PineApp™ Mail-SeCure™

User Manual
v3.70

1000/2000/3000/5000 series

Mail-SeCure User Guide
1000/2000/3000/5000 Series
Version 3.70
Revision 1
January 2013

PineApp International
8, Hata'asia Street
Nesher, 36601
Israel
Tel. +972 4 8212 321
Fax. +972 4 8203 676
http://www.PineApp.com

Contents

CHAPTER 1

INTRODUCTION

Before you start

Mail-SeCure is a leading security appliance that protects organizations of all sizes from both targeted and non-targeted threats. Mail-SeCure's improved scanning capabilities enable better content control and increased mail-server performance.
All email traffic is scanned and the internal network is protected from known and unknown threats such as Viruses, Worms, Trojan Horses, Backscatter and Spam. Mail-SeCure's five Anti-Virus layers and eleven Anti-Spam engines make up the comprehensive security protection suite.

The system provides administrators with tools to enforce advanced local policy and provides users with a mechanism to control and manage their own mail flow.

Mail-SeCure products are user-friendly, designed with an intuitive management interface and custom policy management tools.

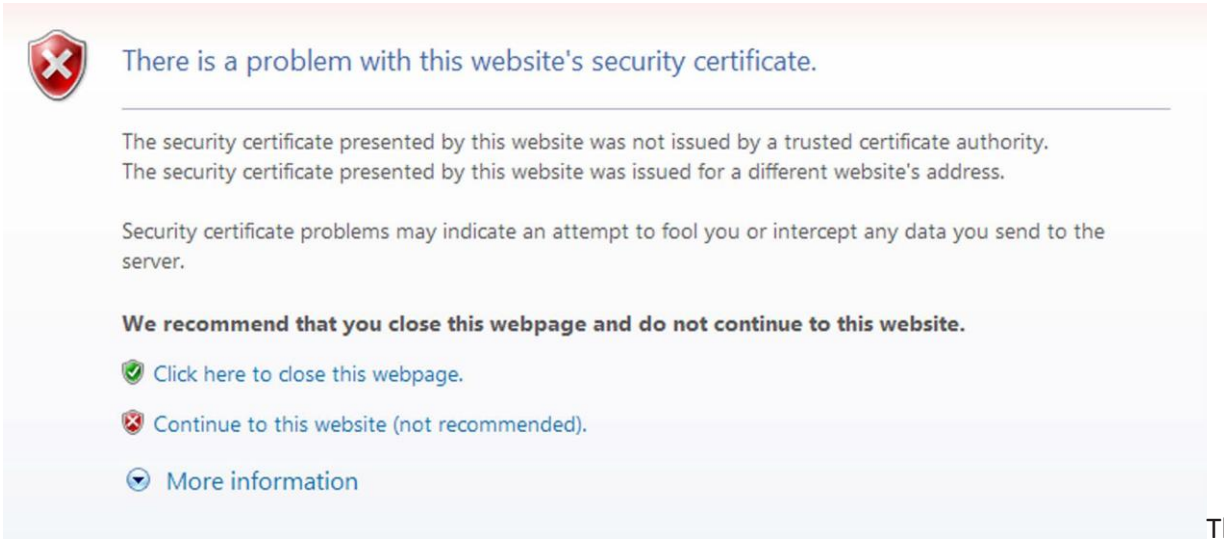
Before changing the configuration, it is important to understand all of the different features, their function in the system and what results will occur when making changes to these features.
This document provides information about operating and managing Mail- SeCure™ 1000, 2000, 3000 and 5000 series.
Note All units are shipped with a Limited Hardware Warranty card and an End User License Agreement. If these items are missing, please contact your local reseller or distributor.

Accessing Mail-SeCure via web browser

Mail-SeCure is accessed easily using any common web browser.
Connect the appliance to your internal network (port 1 on the appliance). Open any web-browser.

To access Mail-SeCure™ for the first time you need to type the default IP address of your appliance which is **https://192.168.24.24:7443**. If you are having trouble connecting, check your firewall setting and be certain that it is configured for this IP range.
To access your appliance without having to make changes to your firewall settings, you can simply create a static route to the device in your firewall. Once you have logged into the device you can change the IP address.

A security alert message will appear. Click OK to continue. In IE 7.0, an error page will be displayed. Click on **"Continue to this website (not recommended)"** (marked in a red square in the picture below) in order to continue.



The following login window will be displayed.
Log into the system, using the default username (**pineapp)** and the default password (**password)**.

The system will use the local default language settings to identify the default language. It is also possible to select the desired language from the scroll down menu.

Upon entry, the System Information pane will be displayed.
This pane provides a variety of information about the system. The information presented in this pane will be discussed at length in the *System* chapter.
Note Mail-SeCure's Pre-configured IP: 192.168.24.24
Username: pineapp
Password: password
It is highly recommended to change the password after logging in for the first time.

CHAPTER 2

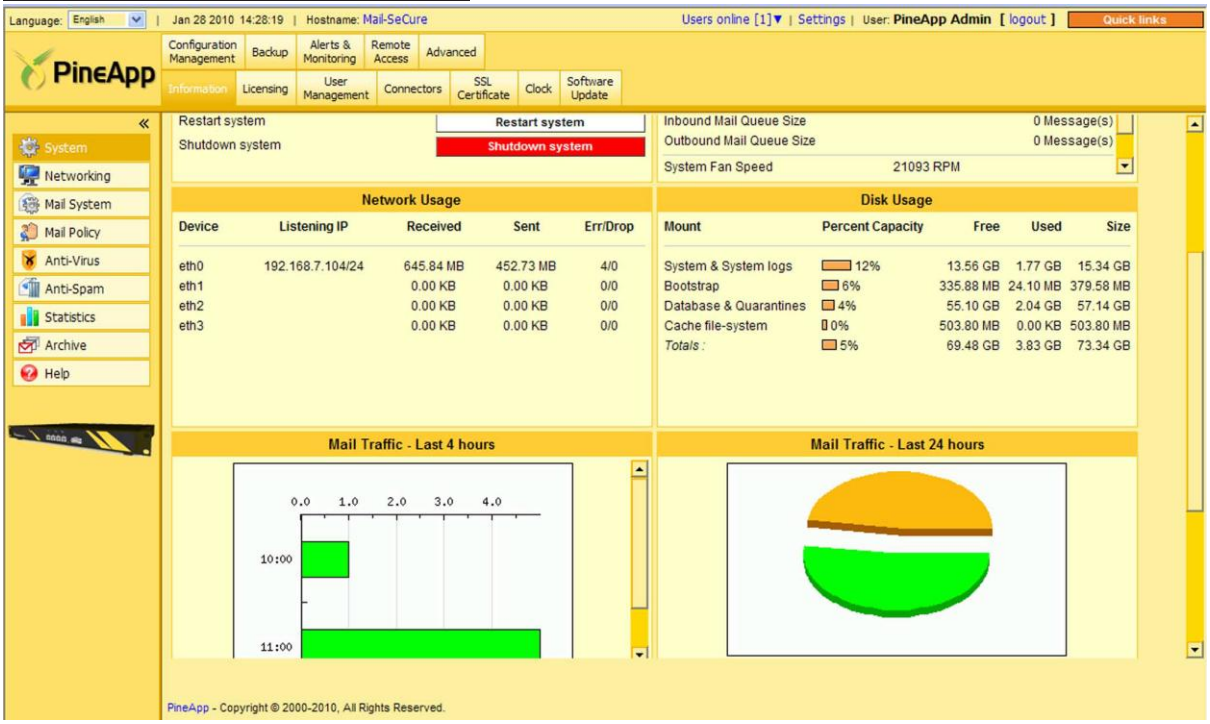
SYSTEM

Note Before any changes are made to the configuration we recommend that you make a backup of the default set-up. This can be done by choosing the Configuration Management option in the System menu.

General information

Once successfully logged in for the first time you will need to approve the
EULA (End User License Agreement). Once approved, the EULA will not appear again.

How to work with Mail-SeCure's GUI



The GUI is divided into three panels:

1. **Top panel** (marked green in the picture above)
2. **Left Panel** (marked blue in the picture above)
3. **Main Panel** (marked red in the picture above)

Top Panel

The top panel contains some important features that will help manage the device in an easier and more intuitive manner.

The top panel will always stay in place while you browse the GUI

1. **Language** - Changing the language interface can be done any time by choosing the desired language from the dropdown menu.

2. **Settings** - The purpose of the *settings* link is to determine how many records will be displayed in different tabs and menus.

3. **Logout link** - Clicking on the *logout* link will logout the current user and bring the GUI to the initial login screen.

4. **Quick links** - Quick links are a shortcut to the most commonly used tabs. Moving the mouse over the *quick links* bar will show the different links.

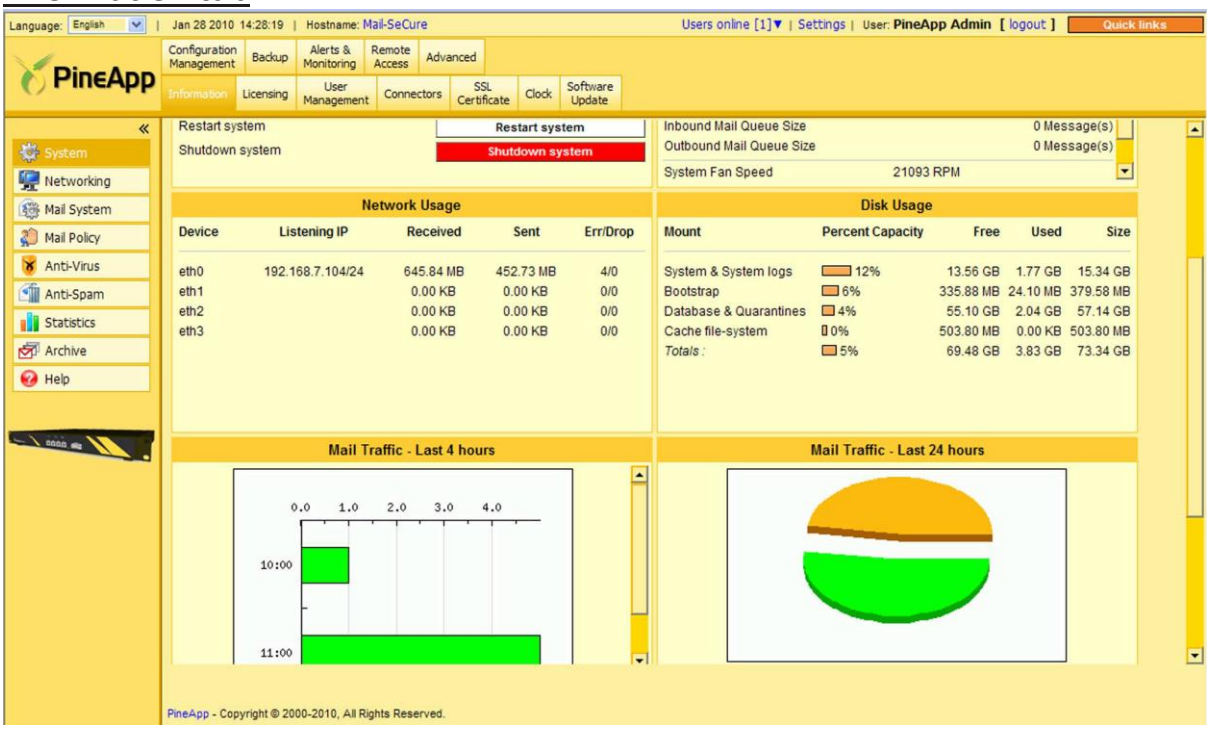
Left Panel

The left panel contains links to the different menu tabs. Clicking on the desired menu will open its content in the main panel. There are two ways to reach different tabs:
A) By clicking on the menu and then on the required tab.
B) By right-clicking on the required menu and choosing the tab you wish to access
Clicking on the arrows will minimize the left panel, thus increasing the main panel area.

Main Panel

Clicking on different options in the left panel will open different options in the main panel. Follow the instructions of this user guide in order to understand the different functionalities of the system.

Information tab



This is the first pane that appears after logging in.

The screen provides the most important and essential information regarding the system. This pane contains four main tables: System Summary, Network Usage, System Status and Disk Usage.

System Summary

This table contains information such as the licensing, model, version, latest Anti-Virus update and information about who is logged into the system.
Restart System - Use this button in order to reboot the system properly.
Shutdown System - Use this button in order to shutdown the system properly.

Network usage

This table provides network information such as IP addresses and Data flow. In addition, Errors and Drops can be monitored here.

System status

This table is divided into three sections:
1. This provides information on the domain name, Uptime and Load averages.
These calculate the average amount of processes handled by the CPU, in the last 1, 5, and 15 minutes.
2. Hardware Vitals - this contains four important parameters that determine the temperature of the system: CPU Fan Speed, System Temperature, CPU Temperature and System Board Temperature. If a value exceeds its normal limits, it will turn red.
3. Operational Vitals - Displays Mail-SeCure's operational vitals. An extended explanation regarding each feature will be provided later in this guide.

Mail System - This section shows weather Mail-SeCure's Mail system, in charge of all mail delivery processes, is Operational/Down

Advanced Anti-Spam System - This section shows weather Mail-Secure's Anti-Spam system, in charge of all perimeter & content inspections, is Operational/Down/Disabled

Scanning Queue Size - This section shows the number of messages queuing to be scanned. A large number of messages may indicate a problem with the scanning engine or an overflow of messages.

Inbound Mail Queue Size - This section shows the number of messages waiting to be delivered to the mail server. A large number of messages may indicate a problem with the external mail server (i.e Exchange server).

Outbound Mail Queue Size - This section shows the number of messages waiting to be delivered to external mail servers. When mail is stuck in this queue, it usually indicates on a problem with the recipient's mail server (it may be down; may have connection timeouts, etc.). It may also indicate that the message is too large to go through the system.

Disk usage

This shows the disk usage and the percentage of free space on the disk. If the percentage capacity of any of the partitions is too high, please contact **support@pineapp.com**.

Mail Traffic - Last 4 hours - This section provides graphic statistical analysis for the traffic that has arrived the system during the last 4 hours.

