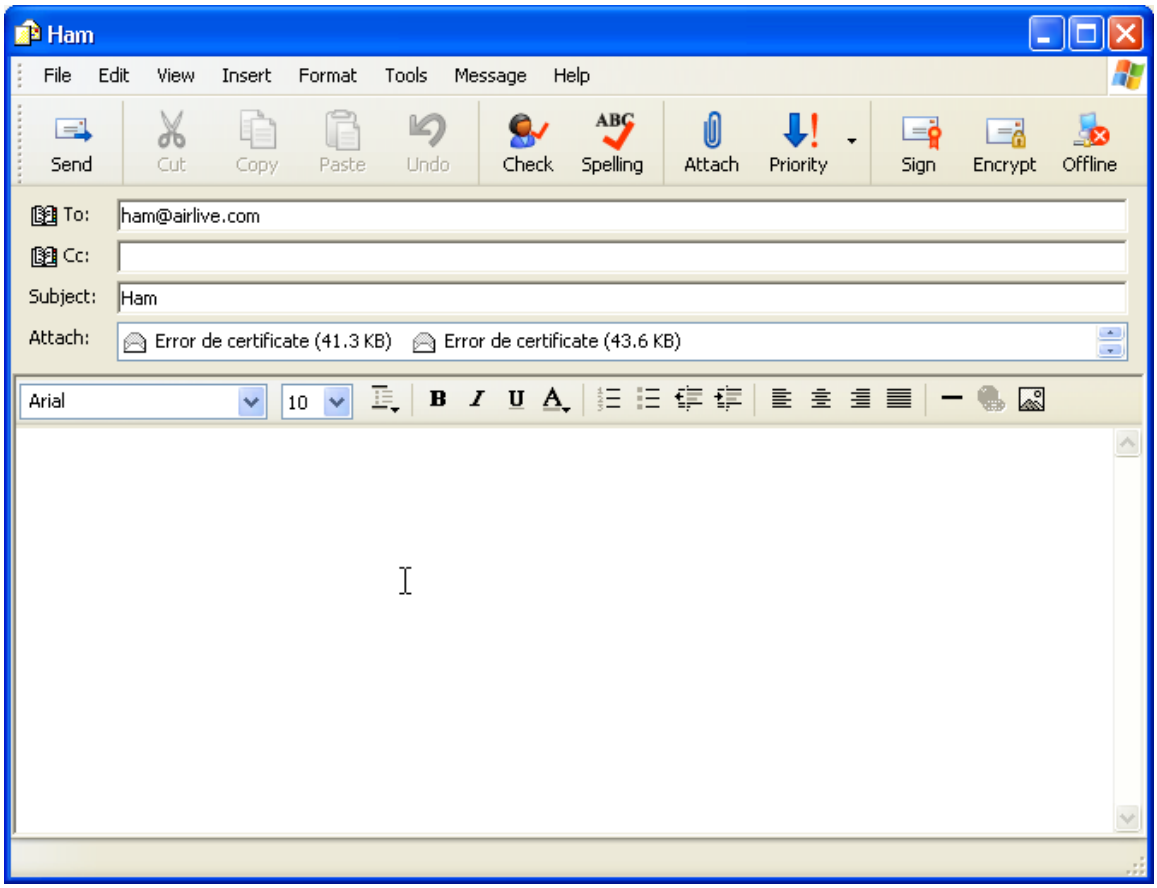


Figure 6-59 Forwarding Ham E-Mails as Attachment

Step6. Multi-functional firewall will retrieve e-mails from spam or ham account periodically and train itself on scheduled time. (Figure 6-60)

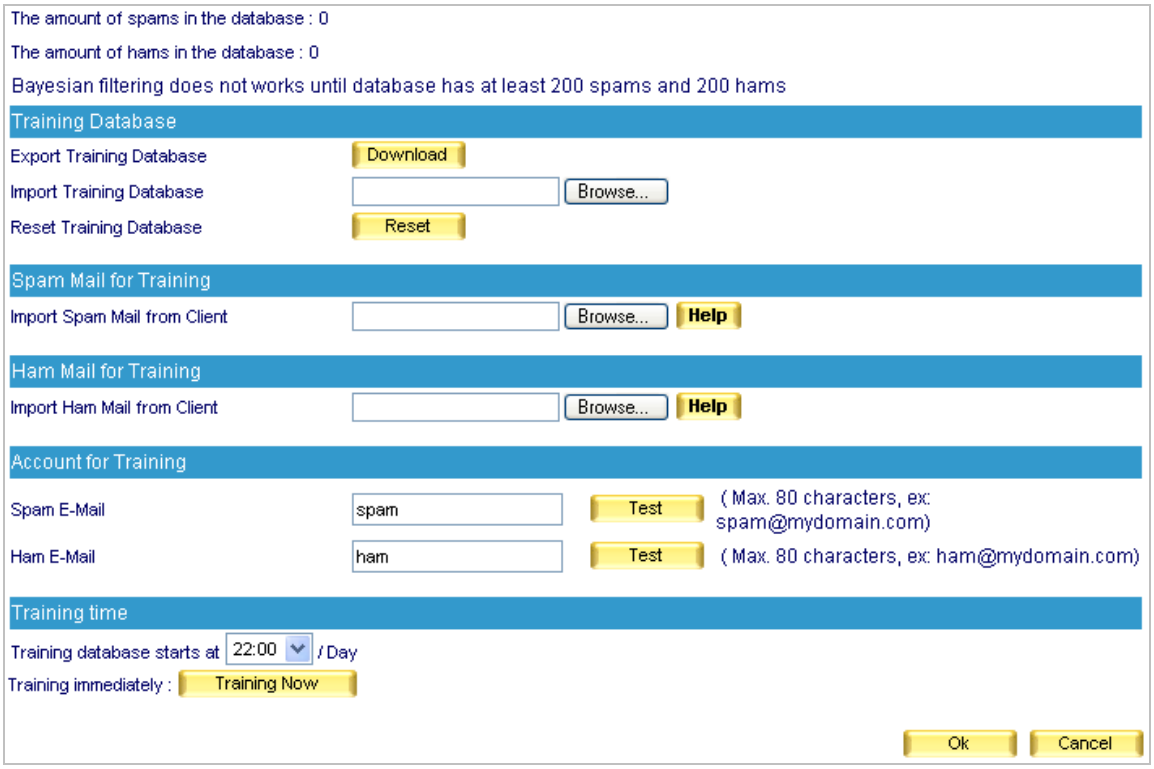


Figure 6-60 Configuring to Train Itself on Scheduled Time

6.4 Anti-Virus

Sending or receiving e-mails through ES-6000 can avoid your company / organization from ceasing function due to virus e-mails. Keep your business always running and money-making.

6.4.1 Anti-Virus Setting

- Scans Inbound and Outbound mails for virus.
- If a virus infected mail is detected, that mail will be marked as **---virus---** in the subject line. On the contrary, if a mail is clean, there will not be any mark in the subject line.
- Virus pattern updates automatically every ten minutes or can be updated manually at once. After each update, it will show its virus pattern version and update time.
- Available virus engines are:
  - Clam ─ a default and free for charge virus scan engine.
  - Sophos - The purchase of end-user license is required for legal use.

To assure ES-6000 a successful update, use **Test** to check if the connection to the virus pattern server works or not before running update.

Inspection Direction:

- If an Inbound mail is detected as virus-infected, it can be deleted, deliver to the recipient (deliver the virus mail or a notification mail instead), or stored in the quarantine.
- If an Outbound mail is detected as virus-infected, it can be deleted, deliver to the recipient (deliver the virus mail or a notification mail instead), or stored in the quarantine.
  - Set as followed :
    1. Select **Clam** for **Virus Scan Engine**.
    2. In **Inspection Direction**, enable both Inbound and Outbound **Action of Infected Mail** and check **Deliver to the recipient**, and then check **Deliver a notification mail instead of the original virus mail**.
    3. Add a virus string **---virus---** to the subject line of a virus infected mail.
    4. Click **OK**. (Figure 6-61)

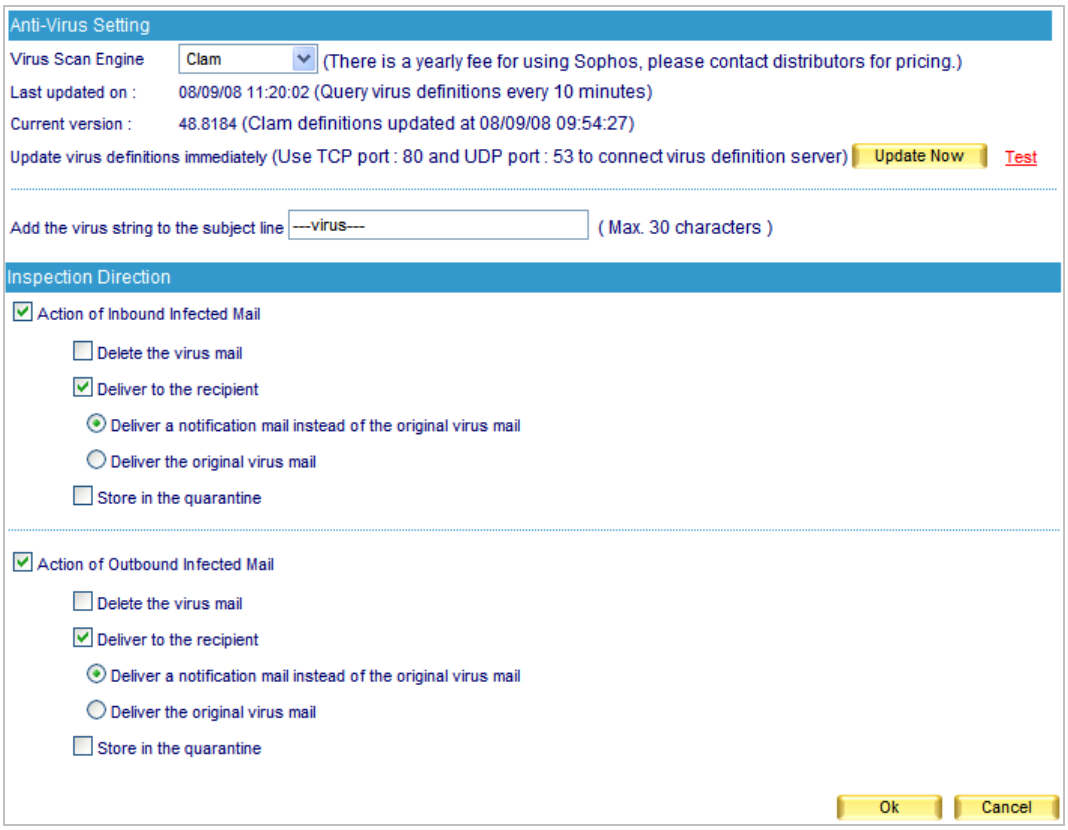


Figure 6-61 Anti-Virus settings

◆ Whoever receives a virus mail detected by ES-6000 will see a warning tag, such as **---virus---**, in the subject line. (Figure 6-62)

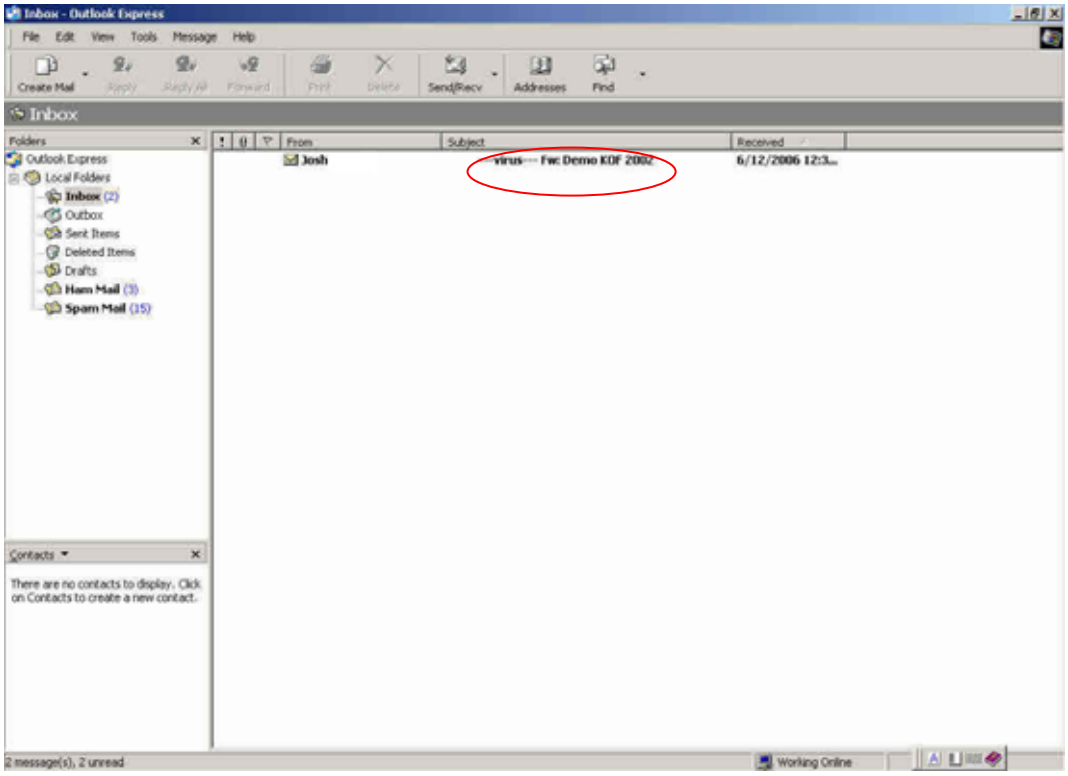


Figure 6-62 A mail scanned as virus mail

Available virus-scanning modes for users are Clam, Sophos, and Clam+Sophos.

6.4.2 Anti-Virus Configuration Example

Scanning Inbound or Outbound Mails for Virus

Step1. In the path of **Mail Security → Anti-Virus →Setting**, set as followed: (Figure 6-63)

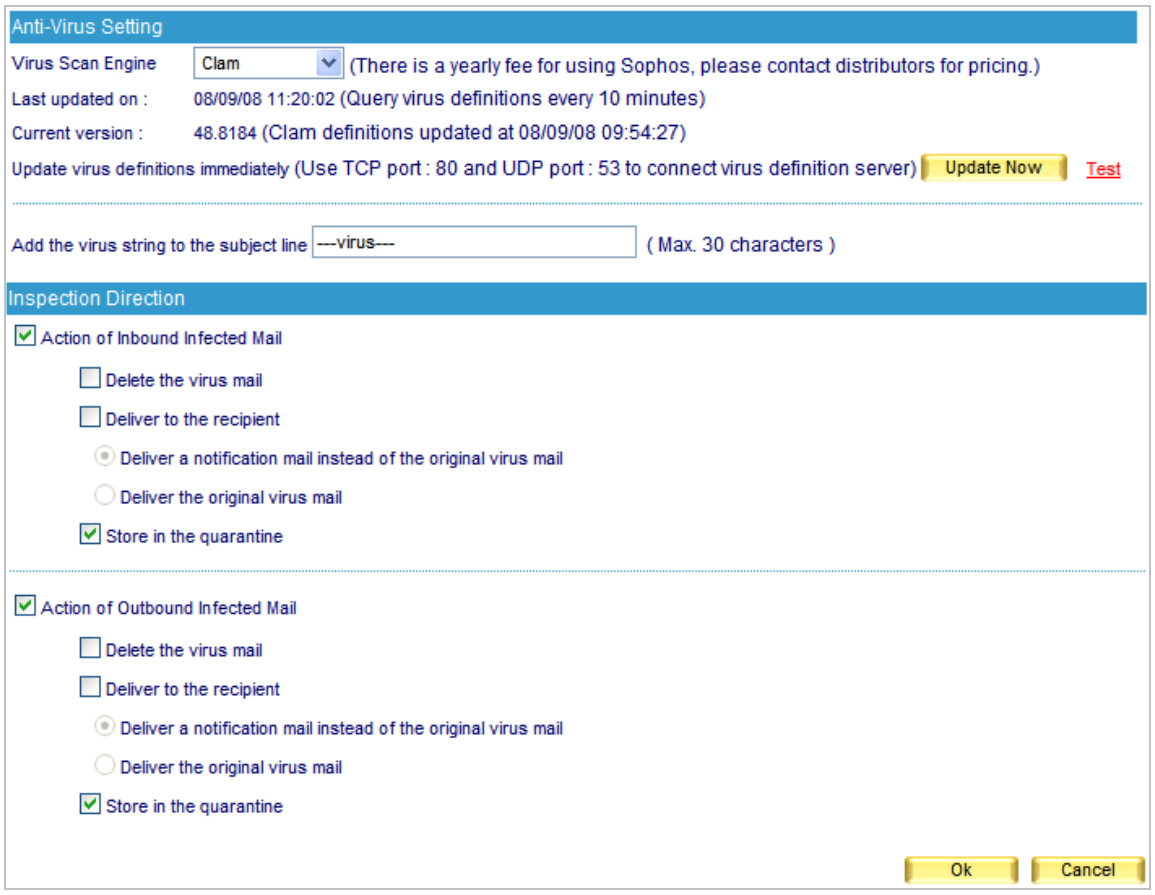


Figure 6-63 The scan and action of infected mail

Action of infected mail only allowed one option at a time. If action sets as **Delete the virus mail**, virus mail will be deleted at once when it is detected, and a corresponding log will be created under **Mail Security → Mail Report → Log**.

Step2. When an external mail account, for instance hotmail, sends a mail to internal mail account, such as ryan@airlive.com:

- A hotmail mail account, jacky@hotmail.com, sends a virus mail, and then it would be stored in the quarantine.
- A hotmail mail account, portia@hotmail.com, sends a clean mail, and then ryan@airlive.com would receive it.

Step3. If an internal mail account, for example josh@airlive.com, sends a mail to external accounts, such as hotmail:

- The mail sent to jacky@hotmail.com is infected, and then it would be stored in the quarantine.
- The mail sent to portia@hotmail.com is clean, and then it would be sent to the account.

6.5 Mail Report

ES-6000 provides enterprise mail report in statistics and log. With the help of them, enterprise could have a clear view of mail activities.

6.5.1 Setting

Periodic Report

■ It can generate and send the periodical report to recipient according to the time setting.

History Report

■ It can generate and send the history report to recipient according to the time setting.

◆ In **System → Setting**, enable **E-mail Alert Notification / Report**. Then go to **Mail Security → Mail Report → Setting**, set as below.

1. **Enable E-mail periodic report**, and check **Yearly report**, **Monthly report**, **Weekly report**, and **Daily report**.
2. Click **OK.** (Figure 6-64)
3. When the time comes, the ES-6000 will send the report to recipient. (Figure 6-65, 6-66, 6-67, 6-68, 6-69)
4. In **History Report**, select an issue date from the calendar icon.
5. Click **Mail Report**. (Figure 6-70)
6. Reports will be delivered to the recipient on the time setting. (Figure 6-71, 6-72, 6-73, 6-74, 6-75)

Scheduling for periodic report:

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

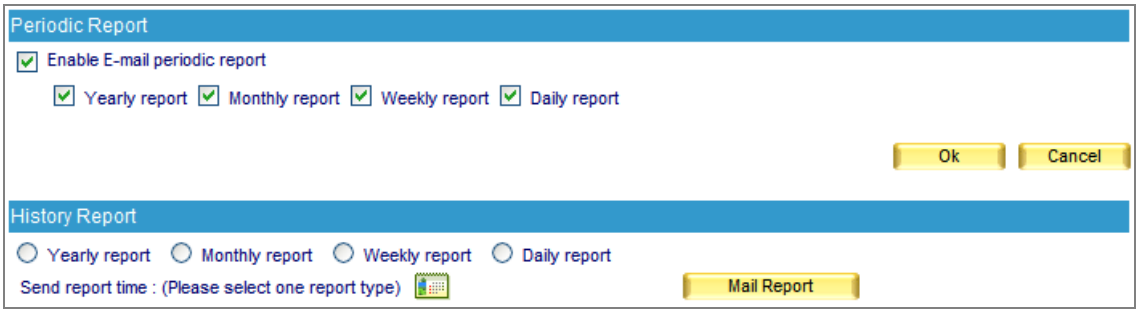


Figure 6-64 The periodic report setting

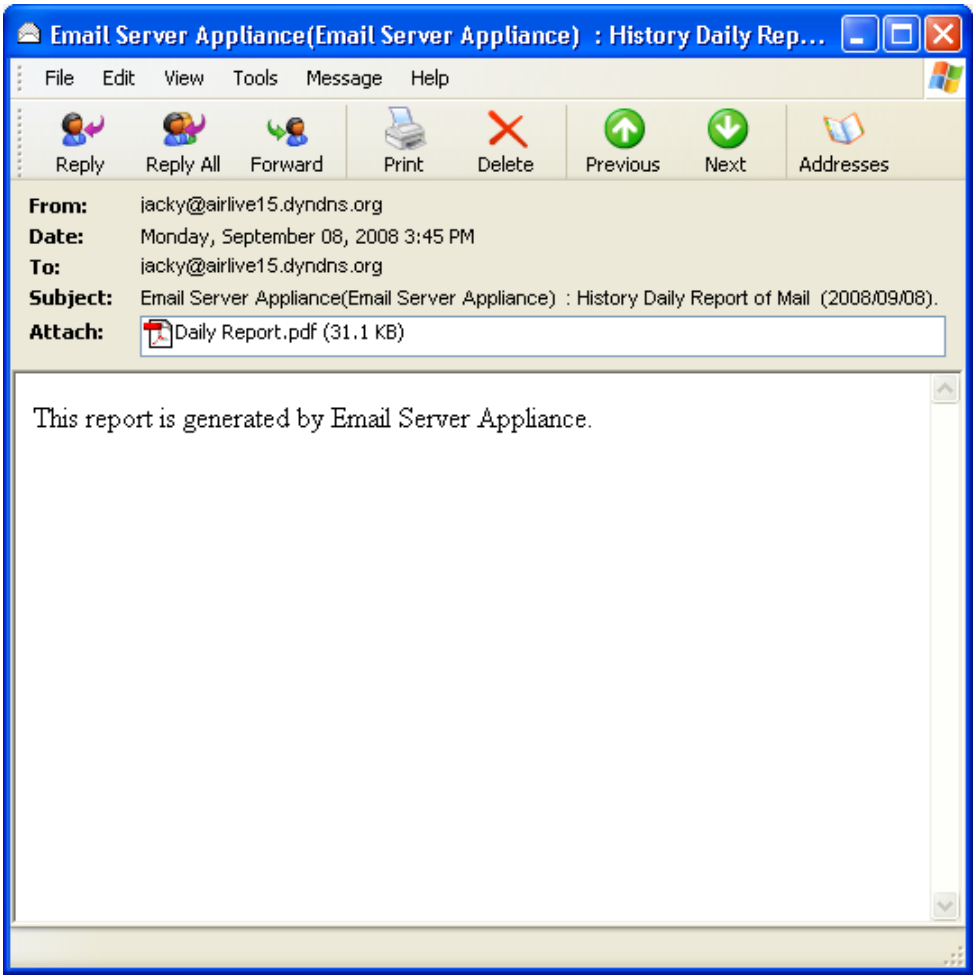


Figure 6-65 Receive the periodic report

E-Mail Server

Daily Report - Inbound Mails of Each Domain

Time : (2008/09/08)

Email Attributes in Percentage

Spam Mails	Virus Mails	Normal Mails	Total Mails
519 [41.2%]	7 [0.6%]	734 [58.3%]	1260 [100.0%]

TOP-5 Domain (Sorted by Total Mail Amount) spam mails virus mails normal mails

No.	Domain Name	Spam	Virus	Normal	Total	Inbound Mails
1	airlive.com	519	7	734	1260	1260

TOP-10 Accounts (Sorted by Total Mail Amount) spam mails virus mails normal mails

No.	Account	Spam	Virus	Normal	Total	Inbound Mails
1	john.lai	35	1	55	91	91
2	chan	30	0	45	75	75
3	janeju	27	1	37	65	65
4	edwardwang	29	1	28	58	58
5	rma1	30	1	20	51	51
6	benny.lai	28	1	18	47	47
7	tommy.wang	29	0	13	42	42
8	sandy	28	0	12	40	40
9	jay	28	0	11	39	39
10	lynn.yang	15	0	22	37	37

Average: 52.50 Mails/Hour

Statistics Graph spam mails virus mails normal mails

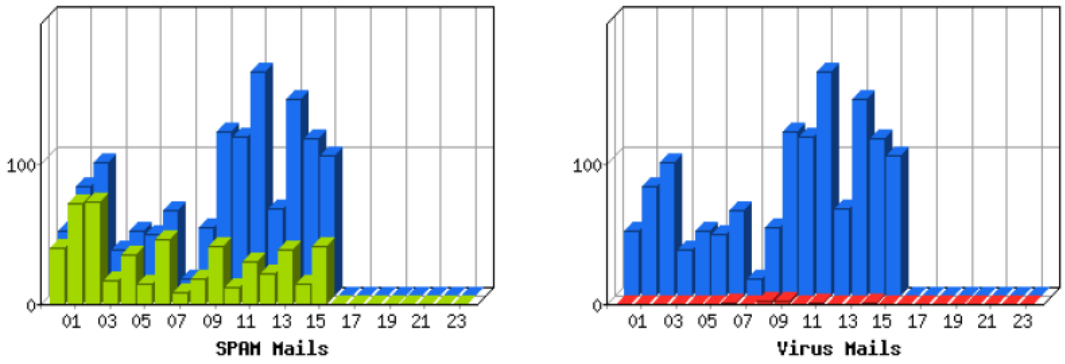


Figure 6-66 The first page in periodic report

E-Mail Server

Daily Report - Inbound Mails of airlive.com

Time : (2008/09/08)

Email Attributes in Percentage

Spam Mails	Virus Mails	Normal Mails	Total Mails
519 [41.2%]	7 [0.6%]	734 [58.3%]	1260 [100.0%]

TOP-10 Accounts (Sorted by Total Mail Amount) spam mails virus mails normal mails

No.	Account	Spam	Virus	Normal	Total	Inbound Mails
1	john.lai	35	1	55	91	91
2	chan	30	0	45	75	75
3	janeju	27	1	37	65	65
4	edwardwang	29	1	28	58	58
5	rma1	30	1	20	51	51
6	benny.lai	28	1	18	47	47
7	tommy.wang	29	0	13	42	42
8	sandy	28	0	12	40	40
9	jay	28	0	11	39	39
10	lynn.yang	15	0	22	37	37

Average: 52.50 Mails/Hour

Statistics Graph spam mails virus mails normal mails

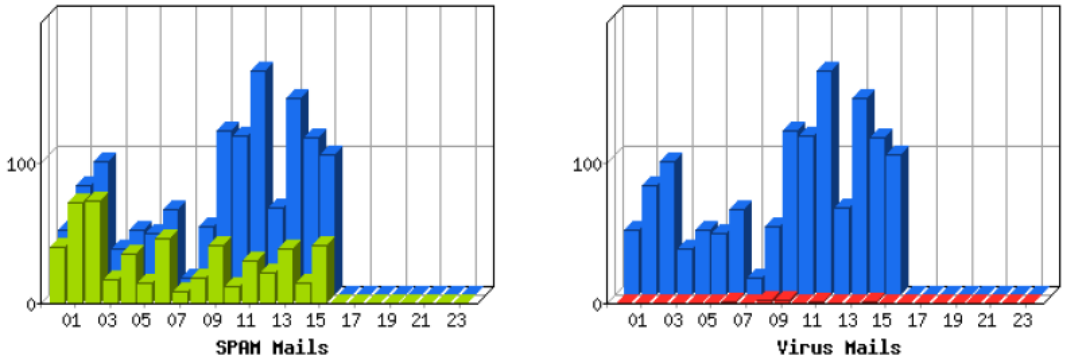


Figure 6-67 The second page in periodic report

E-Mail Server

Daily Report - Outbound Mails of Each Domain

Time : (2008/09/08)

Email Attributes in Percentage

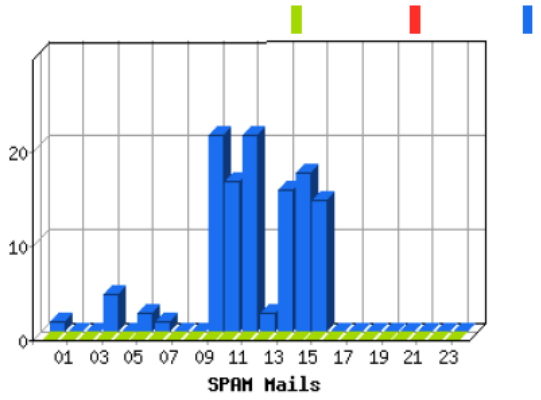
Spam Mails	Virus Mails	Normal Mails	Total Mails
0 [0.0%]	0 [0.0%]	114 [100.0%]	114 [100.0%]

TOP-5 Domain (Sorted by Total Mail Amount) spam mails virus mails normal mails

No.	Domain Name	Spam	Virus	Normal	Total	Outbound Mails
1	airlive.com	0	0	114	114	114

TOP-10 Accounts (Sorted by Total Mail Amount) spam mails virus mails normal mails

No.	Account	Spam	Virus	Normal	Total	Outbound Mails
1	benny.lai	0	0	18	18	18
2	john.lai	0	0	12	12	12
3	jacky.ko	0	0	6	6	6
4	josh.lin	0	0	6	6	6
5	vincent.chang	0	0	5	5	5
6	liba	0	0	5	5	5
7	ryan.cheng	0	0	5	5	5
8	emily.hsu	0	0	5	5	5
9	david.cheng	0	0	4	4	4
10	edwardwang	0	0	4	4	4



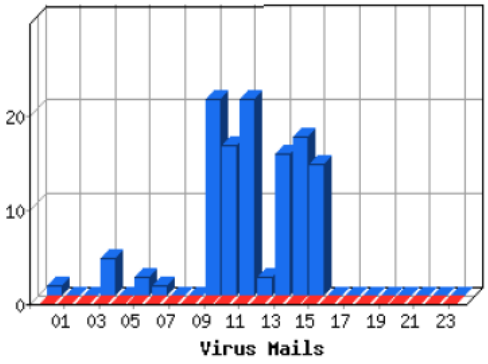


Figure 6-68 The third page in periodic report

E-Mail Server

Daily Report - Outbound Mails of airlive.com

Time : (2008/09/08)

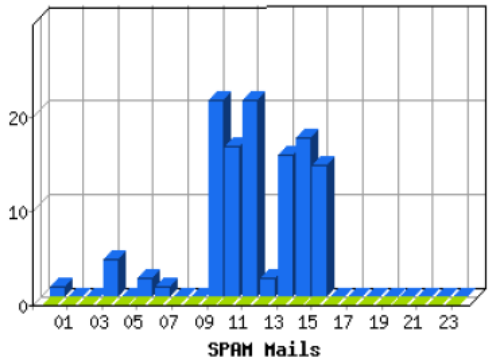
Email Attributes in Percentage

Spam Mails	Virus Mails	Normal Mails	Total Mails
0 [0.0%]	0 [0.0%]	114 [100.0%]	114 [100.0%]

TOP-10 Accounts (Sorted by Total Mail Amount) spam mails virus mails normal mails

No.	Account	Spam	Virus	Normal	Total	Outbound Mails
1	benny.lai	0	0	18	18	18
2	john.lai	0	0	12	12	12
3	jacky.ko	0	0	6	6	6
4	josh.lin	0	0	6	6	6
5	vincent.chang	0	0	5	5	5
6	liba	0	0	5	5	5
7	ryan.cheng	0	0	5	5	5
8	emily.hsu	0	0	5	5	5
9	david.cheng	0	0	4	4	4
10	edwardwang	0	0	4	4	4
						Average: 4.75 Mails/Hour

Statistics Graph spam mails virus mails normal mails



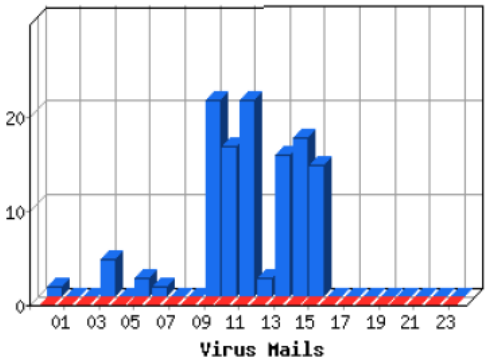


Figure 6-69 The fourth page in periodic report

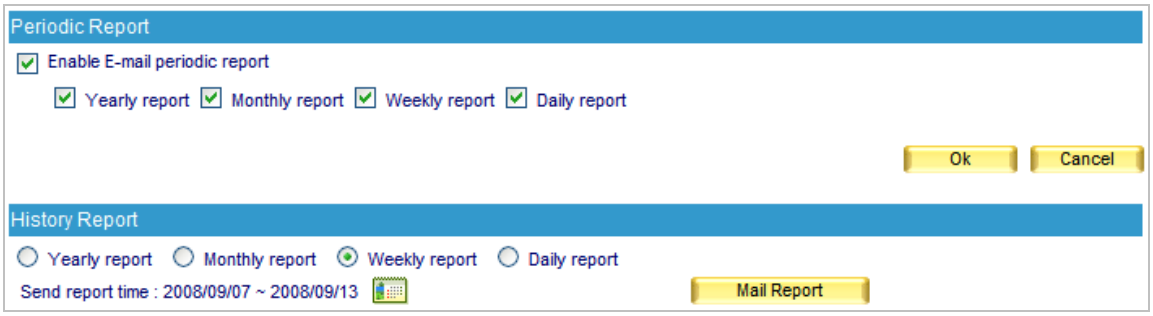


Figure 6-70 The history report setting

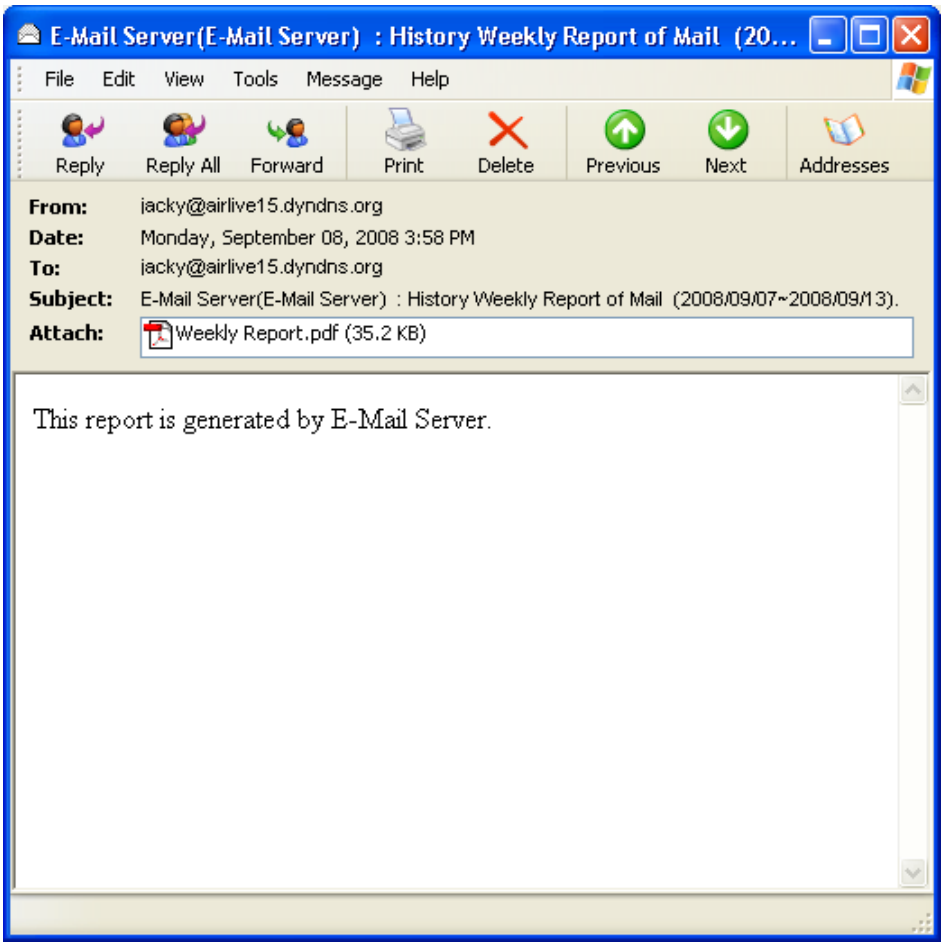


Figure 6-71 Receive the history report

E-Mail Server

Weekly Report - Inbound Mails of Each Domain

Time : (2008/09/07~2008/09/13)

Email Attributes in Percentage

Spam Mails	Virus Mails	Normal Mails	Total Mails
1208 [59.1%]	19 [0.9%]	816 [39.9%]	2043 [100.0%]

TOP-5 Domain (Sorted by Total Mail Amount) spam mails virus mails normal mails

No.	Domain Name	Spam	Virus	Normal	Total	Inbound Mails
1	airlive.com	1208	19	816	2043	2043

TOP-10 Accounts (Sorted by Total Mail Amount) spam mails virus mails normal mails

No.	Account	Spam	Virus	Normal	Total	Inbound Mails
1	john.lai	78	2	71	151	151
2	chan	80	0	58	138	138
3	benny.lai	71	6	27	104	104
4	edwardwang	69	2	28	99	99
5	janeju	59	1	38	98	98
6	rma1	67	2	20	89	89
7	tech	71	1	13	85	85
8	tommy.wang	71	0	13	84	84
9	sandy	68	0	13	81	81
10	jay	61	0	13	74	74

Average: 291.86 Mails/Day

Statistics Graph

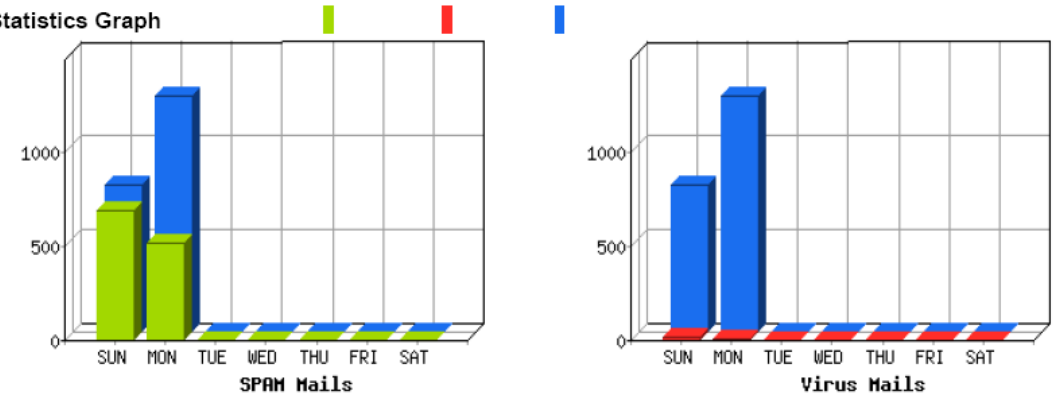


Figure 6-72 The first page in history report

E-Mail Server

Weekly Report - Inbound Mails of airlive.com

Time : (2008/09/07~2008/09/13)

Email Attributes in Percentage

Spam Mails	Virus Mails	Normal Mails	Total Mails
1208 [59.1%]	19 [0.9%]	816 [39.9%]	2043 [100.0%]

TOP-10 Accounts (Sorted by Total Mail Amount) spam mails virus mails normal mails

No.	Account	Spam	Virus	Normal	Total	Inbound Mails
1	john.lai	78	2	71	151	151
2	chan	80	0	58	138	138
3	benny.lai	71	6	27	104	104
4	edwardwang	69	2	28	99	99
5	janeju	59	1	38	98	98
6	rma1	67	2	20	89	89
7	tech	71	1	13	85	85
8	tommy.wang	71	0	13	84	84
9	sandy	68	0	13	81	81
10	jay	61	0	13	74	74

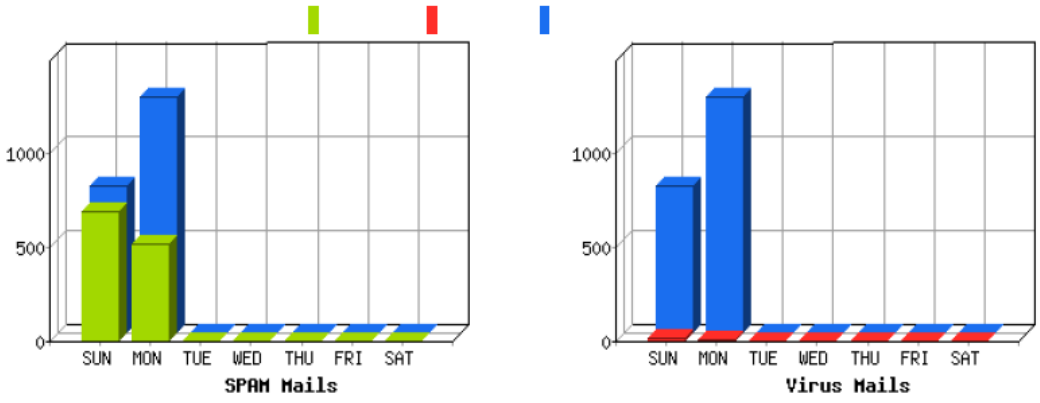


Figure 6-73 The second page in history report

E-Mail Server

Weekly Report - Outbound Mails of Each Domain

Time : (2008/09/07~2008/09/13)

Email Attributes in Percentage

Spam Mails	Virus Mails	Normal Mails	Total Mails
0 [0.0%]	0 [0.0%]	115 [100.0%]	115 [100.0%]

TOP-5 Domain (Sorted by Total Mail Amount) spam mails virus mails normal mails

No.	Domain Name	Spam	Virus	Normal	Total	Outbound Mails
1	airlive.com	0	0	115	115	115

TOP-10 Accounts (Sorted by Total Mail Amount) spam mails virus mails normal mails

No.	Account	Spam	Virus	Normal	Total	Outbound Mails
1	benny.lai	0	0	18	18	18
2	john.lai	0	0	12	12	12
3	josh.lin	0	0	6	6	6
4	jacky.ko	0	0	6	6	6
5	ryan.cheng	0	0	5	5	5
6	emily.hsu	0	0	5	5	5
7	liba	0	0	5	5	5
8	vincent.chang	0	0	5	5	5
9	david.cheng	0	0	4	4	4
10	edwardwang	0	0	4	4	4

Average: 16.43 Mails/Day

Statistics Graph spam mails virus mails normal mails

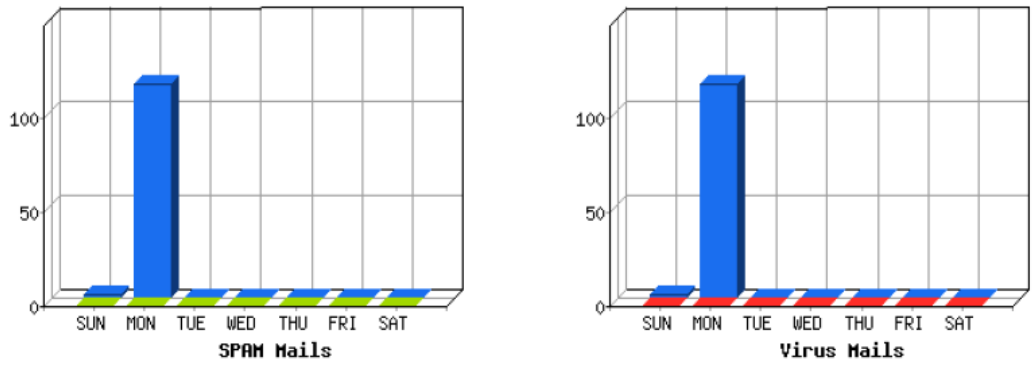


Figure 6-74 The third page in history report

E-Mail Server

Weekly Report - Outbound Mails of airlive.com

Time : (2008/09/07~2008/09/13)

Email Attributes in Percentage

Spam Mails	Virus Mails	Normal Mails	Total Mails
0 [0.0%]	0 [0.0%]	115 [100.0%]	115 [100.0%]

TOP-10 Accounts (Sorted by Total Mail Amount) spam mails virus mails normal mails

No.	Account	Spam	Virus	Normal	Total	Outbound Mails
1	benny.lai	0	0	18	18	18
2	john.lai	0	0	12	12	12
3	josh.lin	0	0	6	6	6
4	jacky.ko	0	0	6	6	6
5	ryan.cheng	0	0	5	5	5
6	emily.hsu	0	0	5	5	5
7	liba	0	0	5	5	5
8	vincent.chang	0	0	5	5	5
9	david.cheng	0	0	4	4	4
10	edwardwang	0	0	4	4	4
						Average: 16.43 Mails/Day

Statistics Graph spam mails virus mails normal mails

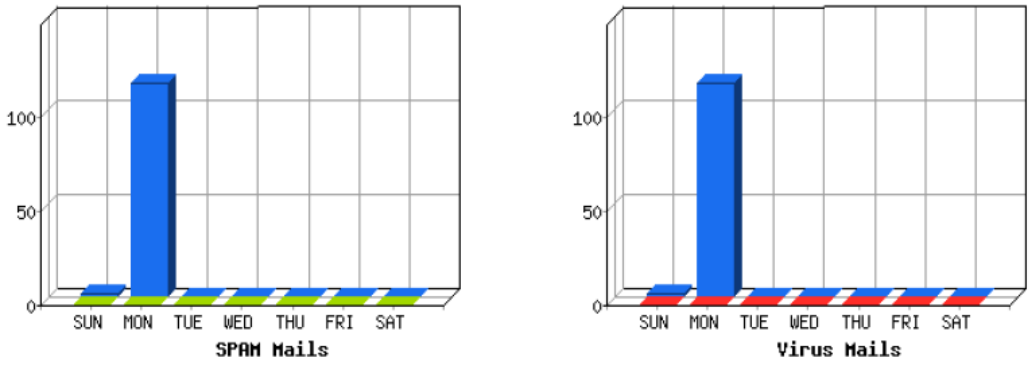


Figure 6-75 The fourth page in history report

The recipient will be receiving the mail report with an attachment in PDF format.

6.5.2 Statistics

Step1. In the path of **Mail Security → Mail Report → Statistics**, there it shows a full-scale statistics report of scanned result.

Step2. In **Statistics**, on the upper left corner, click **Day** for daily statistics report; click **Week** for weekly statistics report; click **Month** for monthly statistics report; click **Year** for annual statistics report.

Step3. Below it shows scanned mail statistics report. (Figure 6-76)

- Vertical axis indicates the amount of scanned mail.
- Horizontal axis indicates time.

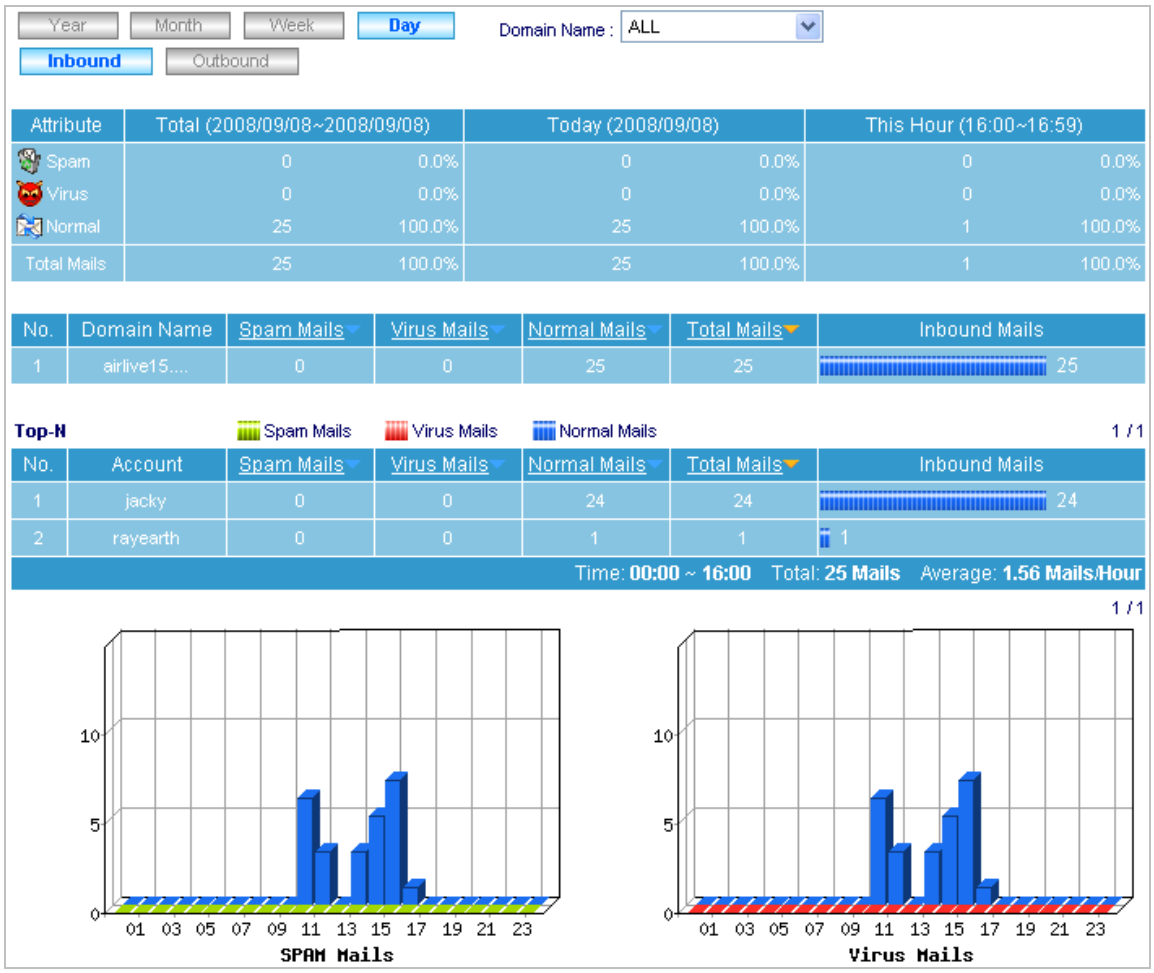


Figure 6-76 Scanned mail statistics report

6.5.3 Log

- User can use date, sender, sender IP address, recipient, subject, attribute, action, and attachment as keyword to search matched records stored in ES-6000.
  - To use this feature, please follow the steps below :
    1. Enable searching duration and assign a period of time.
    2. Input a sender as keyword.
    3. Select **All** for **Attached File**.
    4. Select **All** for **Attribute**.
    5. Select **All** for **Action**.
    6. Click **Search**. (Figure 6-77)
    7. Click **Download Report** to download the search results as a ".txt" file onto local computer. (Figure 6-78)
    8. Click **Export Mail** to download the search results as a ".mbx" file onto local computer. (Figure 6-79)

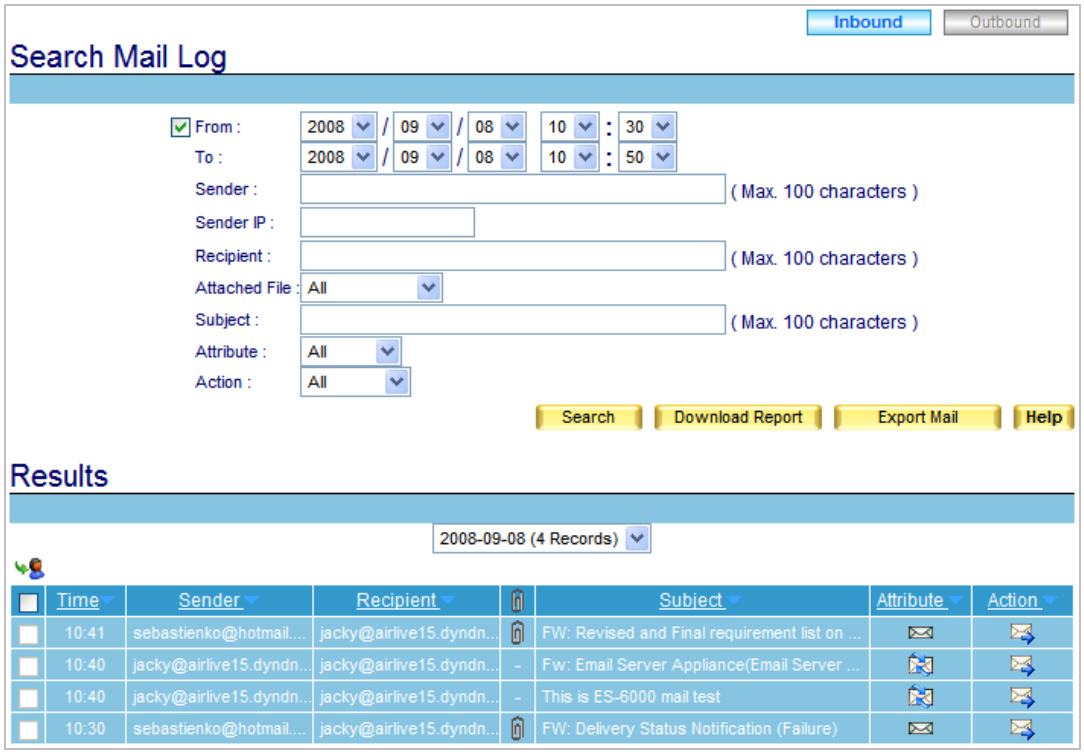


Figure 6-67 Search for specific record

1. Both **Statistics** and **Log** have Inbound and Outbound scanned mail report.
2. In **Log**, click any sender email address link to show its recipient list (a recipient list is a list of all recipients receiving mails from the email address that you click on); click any recipient email address link to show its sender list (a sender list is a list of all senders sending mails to the email address that you click on).
3. **Log** can be sorted by time, sender, recipient, subject, attribute and action. So do sender list and recipient list.

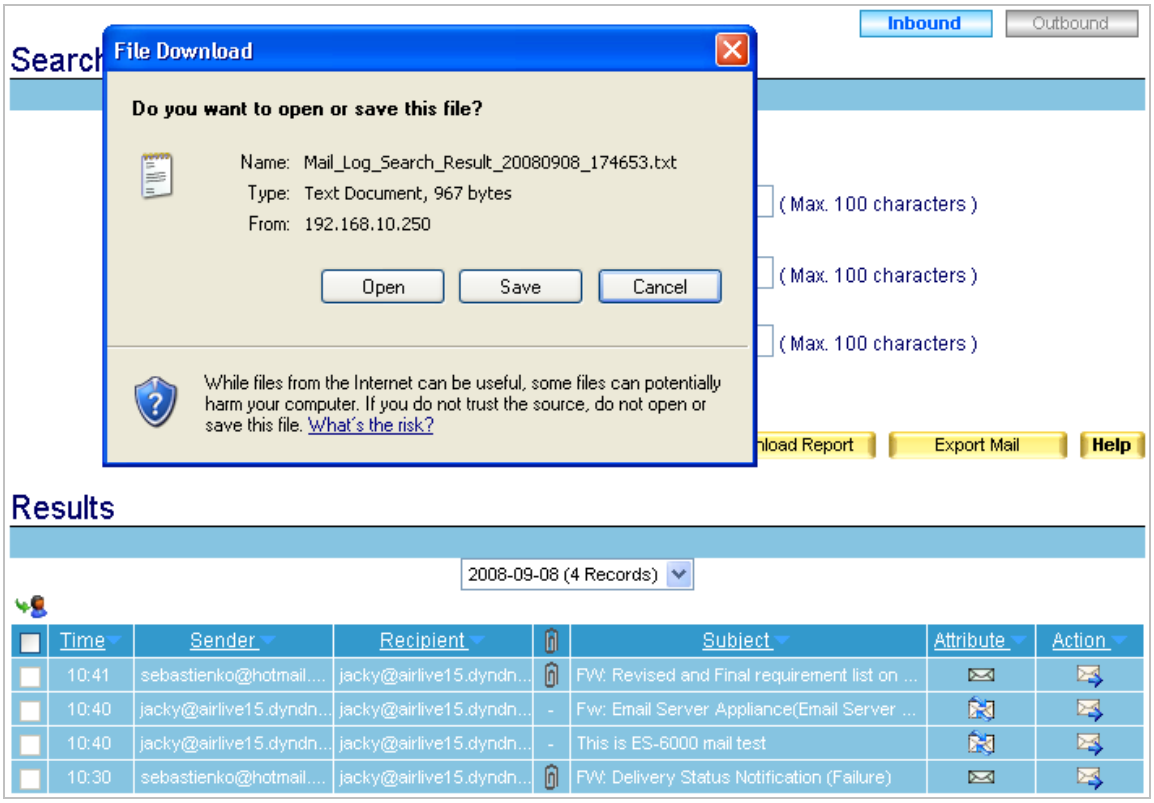


Figure 6-78 Downloading the Search Results as a ".txt" File

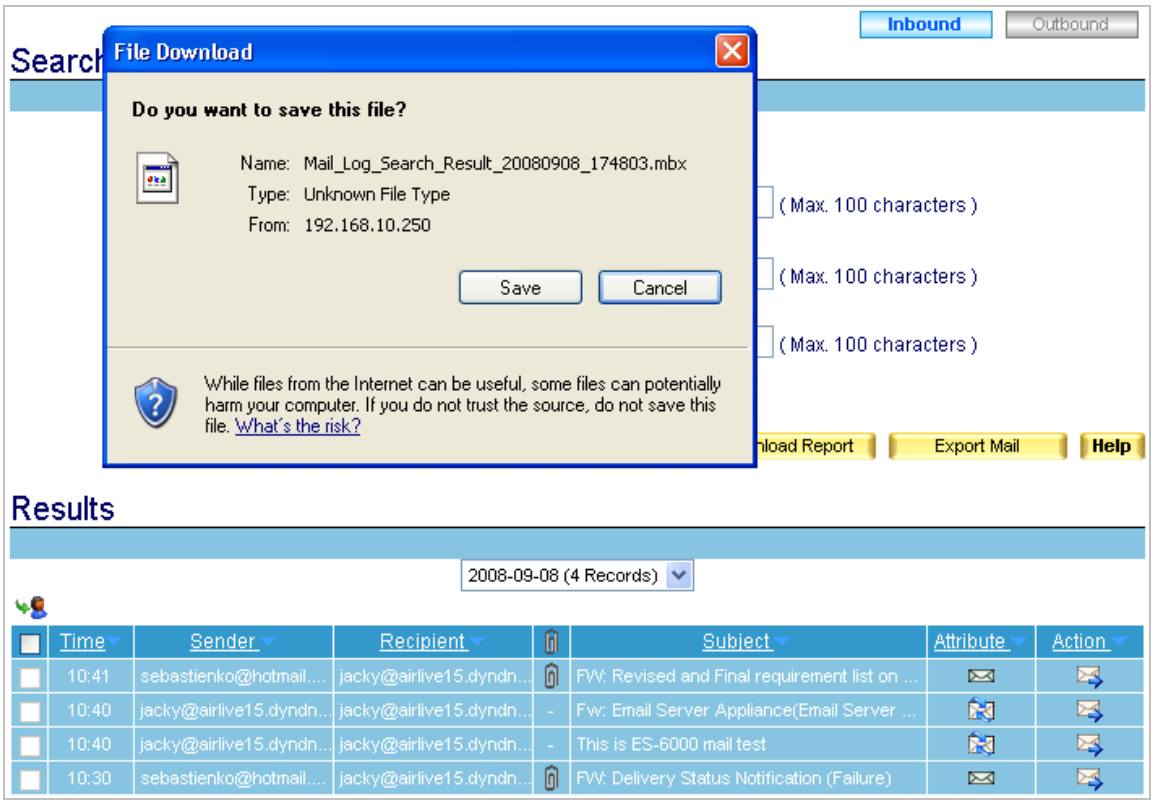


Figure 6-79 Exporting the Search Results as a ".mbx" File

How to open ".mbx" file on your local computer:

1. 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, Select **Tools → mbox2eml** on the menu bar, and then click it. (Figure 6-80)
   - In the mbox2eml window, click "**Select mbox files to convert**" button, locate the ".mbx" file, click **Open**, and then click **Convert** to start converting the file into ".eml" file. (Figure 6-81, Figure 6-82, Figure 6-83)
   - Run Outlook Express to open the ".eml" file. (Figure 6-84)

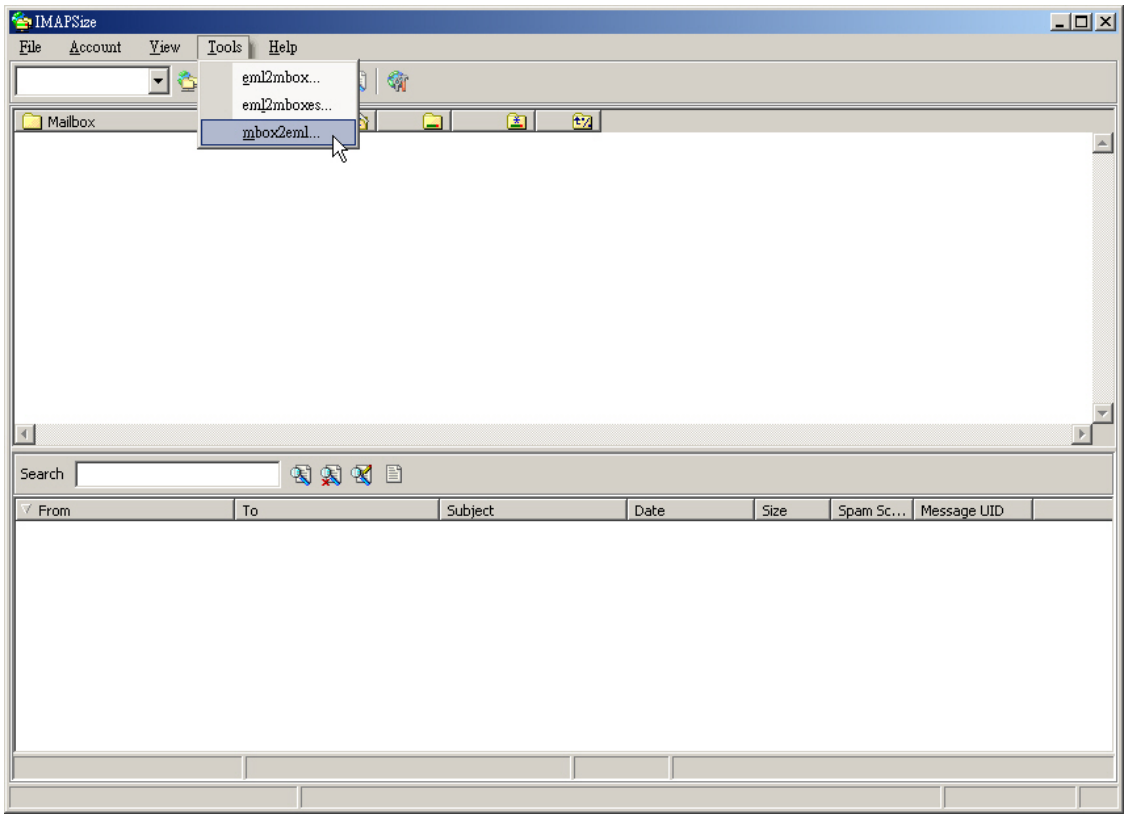


Figure 6-80 Navigating to Tools → Mbox2eml on the Menu Bar

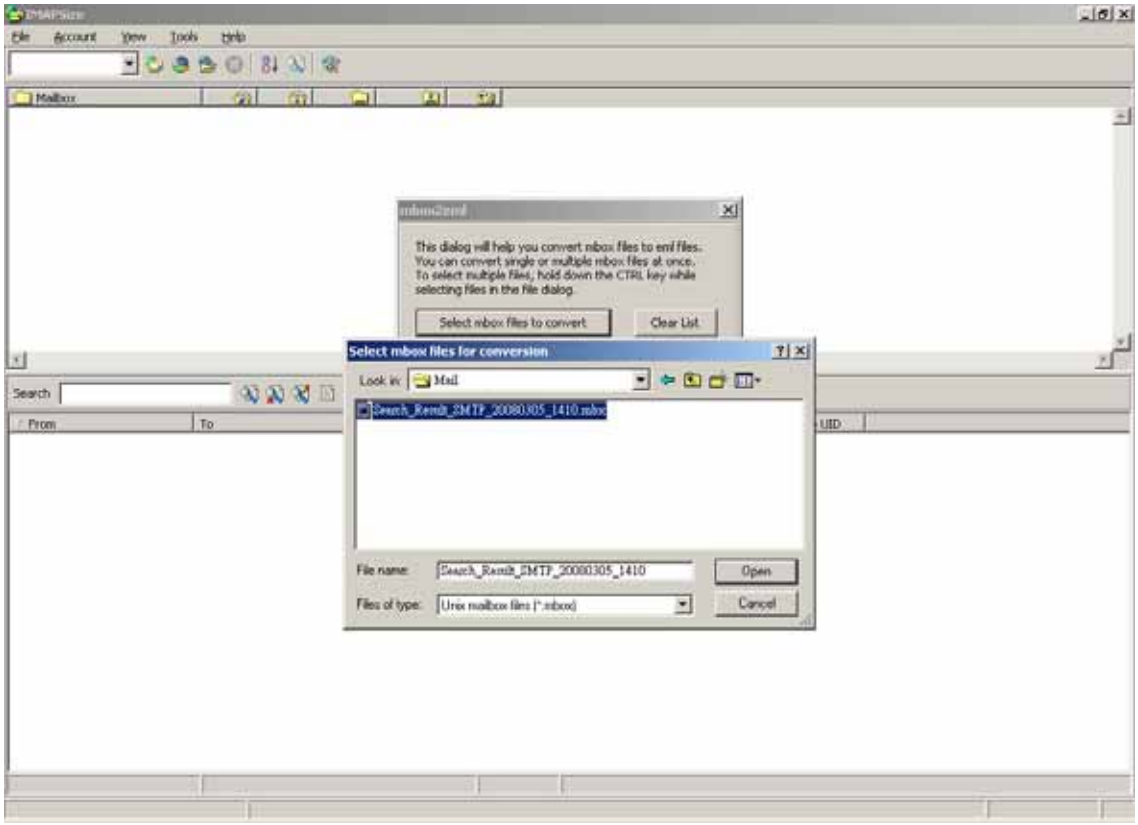


Figure 6-81 Specifying the ".mbx" File to be Converted

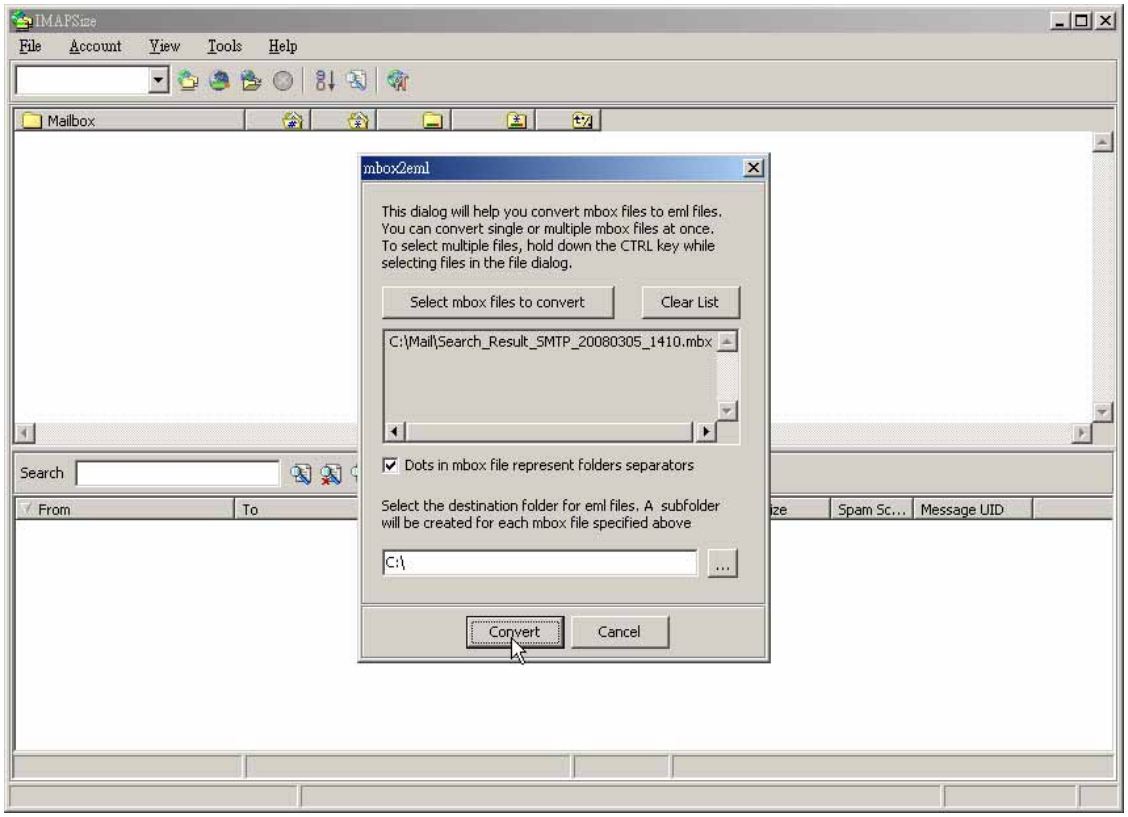


Figure 6-82 Converting the ".mbx" File into a ".eml" File

2.

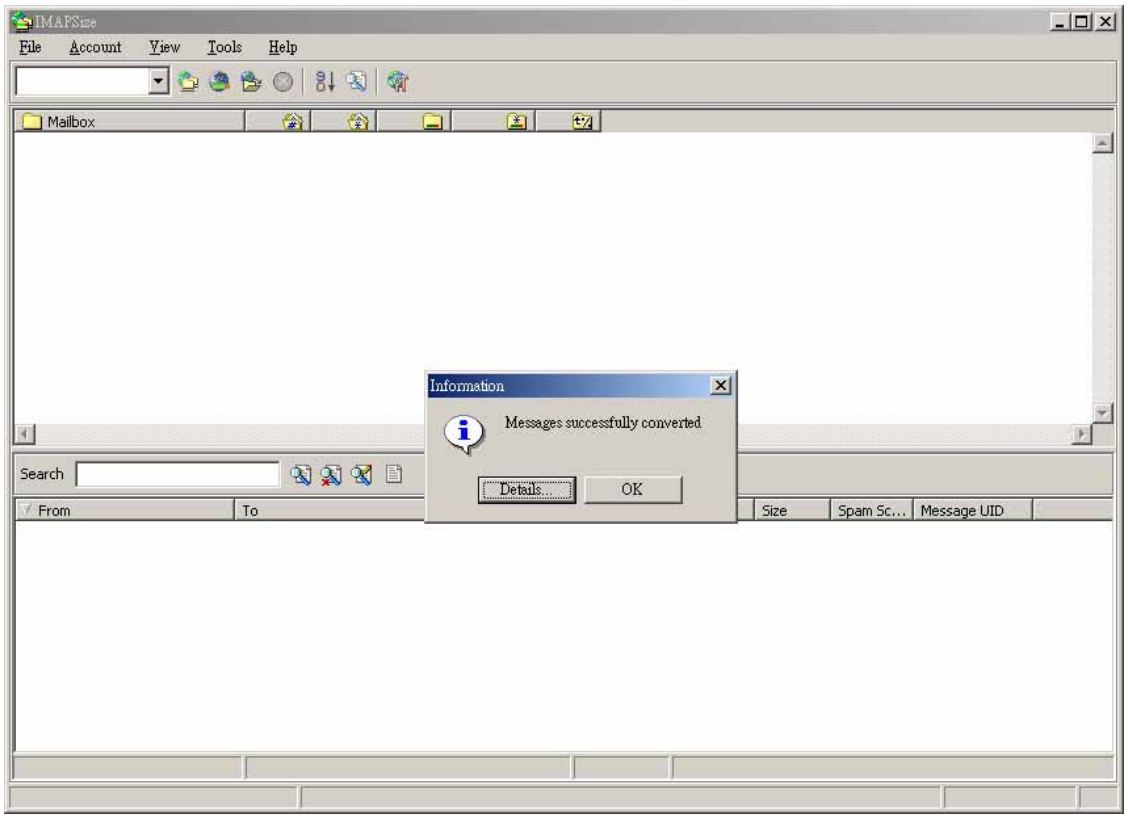


Figure 6-83 File Conversion Completed

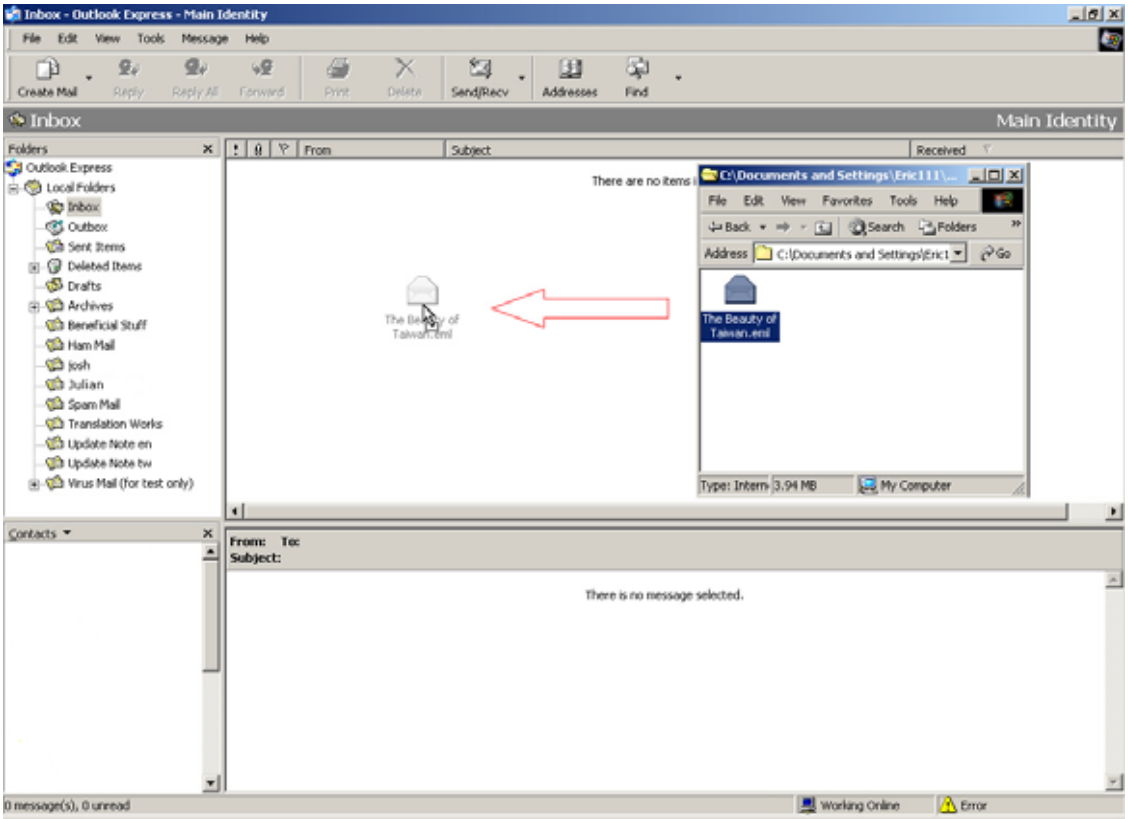


Figure 6-84 Clicking and Dragging the ".eml" File into Outlook Express to Open It

■ The mail stored at quarantine can be retrieved and delivered to recipient.