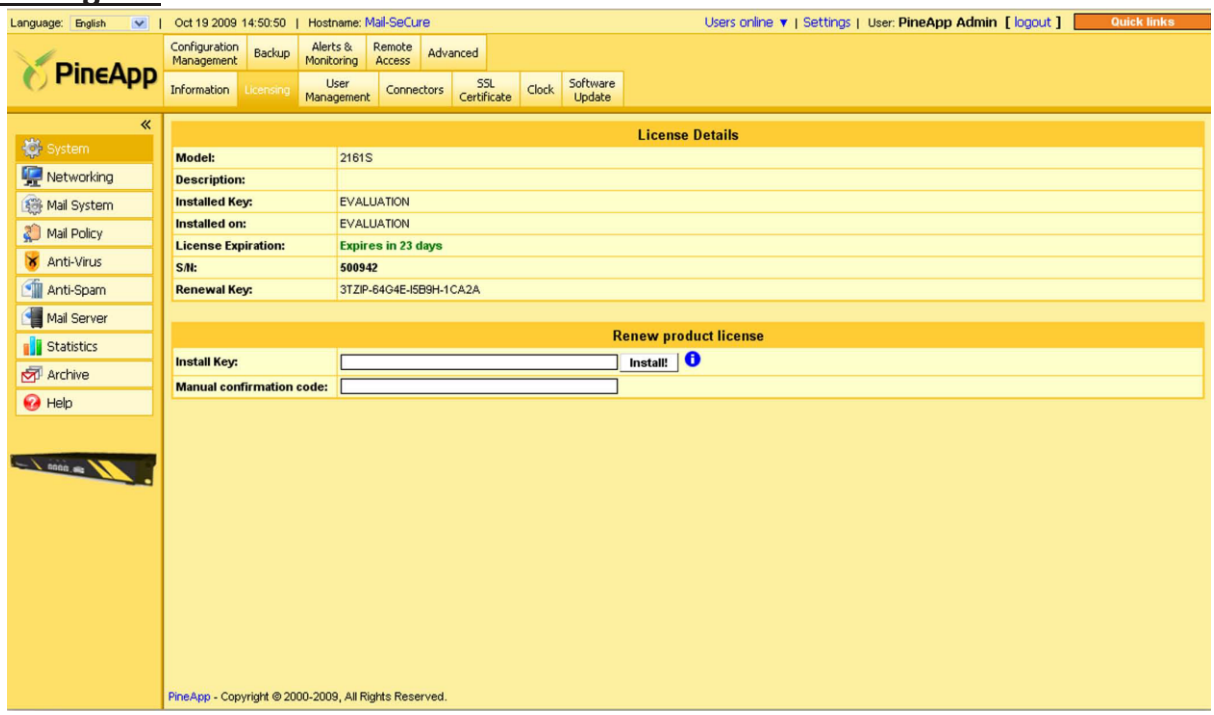
Mail Traffic - Last 24 hours - This section provides graphic statistical analysis for the traffic that has arrived the system during the last 24 hours.

System Log - This section provides recently displays system log records.

AV Update Log - This section displays recently added Anti-Virus update log records.

Some features in Mail-SeCure must be handled only by a network manager or other personnel who are familiar with the network in which they are working.

Licensing tab



This tab contains all license related information, including model and modules purchased, as well as the installation and expiration dates.
In this pane the license key can be renewed or updated.

Installing license key

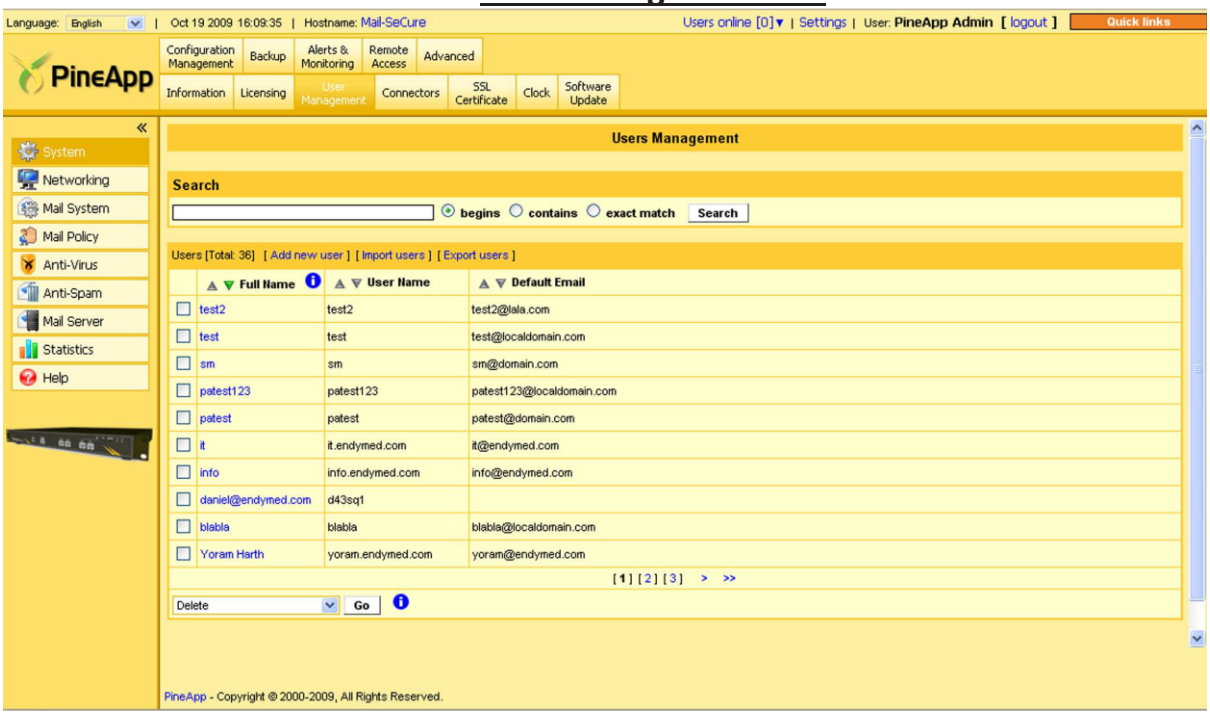
Copy and paste the renewal or update key received from PineApp or the distributor into the *Install key* field and click the **Install** button. The new updated info will be displayed in this pane.

If the system is not connected to the Internet, update the unit manually:
A) Log into PineApp's web site (**http://212.235.58.200/support/product-registration.html**) and enter the key received from PineApp and the renewal key as listed in the *Licensing* tab page.
B) The site will generate a confirmation code.
C) Type the confirmation code in the correct field, enter the install key received from PineApp and click the **Install** button.

* Mail Encryption Solution users can both install their license key, and also view the remaining number of mail encryptions for their license via this window.

Make sure the device is connected to the internet (port 80 is open from the device to the world) before installing the license

User management tab



User management tab allows configuration and adjustments for new and existing users.
There are three methods for configuring users:
1. Manually - Each user can be configured manually.
2. Synchronizing with an authentication (LDAP) server - See Connectors tab
3. Import users list from a CSV file or a passwd file.

There are four purposes for defining users:

1. **GUI Management** - It is possible to assign different management permissions to different users. There are five levels of permissions:
Default - This default permission is taken from the default permission setting dropdown menu in Mail Policy >General. This is the default permission the user receives after he is created on the system.
None - Users cannot log into the Management GUI at all.
Manager - Users can log into the Management GUI and have full manageable privileges and full access to all panes.
Quarantine Manager - Users can log into the Management GUI but will have access only to the quarantine menu (Mail Traffic Management tab).
Network Manager - Users can log into the Management GUI but will have access only to the Networking menu.

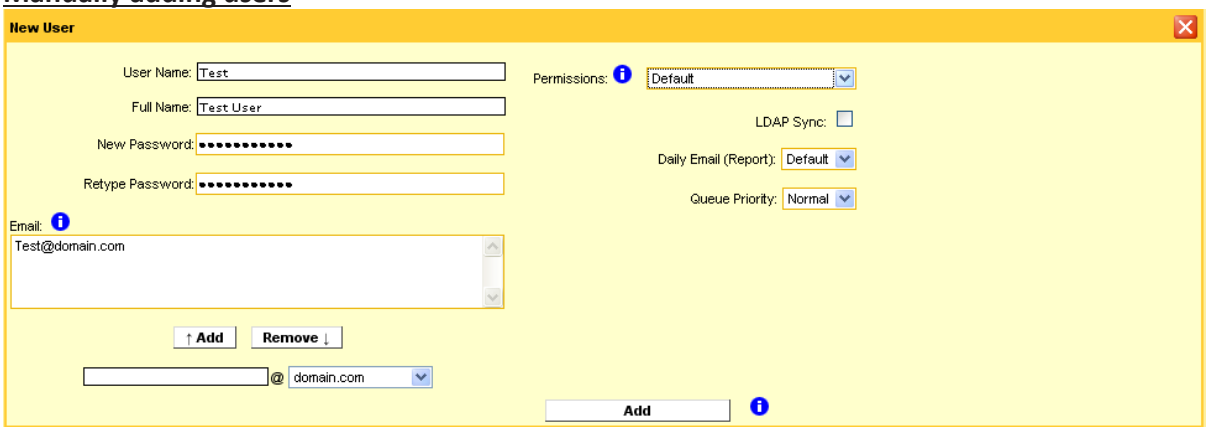
2. **User Management** - in order to initiate Group/User policy management, users must first be defined. There is no need to define all of the organization's users - Only users with different policy privileges than the "Everyone" group.
If the user database in this tab is synchronized with an LDAP server, check the box. The information will be updated using the LDAP server connection settings, configured in the Connectors tab.

Mail & System Users can login to the Management GUI but will have access only to the Mail Server menu.
Personal Quarantine Manager Users can login and manage their Quarantined mail. They can release, view, add addresses to their Black & White lists and download quarantined mail. The personal Black & White list can also be managed from within their GUI.
Users can also search the logs of all the mail that they sent or was sent to them.
Personal Spam Manager Users can login and manage their Spam. They can release and view their quarantined Spam messages. However, only mail that was quarantined as Spam will be visible to these users.
Domain quarantine managers can login and manage their domain's Quarantined mail. They can release and view their domain's quarantined mail. They are also able to view and search the logs of all the mail that was sent to and from their domain. The domain manager can manage all domains of emails that where assigned to him.
For example, if he has 2 emails: aa@aa.com and aa@bb.com, he will manage domains aa.com and bb.com.
Domain Spam managers can login and manage Quarantined Spam messages for their entire domain. They can release and view their domain's quarantined mail. However, only mail that was quarantined as Spam will be visible to the Domain managers. The domain manager can manage only one domain. The managed domain is set by choosing the default email in the user management.
Read only Allow read only permission to all menus

3. Daily Report - In order to allow the user to receive daily reports regarding his mail traffic and personalized Black & White lists, the appropriate settings must be chosen.

4. Special handling for non-existing users - In order to prevent harvest attacks, once all users are configured, it is possible to activate the special handling for non-existing users (Chapter 5, Mail Policy > General).
Queue Priority - It is possible to prioritize the queue of the user compared to the rest of the users in the organization. This feature has a true effect when the scanning queue starts to accumulate (default: Normal).

Manually adding users



A) Click on the *Add new user* link. A new panel will pop-up (as seen above) on the right hand side of the screen:
Default - When creating a new user (manually or by synchronizing to an LDAP server), the user will receive the "default" settings. If the option in *Anti-Spam > Daily Report > Send user daily report* is checked, then all users with the default permission will receive the daily report. If it is unchecked, they will not.

YES - The user will receive the daily report regardless of weather the option in *Anti-Spam > Daily Report > Send user daily report* is unchecked.
NO - The user will NOT receive the daily report, regardless of weather the option in *Anti-Spam > Daily Report > Send user daily report* is checked.
B) In the empty fields, under the new user title, enter a user name, full name (optional), email (It is possible to add more than one email).
Use the dropdown menu to pick the domain. The domains are configured in the Local Domains tab/
C) After adding the emails, choose the default email by clicking on it.
D) Click on the **Update** button.
E) Type and retype the password for that user.
F) Choose the permission of the user from the menu.
G) Choose whether the specific user will be synchronized with an LDAP server
(Check the box). If the user was synchronized with a LDAP server, this box will be checked.
H) Daily Report - When set to default, the user will receive (or not receive) a daily report according to the Default status (configured in Daily Report tab). If, for that specific user, you wish to configure otherwise to the default, choose Yes/No from the drop-down menu.
I) Click the **Add** button to finalize the procedure. The new user's name should appear in the left column.
Once added, the user will appear in the user list: By default, the order of the list is by the full name - Alphabetically. It is possible to view the list by user name or by the default Email by clicking on the arrows next to the header.

Modifying users
By clicking on the Full name in the left column, user details will appear on the right hand side of the screen. There, all modifications can be made – including changing the password. When you finish changing the password, click the **Update** button.