Step1. In the path of **Mail Security → Mail Report → Log**, there it shows actions of mails. (Figure 6-85)

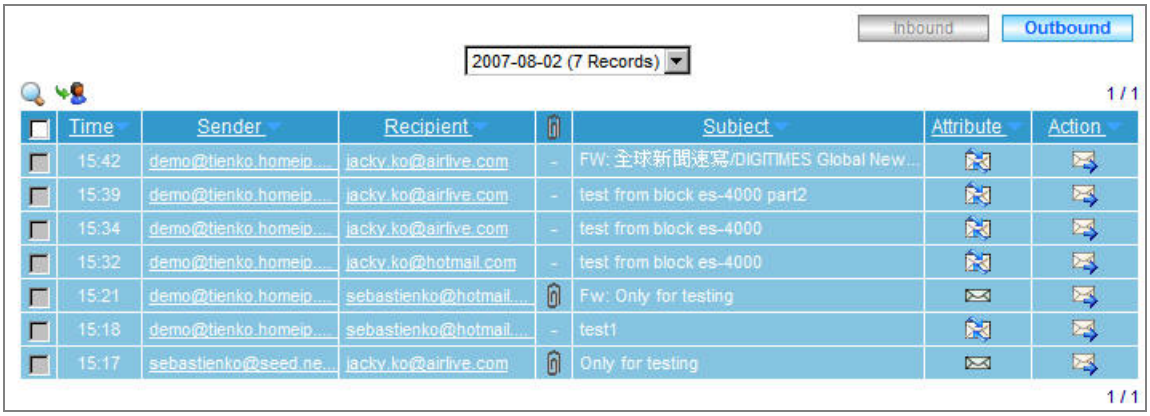


Figure 6-85 Scanned mail log

In **Log**, quarantined spam and virus mails can be retrieved by assigned recipient or viewed its content simply by clicking its subject. (Figure 6-86, 6-87)

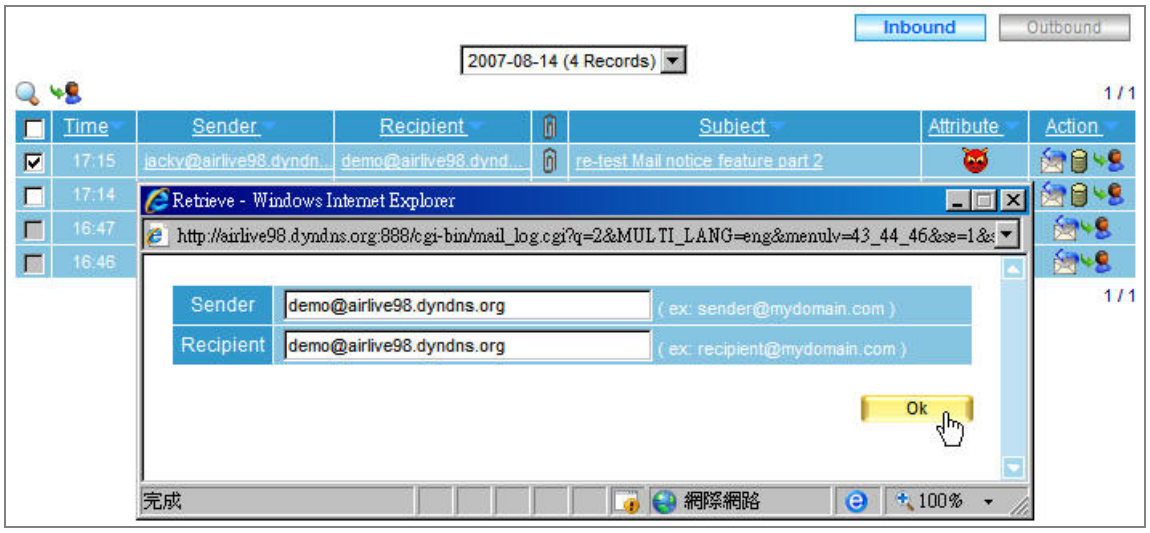


Figure 6-86 Retrieve quarantined virus mail

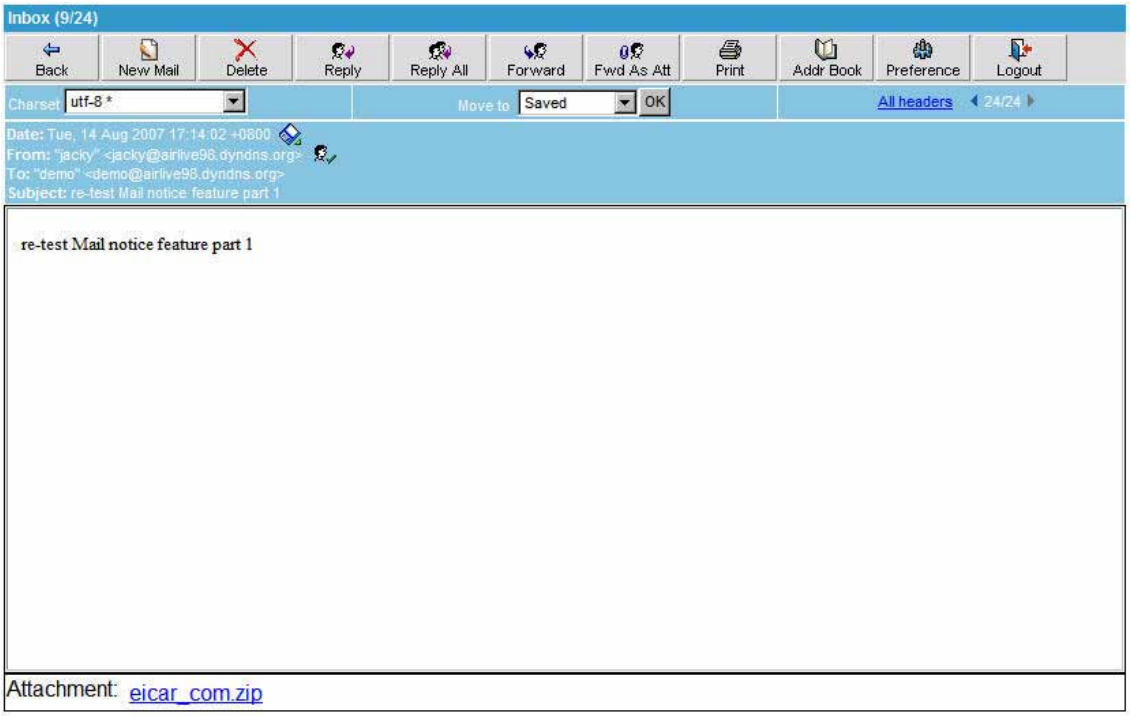


Figure 6-87 View a quarantined virus mail

Log icon descriptions:

1. Attribute:

Icon					
Definition	Allowed	Spam	Virus	Unscan	Invalid Recipient

2. Action:

Icon				
Definition	Delete	Deliver	Store	Retrieve

3. Attached File:

Chapter 7 Mail Archie / Audit

ES-6000 can audit and archive the e-mails individually while processing the e-mails. In this chapter, it will be discussing the functionality and application of *Mail Archive / Audit*.

7.1 Setting

Definition:

- **Mail Archive / Audit Storage Setting**
  - E-mails to be archived or audited can be assigned a storage time and deleted when expired.
  - All inbound and outbound e-mails can be archived.

- **Mail Delay Setting**
  - E-mails can be assigned a time to delay e-mail delivery. User can refer to the following steps to configure settings:
    1. Enable **Inbound Mail Archive**.
    2. Enter “14” in its **Storage Lifetime** field.
    3. Enable **Outbound Mail Archive**.
    4. Enter “60” in its **Storage Lifetime** field.
    5. Select “20:00” from the **Send Mail at** pull-down menu under the **Mail Delay Setting** bar.
    6. Click **OK**. (Figure 7-1)

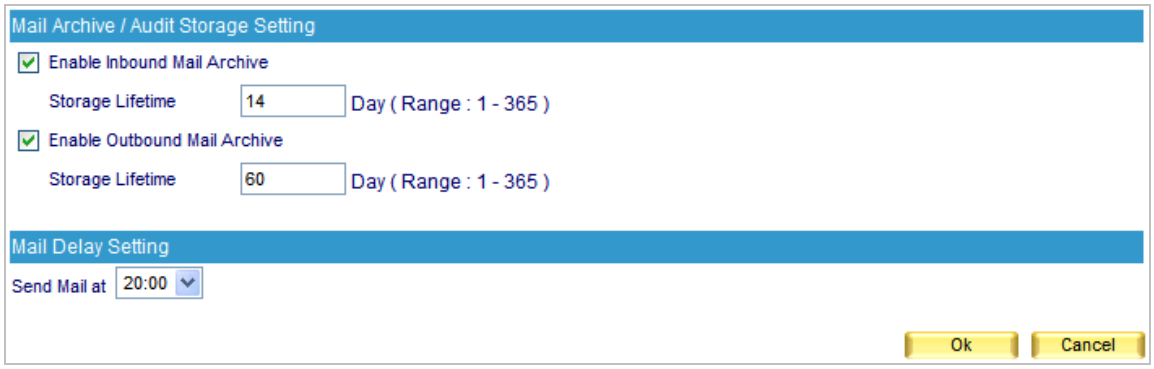


Figure 7-1 Mail Archive and Audit Settings

The priority of **Audit** settings overrides the one of **Mail Audit / Archive Storage Setting**.

7.2 Audit

Definition:

- **Rule Name**
  - The name for an audit rule
- **Comments**
  - The description of an audit rule
- **Combination**
  - **And:** Only when an e-mail meets all criteria is it to be audited
  - **Or:** Only when an e-mail meets merely one criterion is it to be audited
- **Action**
  - E-mails can be deleted, delayed, passed, inspected, or copied. If action is selected as "***Inspect***" or "***Copy To***", then an e-mail address should be specified in the blank field next to it to decide by whom it is inspected or to where it is copied.
- **Archive Mail**
  - E-mail that meets audit criteria can be archived.
- **Item**
  - Audits e-mails by e-mail header, body, attachment name, or size.
  - E-mail header includes from, to and subject.
- **Condition**
  - When **Item** set as ***From*** / ***To*** / ***Subject*** / ***Body*** / ***Attachment Name***, the corresponding conditions are ***Contains***, ***Does Not Contain***, ***Is Equal To***, ***Is Not Equal To***, ***Starts With***, ***Ends With***, ***Exists*** and ***Does Not Exists***.
  - When **Item** set as ***Size***, the corresponding conditions are ***More Than***, ***Is Equal To***, ***Is Not Equal To*** and ***Less Than***.
- **Pattern**
  - Configure the **Item** and **Condition** based on **Pattern**. For example, select "From" for **Item**, "Contains" for **Conditions** and then type "Josh" as **Pattern**, then e-mails from "Josh" will be audited by the device. (Figure 7-2)

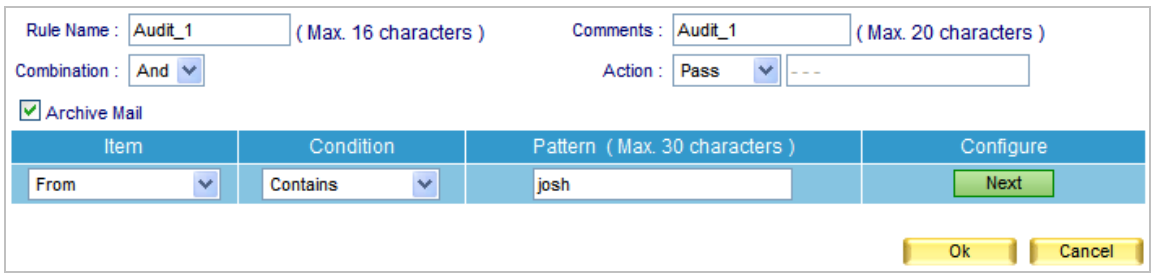


Figure 7-2 Mail Audit

7.3 Archive

- **Search**
  - Available search criteria are date, recipient, sender, subject, action, attached, and non-attached. User can refer to the following steps to configure settings:
    1. Type the complete e-mail address or a word from the e-mail address in the **Recipient** field.
    2. Enable searching duration and assign a period of time.
    3. Select “All” for **Action**.
    4. Select “All” for **Attached File**.
    5. Click **Search**. (Figure 7-3)

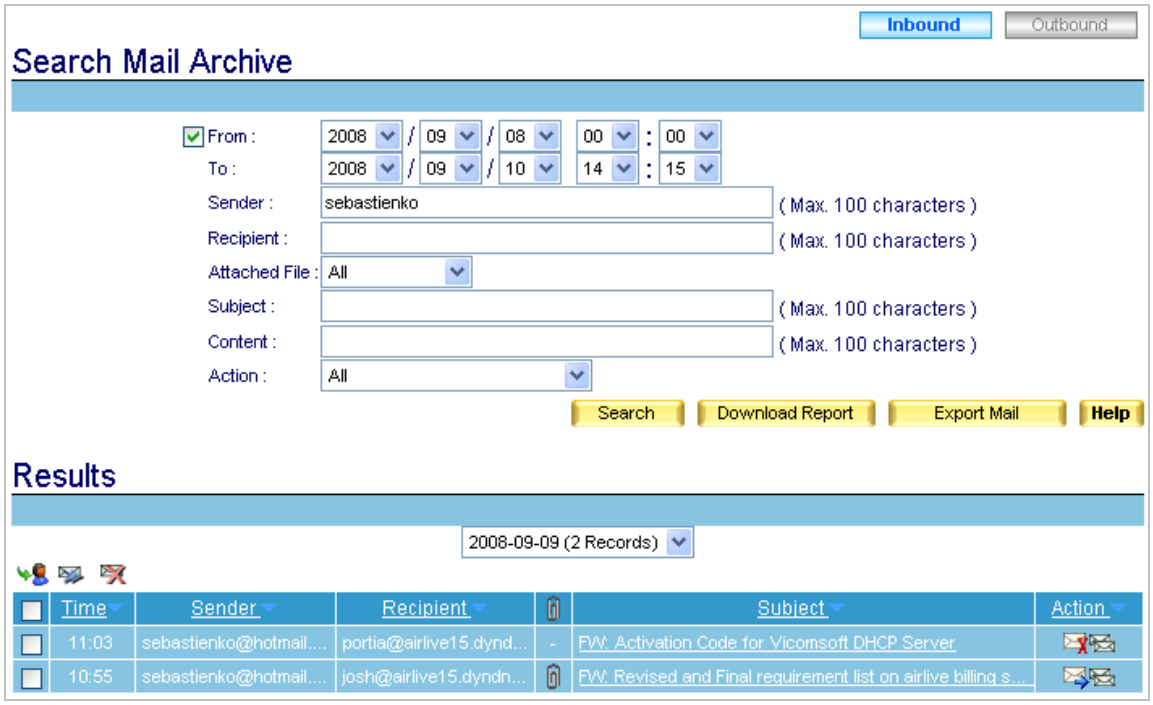


Figure 7-3 Searching for a Specific E-Mail

Archive list is available in both inbound and outbound directions.

Archive list can be sorted by recipient, or sender, or subject, or delivered / received time.

To open the exported “.mbx” file, please refer to Figure 6-80 to 6-84.

7.4 Mail Archive / Audit Configuration Example

Auditing E-Mails Processed by ES-6000

Step1. Select **Mail Archive / Audit → Setting**, and then set as below: (Figure 7-4)

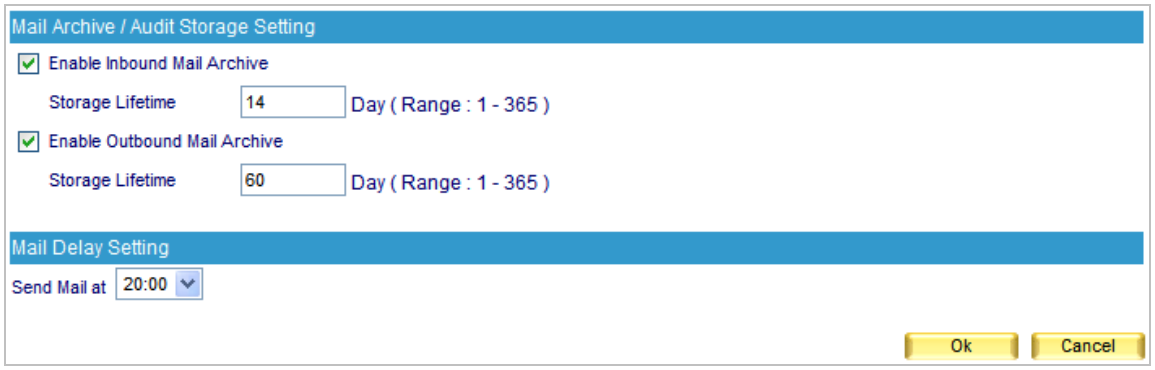


Figure 7-4 Mail Archive / Audit Settings

E-mail that meets **Audit** criteria will be processed based on the **Action** of an **Audit** rule.

Step2. Select **Mail Archive / Audit → Audit**, and then set as below:

- Click **New Entry**.
- Type “Mail_Delivery” in the **Rule Name** field.
- Type “Deliver Mail To User” in the **Comments** field.
- Tick **Archive Mail**.
- Select “Or” for **Combination**.
- Select “Pass” for **Action**.
- Select “From” for **Item**, “Contains” for **Condition** and then type “airlive_jacky” as **Pattern**.
- Click **Next Row**.
- In the second row, select “To” for **Item**, “Contains” for **Condition** and then type “airlive_jacky” as **Pattern**.
- Click **Next Row**.
- In the third row, select “From” for **Item**, “Contains” for **Condition**, and then type “Josh” as **Pattern**.
- Click **Next Row.**
- In the fourth row, select “To” for **Item**, “Contains” for **Condition** and then type “Josh” as **Pattern**. (Figure 7-5)
- Click **OK**. (Figure 7-6)

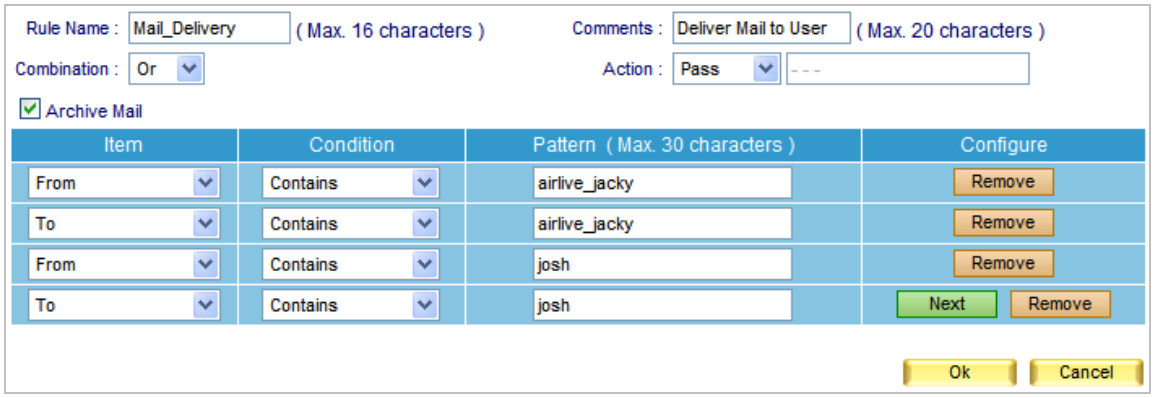


Figure 7-5 First Audit Rule

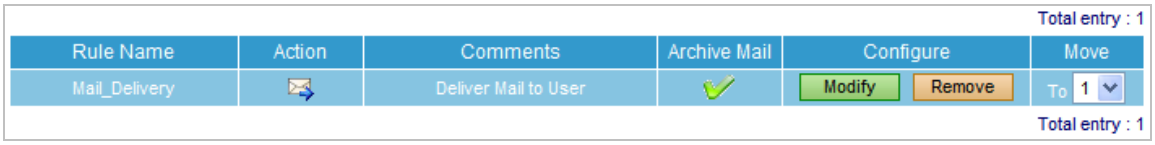


Figure 7-6 First Audit Rule Completed

Step3. Select **Mail Archive / Audit → Audit**, and then set as below:

- Click **New Entry**.
- Type “Mail_Deletion” in the **Rule Name** field.
- Type “Delete Mail” in the **Comments** field.
- Tick **Archive Mail**.
- Select “Or” for **Combination**.
- Select “Delete” for **Action**.
- Select “From” for **Item**, “Contains” for **Condition** and then type “hotmail” as **Pattern**.
- Click **Next Row**.
- In the second row, select “To” for **Item**, “Contains” for **Condition** and then type “hotmail” as **Pattern**. (Figure 7-7)
- Click **OK**. (Figure 7-8)

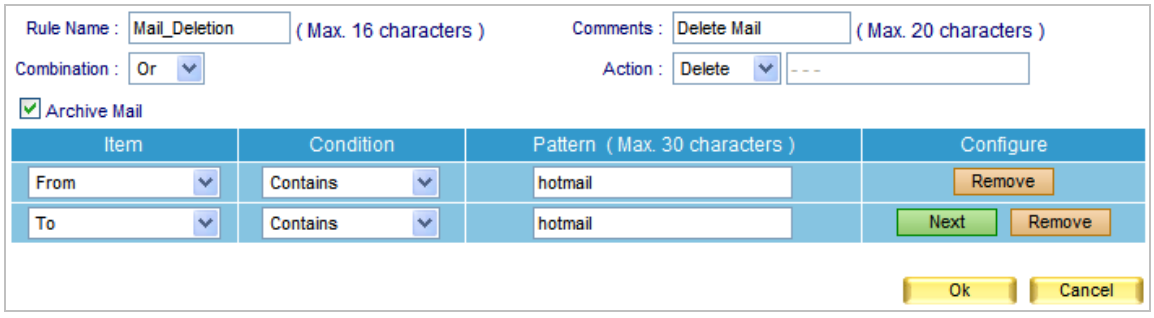


Figure 7-7 Second Audit Rule

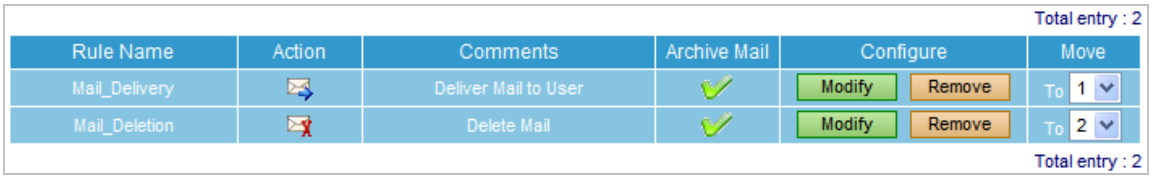


Figure 7-8 Second Audit Rule Completed

Actions to e-mails can be **Delete**, or **Inspect**, or **Delay**, or **Pass** or **Copy to**.

When an e-mail has been scanned for virus and inspected for spam, it will be then audited and processed according to the **Action**.

Right-click any e-mail in your **Outlook Express**, and then click **Properties** on the pop-up menu. After that, click **Details** tab for information on e-mail header of which can be used as reference while configuring the **Condition** and **Item** of an **Audit** rule. (Figure 7-9)

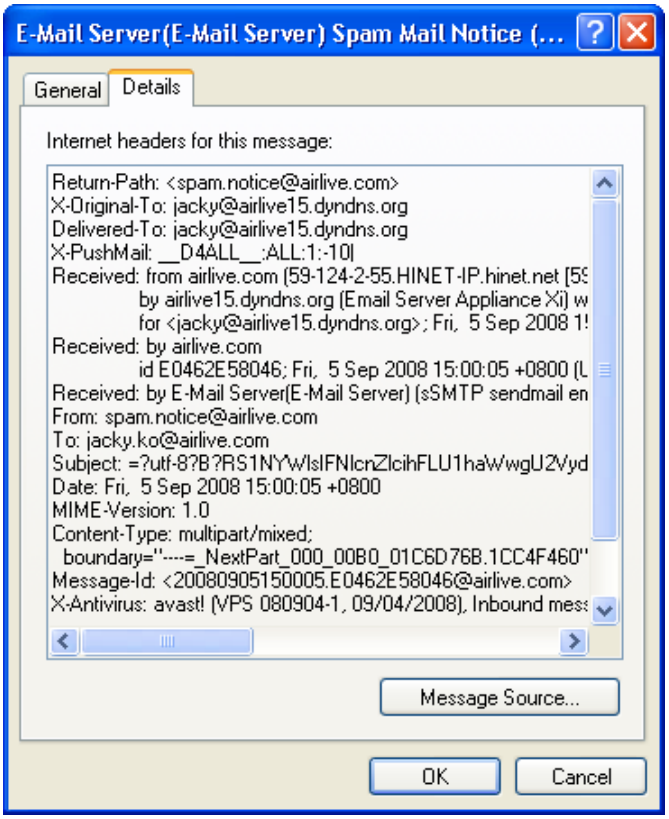


Figure 7-9 The Detailed Information of an E-Mail

Step4. When an external user using hotmail account to send an e-mail to both josh@airlive15.dyndns.org and portia@airlive15.dyndns.org:

- If the sender's address is jacky_airlive@hotmail.com, both of them will receive it.
- If the sender's address is sebastienko@hotmail.com, then only josh@airlive15.dyndns.org will receive the e-mail. E-mails that sent to portia@airlive15.dyndns.org will be deleted.
- A report is generated under **Mail Archive / Audit → Archive**. (Click the upper left **Inbound**). (Figure 7-10)
- Tick the boxes of desirable e-mails and click the upper left "little man" icon to retrieve.
- Type the sender's and recipient's address accordingly in the **Retrieve** window and click **OK**. (Figure 7-11)
- Tick the boxes of desirable e-mails and click the upper left "envelope-with-a-blue-arrow" icon to resend.
- Click **OK** in the dialogue box to confirm resending the selected e-mails. (Figure 7-12)
- Tick the boxes of unwanted e-mails and click the upper left "envelope-with-a-red-cross" icon to remove.
- Click **OK** in the dialogue box to confirm the deletion of selected e-mails. (Figure 7-13)

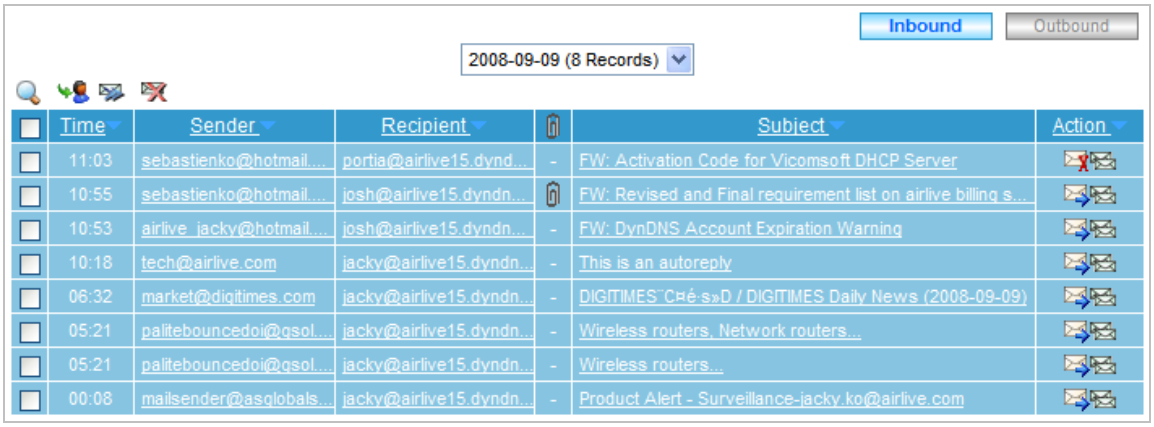


Figure 7-10 The Archive Report

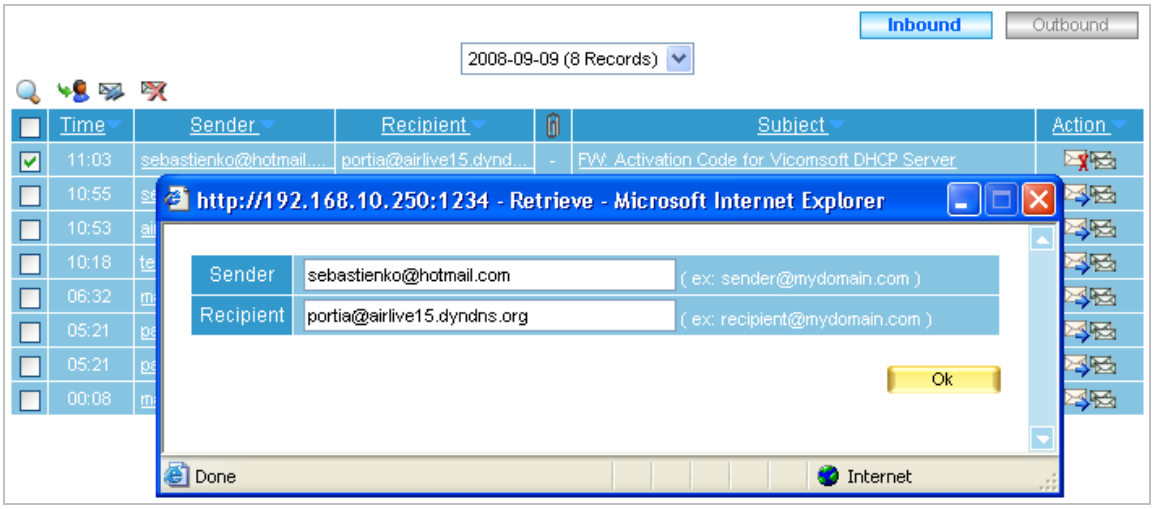


Figure 7-11 Confirming to Retrieve the E-Mails

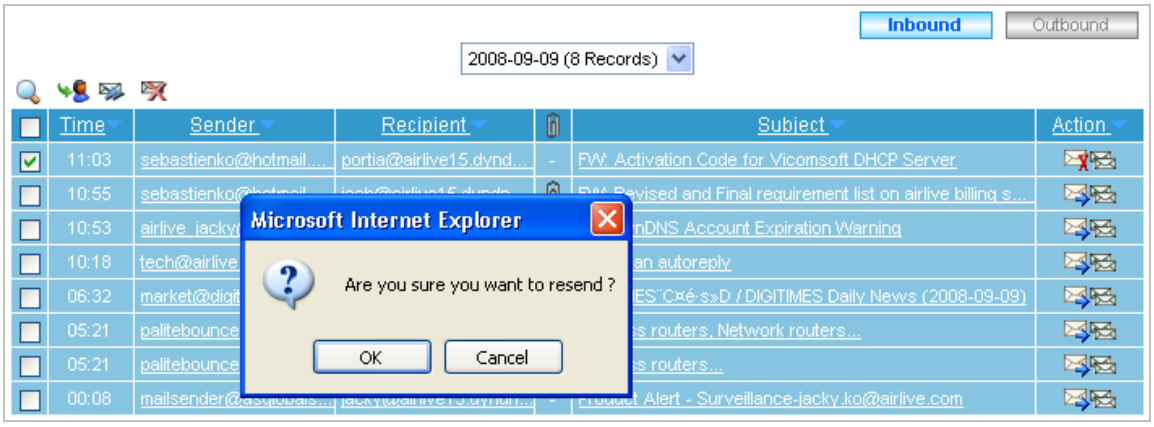


Figure 7-12 Confirming to Resend the E-Mails

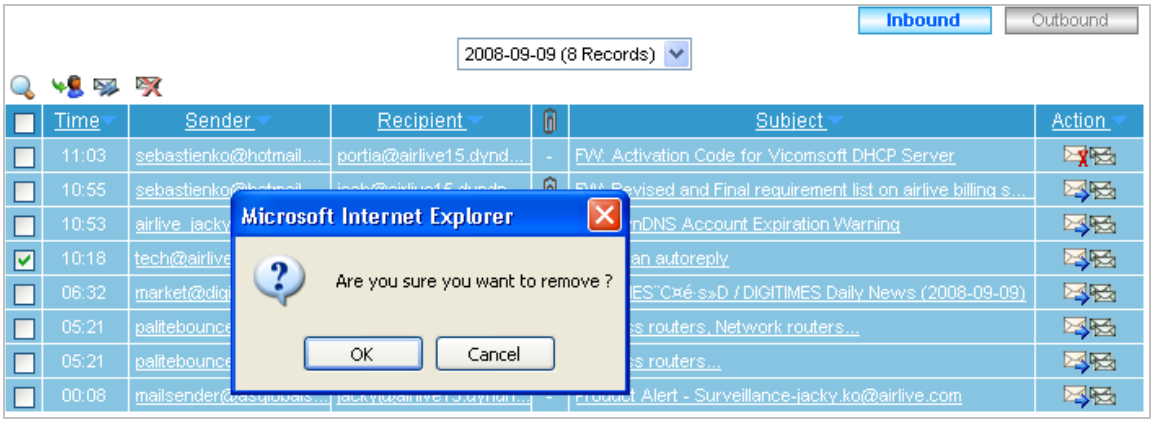


Figure 7-13 Confirming to Remove the E-Mails

Step5. When an internal user from airlive15.dyndns.org mail domain sends an e-mail to both airlive_jacky@hotmail.com and sebastienko@hotmail.com:

- If the sender's address is josh@airlive15.dyndns.org, then both of them will receive it.
- If the sender's address is portia@airlive15.dyndns.org, then airlive_jacky@hotmail.com will receive the e-mail only. E-mails that sent to sebastienko@hotmail.com will be deleted.
- A report is generated under **Mail Archive / Audit → Archive**. (Click the upper left **Outbound**). (Figure 7-14)
- Tick the boxes of desirable e-mails and click the upper left "little man" icon to retrieve.
- Type the sender's and recipient's address accordingly in the **Retrieve** window and click **OK**. (Figure 7-15)
- Tick the boxes of desirable e-mails and click the upper left "envelope-with-a-blue-arrow" icon to resend.
- Click **OK** in the dialogue box to confirm resending the selected e-mails. (Figure 7-16)
- Tick the boxes of unwanted e-mails and click the upper left "envelope-with-a-red-cross" icon to remove.
- Click **OK** in the dialogue box to confirm the deletion of selected e-mails. (Figure 7-17)