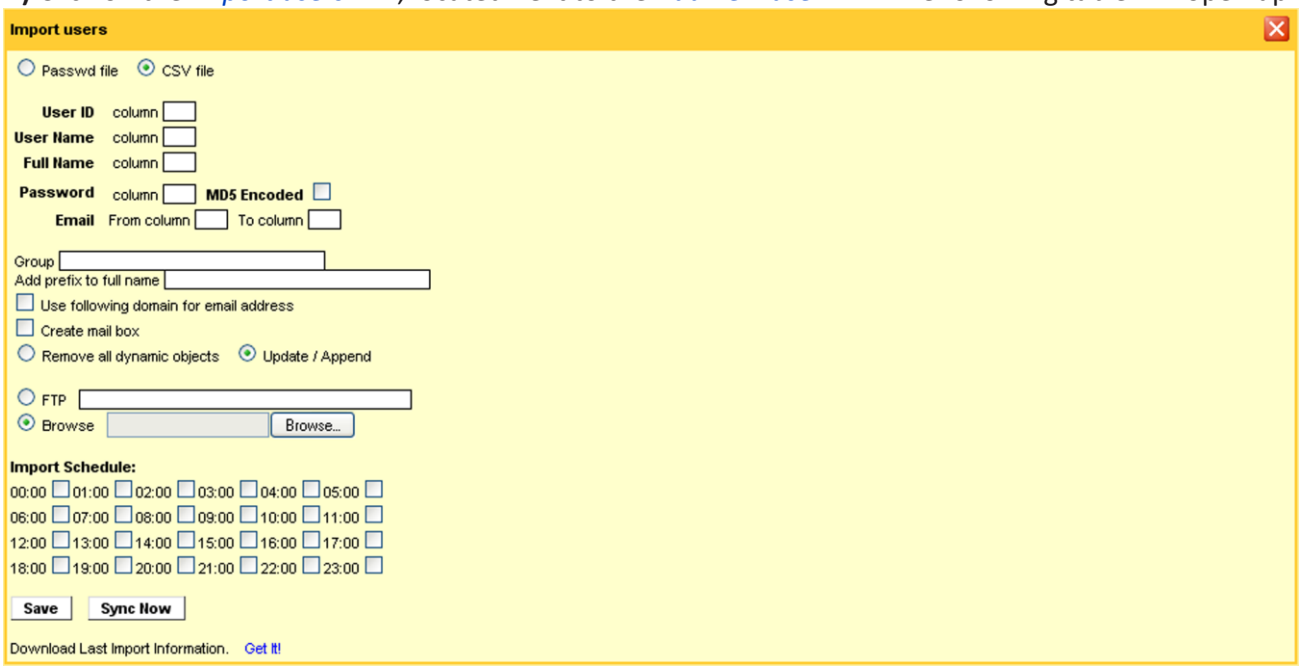
Deleting users
In order to delete users which were created manually, check the box(es) next to the user(s) that you wish to delete in the left column, choose "Delete" from the below dropdown menu and click the **Go!** button.
In order to delete users which are syncronized from the organization's LDAP server, delete the users on your LDAP server first, and perform user syncronization on the Connectors tab/

Remove all dynamic objects
This will remove **all** users that were synchronized through the LDAP server. It will also delete all group and user's level rules. There is no need to check the users before pressing the **Go** button.

Importing and exporting users

It is possible to import existing users from CSV or Password files.

A) Click on the *Import users* link, located next to the *Add new user* link. The following table will open up.



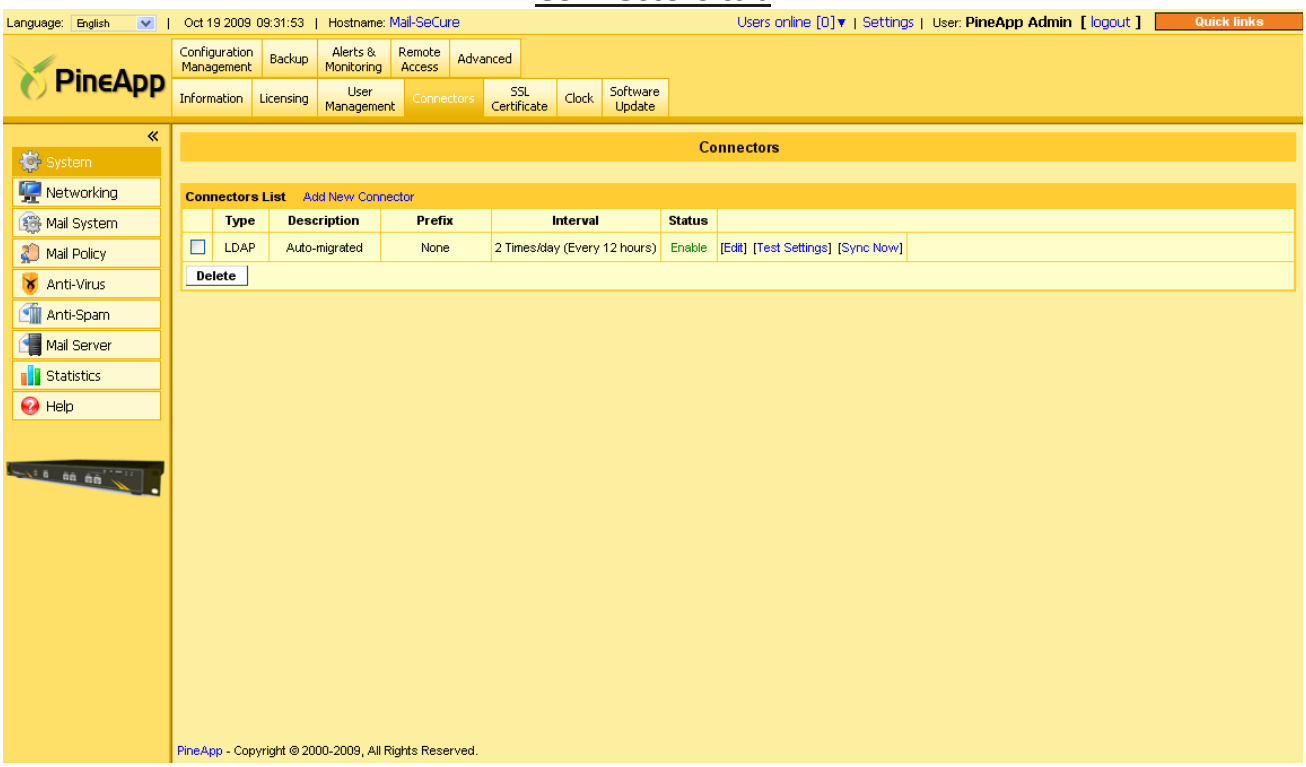
B) From within the table, choose whether you want to import the users from a password file or a CSV file. The table will change according to the method chosen.

C) After filling the proper fields, hit the **save** button in order to save the settings and then the **Sync now** button (marked in red and green squares respectiively in the picture above) in order to upload the new users.

Make sure you have the files properly edited and that you have the import table configured accordingly. Exporting users is done by clicking on the *export users* link. Mail-SeCure will export the users to a CSV file that you can save or open.

The first column on the CSV file has index 0 and not 1.

Connectors tab



In this tab, it is possible to configure different connectors such as LDAP. It is possible to configure more than one connector.

The system supports the following LDAP servers: Exchange 5.5, Windows 2000, Windows 2003, Communigate pro 5.x, Lotus Notes and Open LDAP.

This feature provides the ability to authenticate SMTP connections to PineApp. It will also import the users from the LDAP server into the User Management tab, thus easing all management and email policy aspects significantly.

Once synchronized, it is possible to perform the following actions on the users:

1. Send daily reports.

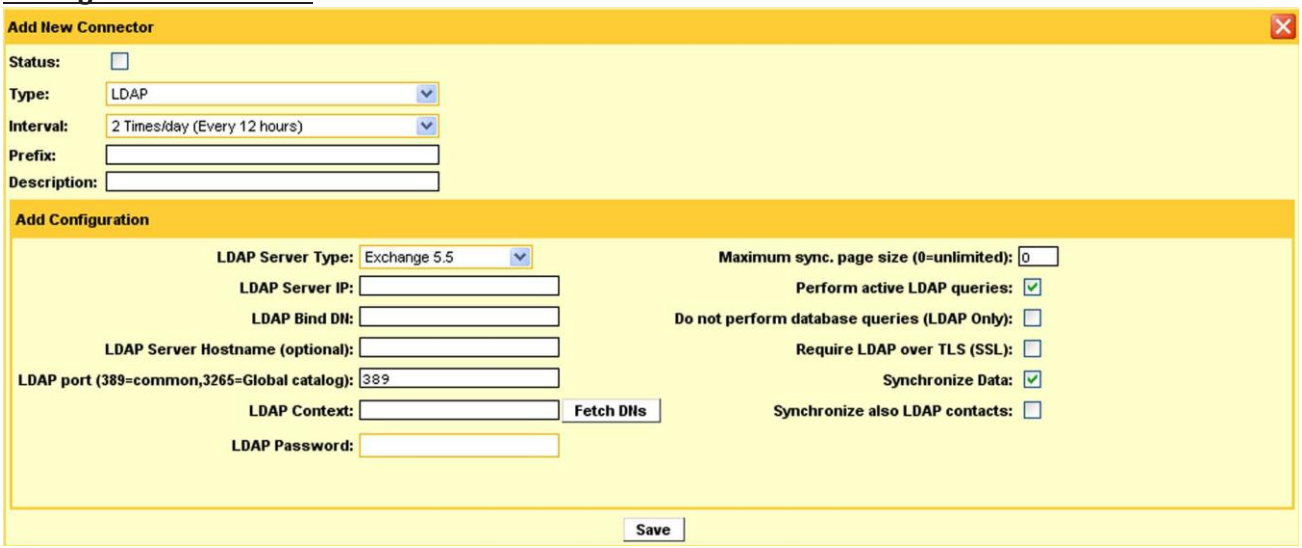
2. Use the users' information for SMTP Authentication.

3. Activate the "Special handling for Non-Existing users" feature.

4. Personal Quarantine.

5. Personal Black & White lists.

Adding a new connector



In order to create a new connector, click on the *Add new Connector* link. The above screen will open up.

Status - Check box to activate module.

Type - At this stage, Mail-SeCure only supports LDAP-based connectors.

Interval - Choose the synchronization intervals to the LDAP server from the drop-down menu. It is recommended not to define intervals more than 8 times per day.

Prefix - The text written in this input field will be added before each of the connectors' synchronized users Full Name credential. This feature is used in order to differentiate between users of different LDAP connectors.

Description - Describe (not mandatory) the LDAP connector.

LDAP Server type - Choose the type of the LDAP server from the dropdown menu.

LDAP Server IP - Enter the LDAP server's IP.

LDAP Bind DN - Enter credentials for a user that has searching privileges in the tree. Example: administrator@pineapp.com.

LDAP Server Hostname (optional) - Enter the LDAP server's Hostname (optional).

LDAP port (389=common, 3265=Global catalog) - If you are not using the default port (389), type the alternate port you are using to synchronize the LDAP server.
LDAP Context - Enter the Root Branch definition. For example, if the domain is pineapp.com, type: dc=pineapp, dc=com (There must be a space between the comma and "dc").

Pressing the **Fetch DNs** button will cause the different DNs that are available on the specific Active directory to pop up. Make sure you have defined the IP of the LDAP server, Bind DN and password before pressing it.

LDAP Password - Enter the Password for the above user.

Maximum sync, page size (0=unlimited) - If the LDAP server does not support paging (like communigate Pro 5.x), paging is necessary for higher performance (default = 100).

Perform active LDAP query - When the special handling mail for non-existing users is activated (page 5-2), please check this box if you want the system to perform an LDAP query if the user doesn't appear in the local user management or cache. This is useful if a new user was added to the LDAP server but wasn't synchronized with the Mail-SeCure (Default: Checked).

Do not perform database queries (LDAP Only) - When checked, the Mail-SeCure will not perform database queries. We recommend checking this box only if the user's information is needed. Do not check this if other information such as Email or password is required (Default: Unchecked)

Require LDAP over TLS (SSL) - If using LDAPS (secured LDAP), check this box and copy the LDAP server's certificate to the next box.

Synchronize Data - When checked, the Mail-SeCure will Sync the data - but will not perform queries.

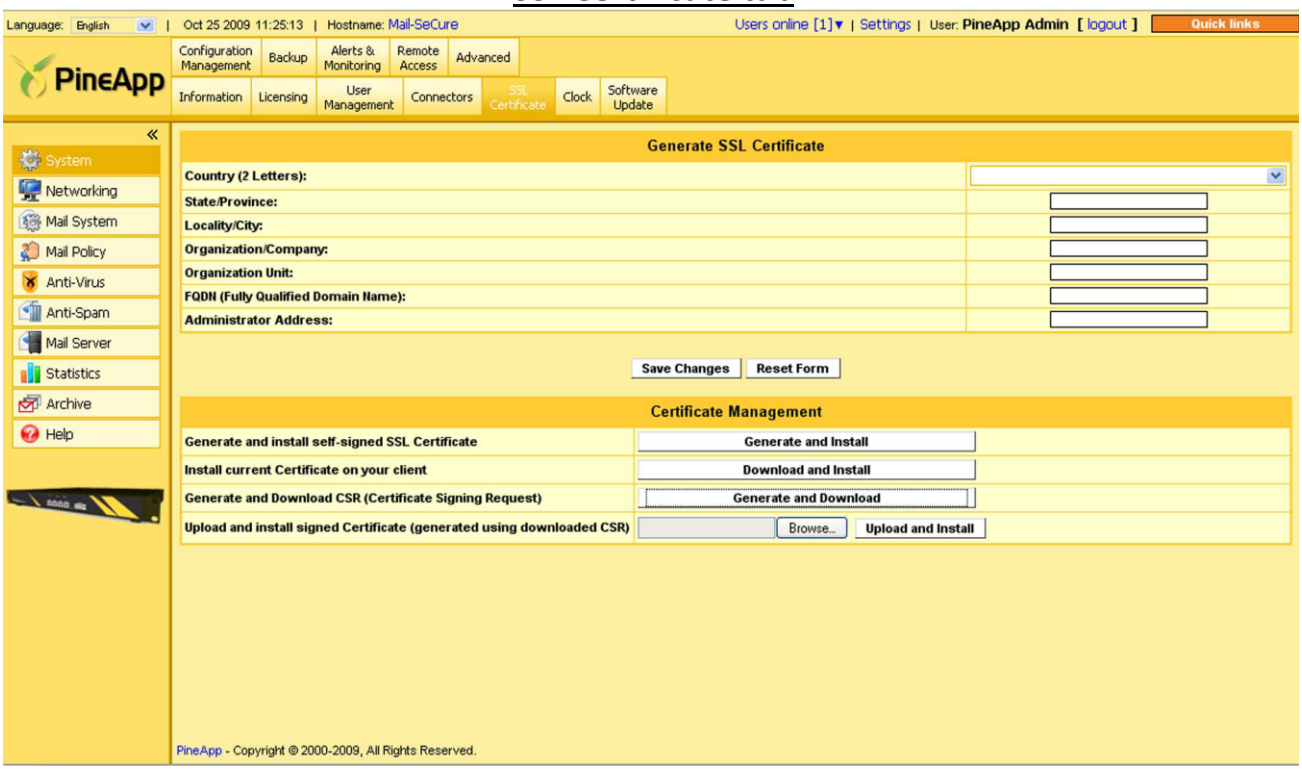
Synchronize also LDAP contacts - Check if you wish for the contacts to also be synchronized.

Once configured, click on the **save** button. It is possible to test the connectivity by clicking on the **Test Settings** button.