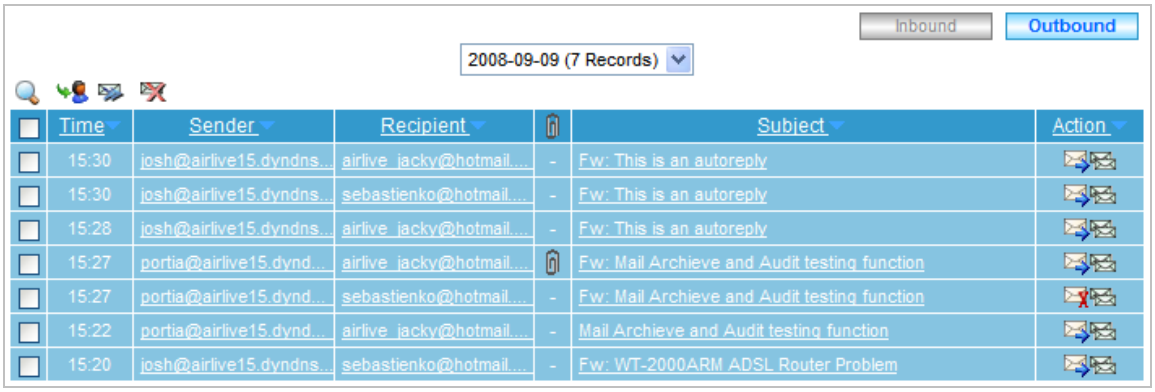


Figure 7-14 The Archive Report

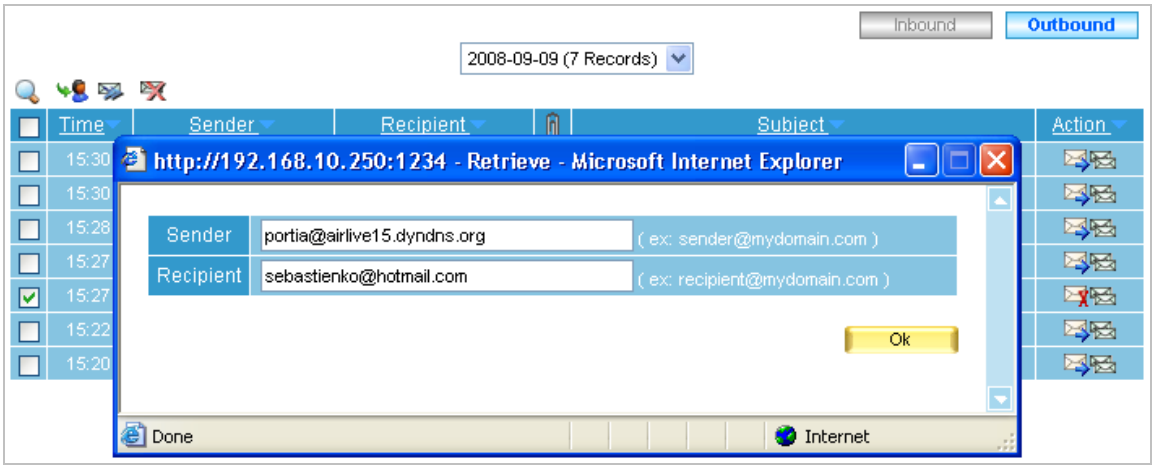


Figure 7-15 Confirming to Retrieve the E-Mails

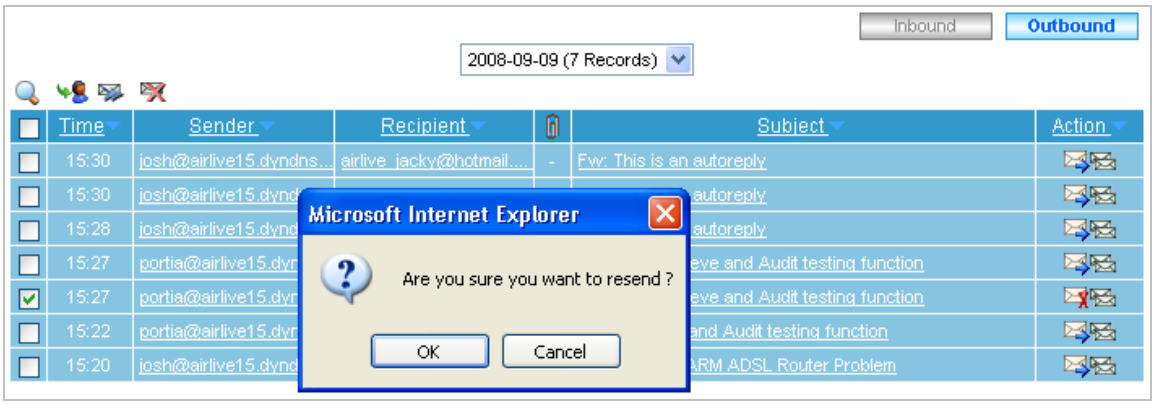


Figure 7-16 Confirming to Resend the E-Mails

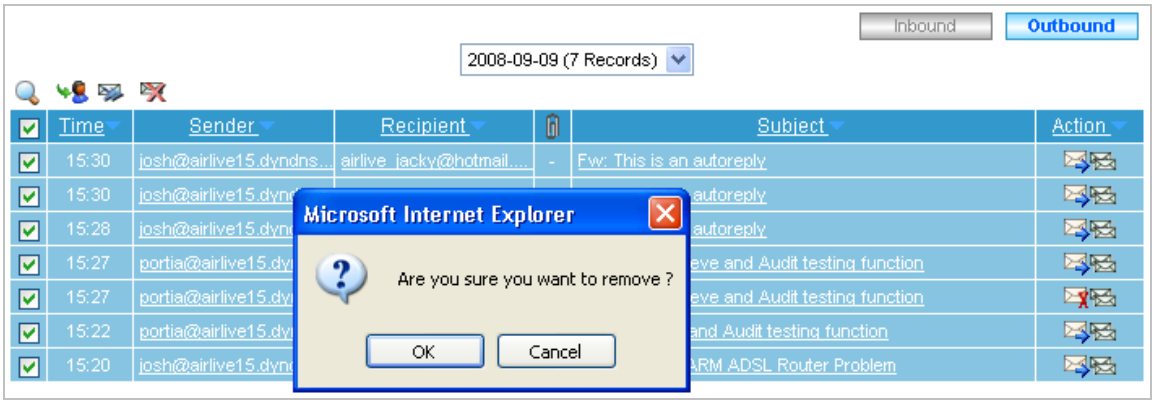


Figure 7-17 Confirming to Remove the E-Mails

The icons and descriptions of **Archive**:

Icon						
Description	Deleted	Inspect	Delayed	Archived	Copied	Passed

Chapter 8 Push Mail

ES-6000 features automatic e-mail transfer functionality. Whenever it receives an e-mail, it will instantly and actively transfer (push) the e-mail to user's mobile phone. With the help of ***Push Mail***, users may have e-mail access anytime anywhere without any complex login process.

8.1 Push Rule

Definition:

- **User Status**
  - Denotes the total amount of accounts and of how many are using push e-mail.

- **Classification**
  - Offers users a view of the accounts began with the same initial character.

- **Enabled Account**
  - The accounts of which push e-mail function are enabled.

- **Disabled Account**
  - The accounts of which push e-mail function are disabled.

- **The default rule for the selected account is**
  - Used as a default for e-mails which fail to meet the criteria of **User-defined Rule**.

- **Rule Name**
  - The name for user-defined rule.

- **Comments**
  - The description which explains the purpose of the rule.

- **Combination**
  - **And:** Only when e-mail meets all the criteria is it to be pushed.
  - **Or:** Only when e-mail meets merely one criterion is it to be pushed.

- **Action**
  - Determines whether to push e-mails to user's mobile device or not.

- **Item**
  - Available criteria for **Item** are Received, Envelope-To, From, To, Cc, Bcc, Subject, Sender, Reply-To, Errors-To, Message-ID, Date, Header, Attach File Name, and Size.

- **Condition**
  - When **Item** set as Received / Envelope-To / From / To / Cc / Bcc / Subject / Sender / Reply-To / Errors-To / Message-ID / Date / Header / Attachment Name, the corresponding **Conditions** are Contains, Does Not Contain, Is Equal To, Is Not Equal To, Starts With, Ends With, Exists, and Does Not Exists.
  - When **Item** set as Size, the corresponding **Conditions** are More Than, Is Equal To, Is Not Equal To, and Less Than.

- **Pattern**
  - Configure the **Item** and **Condition** based on **Pattern**. For example, select “From” for **Item**, “Contains” for **Condition** and then type “Josh” as **Pattern**, it is to inspect the e-mail of which e-mail address contains the keyword “Jacky”.

ES-6000 can instantly and actively transfer (push) e-mails to users’ mobile devices according to the availability of Internet access and the support in Push-IMAP protocol (also known as IMAP IDLE extension).

8.2 Push Rule Configuration

Configuring ES-6000 Device to Instantly and Actively Push E-Mails to Users' Mobile Devices

Step1. Under **Mail Management → Account Management → Setting**, set as below:

- Allocate a disk space as default capacity to each account for push e-mail storage. (The capacity allocation should be adjusted to an appropriate size, 10 MB for example, in order to avoid wasting disk space). (Figure 8-1)

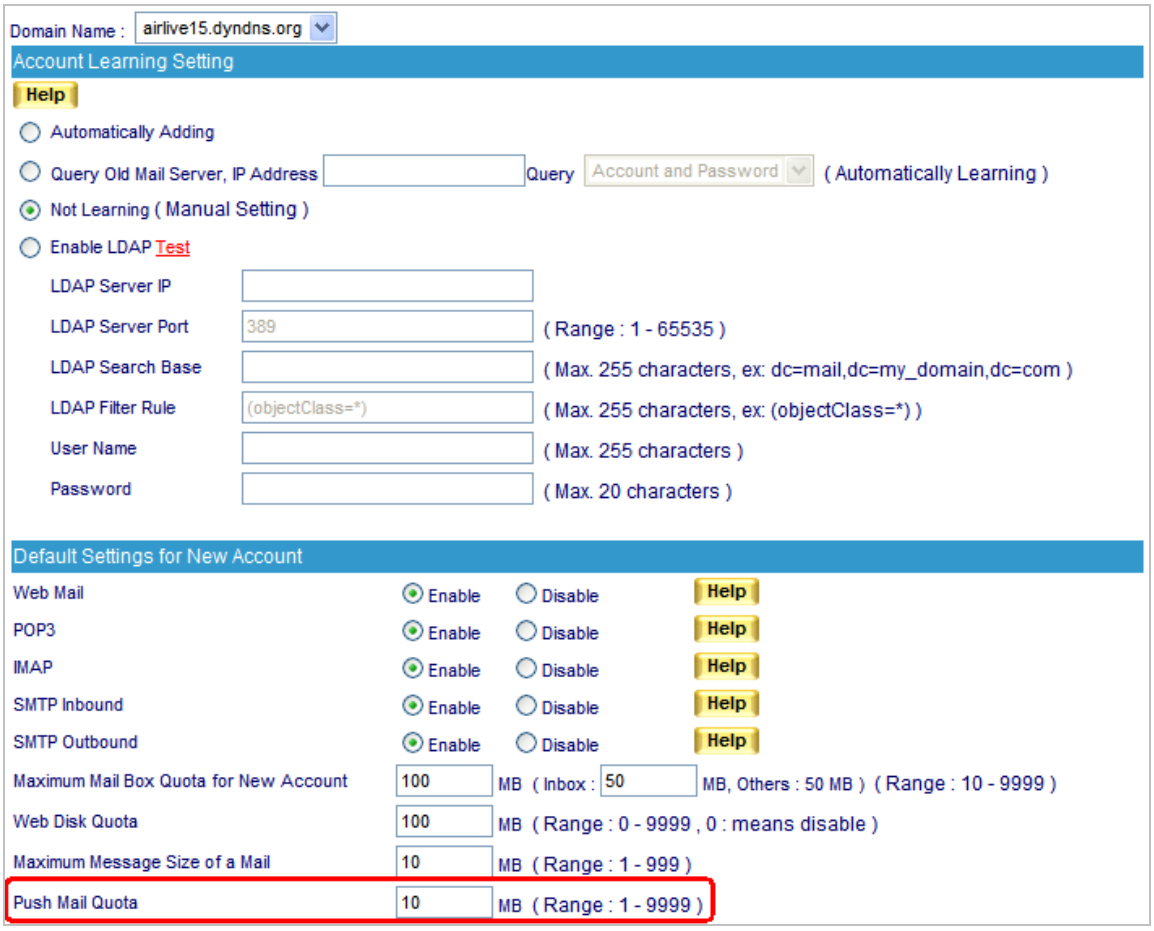


Figure 8-1 Allocating an Appropriate Storage Space to Each Push Mail Account

When ES-6000 receives e-mails dedicated to internal accounts, it will act on user-defined rules to determine whether to duplicate them to each push e-mail storage space as well as to push them to users' mobile devices.

Push e-mails will be cleaned up once the total e-mail size has exceeded the storage quota allocated for push e-mail. Nevertheless, despite the deletion of all push e-mails, the original copies remain available in each account's inbox on ES-6000 device. Users may retrieve them by using e-mail application, such as Outlook Express.

Step2. Under **Push Mail → Push Rule**, set as below:

- Click **ALL** next to **Classification** to show all accounts.
- In the **Enabled Account** table, tick unwanted account(s) and remove it to **Disabled Account** table by clicking **to Disabled Account** in the upper right corner of the table. (Figure 8-2, 8-3, 8-4)
- In the **Enabled Account** table, apply the default rule to the selected account(s) by selecting **to Push Mail** from the pull-down menu and clicking **OK** next to it. (Figure 8-5, 8-6)

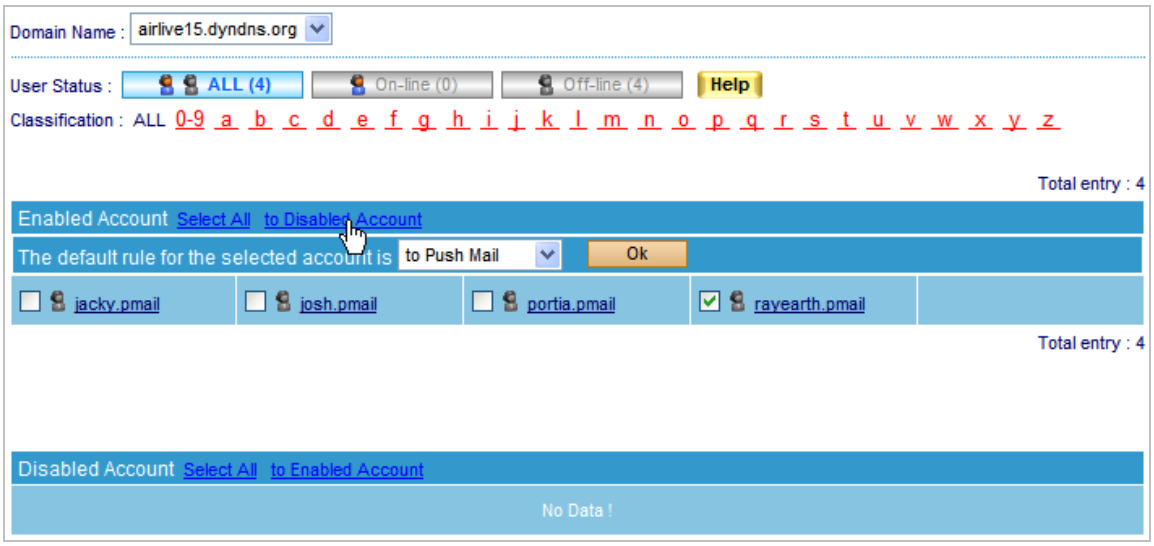


Figure 8-2 Moving Selected Accounts to Disabled Account Table

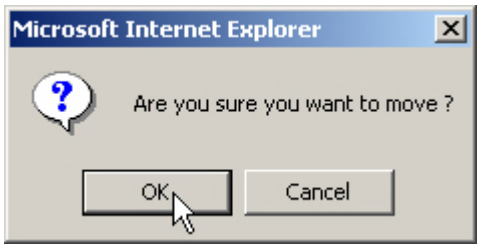


Figure 8-3 Confirming to Move Selected Accounts to Disabled Account Table

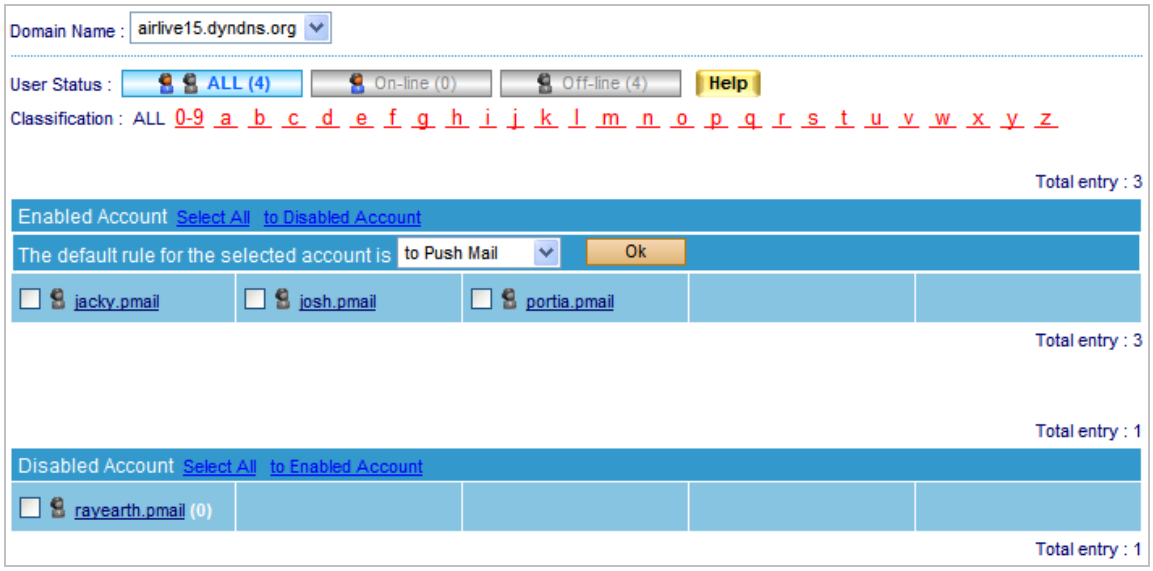


Figure 8-4 Disabling Push Mail by Moving to Disabled Account List

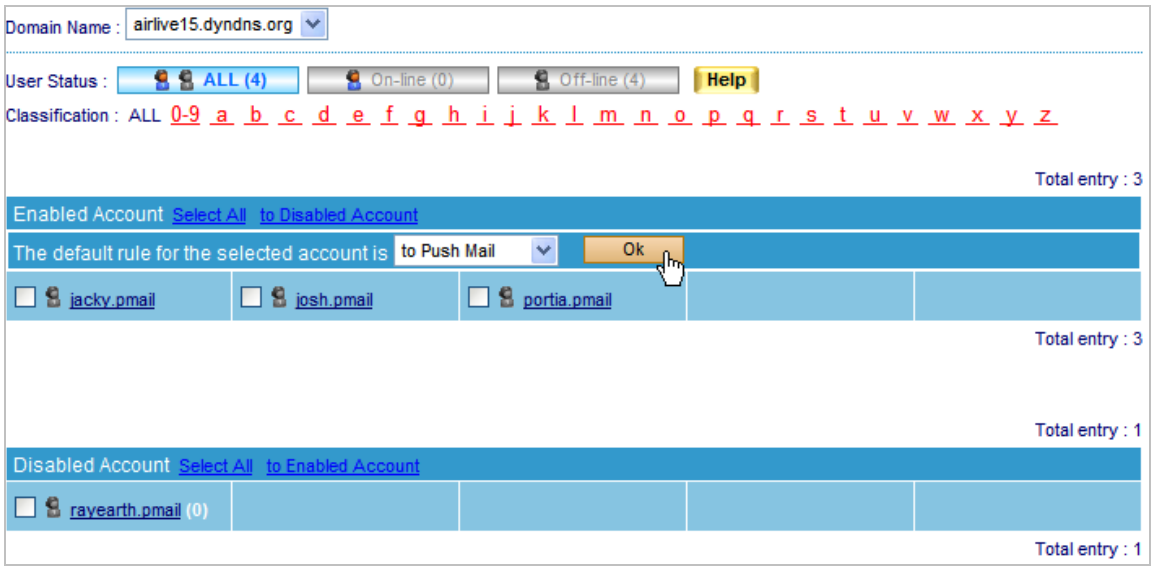


Figure 8-5 Applying Default Rule to the Selected Accounts

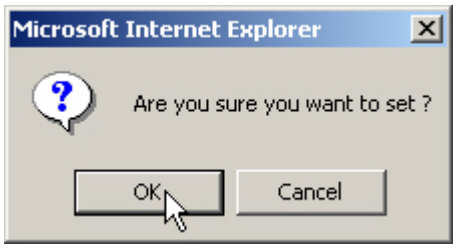


Figure 8-6 Confirming to Apply Default Rule to the Selected Accounts

Step3. Under **Push Mail → Push Rule**, set as below:

- In the **Enabled Account** table, click the desirable account to set up the user-defined rule. (Figure 8-7)
- Click **New Entry**.
- Type “Not Push” in the **Rule Name** field.
- Type “Not Push Mail” in the **Comments** field.
- Select “Or” for **Combination**.
- Select “Not Push” for **Action**.
- Select “From” for **Item**, “Contains” for **Condition** and then type “hotmail” as **Pattern**. (Figure 8-8)
- Click **OK**. (Figure 8-9)

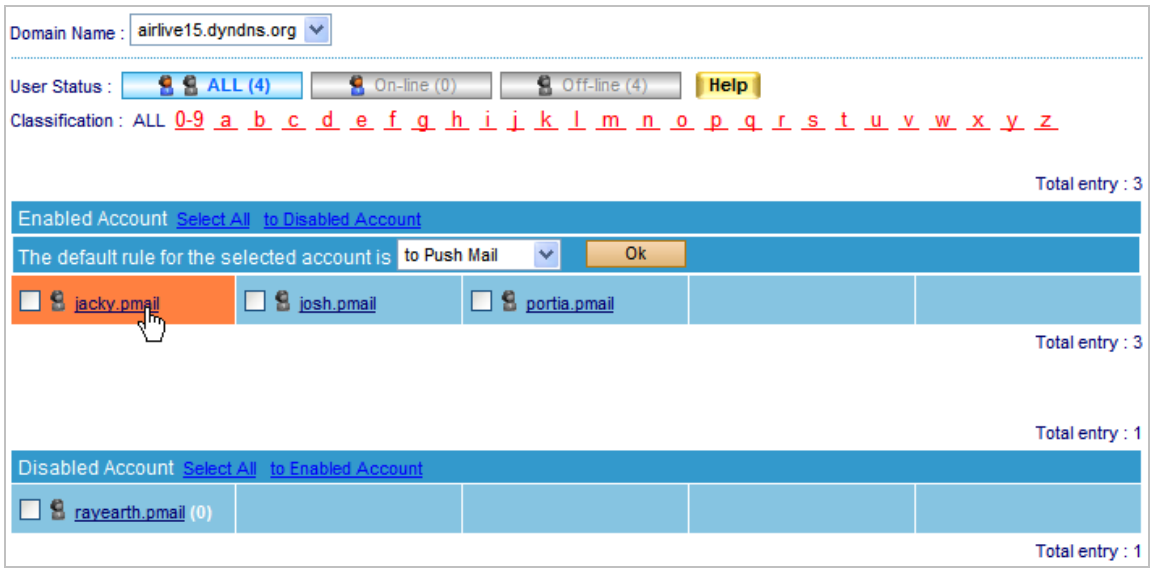


Figure 8-7 Clicking the Desirable Account to Create User-defined Rule

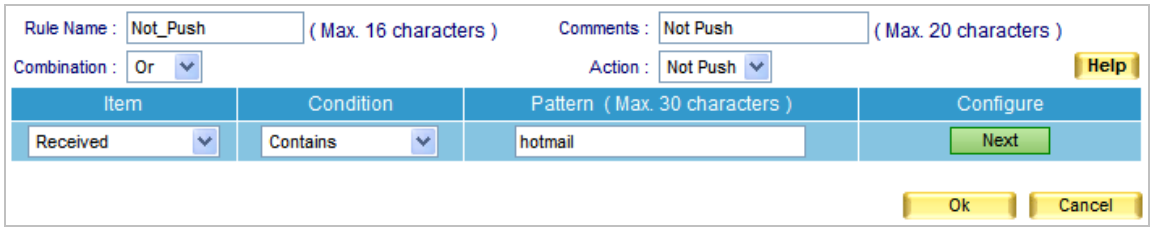


Figure 8-8 Creating a User-Defined Rule

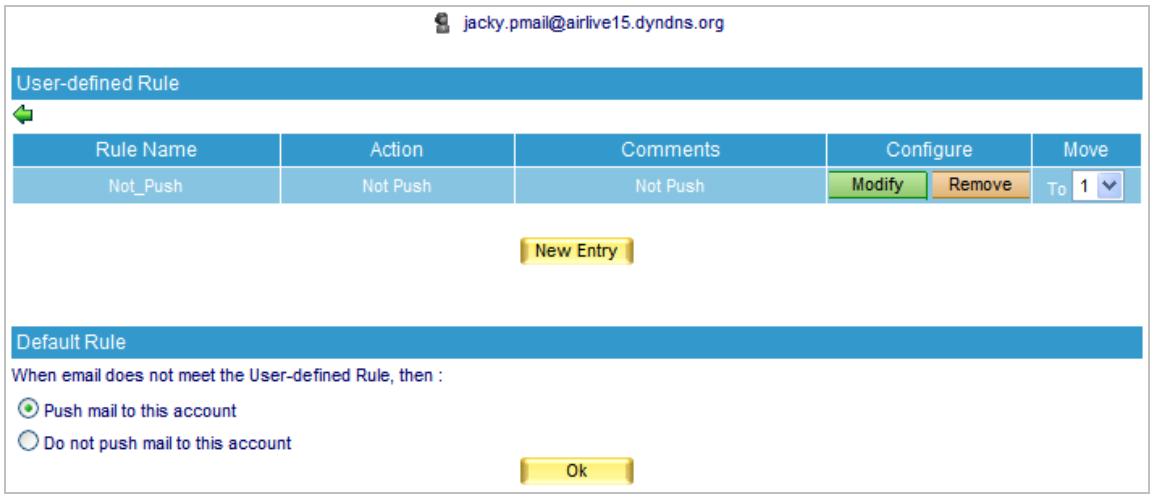


Figure 8-9 User-Defined Rule Created

Whether an e-mail, which has been scanned for virus and inspected for spam, will be pushed to the user's mobile device depends on individual user-defined rule.

Right-click any e-mail in your Outlook Express, and then click **Properties** on the pop-up menu. After that, click **Details** tab for information on e-mail header of which can be used as reference while configuring the **Item** and **Condition** of a **User-defined Rule**. (Figure 8-10)

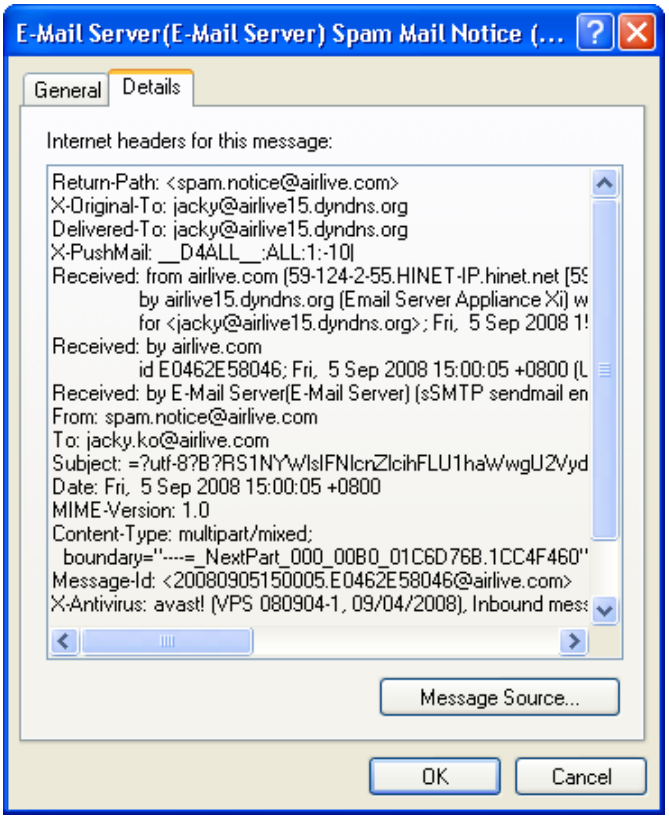


Figure 8-10 The Detailed Information of an E-Mail

Step4. Given that ES-6000 receives e-mails dedicated to an internal account, such as jacky@airlive15.dyndns.org, then: (Based on STEP 3, e-mails from hotmail will not be pushed.)

- Log onto the Internet through a mobile device.
- Use IMAP4 protocol to retrieve e-mails dedicated to jacky@airlive15.dyndns.org.
- Log on with your push e-mail account, such as "jacky.pmail", and password.
- The on-line status will be indicated under **Push Mail → Push Rule**. (Figure 8-11)
- E-mails will immediately be pushed to Reggie's mobile device as long as push e-mail is activated on the mobile device. (Figure 8-12)
- Reading e-mails on a mobile device. (Figure 8-13, 8-14)

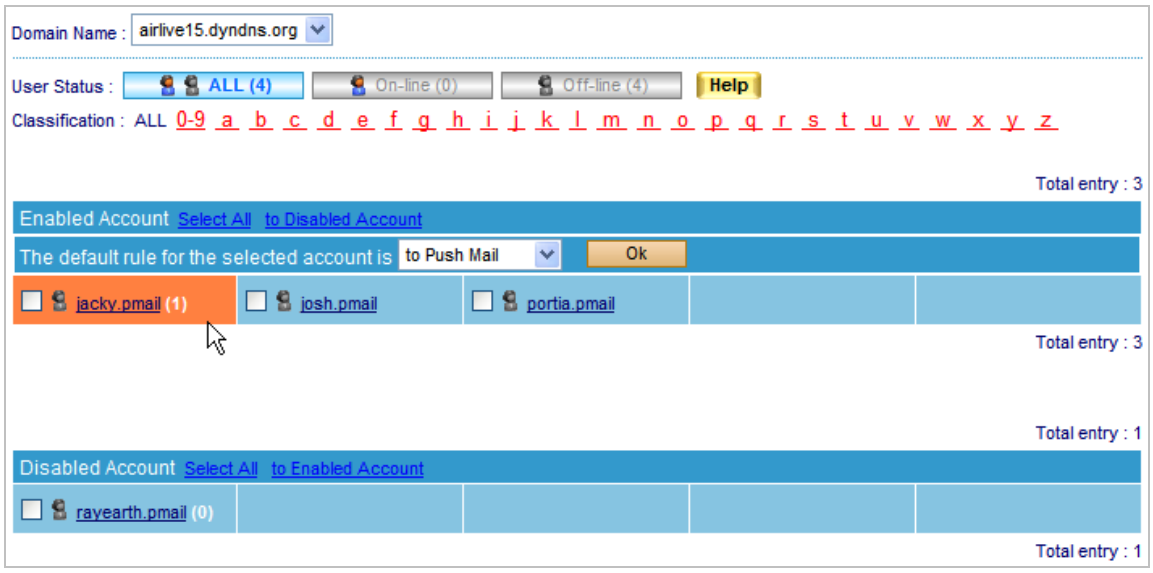


Figure 8-11 A Message Arrives at Reggie's Account

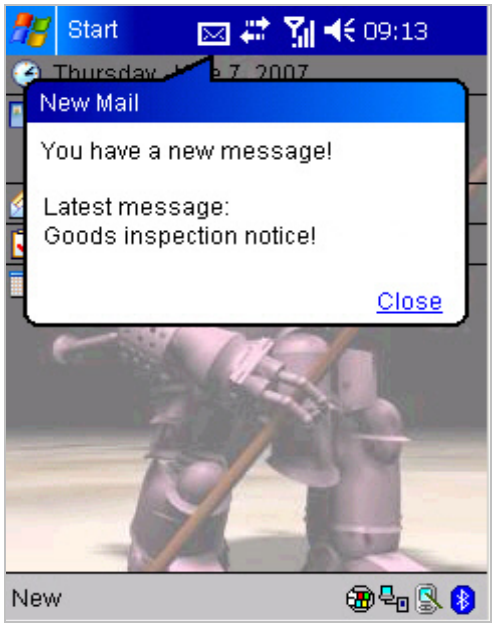


Figure 8-12 An E-Mail Pushed to a Smartphone

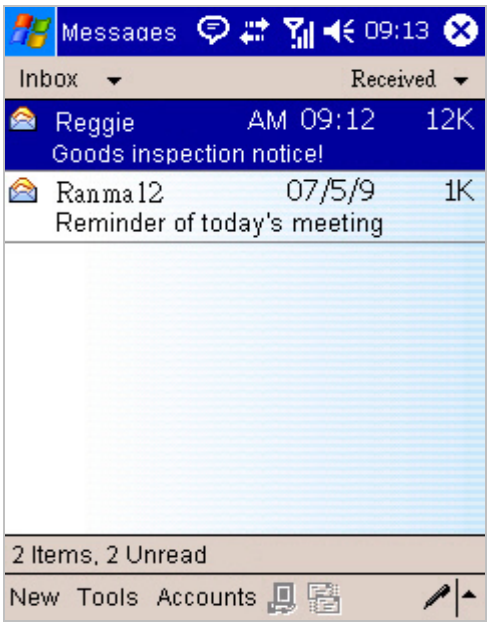


Figure 8-13 An E-Mails Shown on a Smartphone

Figure 8-14 Reading an E-Mail

The icons and descriptions of **Push Mail**:

User / Connection Status:

Icon				
Description	Off-line	On-line	Off-line, Push Mail not supported	On-line, Push Mail supported

To enable push e-mail, configure both the device and your mobile device. Follow the steps below and it will help you with the setting of push e-mail on your mobile phone:

1. **Basic requirement: Internet access on your mobile phone**
   First and foremost, the phone must be a 3G phone or able to access the Internet in any means, such as GPRS or Wi-Fi. Only when your phone meets one of the mentioned above you may proceed to the rest steps. If you are already one of the cases, you could start configuring the connection setting on your mobile phone.

2. **E-mail settings:**
   Accordingly enter the username (it is your account name followed by ".pmail", e.g., "jacky.pmail"), password, e-mail address, incoming server and outgoing server (enter the registered domain name for both incoming and outgoing servers)

3. **Connection type:**
   It determines what protocol the incoming server will be using. In general, POP3 protocol has been widely used on e-mail service. Nevertheless, it requires manual operation to receive e-mails. In response, push e-mail employs a more convenient protocol, **IMAP**, as an approach to automatically receive e-mails.
   Note: Due to the variation among brands and models, some phones demand a manual operation before the push e-mail to act on its own.