Configuring OpenLDAP

If OpenLDAP is chosen from the drop-down menu, new fields will appear:
In order to configure these fields, we recommend you export the LDIF file from the openLDAP and match the fields as configured in the LDIF file to fields in the GUI.
mailto:Support%40pineapp.com?subject=Open%20LDAP%20assistancePlease contact support for further assistance.
mailto:Support%40pineapp.com?subject=Open%20LDAP%20assistance
mailto:Support%40pineapp.com?subject=Open%20LDAP%20assistanceIf successfully synced, the list of all the users will appear in the user management tab.

SSL Certificate tab



Customers that would like to verify the validity of their Mail-SeCure appliance's web page, can assist the SSL Certificate Tab in order to implement an SSL Certificate to the appliance.
SSL certificates can be implemented either independantly (PineApp's self-signed certificate) or by implementing a CA (Certificate Authority) originated certificate, from third-party certificate companies (such as Verisign,)

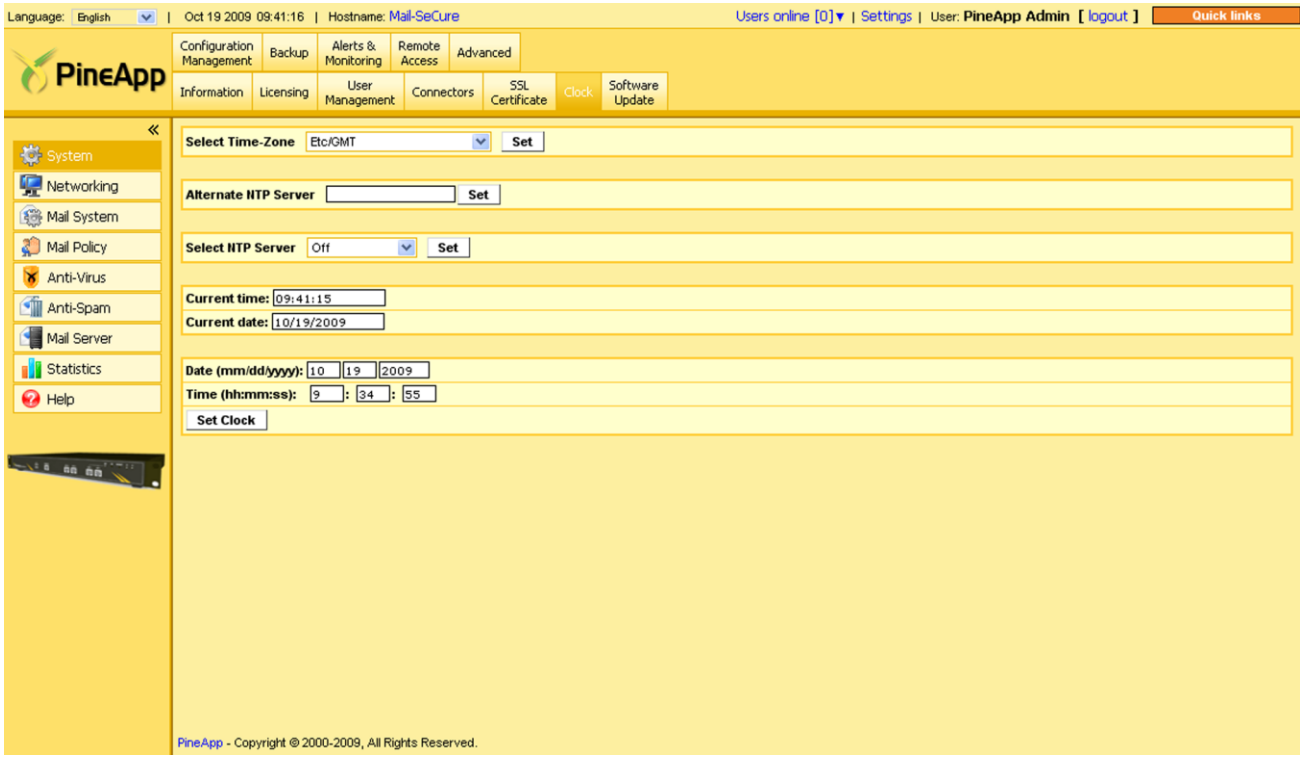
Generating a self signed certificate

Fill in the following details:
A) Country - Choose the country of your company's location (initals) from the dropdown menu.
B) State/Province - Type the state/province of your company's location
C) Locality/City - Type your company's full city name.
D) Organization/Company - Type your company's full name.
E) Organization Unit - Type two initials for the company sector in charge of implementing the certificate (for example: IT, HQ etc.)
F) FQDN (Fully Qualified Domain Name)- Type the full URL address of the Mail-SeCure appliance (for example: mail-relay.company.com).
G) Administrator address - Type the system/network administrator's email address.
I) Click on **Save Changes & Apply Settings**.
J) Click on **Generate & Install Certificate** button.

Generating & Installing a third-party license

A) Repeat steps A-I from **Generating a self signed certificate** section.
B) Click on **Generate & Download CSR**
C) Send the CSR to the CA you've purchased the license from.
D) The CA will send a new certificate file, created using the CSR you've generated. Save this file on your computer.
E) Upload the certificate file to the system, using the **Browse** and **Upload & Install** buttons.

Clock tab

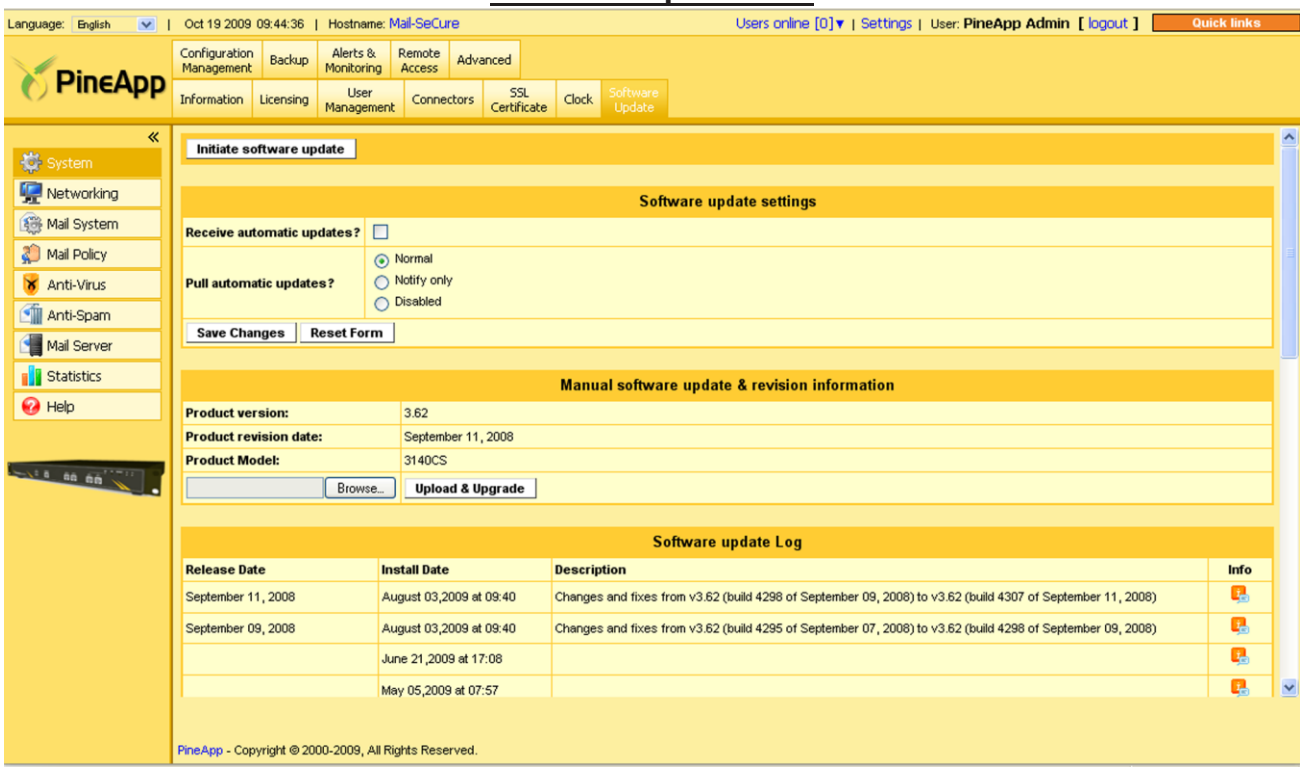


In the Clock tab, the local date, time and time zone are set.
It is possible to use the clock in two ways: NTP and manually.
Using the NTP is simply done by choosing your country from the dropdown NTP menu and clicking on the **Set** button or by manually entering the IP of the NTP server and clicking on the **Set** button.

Setting the clock manually

A) Choose the correct time zone according to your geographic location from the dropdown menu.
B) Modify the date and time values as desired in their appropriate fields.
C) Click the **Set Clock** button.

Software Update tab



The Software Update tab contains Mail-SeCure's software update-related features.

Check the **Receive automatic updates from PineApp Servers** option to enable this feature (Default: Unchecked).

Pull automatic updates from PineApp server - there are three options:

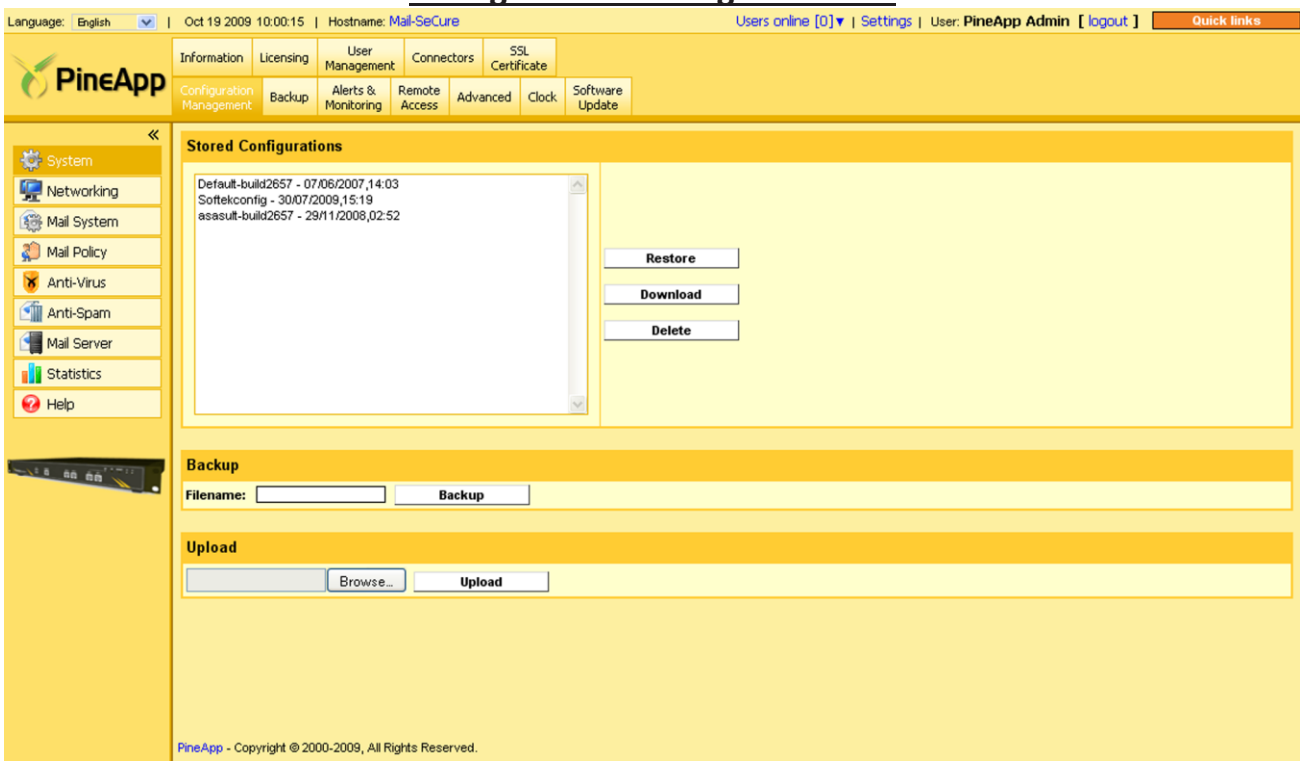
1. **Normal** - Mail-SeCure will initiate a software update by checking PineApp's servers twice a day. Keeping this box checked will assure that the unit stays updated (Default: Checked).
2. **Notify only** - The postmaster will receive an email notifying him there is a new update. Then, the postmaster can log into the system and initiate a software update by clicking on the button. A **New update is available!** notification will also appear on the screen.
3. **Disabled** - When checked, Mail-SeCure will NOT check for new updates. If the update option is disabled, it is possible to update the system manually.

Updating Mail-SeCure manually

1. Contact PineApp support in order to receive the latest update.
2. Click on the **Browse** button.
3. Select the corresponding file from the local disk.
4. Click the **Upload & Upgrade** button to complete the update.
Logs and release notes of the latest updates are generated and can be viewed at the end of this window. The log also provides the status of current and previous updates.

In order to keep the system updated at all times, it is highly recommended that you enable the automatic updates feature.

Configuration management tab



The Configuration Management tab enables you to backup, restore, upload and download a complete snapshot of the Mail-SeCure's configuration.

To backup the configurations, type in the name of the file to create and click the **Backup** button.

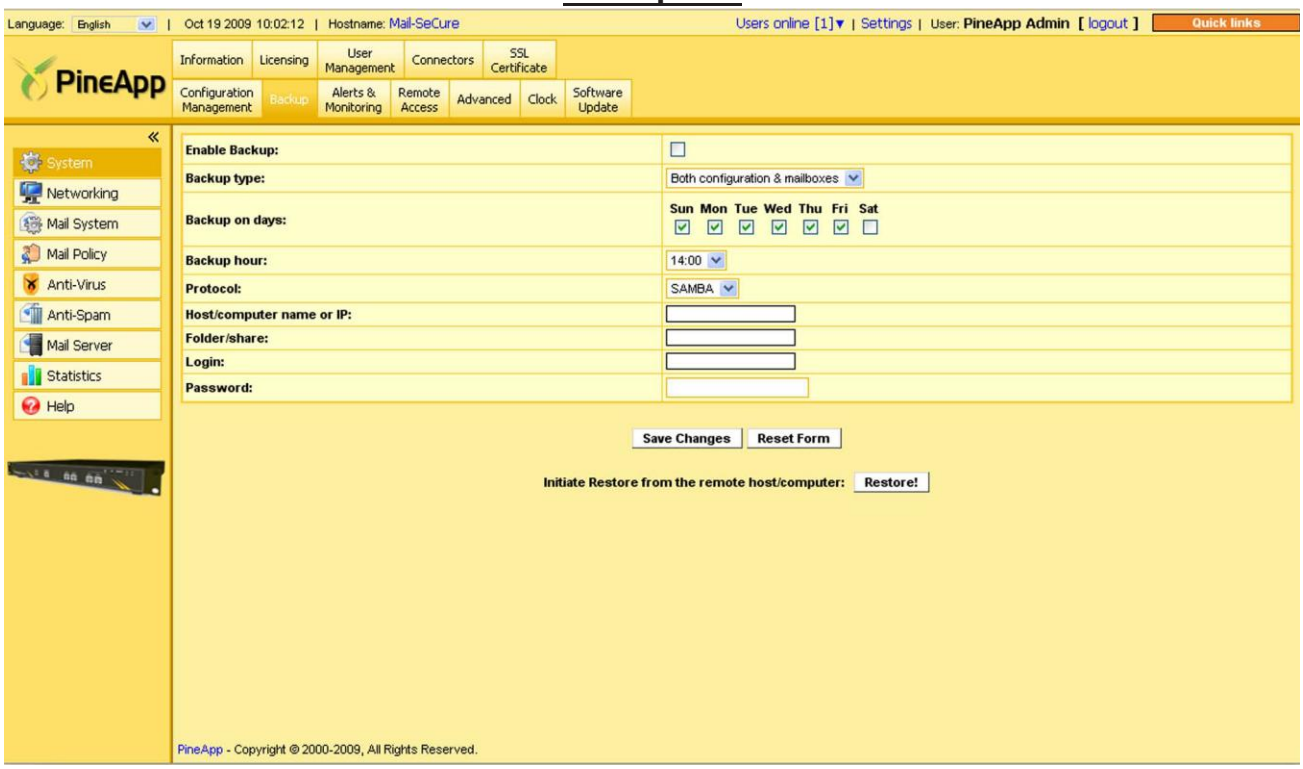
To download a configuration backup to the computer, select the desired set and click the **Download** button. Save the file on the desktop.

To upload a configuration backup, click the **Browse** button, select the desired file from the desktop and click the **Upload** button.

To restore the configuration, select the desired configuration and click the **Restore** button and **Apply changes.**

Make sure that the restored configuration's software version is matching to the software version that is currently updated on the appliance.

Backup Tab



This feature enables you to backup mail boxes and the system's configuration on a daily basis. This feature is only useful when the system acts as a Mail server.
First, check the **Enable backup** box and select to back up the configuration, mailboxes or both. Choose the days and times for the backup to be performed.

Backup instructions

Backing Up Mail-SeCure configuration (SAMBA protocol)

A) Choose the Samba protocol.
B) Go to the server or computer on the network and create a directory to which the backup file will be sent.
C) Configure the folder as shared.
D) In Mail-SeCure's Backup menu, type the server's (or computer's) IP and the name of the shared folder specified in step 3.
E) In the login and password fields, define the username and password to use to log into the server (or computer).
F) Click the **Save Changes** button and when done, click the **Apply Changes** button.
G) After the backup is completed, a file with the latest date will appear in the designated folder.

Backing Up Mail-SeCure configuration (FTP protocol)

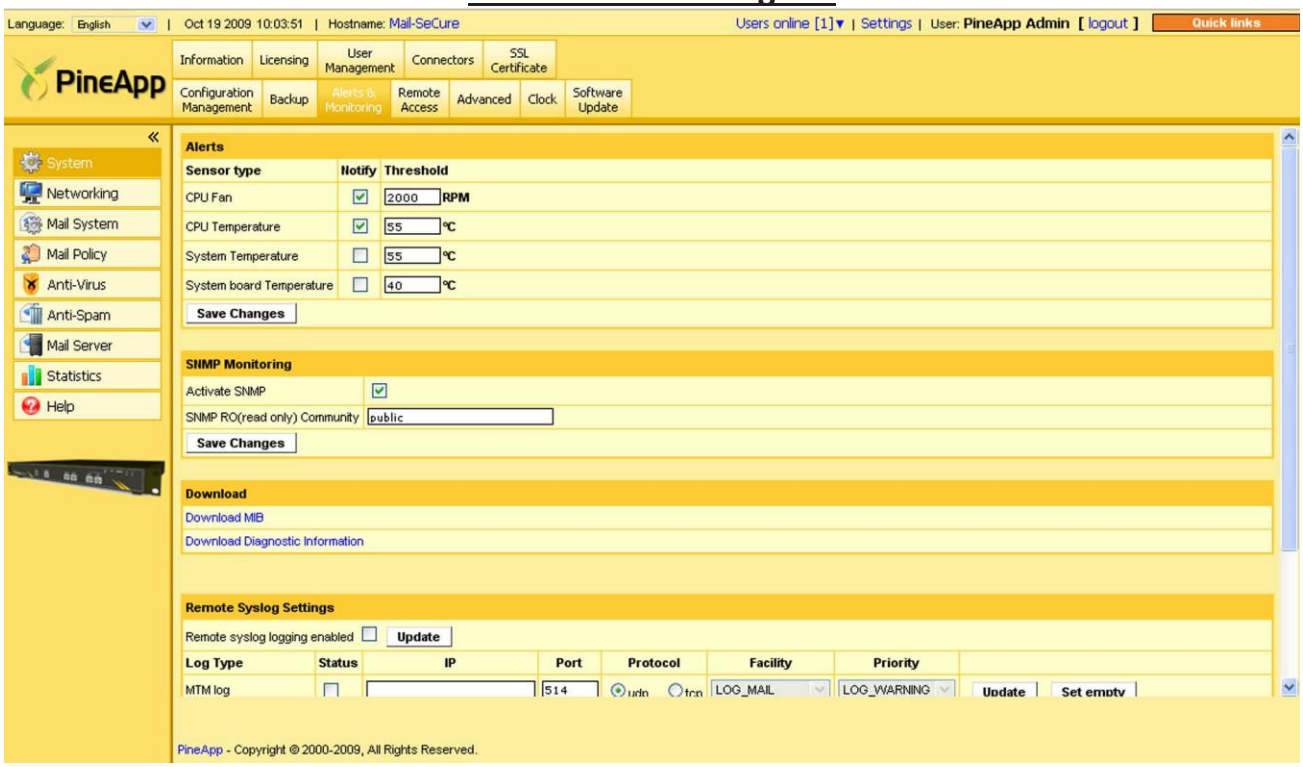
A) Choose the FTP protocol from the protocol menu.
B) Define the FTP server's details.
C) Click the **Save Changes** button and when done, click the **Apply Changes** button.
D) After the backup is completed, a file with the latest date will appear in the designated folder.

Restore instructions

After replacing a unit or after recovering mailboxes, the configuration must be redefined, as described in the above section. Make sure the exact same parameters are defined (share name, username, password etc.). After saving and applying changes, click the **Restore** button.

This stage will take some time, depending on the size of the backup file. No notification will be given when the restoration is completed. After this is completed, a full configuration's snapshot will be restored.

Alerts & monitoring tab



The alerts & monitoring tab allows administrators to receive notifications regarding system vitals. It also allows administrators to activate SNMP on the system. It is possible to download the current MIB from this tab.

As soon as one of the sensors in the system detects a parameter that has exceeded a threshold, an email will be sent to the postmaster. Though PineApp does not suggest modifying the thresholds, it is possible to do so in this pane.

SNMP Monitoring - This feature allows the administrator to monitor the system using the SNMP protocol. Download the MIB file from this page and open it using any MIB client.

Use: enterprises.19801

The file offers the standard host Resources MIB. In addition, information regarding the mail system, system temperature, Scanning queues, SMTP service Status Anti-virus versions and updates, Threads and performance is available using the MIB client.

Download Diagnostic Information - This feature allows the administrator to download information regarding Mail-SeCure's functionality from the unit.

Sending the downloaded file to PineApp's support (support@pineapp.com), will help us troubleshoot problems.

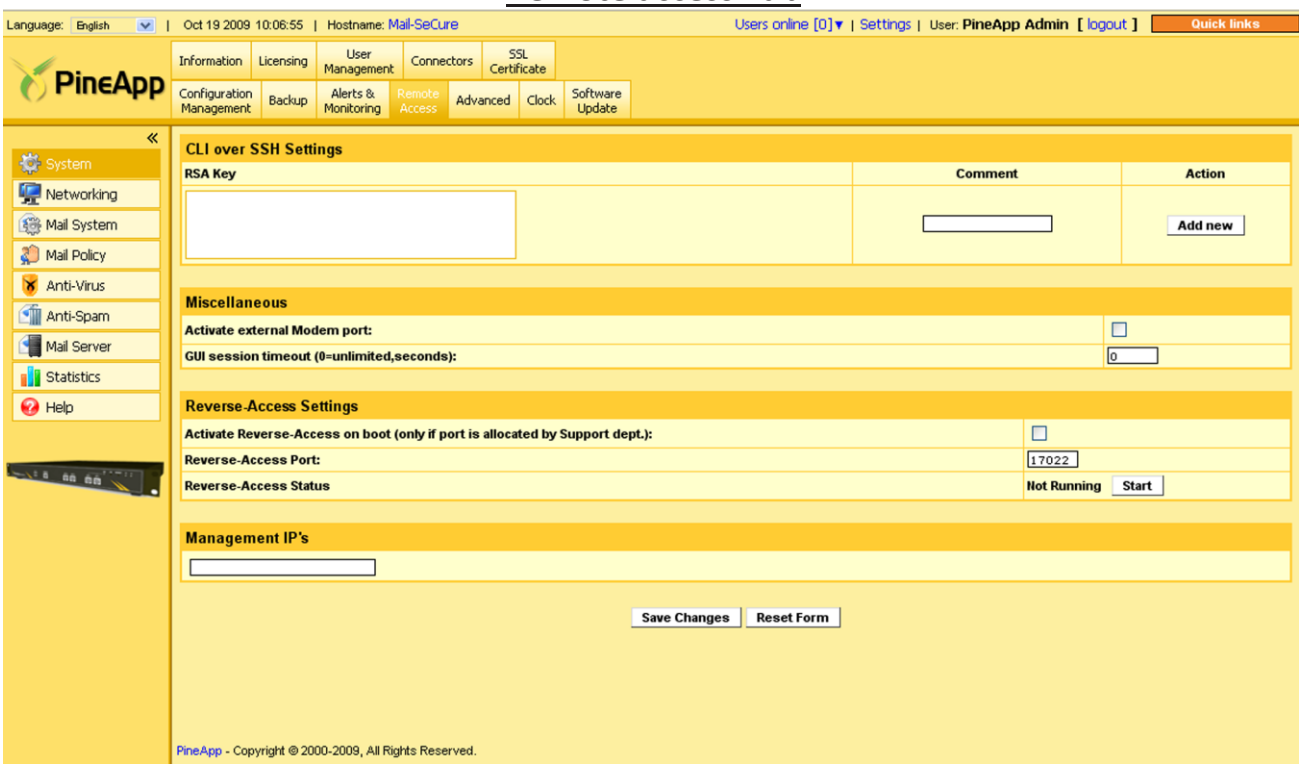
Configuring Remote Syslog settings

Mail-SeCure support Syslog. It is possible to remotely log the Mail-SeCure activities such as: SMTP logs, Incoming and Outgoing mail delivery, POP3.

Setting up remote Syslog

A) Check "Remote Syslog logging enabled" and click on the **Update** button.
B) Check the logs you wish to inspect on your syslog server from the list.
C) IP – Type your syslog server's IP address.
D) Port – By default it's 514, leave it as is if not advised otherwise
E) Protocol – syslog can work with both tcp & udp.
F) Facility & Priority – 2 variables that determines log's behavior on remote syslog server, as well as it's name.
G) Click on **Update**

Remote access Tab



In this tab, you are able to limit or grant access to the system's GUI management from defined IPs, grant Modem Access and define GUI session time-out.

CLI over SSH Settings

This feature allows the administrator to initialize an SSH session to the Mail-SeCure system on port 7022, in order to use Command Line Interface (CLI)

RSA Key - Generate copy and paste the key into this pane.

Reverse access settings

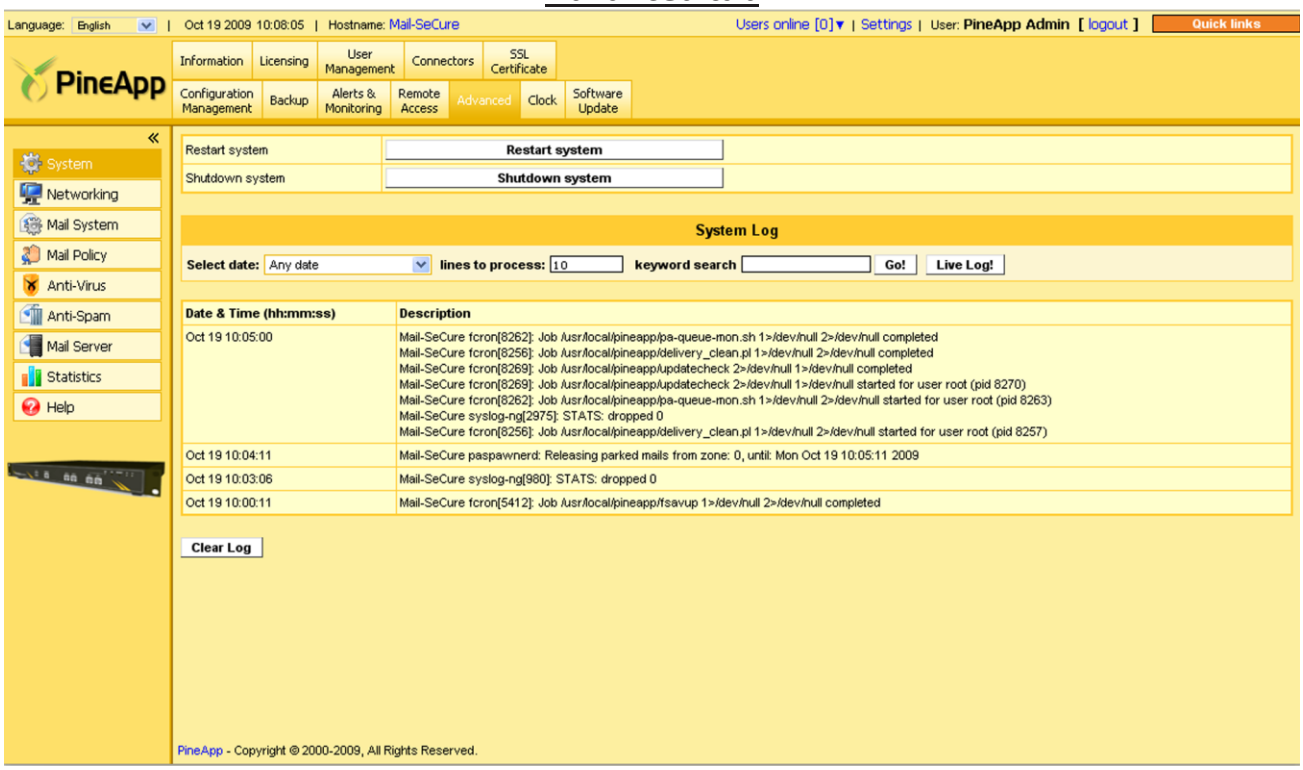
This allows PineApp's support to log into the device using SSH without having to open access to the port on the organization's firewall. Please refer to the manual for further information.