8.3 Push Mail Example

- Below is an example for your reference: (Mobile phone: Nokia E65; Telecom provider: Chunghwa Telecom).
  - Confirm the support for Internet access on your mobile phone.
  - Go to the e-mail setting screen, in this case, it is **Menu → Messag. → Inbox**, press **Options** at left-corner of screen, and select **Settings** function. (Figure 8-15, Figure 8-16, Figure 8-17)
  - Enter **E-mail** function and press **Options** to select **New mailbox**. Press any key to start the **Mailbox setup wizard** as following setting: (Figure 8-18, Figure 8-19, Figure 8-20)
    1. Select **IMAP4**. (Figure 8-21)
    2. Fill in the IP address. In this case we input jacky@airlive15.dyndns.org. (Figure 8-22)
    3. Fill in the IP address or domain name of Incoming mail server. Ex. airlive15.dyndns.org. (Figure 8-23)
    4. Fill in the IP address or domain name of Outgoing mail server. Ex. airlive15.dyndns.org. (Figure 8-24)
    5. Specify the mailbox name, and finish the setting. (Figure 8-25)
  - Select Mailbox → Connection settings → Incoming e-mail to fill in user name and password. (Figure 8-26, Figure 8-27, Figure 8-28, Figure 8-29)
  - Select Mailbox → Connection settings → Outgoing e-mail to fill in user name and password. (Figure 8-30, Figure 8-31)
  - Start the connection to receive mail from ES-6000. (Figure 8-32, Figure 8-33)

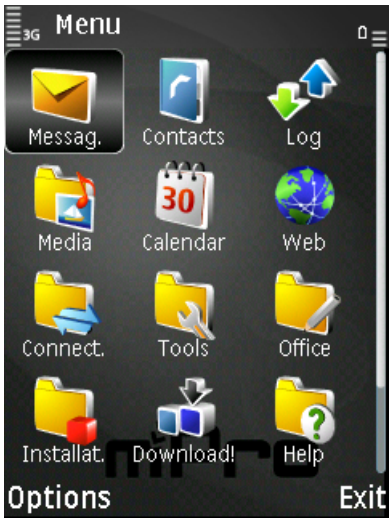


Figure 8-15 Select Messag. on Menu

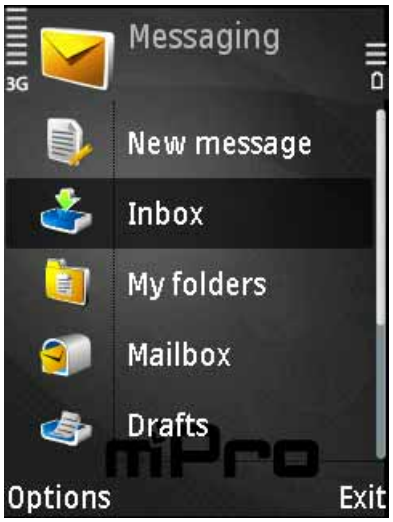


Figure 8-16 Press Options

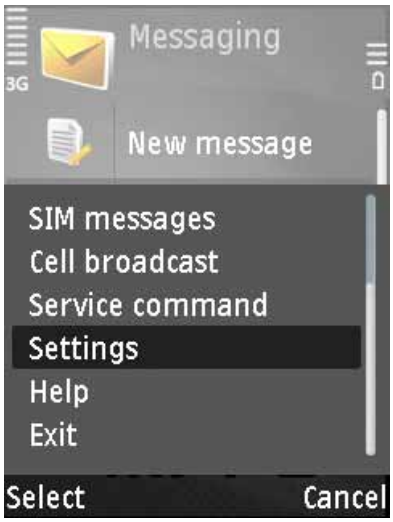


Figure 8-17 Select Settings

Figure 8-18 Select Email

Figure 8-19 Create new mail box

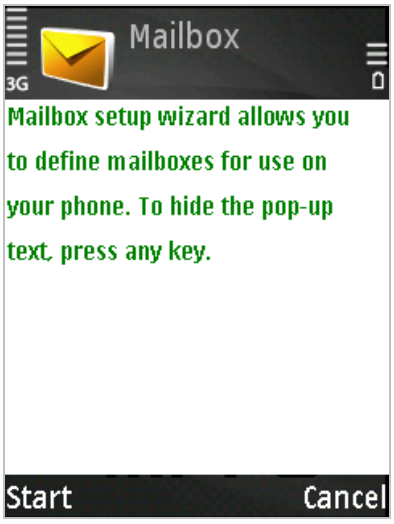


Figure 8-20 Wizard

Figure 8-21 Select IMAP4 protocol

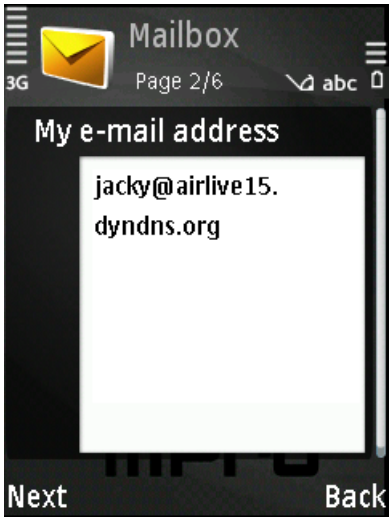


Figure 8-22 Enter Mail address

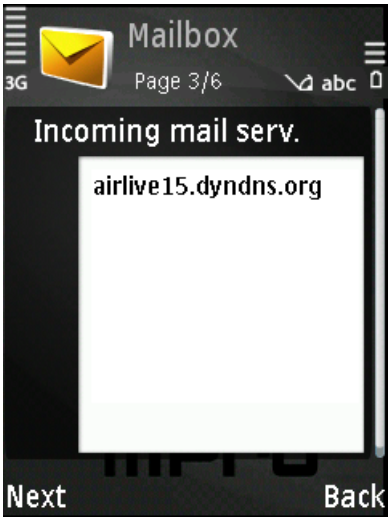


Figure 8-23 Incoming Mail Server

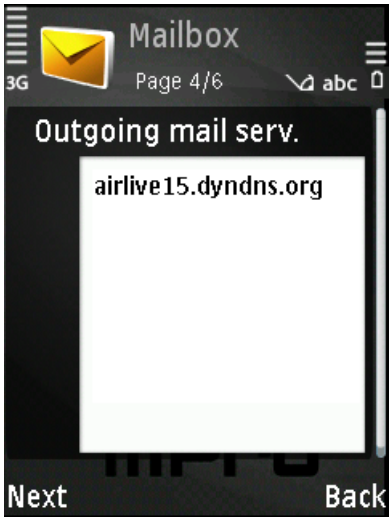


Figure 8-24 Outgoing Mail Server

Figure 8-25 Define Mailbox

Figure 8-26 Edit else setting

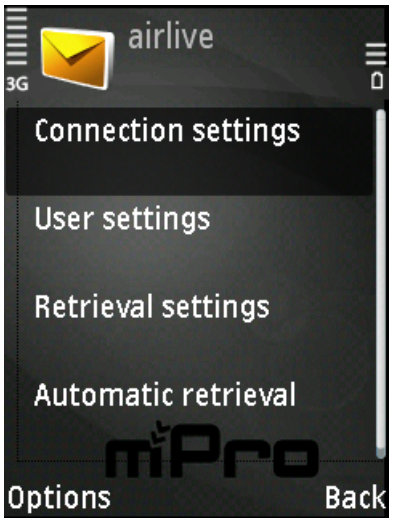


Figure 8-27 Edit Connection setting

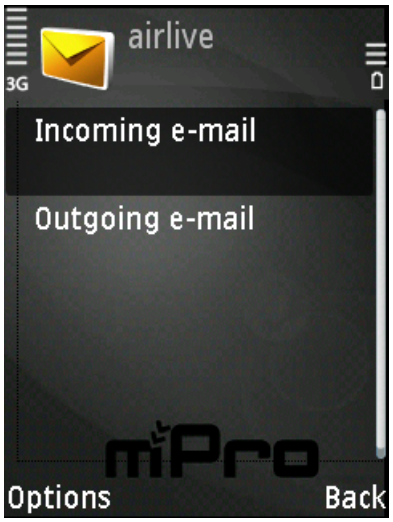


Figure 8-28 Enter Incoming setting

Figure 8-29 Edit Incoming setting

Figure 8-30 Enter Outgoing setting

Figure 8-31 Edit Outgoing setting

Figure 8-32 Connect to Mail server

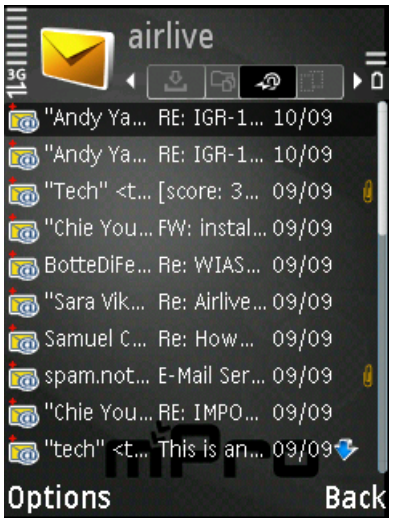


Figure 8-33 Receive and read mail

Chapter 9 Remote Backup

The archived E-mails can be periodically (according to the time setting) transferred to the assigned location to solve the storage space limit and audit time limitation.

9.1 Backup Setting

Definitions:

- **Connection Status of Remote Hard Disk**.
  - The remote hard disk status has the information of connection status, disk space for backup, and hard disk utilization.

- **E-mail Setting**
  - Sending E-mail to inform the recipient of backup completion.

- **Backup Setting**
  - The setting for assigning the backup location and the executing time.

- **Backup Immediately**
  - This can calculate how much disk space the data in a specific duration will take up and provide a real-time backup.

9.2 Browse Setting

Definitions:

- **Connection Status of Remote Hard Disk**
  - The remote hard disk has the information of connection status. (e.g. read / write access)

- **Browse Setting**
  - The setting for assigning the backup location.

The **Browse Mail** function will not be available unless the **Browse Setting** has been configured at first.

9.3 Browse Mail

- Available search criteria are date, sender, recipient, subject, content, action, attached, and non-attached.
  - Set as below :
    1. **Recipient**, enter the keywords or phrases. (For example, Jacky, jacky@airlive.com)
    2. Enable to select the date setting.
    3. **Action**, select All.
    4. **Attached File**, select all.
    5. Click **Search**. (Figure 9-1)

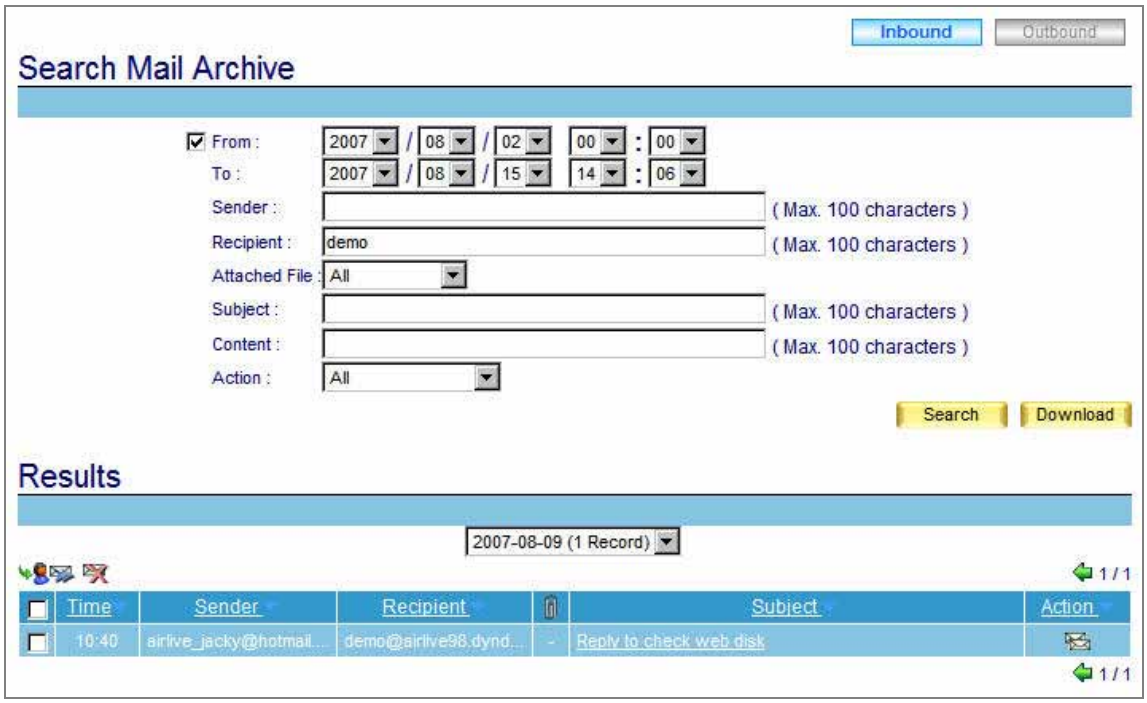


Figure 9-1 Search for the specific mail

9.4 Mail Backup Example

Transfer Archived E-mails to the Assigned Backup Location and Provide Mail Browsing Service

Step1. In **Remote Backup → Backup Setting**, please refer to the figure below to set up. (Figure 9-2)

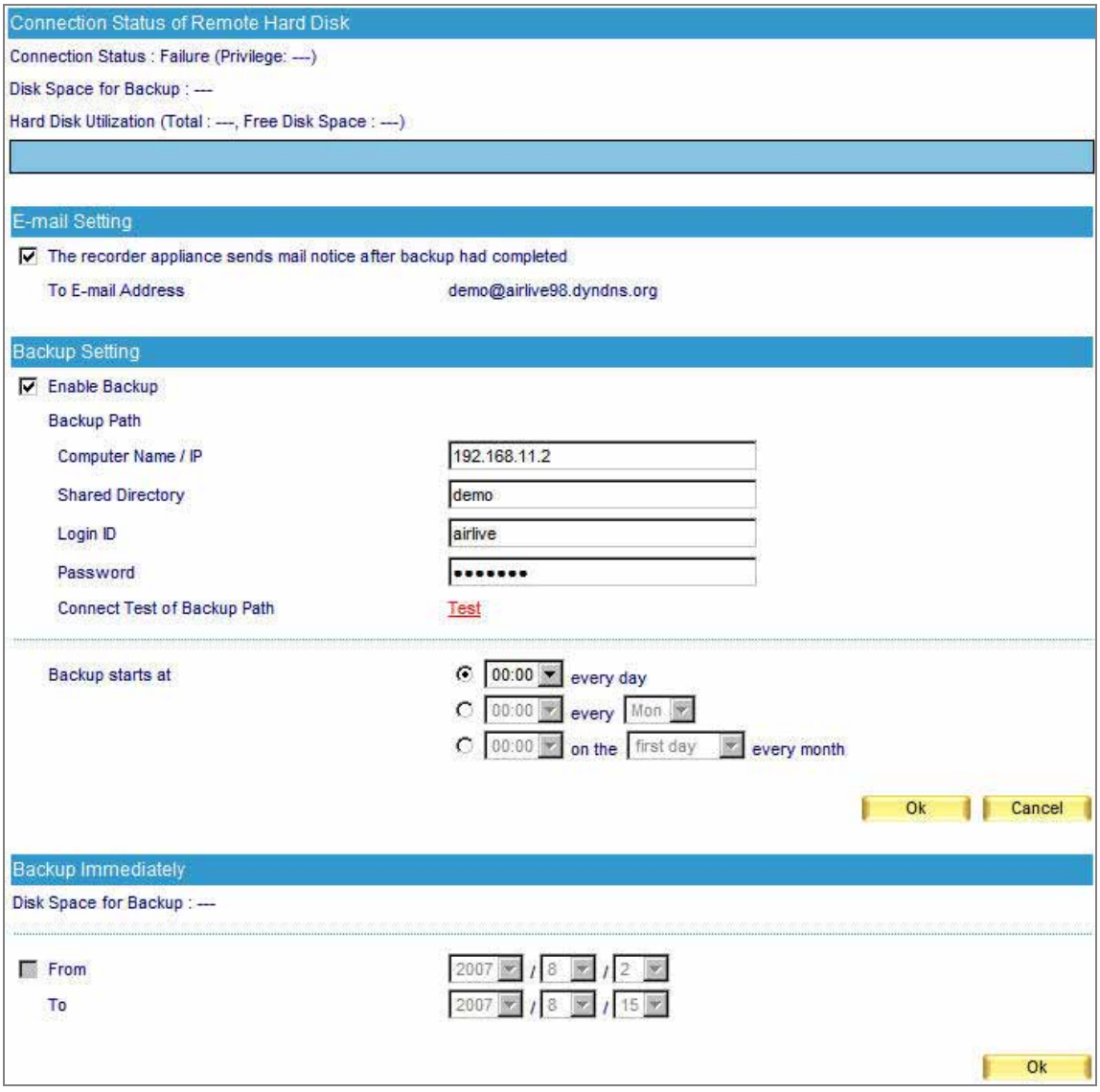


Figure 9-2 The remote backup setting

It is easy to create remote backup server. Just to share a folder of internal PC with read/write access right, and define a specific user name and password for the access right. If the folder can be found in My Network Places, it can also be the remote backup server to store ES-6000 mails record.

Step2. Check up the backup path and available disk capacity. (Figure 9-3)

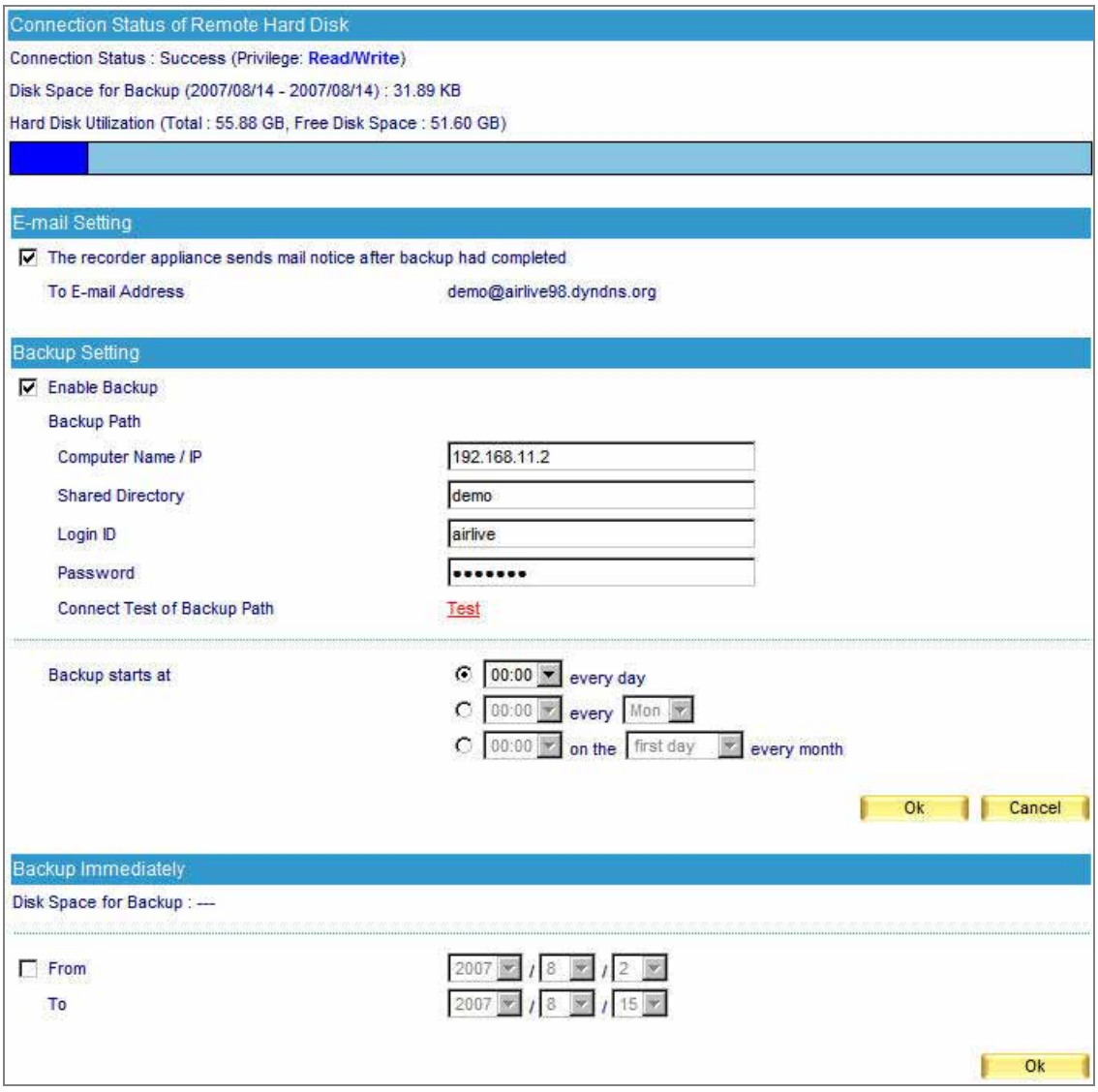


Figure 9-3 Check up the available disk capacity for backup

The archived E-mails of a specific duration can be exported. (Figure 9-4)

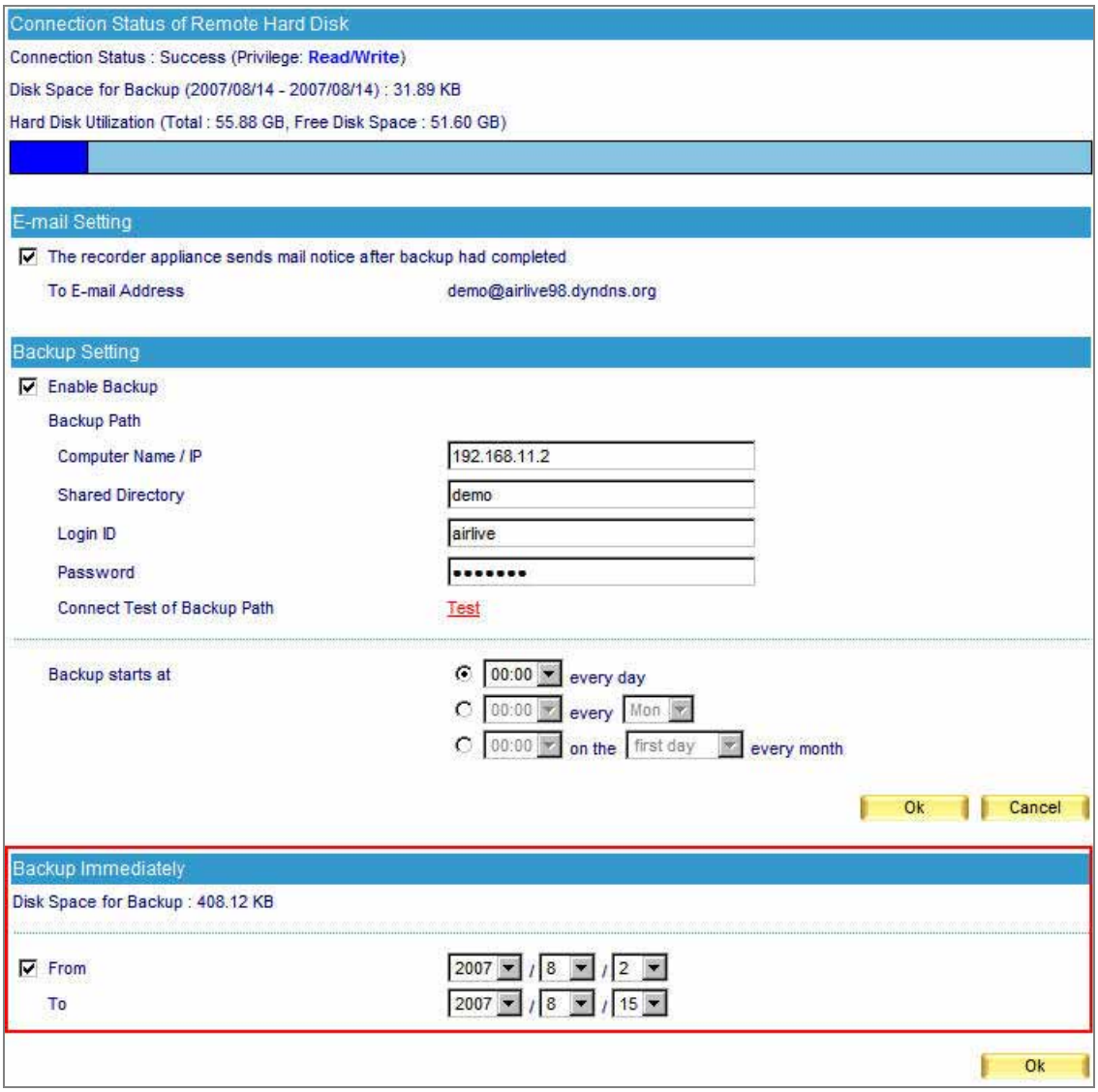


Figure 9-4 The setting of backup immediately

Step3. In **Remote Backup → Browse Setting**, set as below. (Figure 9-5)

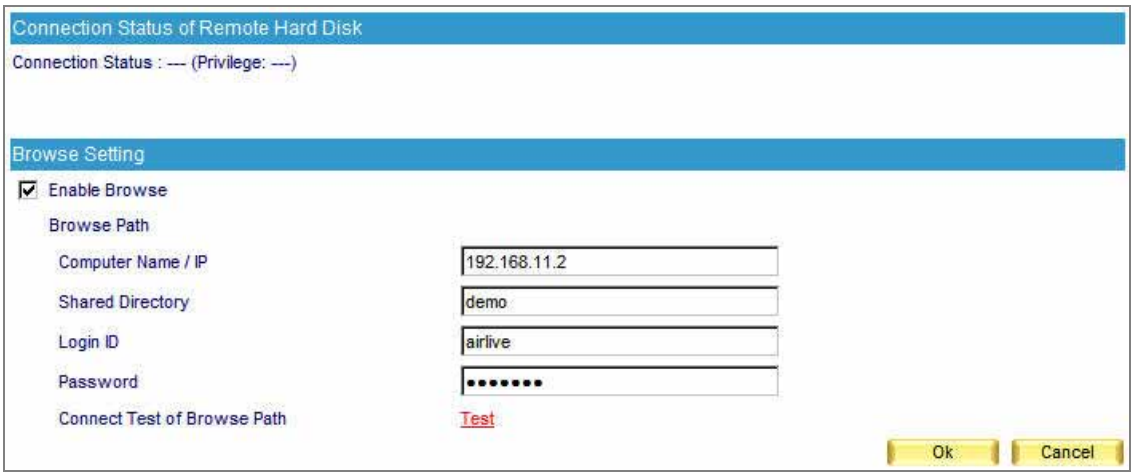


Figure 9-5 The browse setting

Step4. Check up the connection status. (Figure 9-6)

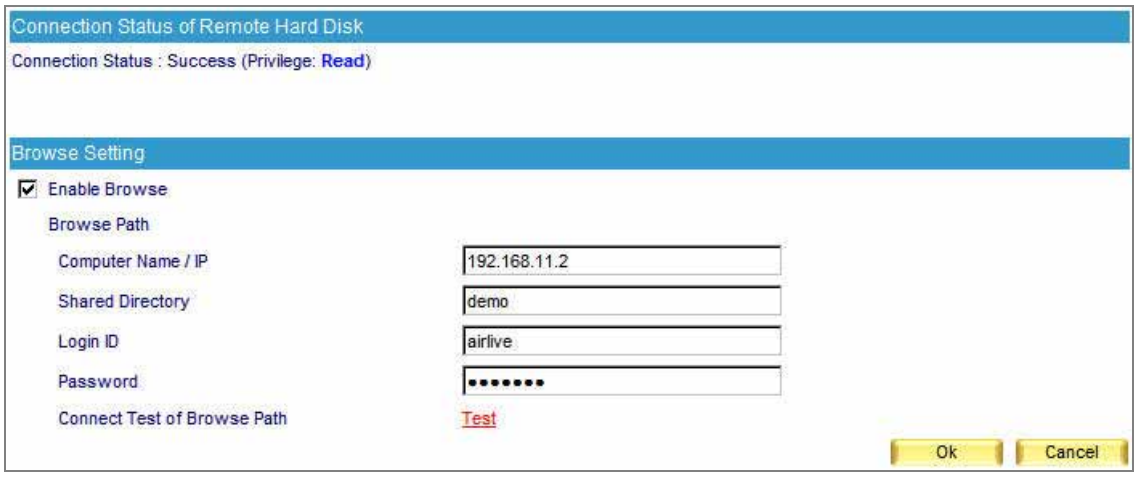


Figure 9-6 Check up the connection status

Step5. When the mails are archived, they will be transferred to a NAS or file server according the remote backup setting.

- A mail report shown in **Remote Backup → Browse Mail**. (Figure 9-7)
- To retrieve, check the box corresponding to the E-mails to be retrieved and click the retrieve icon on the upper left.
- Then a **Retrieve** window appears. Next, apply both the sender and recipient E-mail address and click **OK**. (Figure 9-8)
- To remove, check the box corresponding to the E-mails to be deleted and click the remove icon on the upper left.
- Click **OK** in the confirmation window to confirm the deletion of selected E-mails. (Figure 9-9)

Figure 9-7 Browsing the remote backup e-mails

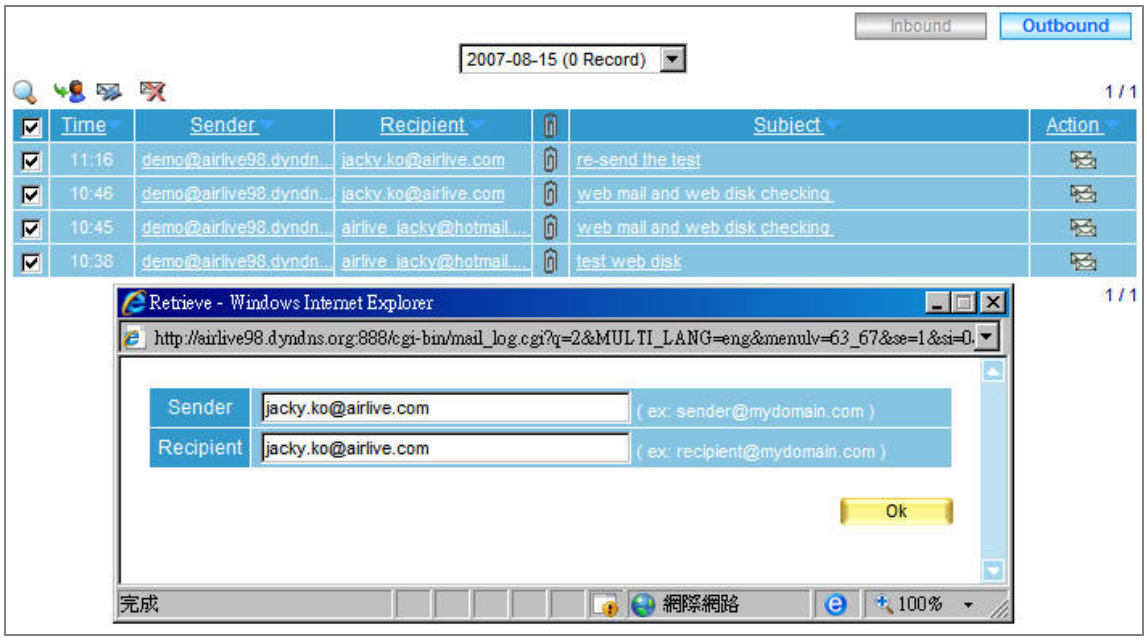


Figure 9-8 The retrieve window

Figure 9-9 Confirm to delete backup E-mails

Chapter 10 HA

ES-6000 features **High Availability** function. While there are two ES-6000 devices available onsite, **High Availability** enables them not only to synchronize to each other but also to substitute for the malfunction one in just no time. It ensures the enterprise an always connecting Internet access.

Definition

- **High Availability Setting**
  - This can synchronize the system configuration and firmware version between Master and Backup devices.

- **Master / Backup Status**
  - It shows the connection and synchronizing status of Master and Backup devices.

Example: To Deploy a High Availability Environment

Step1 Power off and deploy Master and Backup ES-6000, connect both port1 to switch. (Figure 10-1)

Step2 Connect Master ES-6000 port 2 (HA port) to Backup ES-6000 port 2.

Step3 Don't power on Backup ES-6000 before you finish the configuration of Master ES-6000.

Step4 Change interface IP address of Master ES-6000 to differ with default IP 192.168.1.1, ex. 192.168.1.2 (Figure 10-2)

Step5 Change Management IP of Master ES-6000 to differ with default IP 192.168.2.1, ex. 192.168.2.2. (Figure 10-3)

Step6 Make sure the Master ES-6000 and Backup ES-6000 port 1 and port 2 are connected properly.