GUI session timeout - In this screen the definition of the GUI session time-out is made. If the GUI interface is not touched for the amount of seconds defined in this field, the session will time out and the user will need to re-enter his user name and password

(Default: 0).

Management IP's - To define authorized IPs, type the list of IP addresses that will have access to the Web management interface. By default this field is empty, so all IPs are authorized.

Advanced tab



In the Advanced tab, manual restart or shutdown to the Mail-SeCure system can be performed, via the **Restart System** and **Shutdown system** buttons.

It is highly recommended to perform reboot or shutdown to the Mail-SeCure system using these buttons only.

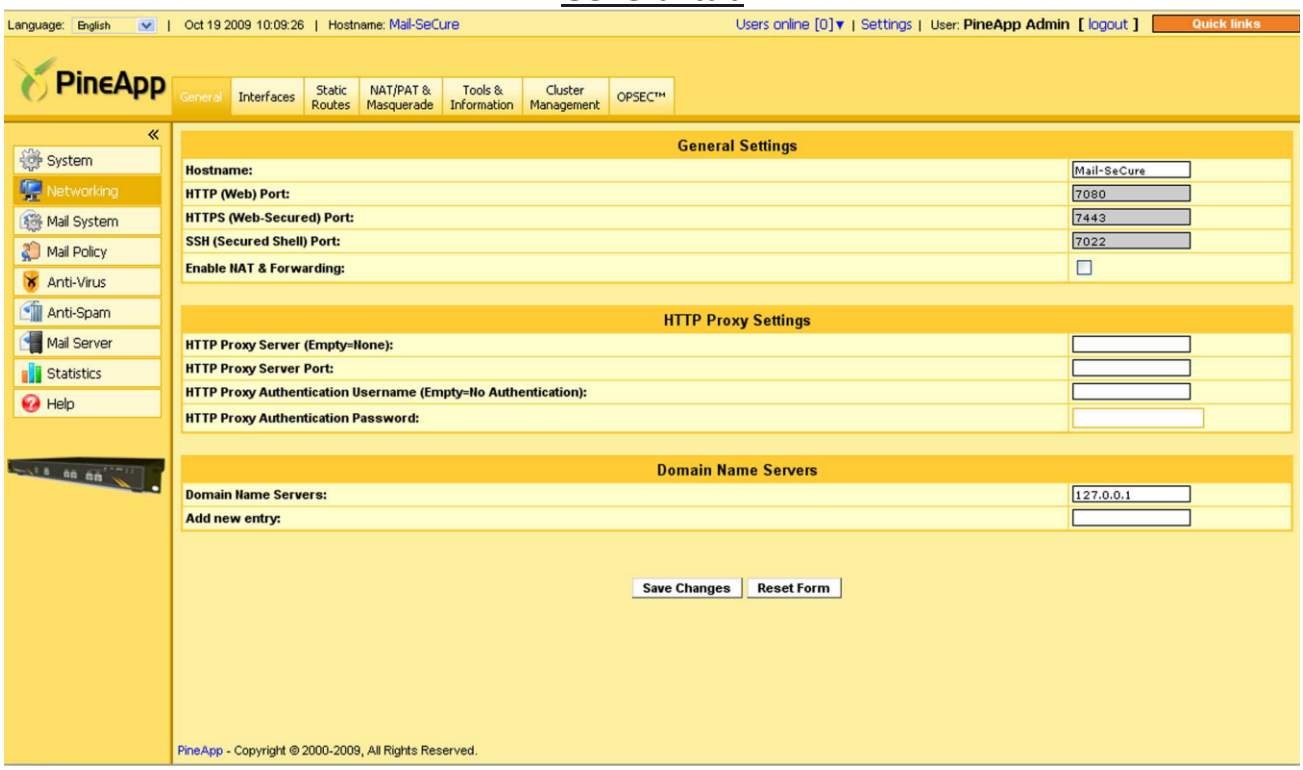
Restart System and **Shutdown system** buttons are also available on Information tab

In addition, generated system logs can be viewed at the bottom of this screen.

CHAPTER 3

NETWORKING

General tab



The General tab provides the following networking-related configuration fields:

General Settings

Mail-SeCure Hostname - In this field type the host-name of the device (type short host name only and not the FQDN*).

HTTP (Web) Port - The port in which the non-secured GUI is managed (Default: 7080).

HTTPS (Web-Secured) Port - The port in which the secured GUI is managed (Default: 7443).

SSH (Secured Shell) Port - The port in which the SSH is managed (Default: 7022).

The above ports' configuration is permanent, and cannot be changed.

Enable NAT & Forwarding - It is essential to enable this feature if the system is configured to be the gateway of a NAT subnet (usually when it is a Firewall or a gateway). Failing to enable this feature will result in users having no access to the Internet.

Domain Name Server - Type the organizational/ISP domain name server's IP address in this text field.

HTTP proxy server - If the organization does not permit direct access to the Internet (port 80 is closed from the system to the world), you will need to configure the organizations proxy.
Enter the proxy's IP address in the empty text field.

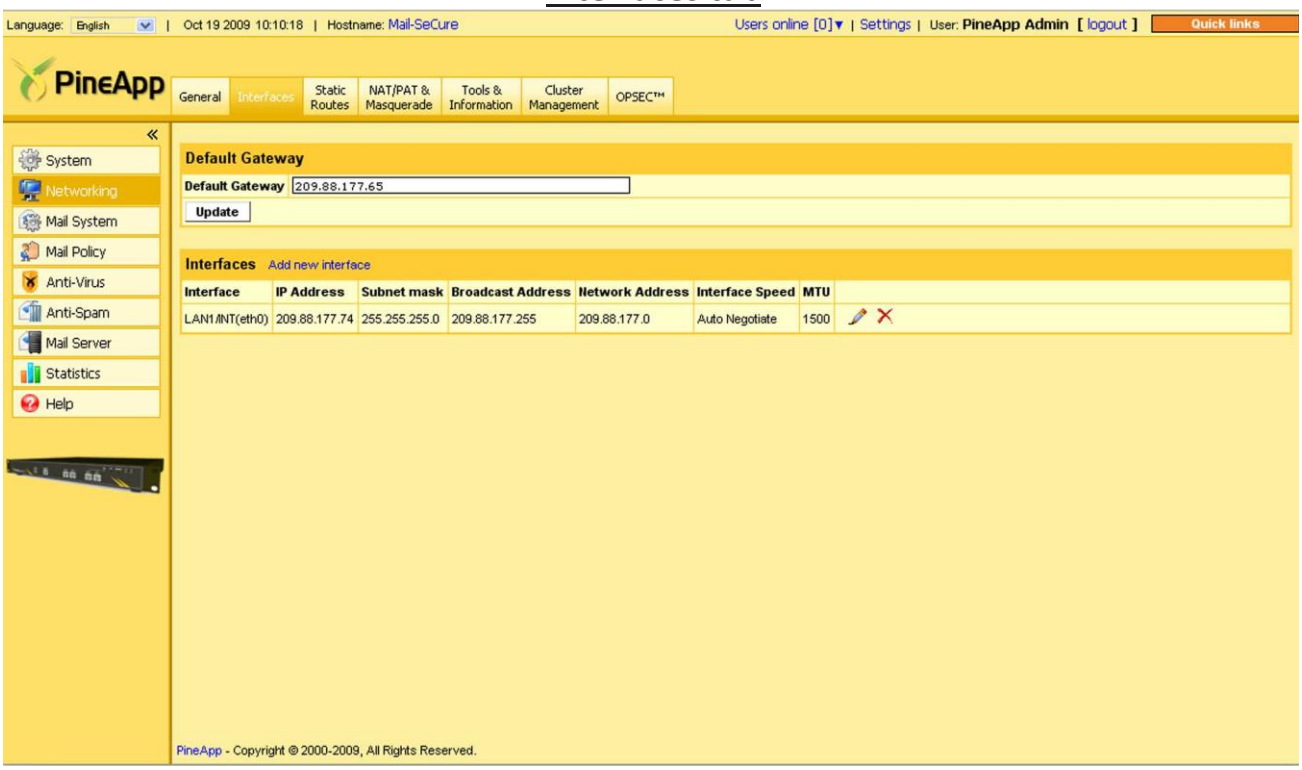
HTTP proxy server port - In case you are using the organization's proxy server, enter the port on which the proxy server is using to access the internet.

HTTP Proxy Authentication Username - If Proxy requires authentication, type the username here (default - empty, no authentication needed).

HTTP Proxy Authentication Password - If Proxy requires authentication, type the password here.

Domain Name Servers - In these fields type the DNS server list used for resolving; properly configuring the DNS is essential for the operation of the Mail-SeCure.
Mail-SeCure has an internal DNS-Cache system. If you wish to use it (127.0.0.1), please confirm that port 53 (tcp and udp) is open from Mail-SeCure to the world. If you wish to use a different DNS server, please confirm that it is properly configured. It is possible to check the validity of the DNS in the **Tools & Information** tab (Default: 127.0.0.1).

Interfaces tab



In the interfaces tab configure the system's NIC's (Network Interface Card) adapters.
The following table describes the connection between the ports in the GUI and the actual ports.

Adding a new entry - Type the data into the empty field(s) and click the **Save Changes** button.

Modifying an entry - Change the desired fields and click the **Save Changes** button.

Removing an entry - Click on the icon next to the entry you with to delete.

ETH	Port Number
INT (eth0)*	1
EXT (eth1)	2
DMZ (eth2)	3
DMZ (eth3)	4

***Default Network Interface**

Very Important!!

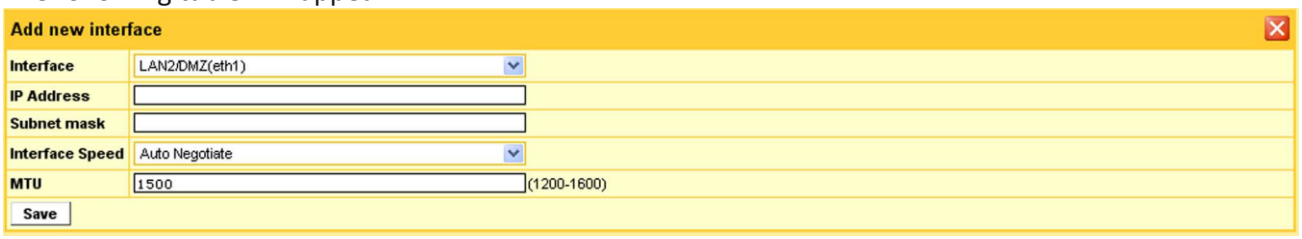
1. Do **not** perform more than one interface change at a time. If you wish to change information in more than one NIC, change the information in one NIC, click the **Save Changes** button and apply it. Only then, change the information in the second NIC.

2. For backup reasons, we strongly suggest to leave the default port IP untouched and to configure the other NIC's with the required IPs.

3. It is possible to configure only one Gateway.

Adding an interface

A) Click on the *Add new Interface* link
The following table will appear:

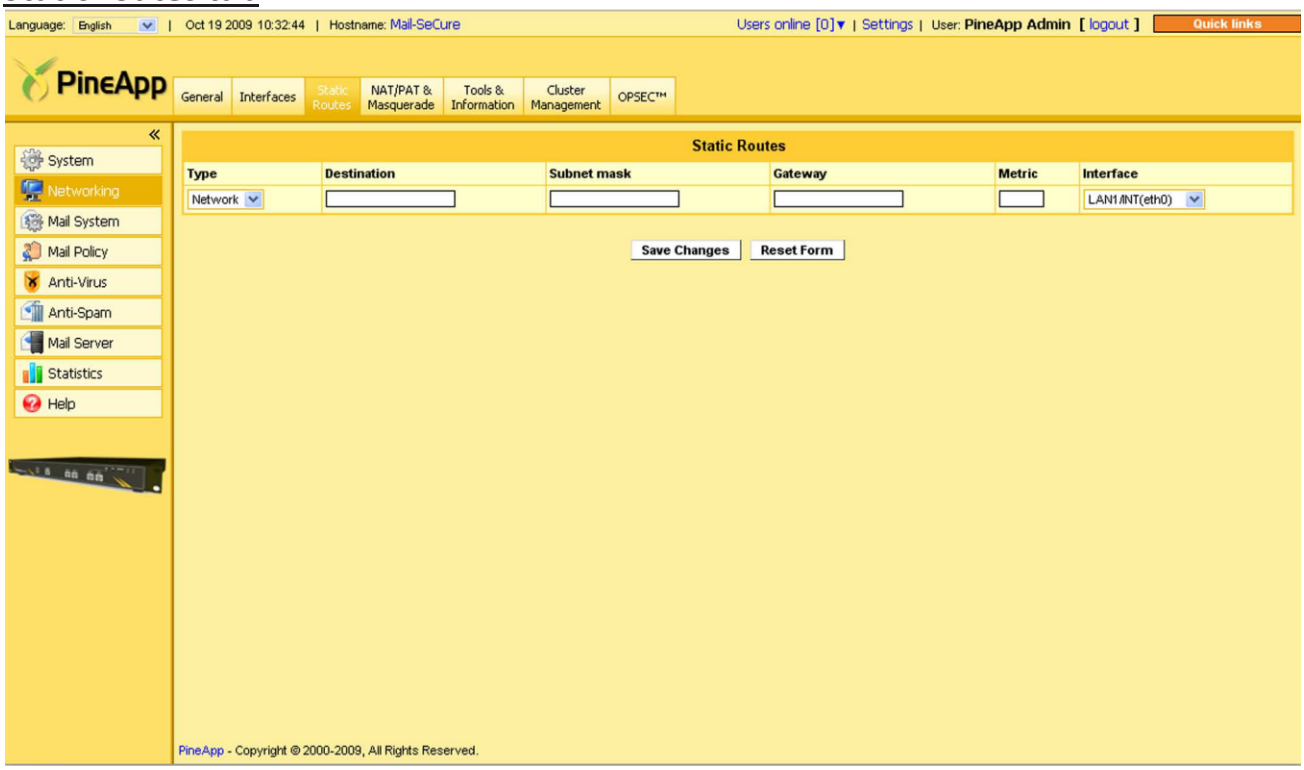


B) Choose the relevant interface from the drop-down menu.
C) Type the desired IP address and Subnet mask in their corresponding fields.
D) It is possible to define the interface's speed and MTU (Maximum Transmission Unit). If unknown, leave on defaults (auto negotiate and 1500).
E) When done, click on the **Save** button.

Modifying and deleting interface

From a configured interface, click on the icon and follow the table as in adding a new interface. In order to delete an interface, click on the **(delete) icon.**

Static routes tab

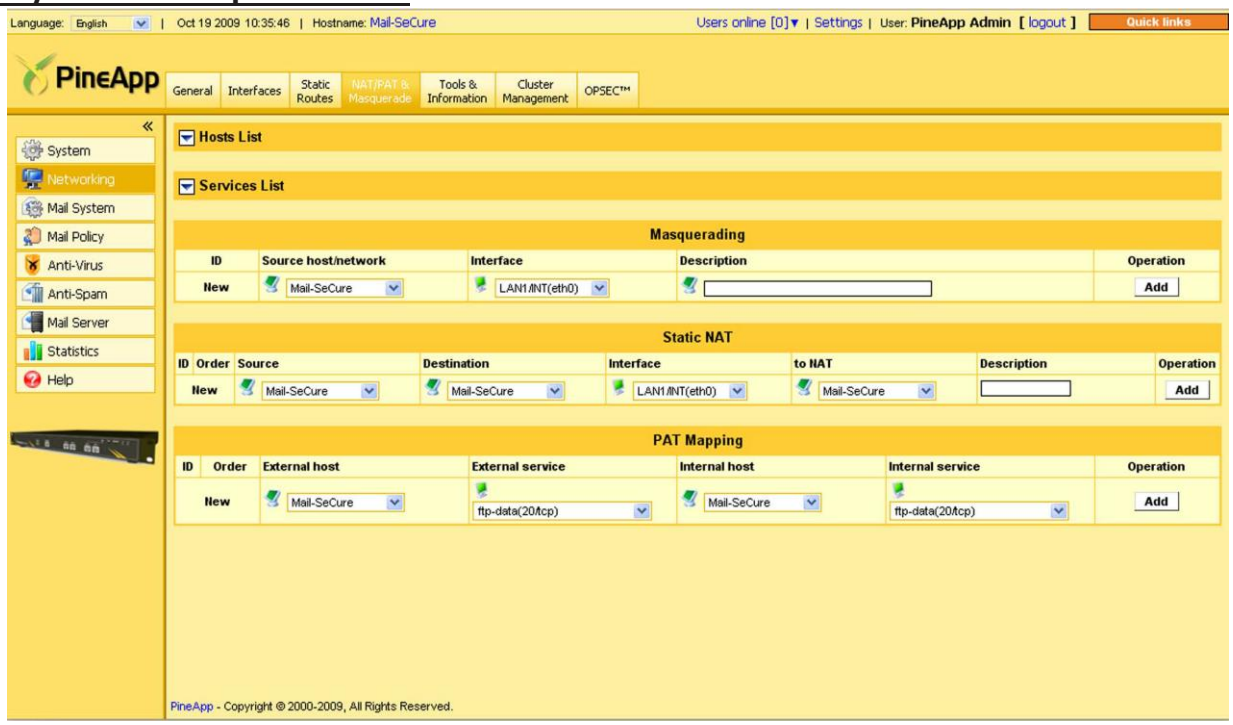


In this tab, the Static routes can be configured.
Static route gives the ability to define certain IPs so when trying to access a certain destination (internal or external), it will be routed through a certain gateway.

Adding a new static route

A) Type – Choose whether you like to assign the Static route rule to a host or a network.
B) Destination – Type the destination network/host IP address.
C) Subnet Mask – Type the destination network/host subnet mask (in case there's a static route to a specific host, type 255.255.255.255).
D) Metric – (Unless advised or required otherwise, type here 1)
E) Interface – Choose the interface through which packets will be routed.

NAT/PAT & Masquerade tab



NAT/PAT & Masquerade tab is used in order to configure advanced traffic forwarding features.

Configuring New Hosts

In order to configure a special forwarding rule to a certain host/network/special service, it is necessary to first configure the required host/network on which the rule will apply.

Adding a new Host

A) Go to Hosts List section and click on the opposite triangle icon.
B) Host Name – Type the requested host's name in the blank text input field.
C) Host IP – Type the new host/network's IP address
D) Netmask – Type a numeric value between 1 to 32, in order to determine the host/network netmask (32 indicates a single computer, whereas all other values indicates on a network's address-range)
E) Type – Choose host/network from the dropdown menu.
F) Description – Type a custom short description for the new host/network (not mandatory)
C) Click on the **Add** button.

Editing an existing Host record

A) Click on the (Pencil) icon next to the record you wish to edit.
B) Edit the information you wish to change.
C) Click on the **Save** button.

Adding a new Service

A) Expand the Services menu, using the triangle icon, and type all parameter in the new blank line at the button of this section.
B) Port – Type the port number(s) you wish to assign for the new service.
C) Protocol – Choose the protocol in which the new service is active.

D) Service – Type the new service's name.
E) Description – Type a custom short description for the new service (not mandatory)
F) Click on the **Add** button.

Editing an existing Service record

A) Click on the  (Pencil) icon next to the record you wish to edit.
B) Edit the information you wish to change.
C) Click on the **Save** button

Masquerade rules

Masquerading is a form of network address translation (NAT) which allows access for internal computers with no known external IP address outside their network.
It allows one machine with an external IP address (usually a broadband internet device, such as modem or router) to act on behalf of several other machines with internal IP addresses, in order to access remote sites (the internet).

Adding a new Masquerade rule

A) Source/host network – Choose the host/network from which connection is established.
B) Interface – Choose the interface through which packets will be routed
C) Description – Type a short description for the new rule (not mandatory)
D) Click on the Add button.

Editing Masquerade rules

A) Click on the  (Pencil) icon next to the record you wish to edit.
B) Edit the information you wish to change.
C) Click on the **Save** button

Deleting Masquerade rules

Choose the rule you wish to delete, and click on the  (Delete) icon next to it.

NAT rules

Routers, firewalls and other gateway based products are maintaining an automatic NAT table, refreshing and registering all NAT entries in real-time.
Static NAT rules are created in order to forward traffic from one specific source to a specific internal destination host/network. Adding a new NAT rule

Adding a new Static NAT rule

A) Source – Choose the source host/network from which connection is established.
B) Destination – Choose the external destination host/network to which connection is originally directed.
C) Interface – Choose the interface from which connections will be re-routed to the internal host.
D) to NAT – Choose the specific host/network to which the connection will be rerouted.
E) Click on the **Add** button.

Editing Static NAT rules

A) Click on the  (Pencil) icon next to the record you wish to edit.
B) Edit the information you wish to change.
C) Click on the Save button

Deleting Static NAT rules

Choose the rule you wish to delete, and click on the  (Delete) icon next to it.

PAT rules

PAT (Port Address Translation) rules are used in order to configure traffic forwarding from a specific external source to a specific internal destination host/network, based on the service (port number) in which the connection is established.

Adding a new PAT rule

A) External host - Choose the external host/IP address to which connection is destined.
B) External service – Choose the service type in which connection is established.
C) Internal host – Choose the specific internal host/network to which the connection will be rerouted.
D) Internal Service – Choose the service type in which internal connection will be established.

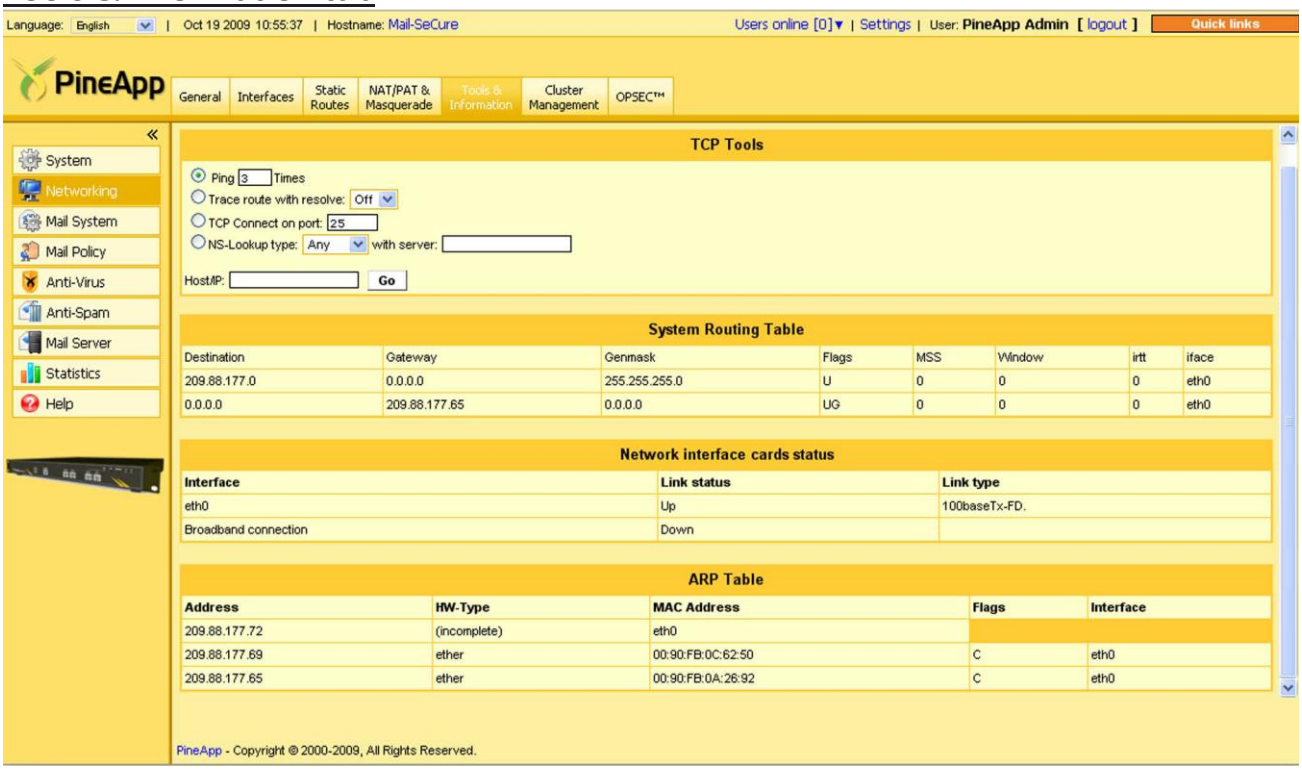
Editing PAT rules

A) Click on the  (Pencil) icon next to the record you wish to edit.
B) Edit the information you wish to change.
C) Click on the **Save** button

Deleting PAT rules

Choose the rule you wish to delete, and click on the  (Delete) icon next to it.

Tools & information tab



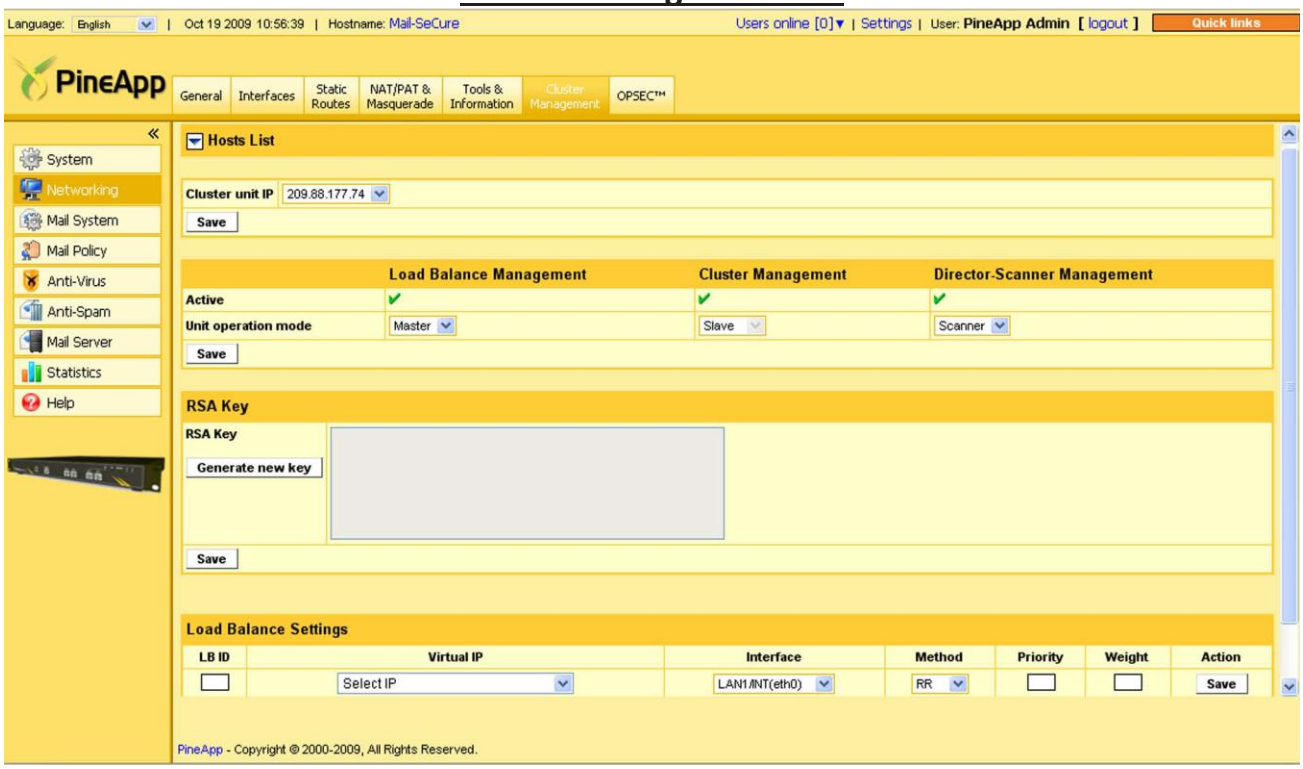
This tab provides useful tools for monitoring the system.