Step7 Power on the Backup ES-6000, then both ES-6000 will synchronize data and setting. (Figure 10-4, 10-5)

Step8 It needs to take 10 hours to synchronize the data and setting. (Figure 10-6)

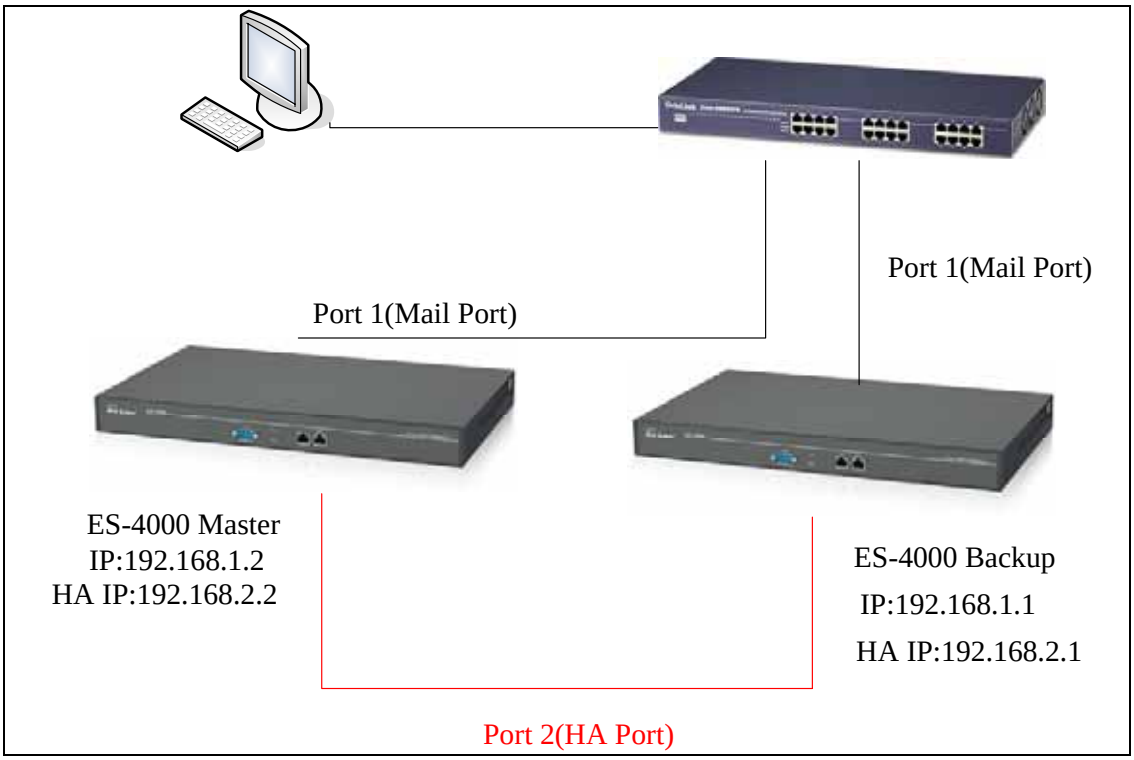


Figure 10-1 The Master device deployment under High Availability mode

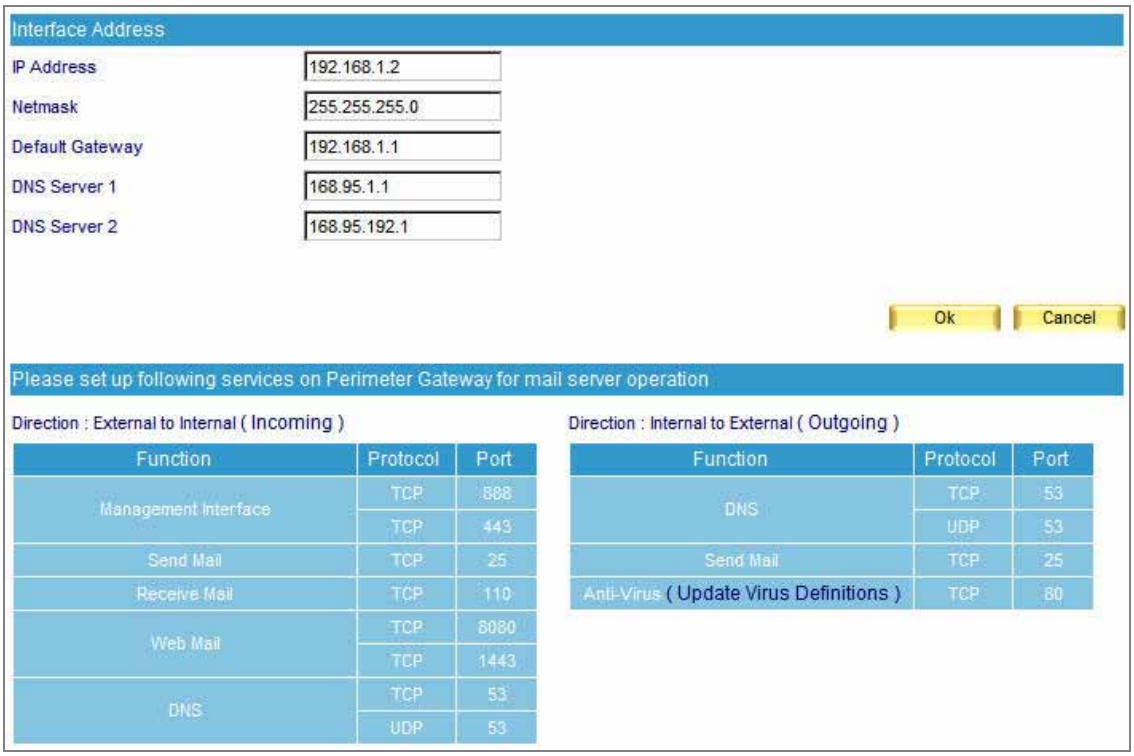


Figure 10-2 Change interface IP of Master ES-6000

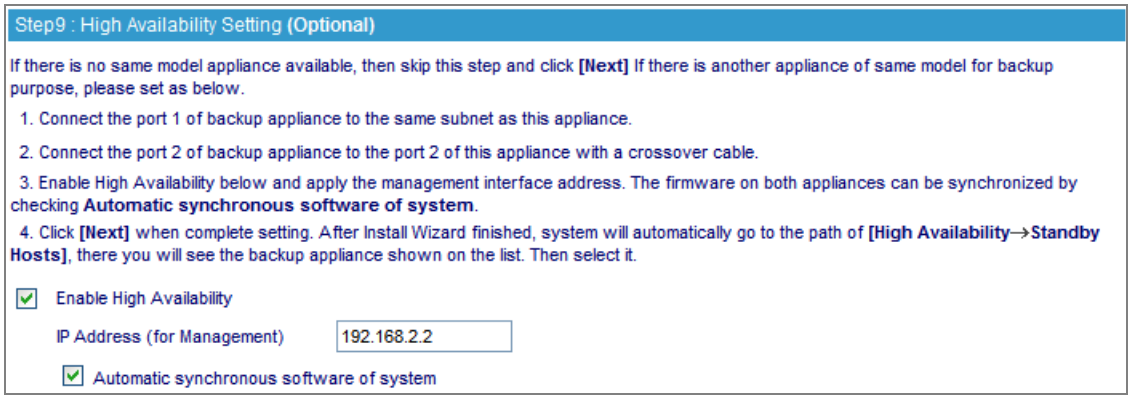


Figure 10-3 Change Management IP of Master ES-6000

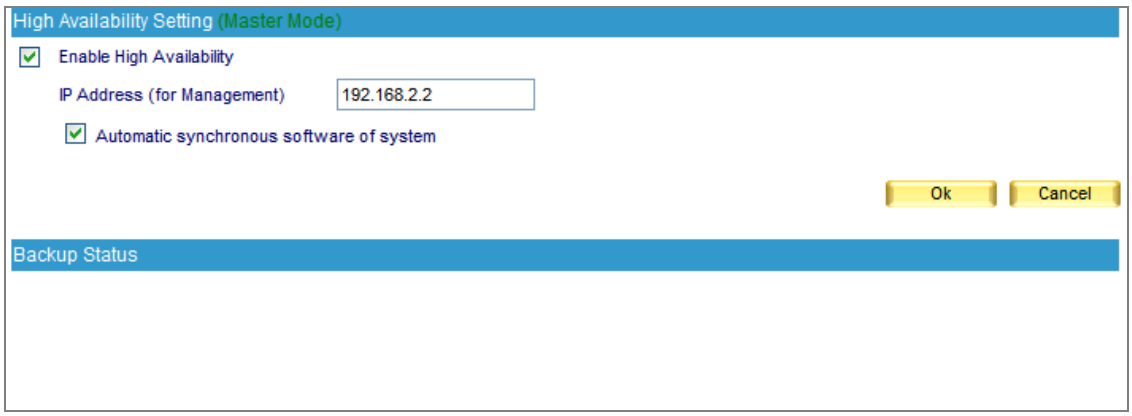


Figure 10-4 Under the process to synchronize both ES-6000's data

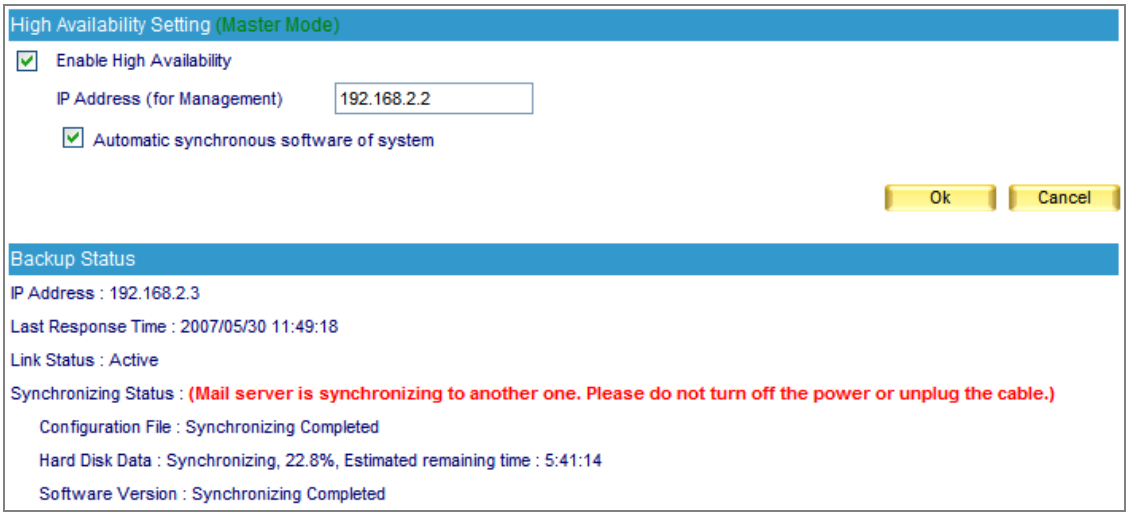


Figure 10-5 Under the process to synchronize both ES-6000's data

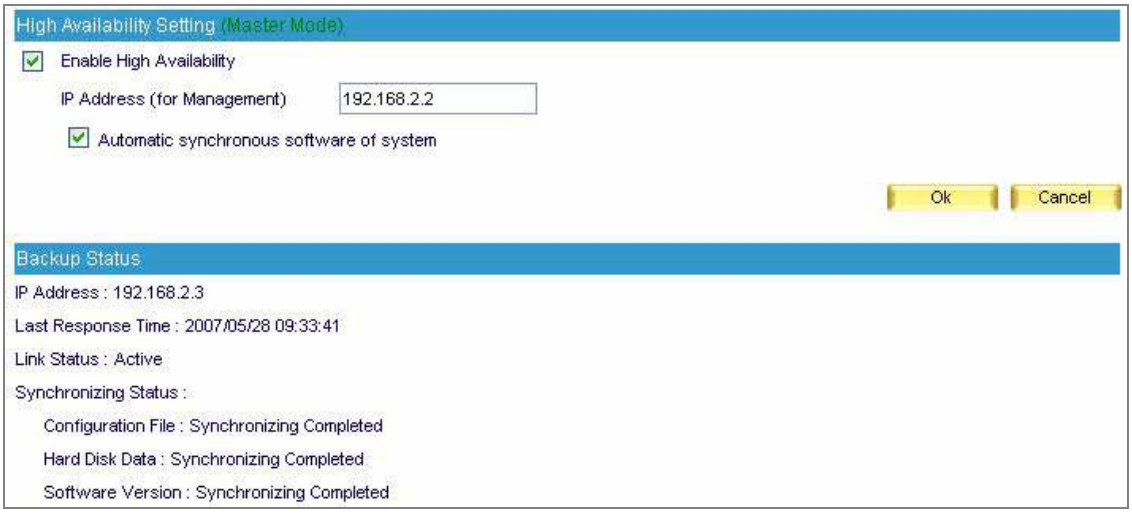


Figure 10-6 Complete High Availability function

After the completion of deployment, the two devices will immediately start synchronizing the system settings. If the process is interrupted by certain reason, then the Backup device has to be removed from the deployment. After that, reset it to factory default and format its hard disk. Next, repeat the steps to complete the synchronization. The synchronizing status is available under **High Availability → Setting**.

To avoid synchronizing error, please make sure the Master device functions properly, which means the machine is functioning and the management interface is accessible, before turning on the Backup device.

The device build-in hard disk is replaceable. However the replacement must be equal to or larger than 500 GB or else anomalous data losing may occur as a result.

Notes:

1. After the deployment finished, the Backup device will substitute for Master device once it breaks down. (The two devices detect each other for status through Port1 and Port 2 connection.)
2. When there is any data or firmware version variation between the two devices, the synchronization will immediately function through the Port 2. (Figure 10-7)

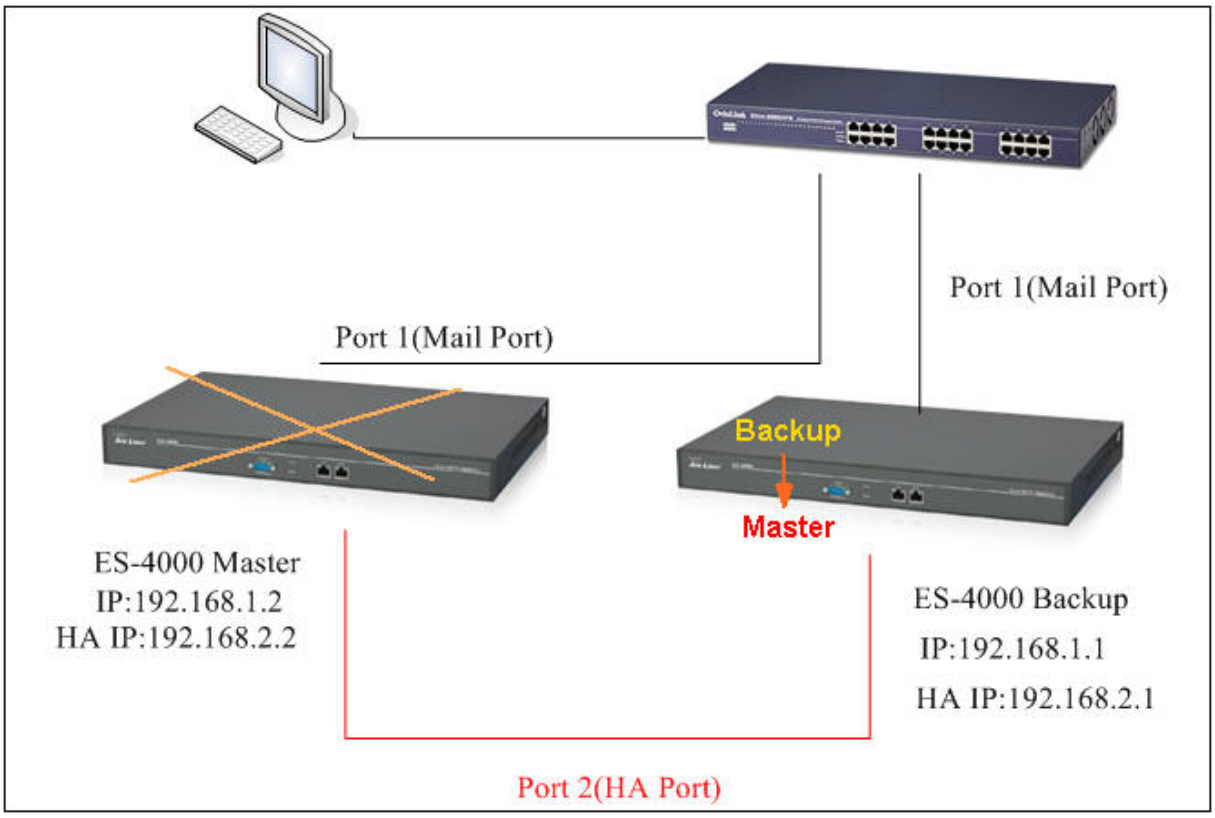


Fig. 10-7 An illustration of how High Availability works

When the Port 2 is broken or the connector is loosened, it only ceases the function of synchronization instead of triggering it off.

Chapter 11 DNS Setting

Generally speaking, DNS server is either set up by an IT company or set up by oneself. ES-6000 has the function of resolving domain name which enables user to set up a DNS server on user's own without any expanded cost. While setting up DNS, please direct the registered domain name to the ES-6000's IP address beforehand. (All types of domain name need to be resolved by a DNS server, whether it's an address type or a mail exchanger one.)

In this chapter, it will walk you through **DNS Setting** with detailed utilization description.

11.1 DNS Setting

Definitions:

- **Domain Name**
  - It refers to a website address that user applies from ISP. An IP address like 198.68.20.78 is not easy for computer users memorizing, therefore, the domain names intend to replace the figure-pattern addresses with meaningful letter-pattern ones, such as www.airlive.com.
  - The website address is composed of two parts, host name and domain name. Web browsers type address like www.yahoo.com to log onto its webpage while it's physical IP is 66.218.71.84. And DNS server is the one who plays the role of mapped domain name and physical IP address together.

- **Enable DNS Zone**
  - Allows users to activate DNS and set up the address mapping policies. (Figure 11-1)

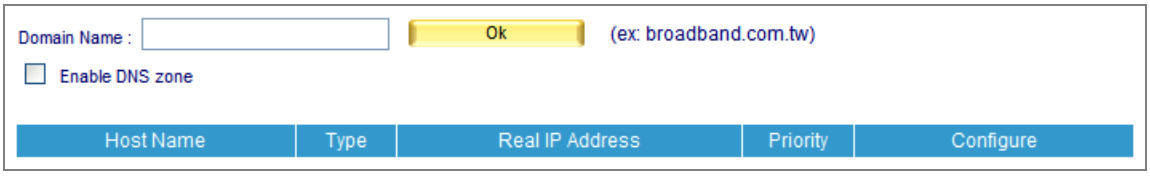


Figure 11-1 DNS setting

- **DNS Configuration**
  - Foremost, register the IP address on IDNs (International Domain Names) official website.
    1. Then register airlive.com as domain name
    2. Supposed that IP segment are given as follow:
       61.11.11.10 ~ 61.11.11.14
       211.22.22.18 ~ 211.22.22.30
    3. Set up primary host name server as:

Host Name: dns1.airlive.com

IP Address: 61.11.11.11

Set up secondary host name server as:

Host Name: dns2.airlive.com

IP Address: 211.22.22.22

- **Select Type**
  - It is divided into three types, namely **Address** (**A**), **Canonical NAME** (**CNAME**) and **Mail eXchanger** (**MX**).

11.2 A (Address)

This is used to map up IP addresses and domain names.

Ex. Build up the mapping between domain names and IP addresses. (Table 11-1, Figure 11-2)

Domain Names	Type	IP Address
host1.airlive.com	A	61.11.11.12
host2.airlive.com	A	61.11.11.13
host2.airlive.com	A	211.22.22.23

Table 11-1 Mapping table of domain name and IP address

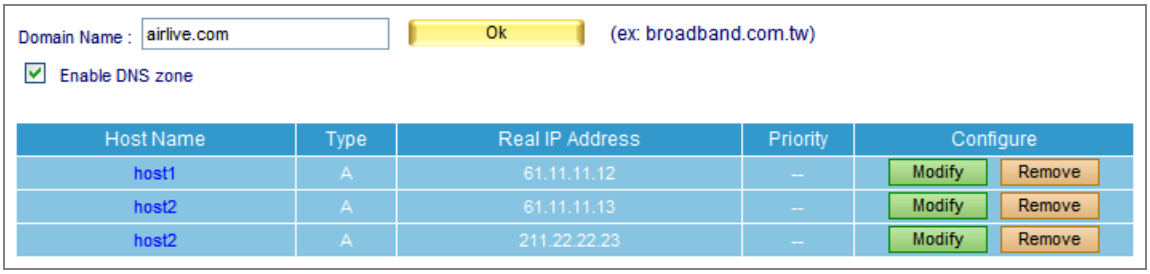


Figure 11-2 Mapping table of domain name and IP address

"**A**" represents IP address. Each domain name is assigned to a corresponding IP address. The table above indicates that host2 is assigned to two IP addresses, so it lists out two entries corresponding to host2. Every DNS inquiry might have one responding address or above and is sorted in address-sorting style or round-robin style.

11.3 CNAME (Canonical NAME)

This type allows mapped domain names to have one website address or above available for web browsers at the same time. Type CNAME is capable of mapping a type "**A**" mapped domain name, yet it is not recommended mapping a type "**CNAME**" domain name.

Ex. Type CNAME as Alias is to map up real domain name. (Table 11-2, Figure 11-3)

Domain Name	Type	IP Address
host23.airlive.com	A	61.11.11.14
host5.airlive.com	CNAME	host23.airlive.com

Table 11-2 Mapping table of domain name and CNAME

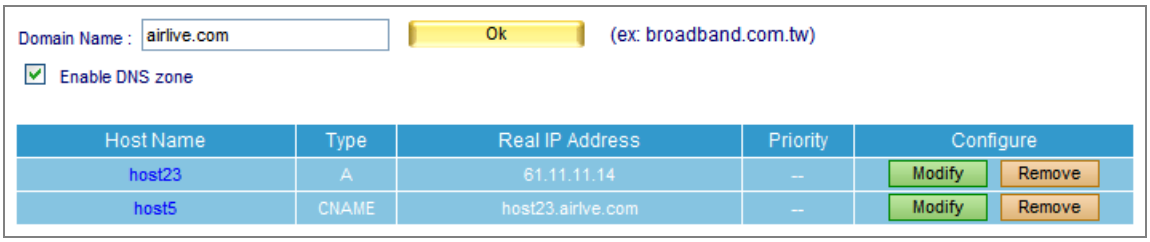


Figure 11-3 Mapping table of Domain name and CNAME

The table above indicates that host5.airlive.com (Alias) is mapping to host23.airlive.com (domain name). Thus, pinging host5.airlive.com under DOS mode will have the result of 61.11.11.14.

11.4 MX (eXchanger)

It served as a mail agent for DNS server and a window to the outside for mail services. In spite of ailing for mail server replacement, the mail server could be back to function in no time just by modifying the DNS address.

Ex.1:

"MX", also known as "Mail eXchanger", is a type of resource record especially designed for mail service. (Table 11-3, Figure 11-4)

Domain Name	Type	IP Address
host25.airlive.com	A	211.22.22.24
mail.airlive.com	MX	host25.airlive.com

Table 11-3 Mapping table of Domain name and Mail eXchanger

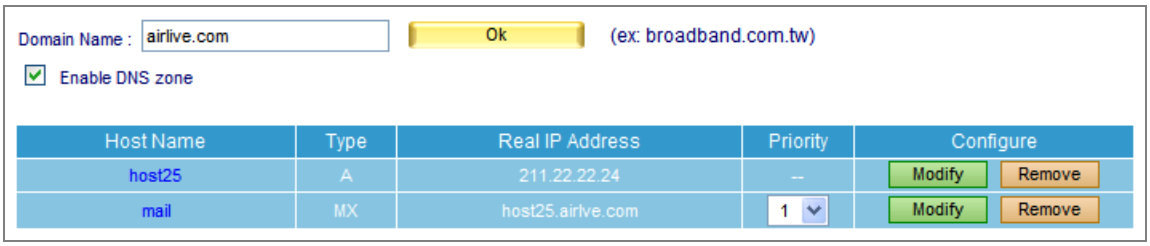


Figure 11-4 Mapping table of Domain name and Mail eXchanger

Under DOS mode, type **nslookup -type=MX mail.airlive.com**, you will find that mail.airlive.com is mapping to host25.airlive.com (the mail eXchanger) and its IP address 211. 22. 22. 24.

1. “nslookup” is the instruction of locating a DNS server.
2. “-type” defines the DNS type.
3. “mail.airlive.com” is the inquired DNS name.

For example, the customer service department of Test company wants to email to mary@mail.airlive.com, a mail server (test.com.tw) served as a SMTP server decides where and how to send the mail by inquiring the target DNS server.

The MX record of the inquiry of mail.airlive.com is as followed: (Table 11-4)

Domain Name	Type	IP Address
host3.airlive.com	A	61.11.11.10
mail.airlive.com	MX	host3.airlive.com

Table 11-4 MX Record of Querying mail.airlive.com

Therefore, mail will go to host3.airlive.com according to SMTP Protocol.

- **Name:** Customize a DNS host name.
- **Reverse:** reverse a domain name lookup of its IP address. Domain mapping distinguish into forward mapping and reverse mapping. Forward mapping served as a translator, a translator transforms a letter-pattern address into a figure-pattern address. On the other hand, reverse mapping goes the other way around.

Ex.2:

Take Ex. 1 for instance, use **nslookup** instruction to verify if forward mapping and reverse mapping function normally. The processes are as followed.

C: \>nslookup host1.airlive.com ---------->forward requiring
Server: dns.hinet.net
Address: 168.95.1.1

Name: host1.airlive.com
Address: 61.11.11.12

C: \>nslookup 61.11.11.12 ---------->reverse inquiring
Server: dns.hinet.net
Address: 168.95.1.1

Name: host1.airlive.com
Address: 61.11.11.12

Result shows that 61.11.11.12 is mapping host1.airlive.com

11.5 SPF (Sender policy FrameWork)

SPF (Sender Policy Framework) is a type of verification process that is used to prevent fake e-mail addresses by identifying the authenticity of the e-mail sender and filtering out spam.

How SPF Works

To apply the SPF verification process, two important things must be done to both the sending and receiving end of the e-mail.

1. The DNS server must be added a SPF record at sender end.
2. The Mail server must enable the SPF verification function into order to make SPF working. (Figure 11-5)

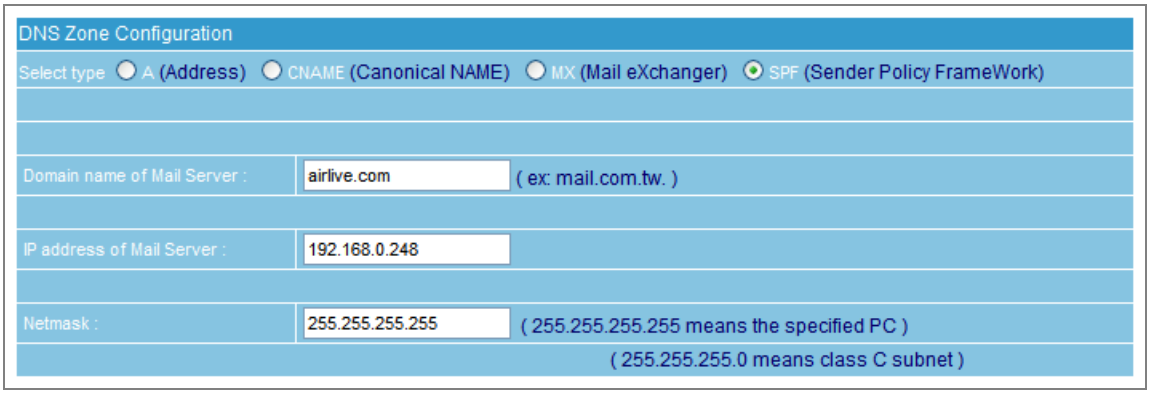


Figure 11-5 SPF setting

For example, suppose someone sends out a spam pretending to be an e-mail from AirLive mail server to your e-mail address.

When this spam e-mail is sent to an account with SPF enabled, the account will ask AirLive mail server for the SPF record based on the e-mail's IP address to check if the IP really came from AirLive.

If AirLive mail server confirms the SPF verification, then the e-mail will pass the account's SPF verification and be sent to the receiver.

On the other hand, if the e-mail does not pass the SPF verification it shall be viewed as junk mail. This means that even if the e-mail is really being sent out from AirLive, yet if AirLive mail server doesn't provide SPF record checking at that time, the e-mail that won't go through the receiver account's SPF verification will still be viewed as junk mail.

The SPF checking process needs the sender account to set up SPF record to provide verification checking in order to send and receive normally. It works best when more people use this verification process to completely put the set up to use. The number of corporations that currently have SPF record checking is still quite small, thus under this condition the SPF process at the receiving end that filters out any junk mail will provide the sender with a great deal of inconvenience.

11.6 Example

Further Description

DNS directing indicates by which DNS server is managing and in which DNS has detailed domain name information. Any specific information can be obtained in the DNS server, such as physical address of website or mail server. Thus, continuous Internet connection and accurate DNS record must be assured.

According to international practice, DNS system must be directed to 2 DNS servers. It is to ensure domain name inquiry works in case one of them breaks down the other can act as substitute. This promises you a well-functional domain name, apart from that, providing a better domain name inquiring service for global Internet users.

11.6.1 Setup a host name server

Procedure:

1. Register airlive.com as domain name.
2. Set primary host name server as 61.11.11.11 and domain name as
   dns1.airlive.com
   Set secondary host name server as 211.22.22.22 and domain name as
   dns2.airlive.com
3. Required for T1or ADSL Internet connection
4. Servers required for resolving:
   www.airlive.com (192.168.1.100) Web server
   mail.airlive.com (192.168.1.101) E-Mail server

Step1. Apply to ISP for two fixed IP ADSL or T1. Supposed that the appointed IP addresses are as followed:

61.11.11.10 ~ 61.11.11.14
211.22.22.18 ~ 211.22.22.30

Register the IP address on IDNs (International Domain Names) official website:

- Primary Host Name Server
  Host Name: dns1.airlive.com
  IP Address: 61.11.11.11
- Secondary Host Name Server
  Host Name: dns2.airlive.com
  IP Address: 211.22.22.22

Domain name must map the fixed IP address when registering the IP address on IDNs (International Domain Names) official website.

Step2. Set up DNS according to the settings below: (Table 11-5, Figure 11-6)

Domain Name	Type	IP Address	Reverse	Priority
airlive.com.	A	61.11.11.11	Enabled	--
airlive.com.	A	211.22.22.22	Enabled	--

Table 11-5 Mapping Table of Domain Name and IP Address

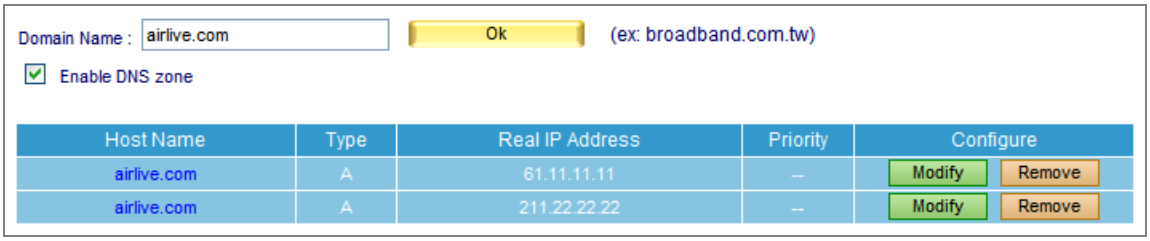


Figure 11-6 Mapping table of domain name and IP address

As seen from Table 11-5, verifying forward mapping and reverse mapping for correctness with nslookup instruction are as followed:

C: \>nslookup airlive.com
Server: dns.hinet.net
Address: 168.95.1.1

Name: airlive.com
Address: 61.11.11.11, 211.22.22.22------->examine IP for correctness (forward mapping)

C: \>nslookup 61.11.11.11
Server: dns.hinet.net
Address: 168.95.1.1

Name: airlive.com ---------->examine domain name for correctness (reverse mapping)
Address: 61.11.11.11

Secondary DNS can act as substitute while primary DNS is down, it keeps domain name available for use.

Step3. Set up DNS according to the settings below: (Table 11-5, Figure 11-7)

Domain Name	Type	IP Address	Priority
web.airlive.com	A	61.11.11.11	--
web.airlive.com	A	211.22.22.22	--
www.airlive.com	CNAME	web.airlive.com	--

Table 11-6 CNAME record of www.airlive.com

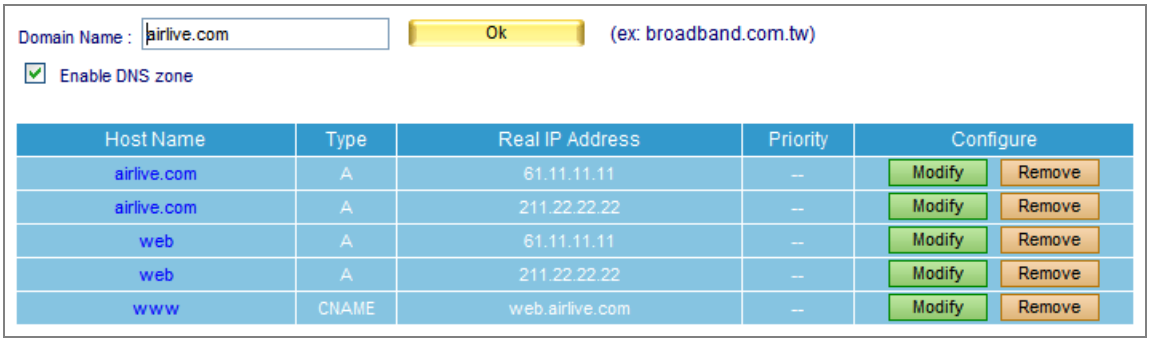


Figure 11-7 CNAME record of www.airlive.com

As seen from Table 11-6, verifying forward mapping for correctness with **nslookup** instruction is as followed:

C: \>nslookup
Default Server: dns.hinet.net
Address: 168.95.1.1

> server 61.11.11.11 ---------->switch to your DNS server
Default Server: web.airlive.com
Address: 61.11.11.11

> www.airlive.com ---------->lookup for real domain name (forward mapping)
Server: web.airlive.com
Address: 61.11.11.11

Name: web.airlive.com ----------> domain name of www.airlive.com
Address: 61.11.11.11, 211.22.22.22 ---------->mapping IP of web.airlive.com
Alias: www.airlive.com ---------->CNAME of web.airlive.com

According to aforementioned, web.airlive.com is used to map host name and its IP address. And www.airlive.com, a CNAME of web.airlive.com, offers inquiry ability and redirection to web.airlive.com.

As seen from Table 11-6, it can be inferred that when browsing www.airlive.com visitors enter different server according to the browsing sequence.
1st visitor enter server 61.11.11.11
2nd visitor enter server 211.22.22.22
3rd visitor enter server 61.11.11.11
4th visitor enter server 211.22.22.22
5th visitor enter server 61.11.11.11
6th visitor enter server 211.22.22.22
.
.
(User are distributed to servers alternatively)

As seen from Table 11-7, the smaller figure it is, the higher priority it gets. For example, the user A wants to email to mary@mail.airlive.com, a mail server (mail.airlive.com) served as a SMTP server decides where and how to send the mail by inquiring the target DNS server.

The MX record of the inquiry of mail.airlive.com is as followed: (Table 11-7)

Domain Name	Type	Address	Reverse	Priority
mail.airlive.com	MX	smtp1.airlive.com	X	1
mail.airlive.com	MX	smtp2.airlive.com	X	2

Table 11-7 MX record of mail.airlive.com

For figure 1 has the highest priority, server will try to deliver the mail to smtp1.airlive.com due to its first priority. If delivery failed, then the mail goes to smtp2.airlive.com the secondary priority.

11.6.2 Mapping between Servers (Web / FTP / Mail) and Domain Name

Preparation

1. Apply to ISP for two fixed IP ADSL Internet connections
（The fixed IP of WAN1 is 61.11.11.10 ~ 61.11.11.14）
（The fixed IP of WAN2 is 211.22.22.18 ~ 211.22.22.30）
2. Apply to ISP for airlive.com as domain name
3. Register the IP address on IDNs (International Domain Names) official website.

Primary Host Name Server

Host Name: dns1.airlive.com

IP Address: 61.11.11.11

Secondary Host Name Server

Host Name: dns2.airlive.com

IP Address: 211.22.22.22

Step1. Settings of Web, FTP, Mail Server are as followed :

- Web server : 61.11.11.12
- FTP server : 211.22.22.20
- Mail server : 61.11.11.11 and 211.22.22.22

Step2. Go to **DNS Setting → Setting**, click **New Entry**.

Step3. Fill in the blank field with registered domain name airlive.com, then click **OK** and check **Enable DNS Zone**, finally click **New Entry**. (Figure 11-8)

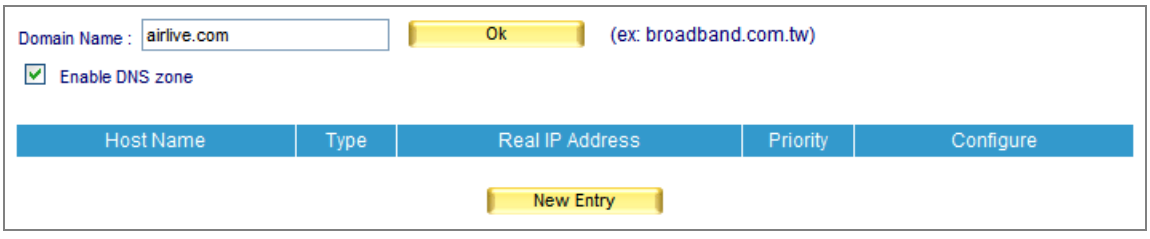


Figure 11-8 Add a domain name

Step4. In DNS Zone Configuration, add the first entry :

- **Select type:** A（Address）
- **Name:** airlive.com. (Be aware there is a dot sign “.” behind the domain name.)
- **Address:** 61.11.11.11
- Click **OK**. (Figure 11-9)
- Primary DNS mapping setup completed.

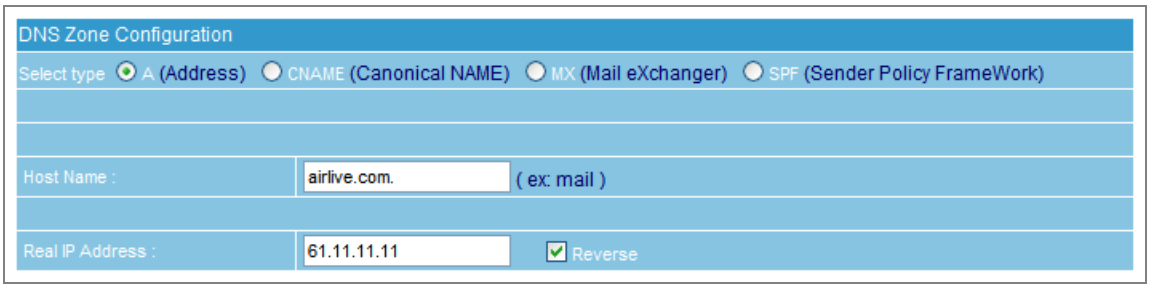


Figure 11-9 Primary DNS mapping setup

Step5. In DNS Zone Configuration, add the second entry :

- **Select type :** A（Address）
- **Name :** airlive.com. (Be aware there is a dot sign “.” behind the domain name.)
- **Address :** 211.22.22.22
- Click **OK**. (Figure 11-10)
- Secondary DNS mapping setup completed.

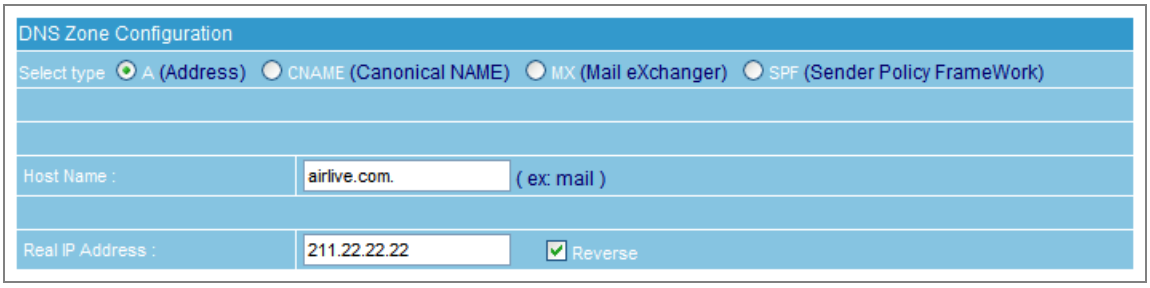


Figure 11-10 Secondary DNS mapping setup

Step6. In DNS Zone Configuration, add the third entry :

- **Select type :** A（Address）
- **Name :** www
- **Address :** 61.11.11.12
- Click **OK**. (Figure 11-11)
- Mapping record between web server and IP setup completed.

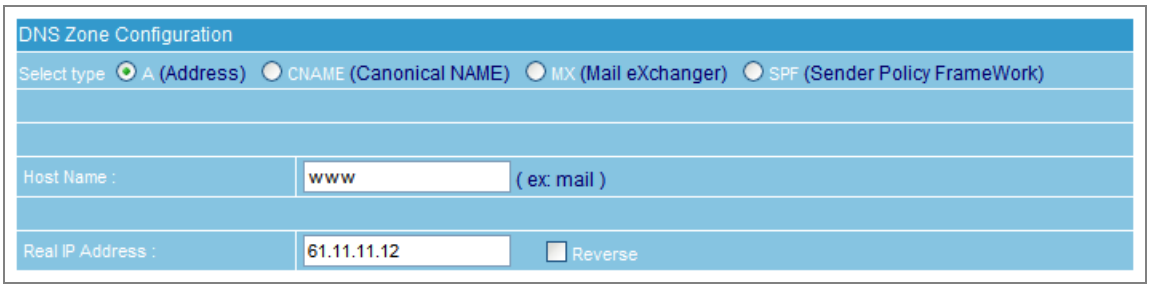


Figure 11-11 apping record between web server and IP setup

Step7. In DNS Zone Configuration, add the forth entry :

- **Select type :** A（Address）
- **Name :** FTP
- **Address :** 211.22.22.20
- Click **OK**. (Figure 11-12)
- Mapping record between FTP server and IP setup completed.

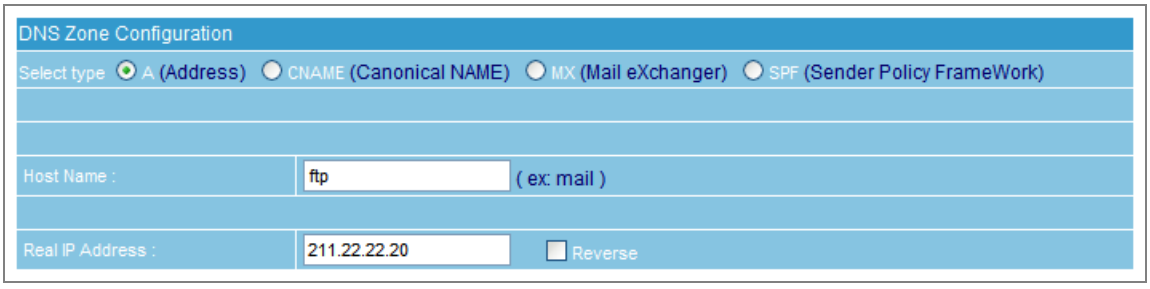


Figure 11-12 Mapping record between FTP server and IP setup

Step8. In DNS Zone Configuration, add the fifth entry :

- **Select type :** MX（mail eXchanger）
- **Name :** mail
- **Mail server :** airlive.com
- Click **OK**. (Figure 11-13)
- Mapping record between mail server and IP setup completed.

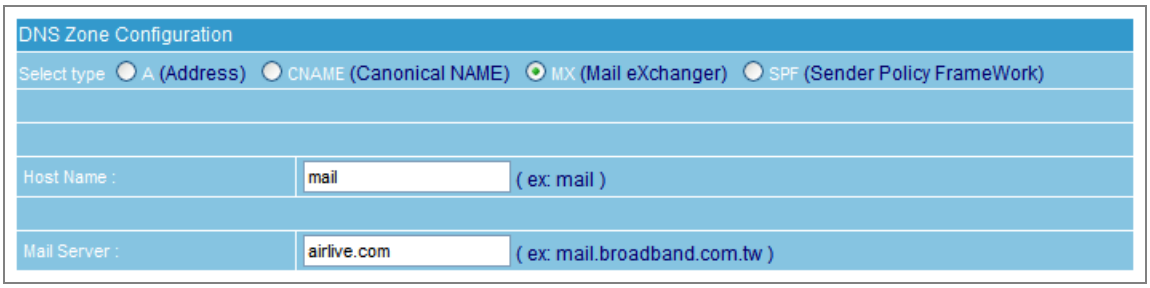


Figure 11-13 Mapping record between mail server and IP setup

Step9. Setup completed. (Figure 11-14)

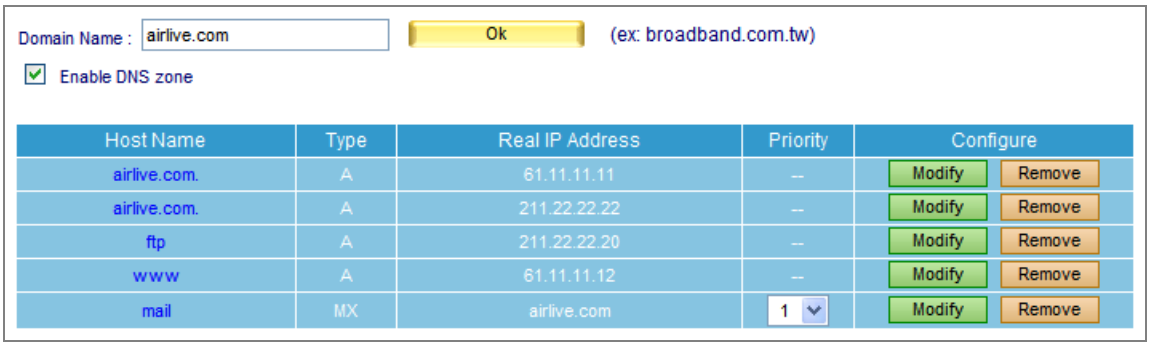


Figure 11-14 Setup completed

Step10. The easy memorized addresses facilitate external inquiries.

- Web server : www.airlive.com
- FTP server : ftp.airlive.com
- Mail server : mail.airlive.com

Chapter 12 Web Server Setting

The key to a thriving business is to provide your potential customers with a stable, reliable access to your company website. Accordingly, ES-6000 makes website building cost effective and expeditious for you by integrating the web server. It meets your demand on building up a company website.

12.1 Setting

The main function of ES-6000 Web Server is described as following: (Figure 12-1)

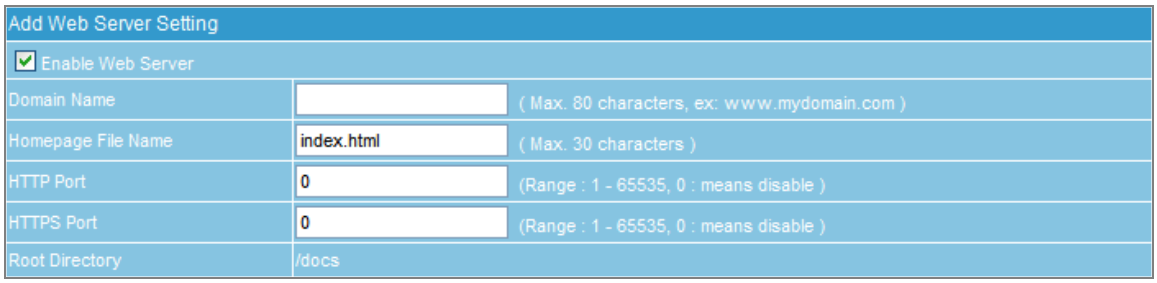


Figure 12-1 Web Server Setting

Definitions:

- **Domain Name**
  - The address of your website
- **Homepage File Name**
  - The default webpage of your website. It is usually named as “index.html” or “index.shtml”
- **HTTP Port**
  - The HTTP port for browsing your website
- **HTTPS Port**
  - The HTTPS port for browsing your website
- **Root Directory**
  - The top-most directory in your website hierarchy where all files of your website are stored. “/docs” is the root directory by default.
- **Web Server File and Folder Setting**
  - Allows you to publish the folder index, create alias, enable authentication, etc.
  - Allows you to change the root directory accordingly.
  - Allows you to upload multiple files at once by file compression. You may extract the compressed file after uploaded. Currently, it supports TAR, TAR.GZ, TGZ, TAR.BZ2, ZIP, GZ, and BZ2 files.

For the time being, the Web Server supports merely a few computer languages (i.e., JavaScript, HTML, SHTML, XML), excluding those which require execution on the Web Server, such as C, Perl, ASP, and PHP.

12.2 Example

Using ES-6000 to Provide Web Service

Step1. ***DNS Setting → Setting***: Create DNS entry to define web server address. (Figure 12-2)

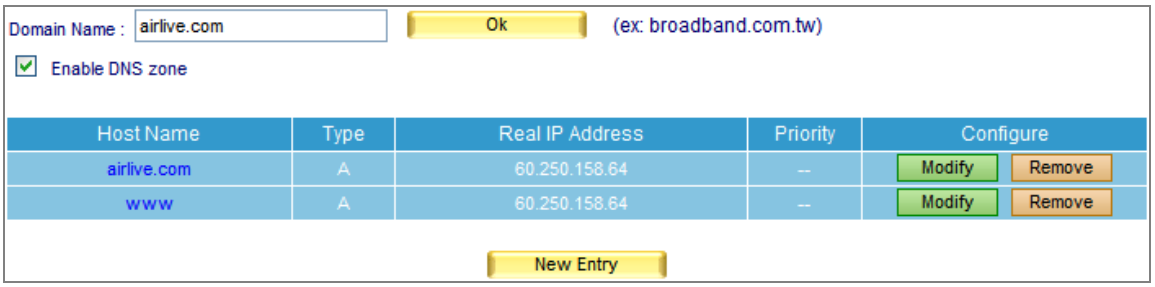


Figure 12-2 The DNS configuration for Web Server

Step2. Select ***Web Server Setting → Setting*** and then set as below:

- Click **New Entry**
- Tick **Enable Web Server**
- Type “www.airlive.com” in the **Domain Name** field
- Type “index.htm” in the **Homepage File Name** field
- Enter “888” in the **HTTP Port** field
- Enter “333” in the **HTTPS Port** field
- Click **OK** (Figure 12-3)
- Click **OK** in the dialogue box to confirm restarting the Web server. (Figure 12-4, 12-5)

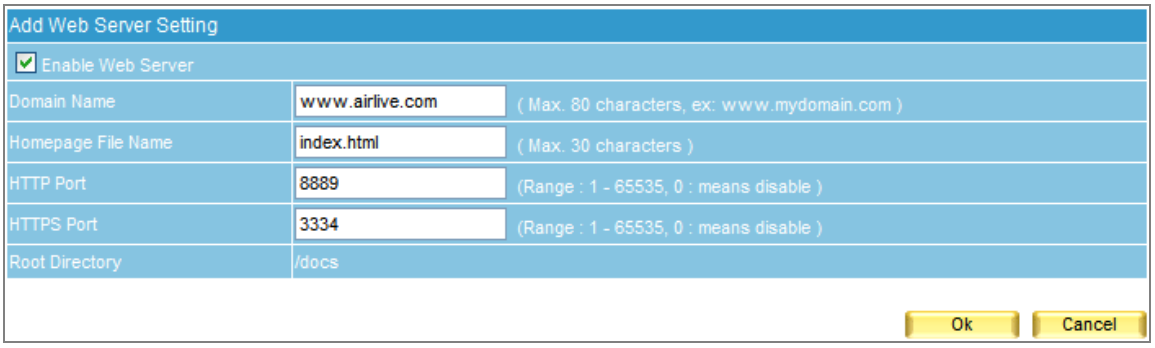


Figure 12-3 Configure the Web Server

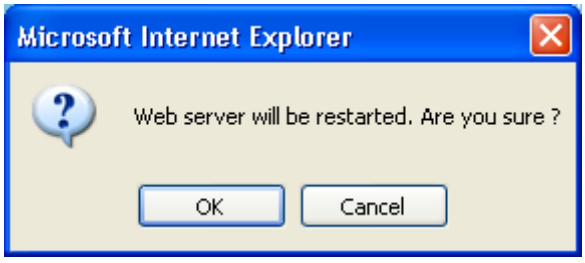


Figure 12-4 Confirming to restart the Web server

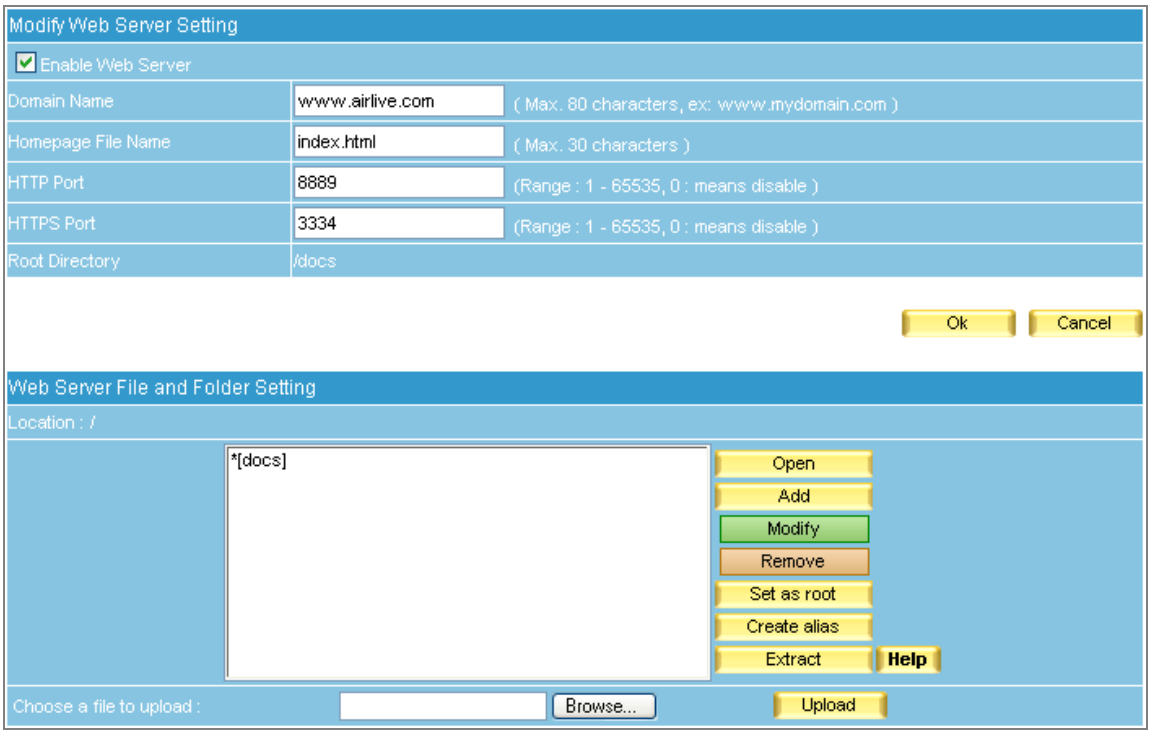


Figure 12-5 Web server setting completed

Step3. In the **Web Server File and Folder Setting** section, upload your website onto the Web server:

- Select the default root directory "*[docs]" and then click **Open** on the right. (Figure 12-6)
- Compress all the content of your website as a ZIP file.
- Use **Browse** to locate the ZIP file and then click **Upload**. (Figure 12-7)
- Select the ZIP file and then click **Extract** on the right. (Figure 12-8)
- Select the ZIP file and then click **Remove** on the right. (Figure 12-9)
- Click **OK** (Figure 12-10)
- Click **OK** in the dialogue box to confirm restarting the Web server. (Figure 12-11, 12-12)
- Now you may visit your website at "http://www.airlive.com.tw:8889" or "https://www.airlive.com.tw:3334". (Figure 12-13)

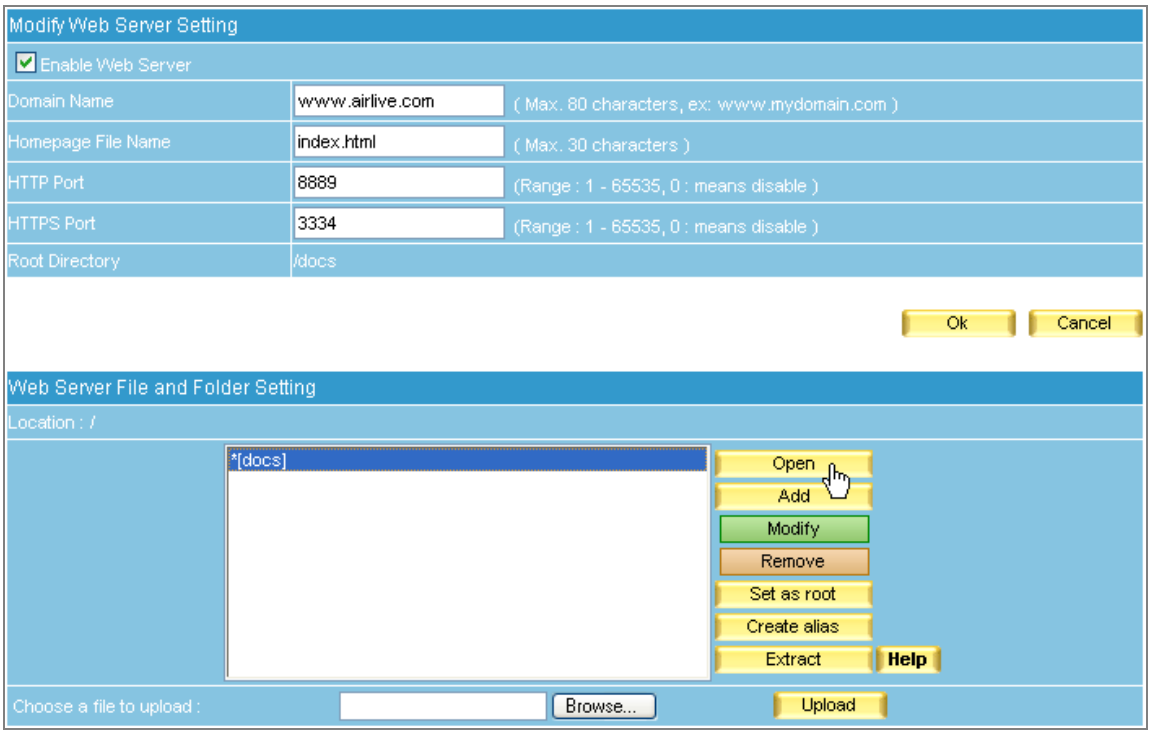


Figure 12-6 Opening the root directory

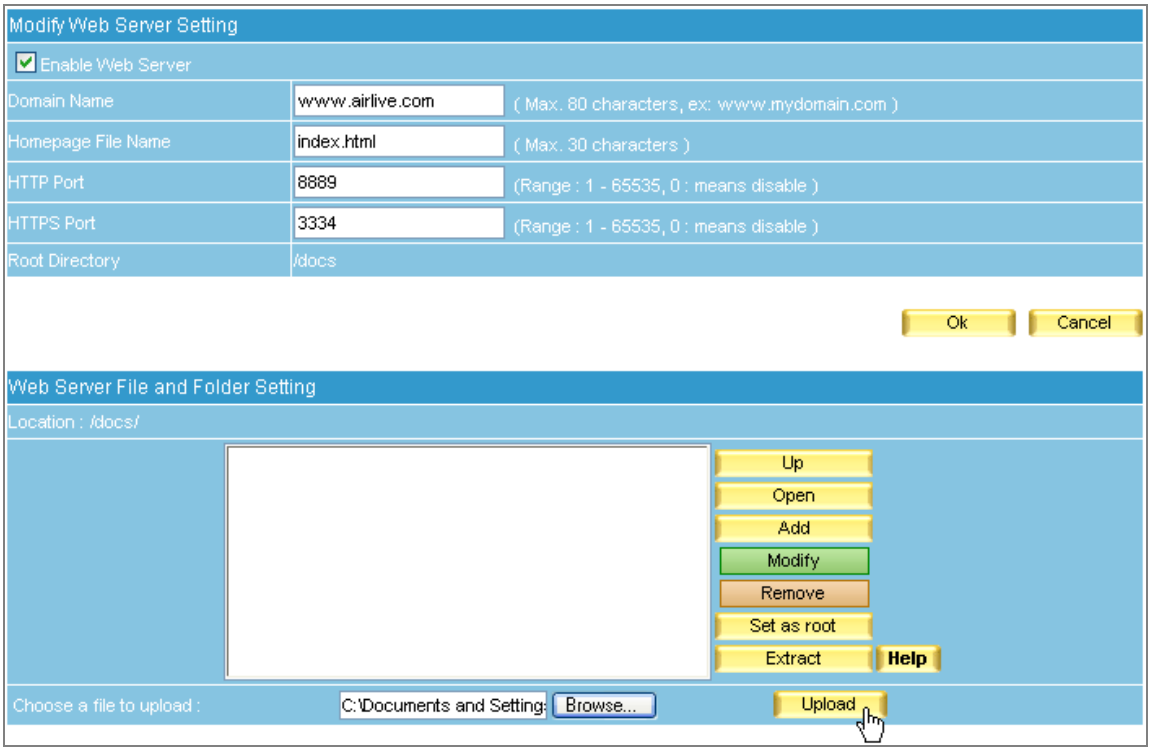


Figure 12-7 Uploading Your Website onto the Web Server

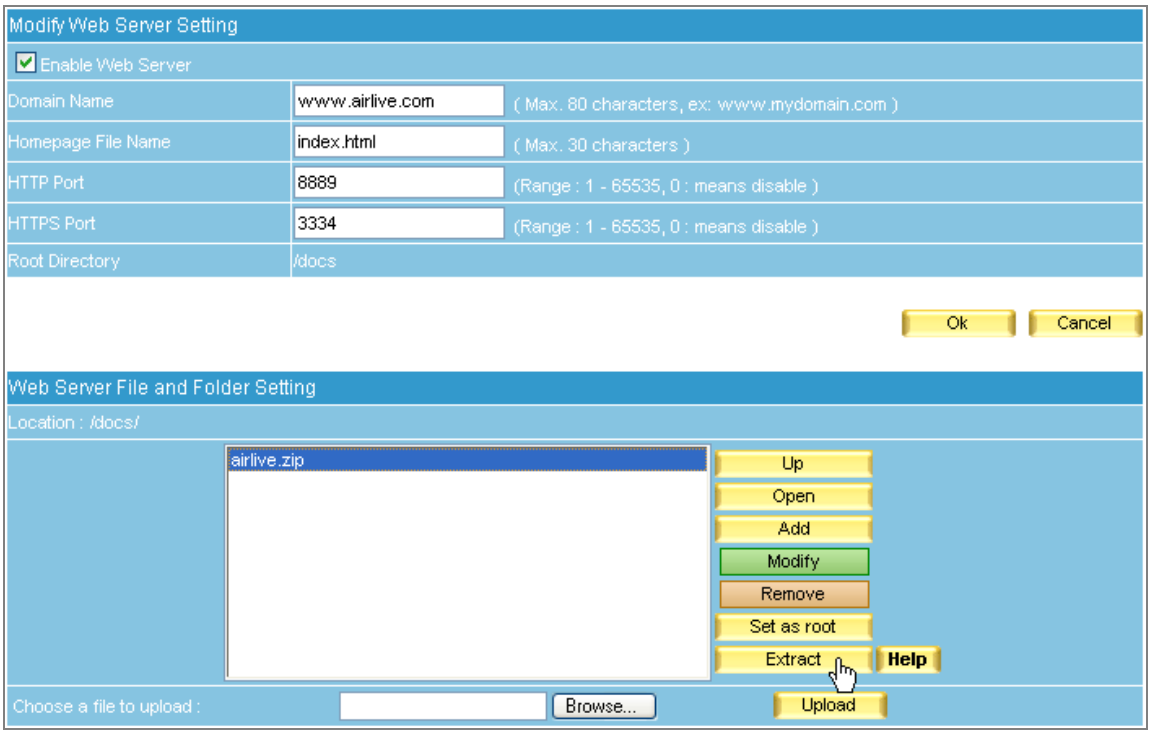


Figure 12-8 Selecting the ZIP File to Extract

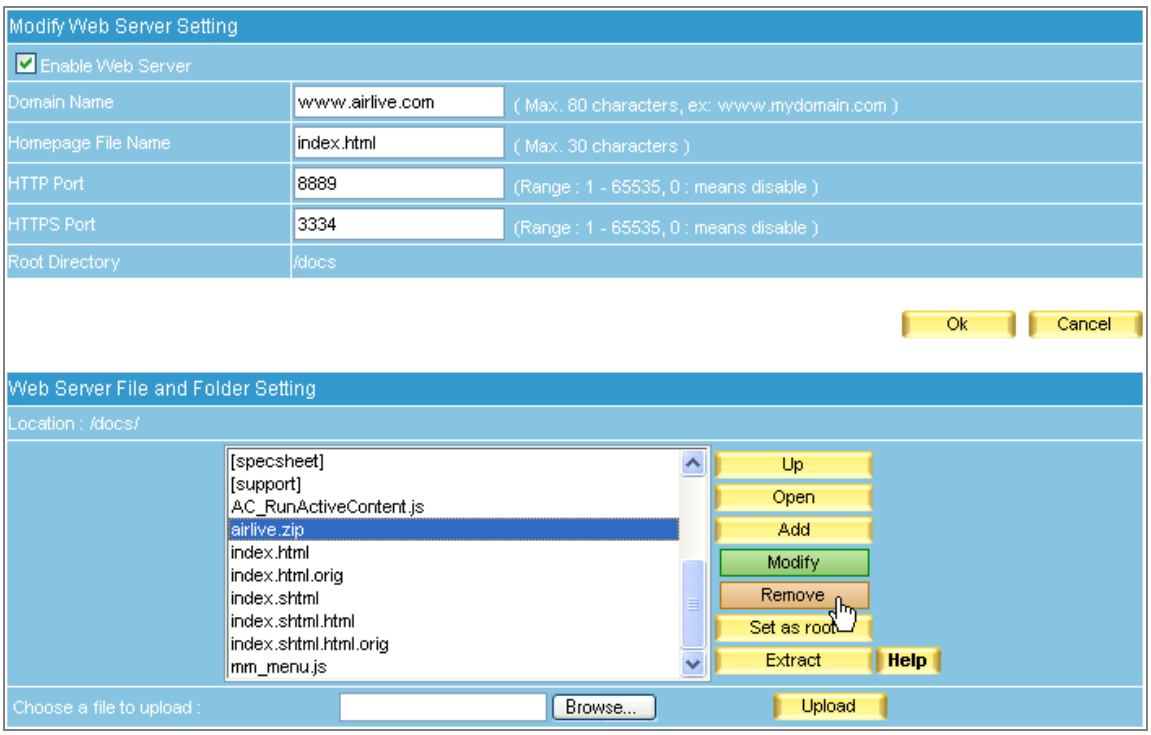


Figure 12-9 Selecting the ZIP File to Remove

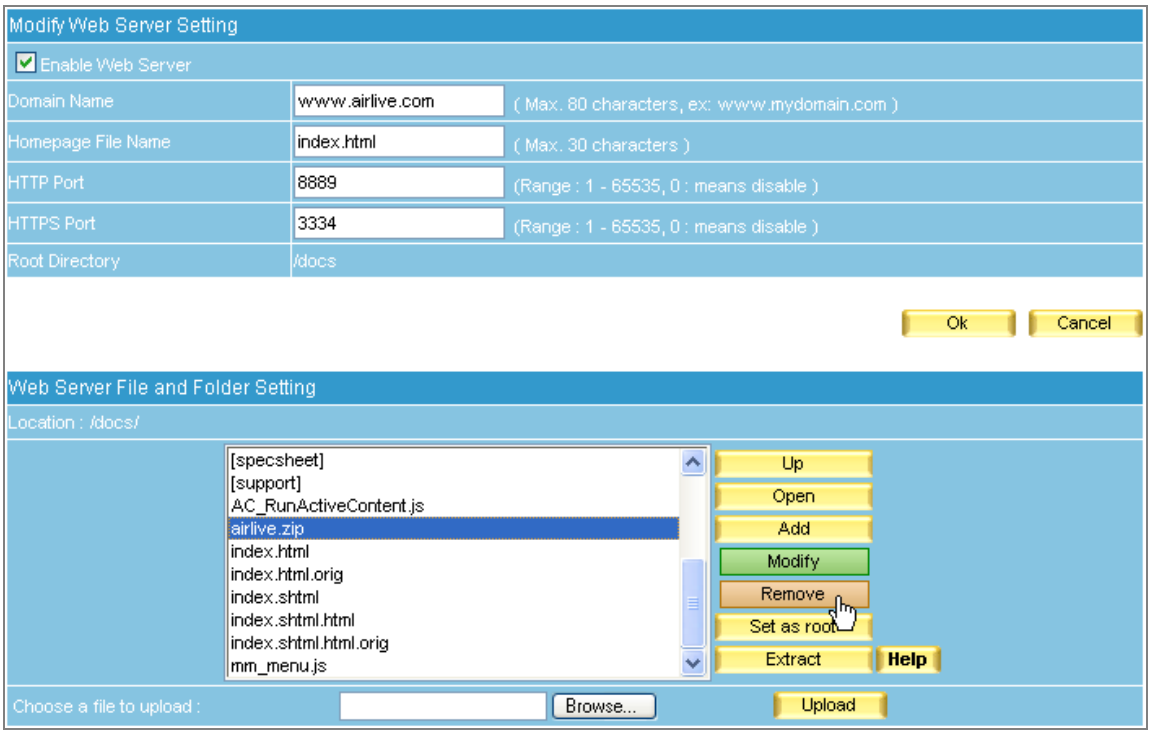


Figure 12-10 Website Uploaded

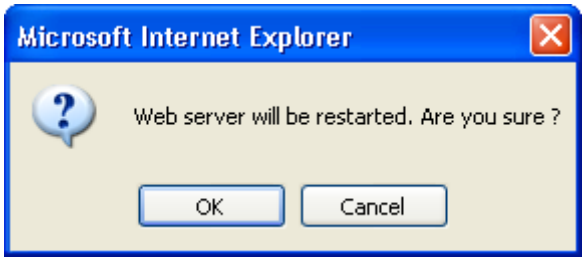


Figure 12-11 Confirming to Restart the Web Server

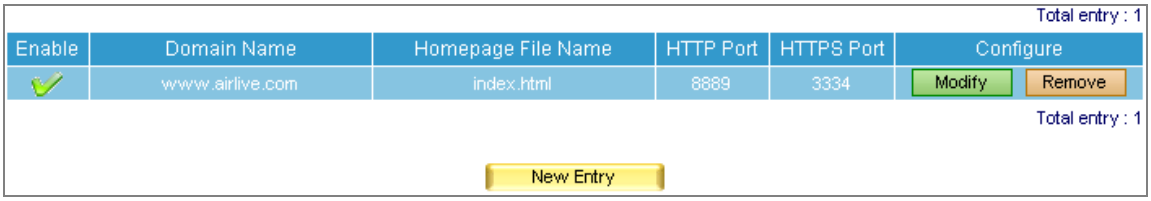


Figure 12-12 Web Server Restarted

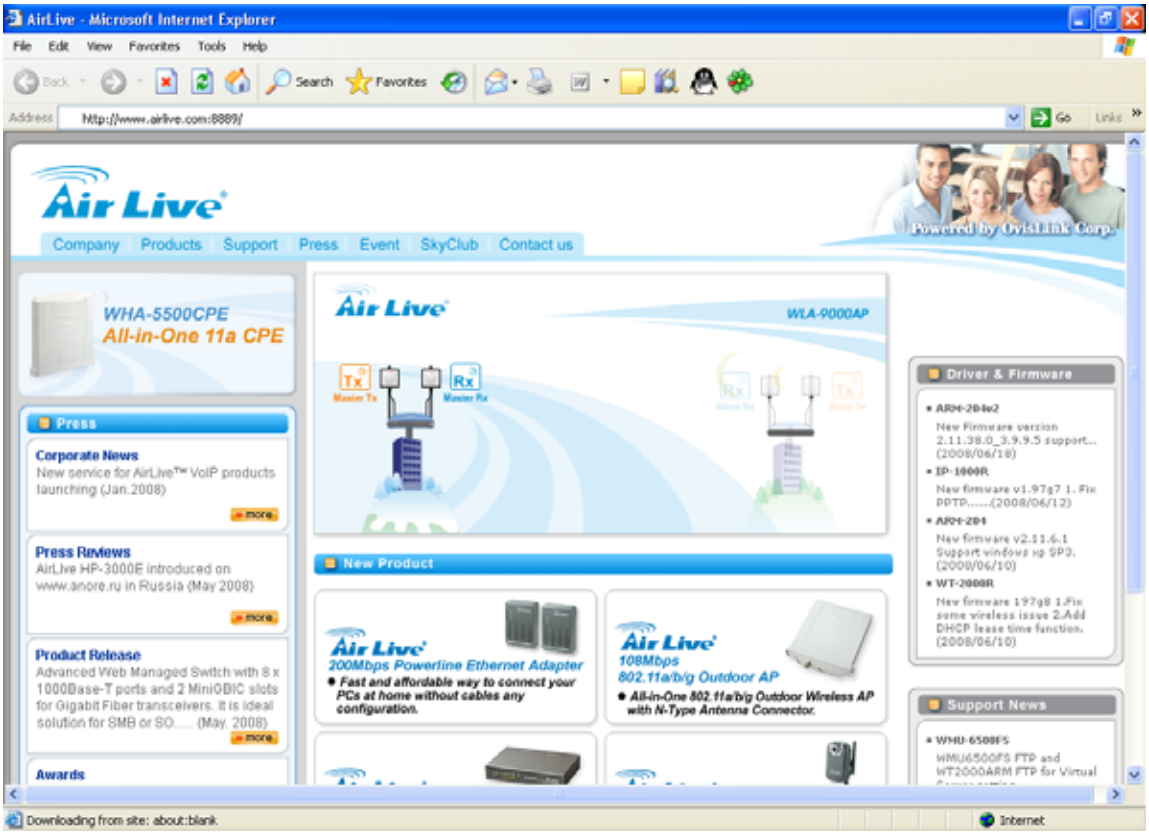


Figure 12-13 Visiting Your Own Website

Step4. In the **Web Server File and Folder Setting** section, set as below:

- Click **Add**. (Figure 12-14)
- Specify the folder name and tick **Publish the Folder Index**.
- Specify the alias name (e.g. /download/) and tick **Enable Folder Alias**.
- Tick **Enable Authentication** and configure the related fields accordingly.
- Click **OK**. (Figure 12-15)
- Select "[spec]" and then click **Open** on the right. (Figure 12-16)
- Use **Browse** to locate the desirable file to upload and then click **Upload**. (Figure 12-17)
- Click **OK**. (Figure 12-18)
- Click **OK** in the dialogue box to confirm restarting the Web server. (Figure 12-19, 12-20)
- Now you may access the files stored on the Web server through the folder index at "http://www.airlive.com:8889/download/" or "https://www.airlive.com.tw:3334/download/" upon authentication. (Figure 12-21, 12-22, 12-23)

Figure 12-14 Adding a New Folder

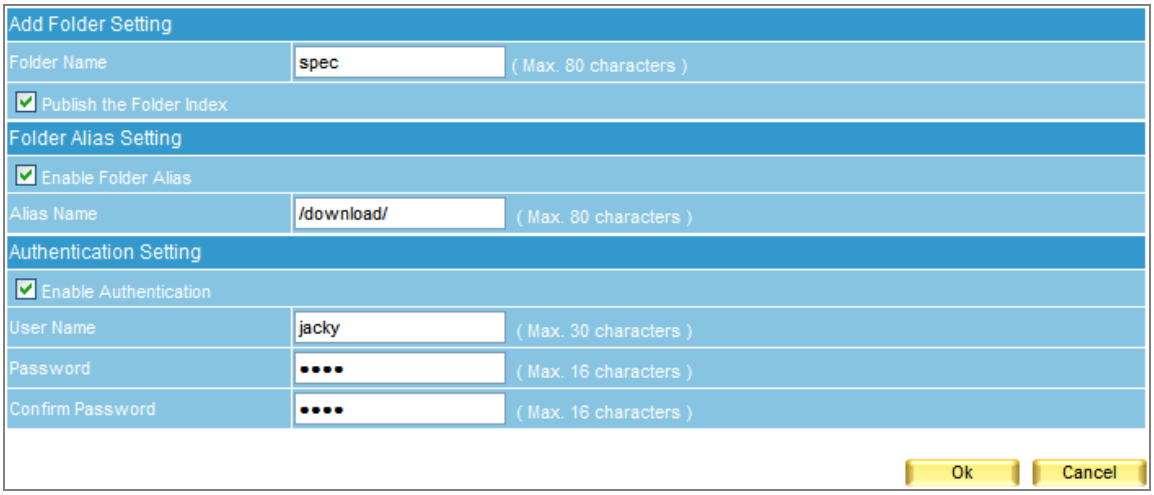


Figure 12-15 The Related Settings of a Folder

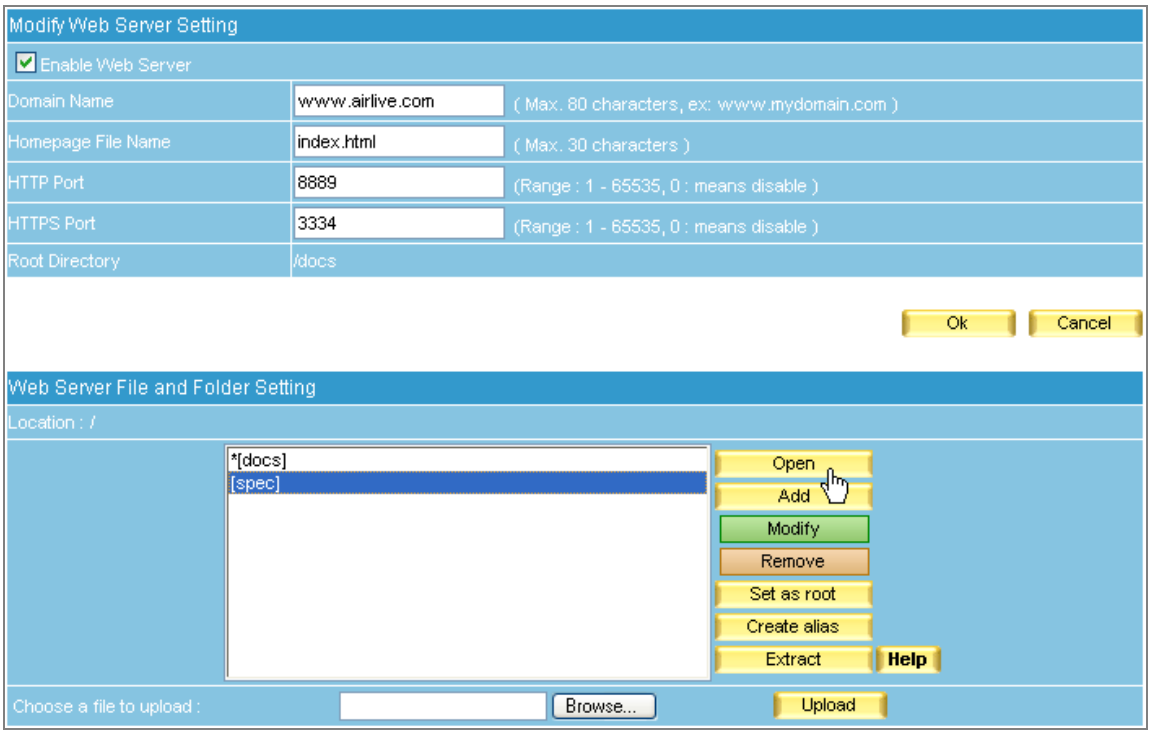


Figure 12-16 Opening a Folder

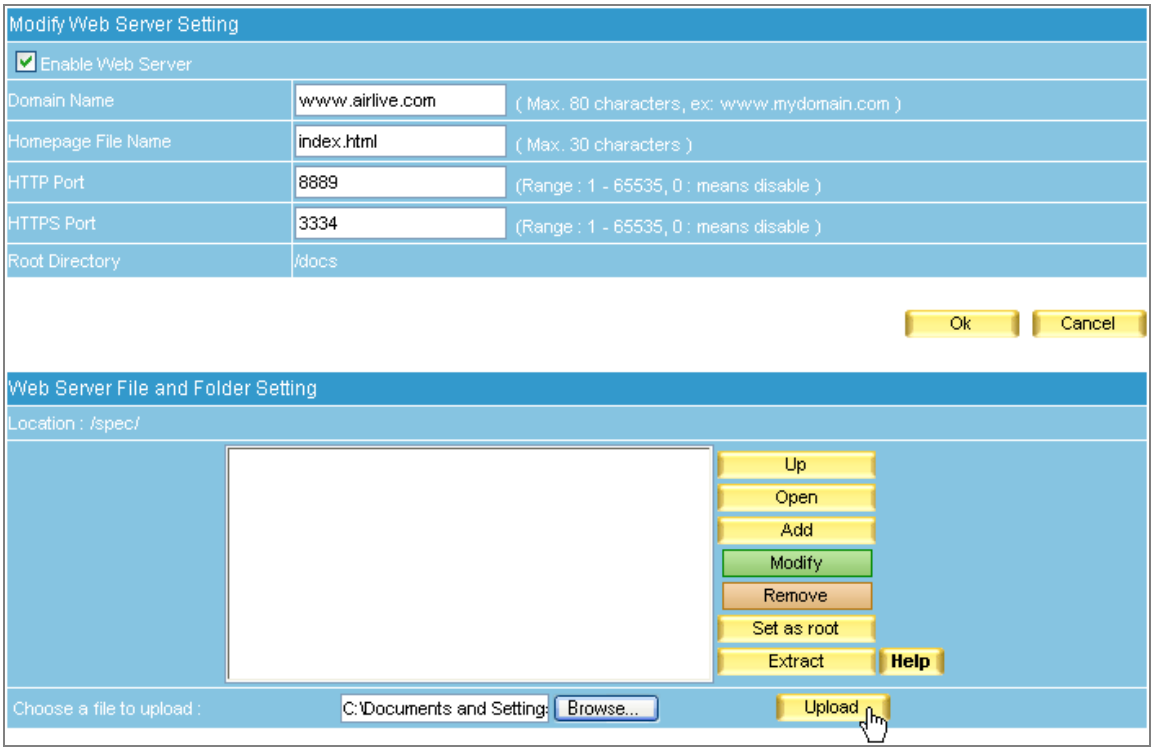


Figure 12-17 Uploading a File

Figure 12-18 File Uploaded

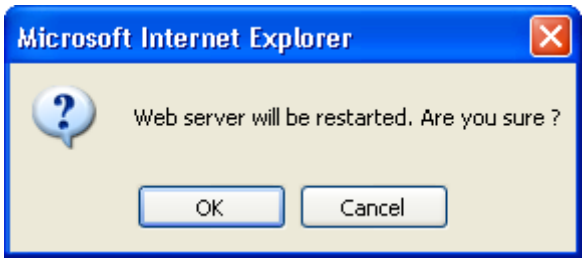


Figure 12-19 Confirming to Restart the Web Server

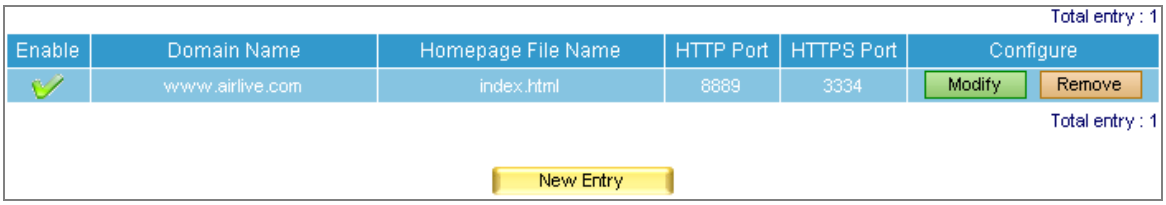


Figure 12-20 Web Server Restarted

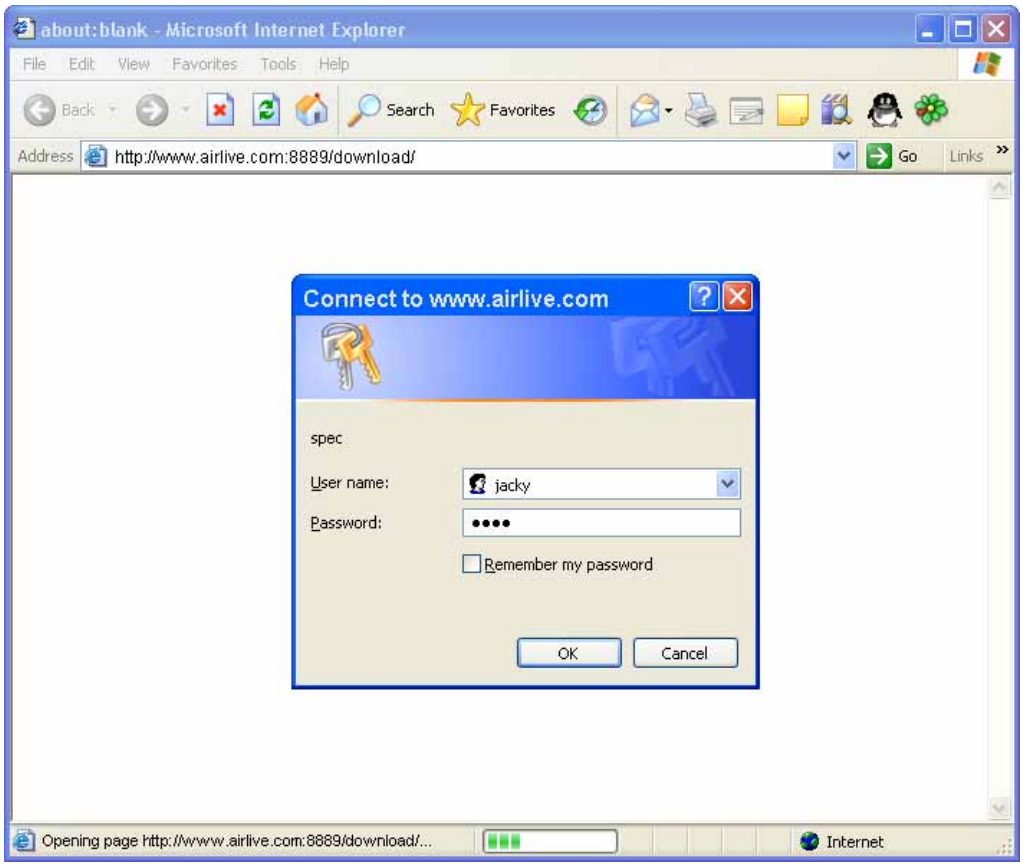


Figure 12-21 The Authentication Dialogue Window

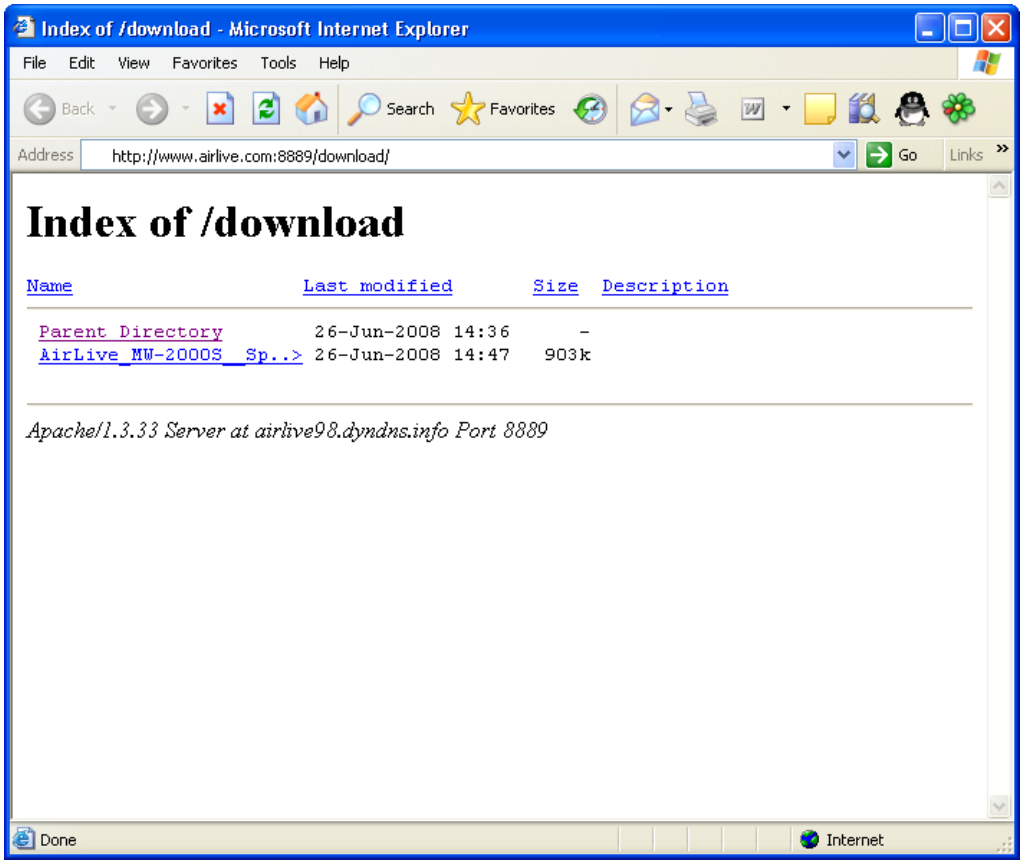


Figure 12-22 Browsing for the Desirable File

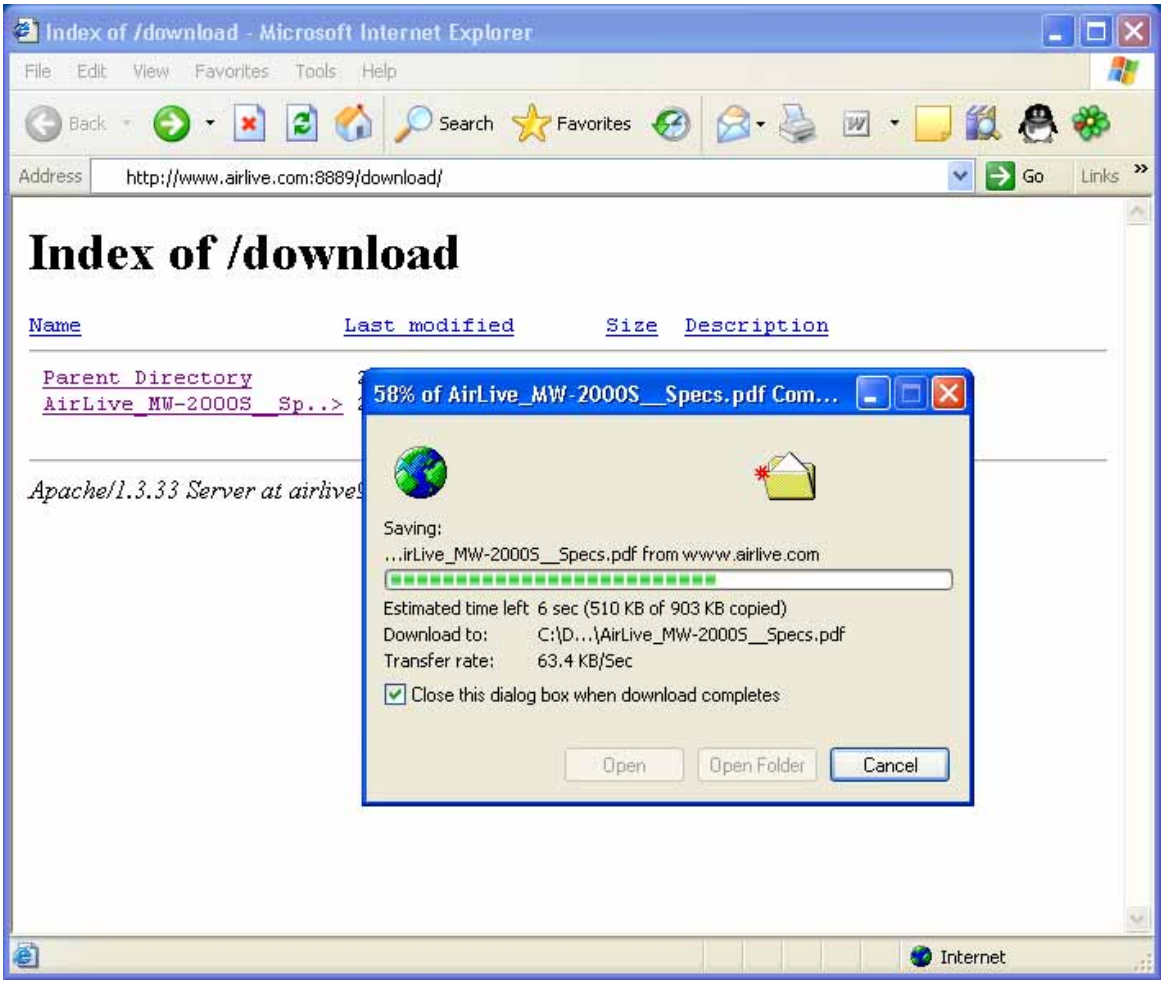


Figure 12-23 Downloading the Desirable File

Chapter 13 Proxy Server Settings

The ES-6000 offers a new function to perform web proxy server, so the LAN client users can define ES-6000's IP address and the port number in browser; the ES-6000 will receive webpage from Internet website and store the pages in ES-6000 hard disc.

While users try to access the same page, the ES-6000 just need to download the updated page from website, so users can browse webpage more faster, and also save the fee to connect Internet.

Definition:

- **Enable Proxy Server**
  - Select to enable ES-6000 web proxy server setting.
- **Cache Utilization**
  - Display the utilization of cache size
- **Port**
  - User can customize the port number for proxy connection
- **Cache Size**
  - User can decide to use how many capacity of hard disk to be the proxy server cache. (Figure 13-1)

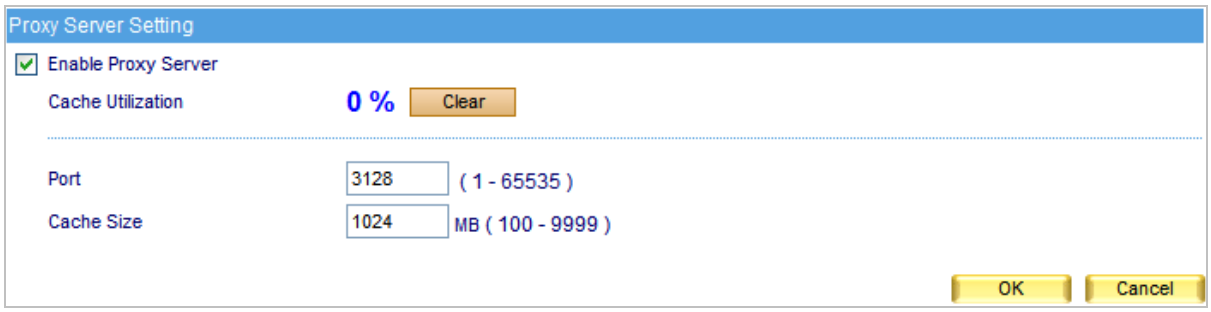


Figure 13-1 Proxy Server Settings

Chapter 14 Monitor

MIS engineer could view the system information and every event log in **Monitor**.

1. System Info indicates the utilization of CPU, Hard Disk, Memory, and Ram Disk.
2. Event Log records every activity in ES-6000, such as modify and remove setting.

14.1 System Info

Step1. In the path of **Monitor → System Info,** it shows system utilization information: (Figure 14-1)

- **CPU Utilization** indicates the CPU usage percentage.
- **Hard Disk Utilization** indicates the hard disk usage percentage.
- **Memory Utilization** indicates the memory usage percentage.
- **Ram Disk Utilization** indicates the ram disk usage percentage

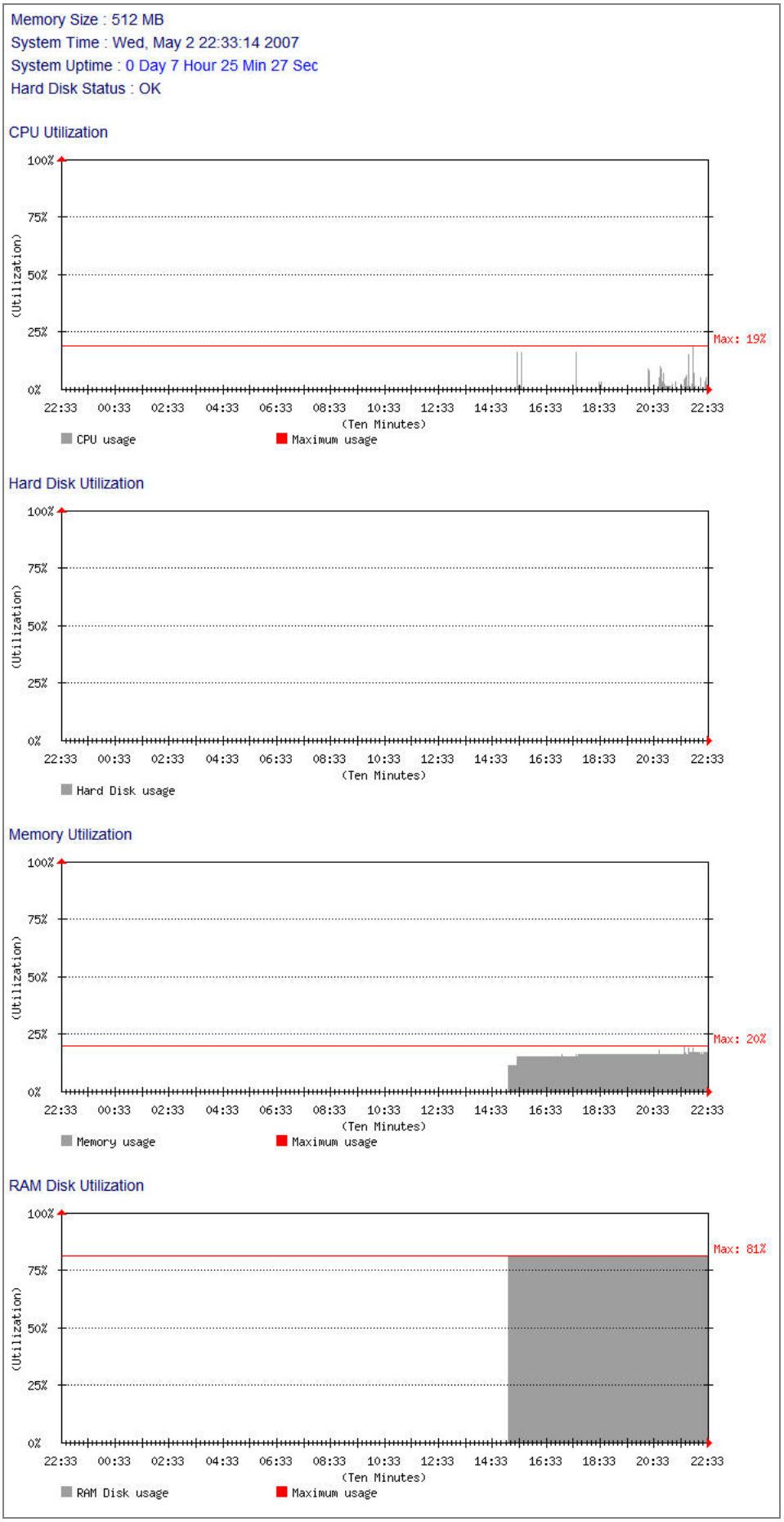


Figure 14-1 Display system info

14.2 Event Log

Step1. In the path of **Monitor → Event Log,** it shows records of every activity in ES-6000, such as modify and remove setting. (Figure 14-2)

- Click to search event log. (Figure 14-3)
- Click to view log detail. (Figure 14-4)

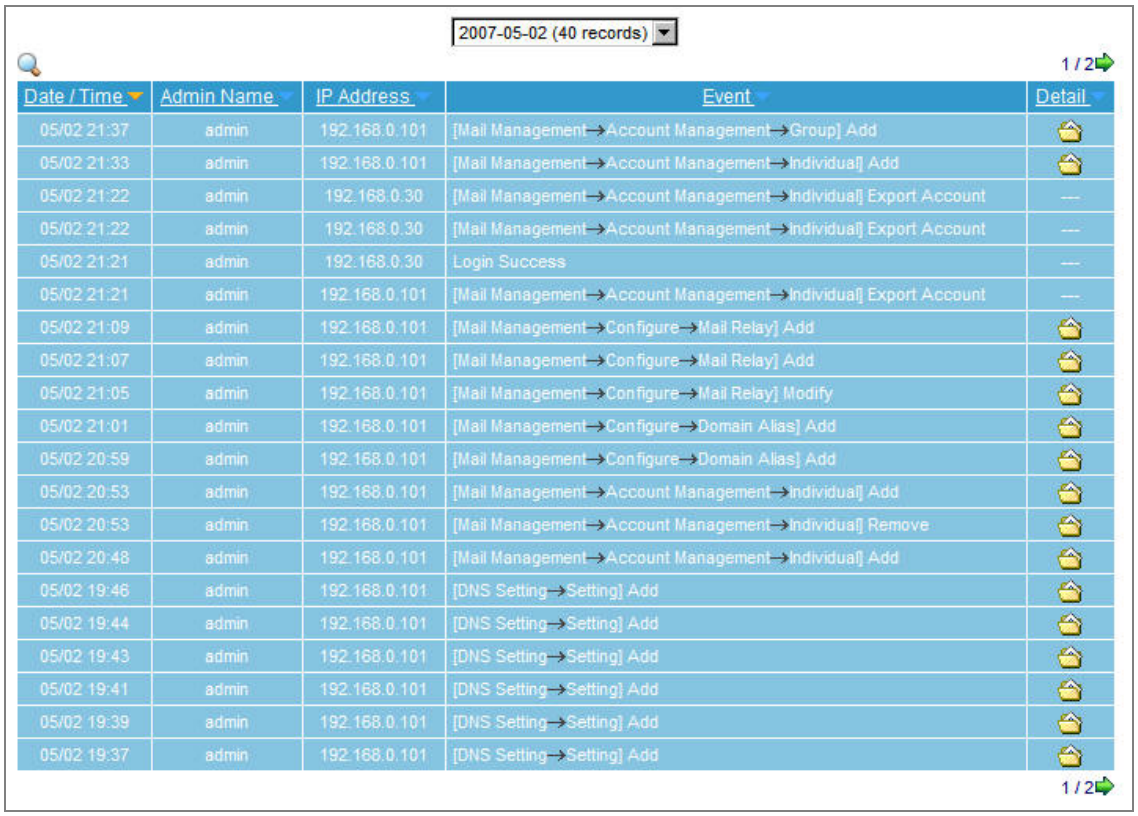


Figure 14-2 Event log

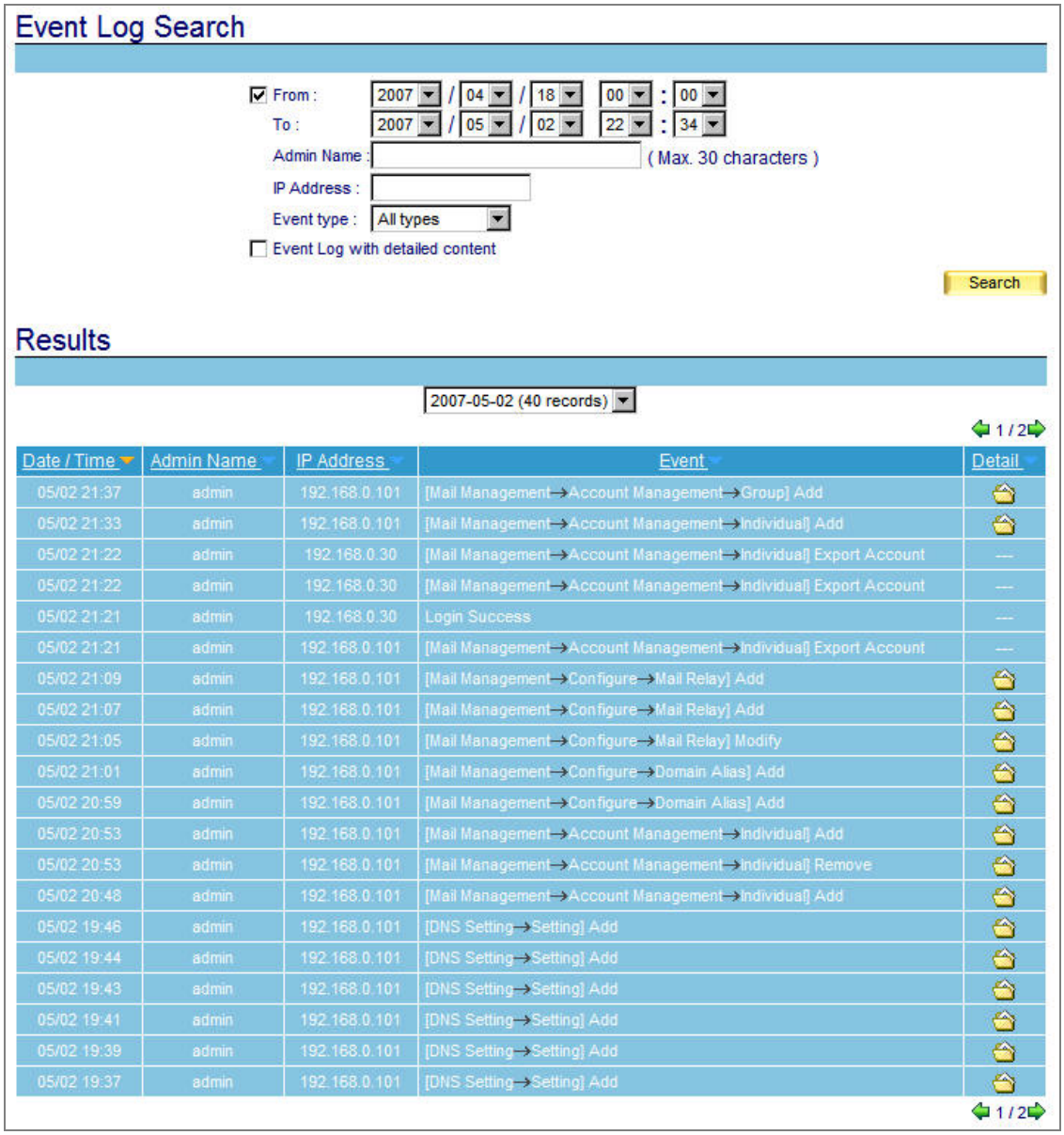


Figure 14-3 Search results

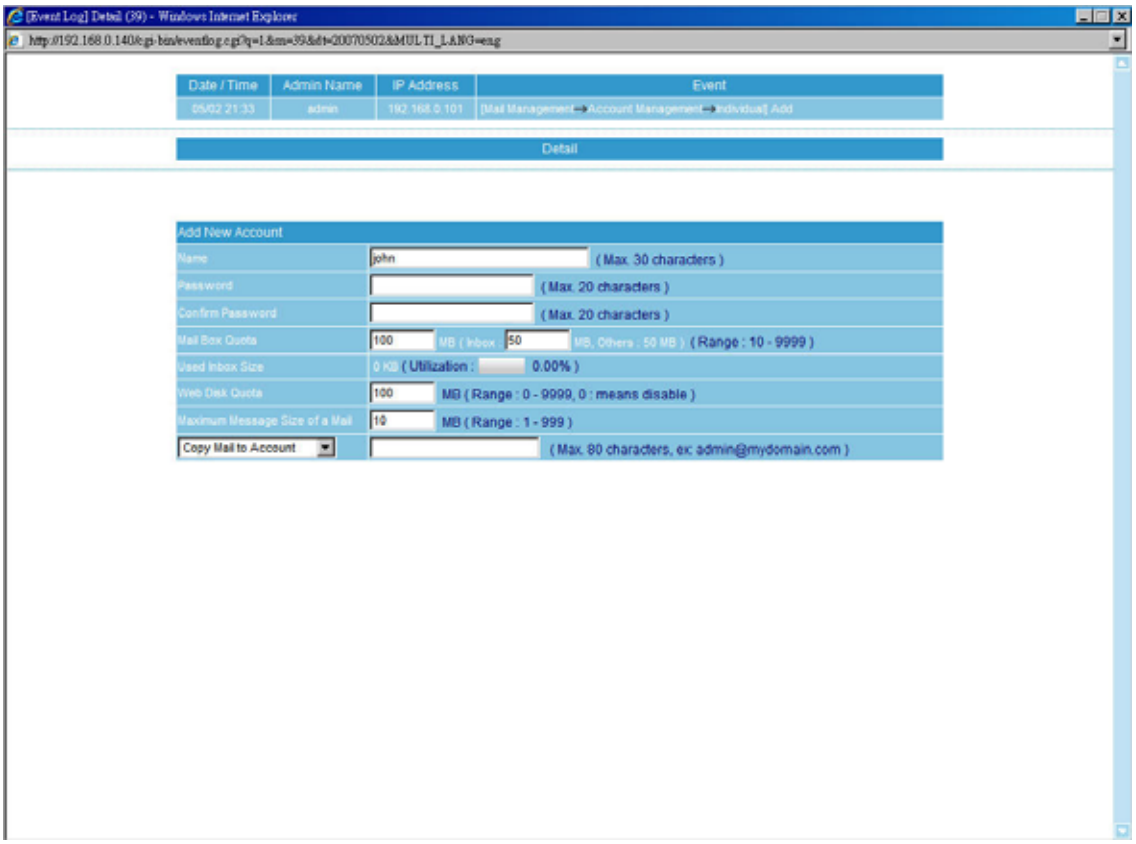


Figure 14-4 Event log details

Chapter 15 Introduction of Mail System

A mail server acts as an intermediate between the Internet and users when sending or receiving mails. The format of email address looks like account@server.name. Info on the left side of at sign (@) indicates an account name, the other side stands for the host name.

For instance, you are sending a mail to josh@yahoo.com.tw, your email software will go to your DNS server for the IP address and mail exchanger record that corresponding to mail server. Mails will go to mail exchanger before sending to the host server, in this case, it is yahoo.com.tw. If the DNS server has more than one MX, then mails will be sent to the MX with the highest priority. Provided that there is no MX, mails will not be delivered until the corresponding IP has found. When mails have been delivered to yahoo.com.tw, mails will be distributed to the user according to its account name which shows on the left side of at sign (@).

Process of an email transmission:
The transmissions are divided into three parts, namely MUA, MTA and MDA.

- **MUA (Mail User Agent):** Whether sending or receiving mail, the end-user client must account on the MUA which provided by the OS, for end-user client can not send mail directly. Outlook Express is a kind of the MUA. It serves as a mail deliver and recipient, and enables user to view and edit mails.
- **MTA (Mail Transfer Agent):** Outgoing and incoming mails are all done by MTA. It allows user to:
  1. Receive mails from other host. As long as user has a account under MTA, then the user will be able to receive mail.
  2. Sent out mails. On condition that the user has the authority, he will be able to send out mails.
  3. Receive personal mails. User can retrieve and view mails that saved on the mail server.

Usually, MTA refers to a mail server.

- **MDA (Mail Delivery Agent):** distributes incoming mails of MTA to local mail accounts according to their account names or sends them to the next MTA.

Take sending and receiving mail for example to illustrate the process of mail transmission.

When user wants to send a mail:

- Send mails to MTA via MUA. While composing email with MUA, make sure to follow steps below :

  1. Enter the sender email address and outgoing mail server (namely the sender MTA)
  2. Enter the recipient email address and incoming mail server (namely the recipient MTA for receiving mails from external host server)

After user finished composing a mail with MUA, such as Outlook Express, mail can deliver to the appointed MTA by clicking on **Send**.

- When MTA receives mails from itself, MDA will distribute received mails to each mailbox according to account names.
- When receiving mails of recipients from other MTA, it will automatically forward these mails to that MTA. This function is called Relay.
- A distant MTA is able to receive mails from local MTA. The distant MDA will take over the received mails and store them waiting for user to log in to download them.

The process of receiving mails:

A remote user inquires his MTA for checking new incoming mails, if MDA detects new mails, mails will be sent to user's MUA. Meanwhile, MTA will clear up the mailbox or keep those mails according to the MUA settings.

Email Protocols: SMTP & POP3

1. Sending Mails: signifies mails transferred from MUA to MTA and from MTA to MTA. Nowadays most mail servers use SMTP (Simple Mail Transfer Protocol) for outgoing mails. And the port 25 is assigned to SMTP protocol.
2. Receiving Mails: signifies MUA using POP (Post Office Protocol) to communicate with MTA so as to read or download mails in user's mailbox. Currently, POP3 (Post Office Protocol version 3) is the most popular protocol for incoming mails. And the port 110 is assigned to POP3 protocol.

Usually MTA needs at least two protocols, namely SMTP and POP3, to receive and send mails. As long as both MUA and MTA support SMTP and POP3 protocols, mail servers will be able to interact with each other.

Relay, a function that MTA transfers mails to another MTA, functions when MTA has learned that mail recipient does not exist on itself will transfer mails to another MTA.

A mail server which could be used to transfer mails by anyone is called Open Relay. To avoid this, presently most of mail servers set Relay as disabled. Only local host can utilize relay to receive mails that specified for this MTA accounts form Internet. Basically, there is no doubt that relay enables MTA to receive mails, yet there is a drawback in it. Since MTA normally allows certain trusted mail servers with specified IPs and segments to relay, so that client user could use mail services without limitation while other unspecified users been blocked. Thus, SMTP Authentication is invented to solve this problem.

SMTP Authentication, a mechanism that MTA inspects sender account and password from MUA, happens when mails transfer from MUA to MTA. It has a benefit of enabling relay function to authentic MTA accounts rather than certain trusted domain name or IP. Because of SMTP Authentication, MTA will neither accept incoming mails nor provide mail delivery service unless the sender is authentic.