It can be used for internet and internal connectivity checks, by using ping, traceroute, NS lookup and telnet commands. It is possible to use the other tools for information regarding other servers and configuration.

This tab also provides details regarding the status of the Network interface cards (Hardware), ARP table and routing table.

The results of ping and trace route are shown in a pop-up. Make sure your browser enables pop-ups.

Cluster management tab



PineApp Mail-SeCure contains an embedded load balancing mechanism. This feature saves the need for a third party load balancing device.
The load balancing feature is available in all Mail-SeCure models. This feature allows customers to install more than one Mail-SeCure device in order to scale SMTP traffic between two or more Mail-SeCure devices, and improve email service's availability.

Load Balancing - Load Balancing allows organizations to install more than one Mail-SeCure device in order to achieve high availability, Load Balancing and Scalability.

Cluster Management - This allows a single point of management for the cluster. Configuration done to the master is distributed to the rest of the devices.

Scanner-Director - This feature activates the Scanner-Director capability of the system.
Scanners, as their name may imply, focus their functionality in scanning all mail traffic according to the different load balancing methods, when one scanner is the Master appliance, responsible for holding the VIP and distribute SMTP connections, in addition to processing emails itself.

The scanners do not keep mail logs or quarantine physically, but move all records to the Director. The Director is a regular Mail-SeCure appliance, equipped with all scanning modules, but it does not participate in the actual mail scanning process.

Its functionality concentrates in centralizing every management aspect for the cluster: in addition to configuration distribution and unified daily report delivery, it stores all mail logs & quarantine items, sent from the scanners, making auditing and searching as simple and comfortable as in a single-appliance mode.

Configuring Hosts

To configure new hosts, please follow the Hosts configuration section in NAT, PAT & Masquerading tab.

Configuring Load Balancing

Load Balancing is configured in order to scale mail traffic between two or more Mail-SeCure appliances.
In order to configure load balancing:

Step 1: Creating hosts and activating load balancing feature.

A) Configure all participating hosts as shown in the configuring hosts section.

B) Check **Load Balance Management** on each of the appliances.

C) Choose Master for the master unit, and slave for the slave unit under "Unit operation mode".

Step 2: Configuring Load Balance Settings

Configure the following settings:

A) LB ID - Configure a similiar numeric value in all of the participating appliances (LB Group ID).

B) Virtual IP - Choose the configured VIP host from the dropdown menu.

C) Interface - Choose the interface on which mail traffic is flowing from the dropdown menu.

D) Method - Choose your preferred traffic distribution method, according to the below table.

E) Priority - Define the priority of the system. The score given to the "Master" unit must be 50 points higher that the "Slave" unit/s.

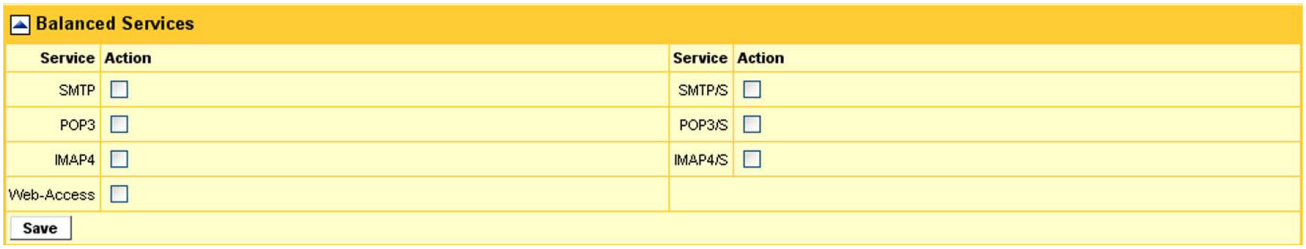
F) Weight - Define the weight of the system. If the weight of "Master" is equal to the "Slaves", the traffic is distributed equally between the systems. If one unit is configured with higher weight, it will be routed with more traffic, according to the configured ratio.

G) Click on **Save** button to finalize your configuration.

Method	Description
RR (Round Robin) - Default	The master unit distributes mail evenly between the units regardless of the configured weight.
LC (List Connections)	The master unit evenly distributes mail by the number of open connections. The master unit verifies which unit has the least open connection and then distributes the mail.
WRR (Weighted Round Robin)	The master unit distributes mail only by the weight of each unit. The master unit distributes the mail by the proportion of weight of each unit. For example, in the above table (5,5), the mail is distributed in proportion of 1:1.
WLC (Weighted list connections)	The master unit distributes mail by the number of open connections. The master unit verifies which unit has the least open connection and then distributes the mail. If there is an equal amount of connections; the distribution goes by the weight.

Step 3: Configuring balanced services

In case you wish to work in active-active mode (all configured appliances participate in mail procession according to a pre-defined distribution method), click on the icon under Balanced Services menu. The following window will appear:



Check the traffic types you wish to scale in all participating appliances, from the Balanced Services menu. In case you wish to work in an Active-Passive mode, leave all traffic types under Balanced Services unchecked. To learn more about LB methods, please refer to the Load Balancing Whitepaper.

Configuring Cluster Management (Configuration distribution)

After configuring the cluster management feature, you will be able to use the "Master" system in order to manage the whole cluster. Configurations and rules performed on the "Master" will be synchronized with the "Slaves".

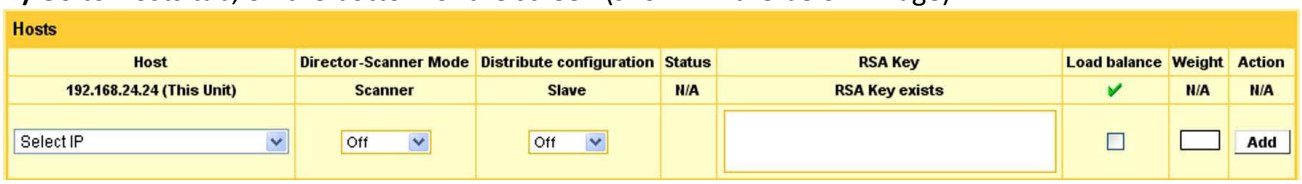
In order to configure the Cluster Management feature in a Configuration Distribution mode, please follow the below table:

Step 1: Initial Configuration

Section	Master	Slave(s)
Hosts List	Configure all participating hosts as shown in the **Configuring Hosts** section	
Load Balance Management	In case you wish to use Load Balancing, choose "Master" in unit's operation mode	In case you wish to use Load Balancing, choose "Master" in unit's operation mode
Cluster Management	Check and choose "Master" from the unit's operation mode	Check and Choose "Slave" from the unit's operation mode
Director-Scanner Management	Leave unchecked	Leave unchecked
RSA Key	Generate and save a new RSA Key by hitting on the **Generate** and **Save** buttons respectively	Generate and save a new RSA Key by hitting on the **Generate** and **Save** buttons respectively
Send Unified Report	Check this option (appears in Master unit only) in case you wish to deliver a concentrated daily report, containing information and blocked/released email records from all scanning appliances.	
Load Balancing settings	Configure load balancing settings as shown in **Configuring Load Balancing** Section	

Step 2: Configuring Hosts' synchronization settings

A) Go to Hosts tab, on the bottom of the screen (shown in the below image)



B) Configure settings for all participating appliances according to the following table:

Section	Master	Slave(s)
Host	Choose the added unit's host from the dropdown menu,	
Director-Scanner Mode	Check the box for all added records	Check the box for all added records
Distribute configuration	Choose "Slave" for all added unit records	Choose "Slave" for all added unit records. When adding the Director unit records, choose "Master"
RSA Key	Copy RSA key from the unit currently being added	
Load balance	Check the box for all added records	Check the box for all added Scanner units. When adding the Director unit record, leave unchecked
Weight	configure weight according to the configured weight in load balancing settings.	
Action	Click on **Add** for button once finished, in order to add the new record.	

The cluster management tool distributes the configuration from the Master to the Slaves.
It distributes the following settings only:

User lists	Spam settings	File types
Black & White lists	DNS servers	ICC settings
Domain lists	Plug-ins	Anti-Virus settings
Notifications and Footnotes	Backscatter settings	
Policy Rules	Content Filtering	
Masquerading		

It does NOT distribute:
Relay Networks
IP Addresses
DNS settings
Mail retriever
Daily Report settings

Configuring Scanner-Director array

The Scanner-Director topology allows you to manage and control an array of Mail-SeCure appliances from the Director unit. The Director unit stores the quarantine, logs and daily report management. It is also possible to use the director to distribute the configuration to the scanners. Further information regarding the Scanner-Director topology can be found in the Scanner-Director Whitepaper.

There are two types of players in the Scanner-Director topology: The Scanners and the Director.

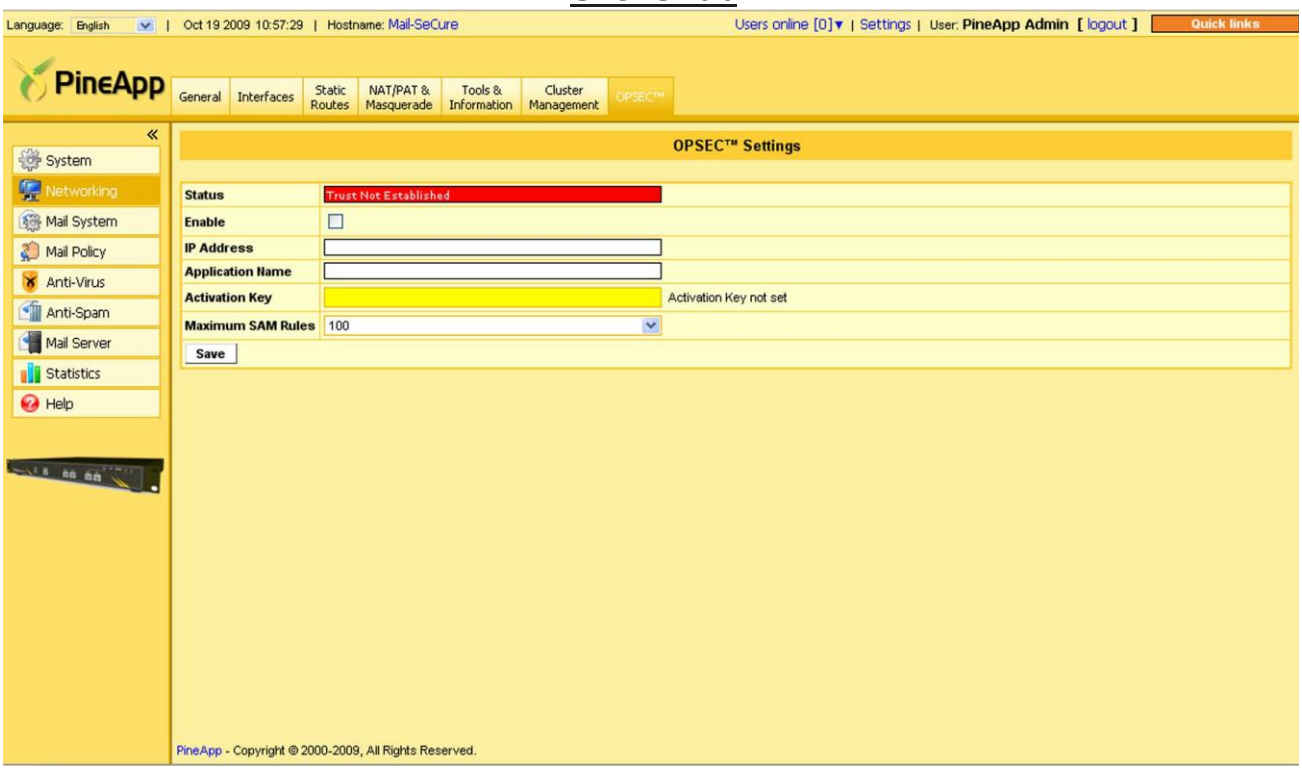
Step 1: Basic configuration

Section	Director	Scanners	
		Master	Slave(s)
Hosts List	Configure all participating hosts as shown in the **Configuring Hosts** section		
Load Balance Management	Leave Disabled	Check and choose "Master" in unit's operation mode	Check and choose "Slave" in unit's operation mode
Cluster Management	Check and choose "Master" from the unit's operation mode	Check and Choose "Slave" from the unit's operation mode	
Director-Scanner Management	Check and choose "Director"	Check and choose "Scanner" for all units.	
RSA Key	Generate and save a new RSA Key by hitting on the Generate and Save buttons respectively	Generate and save a new RSA Key by hitting on the Generate and Save buttons respectively	
Load Balancing settings		Configure load balancing settings as shown in **Configuring Load Balancing** Section	

Step 2: Configuring Hosts' synchronization settings Go to **Hosts** Section on the bottom of the page, and configure settings for all participating appliances as follows:

Section	Director	Scanners	
		Master	Slave(s)
Host	Choose the added unit's host from the dropdown menu,		
Director-Scanner Mode	Check the box for all added records	Check the box for all added records	
Distribute configuration	Choose "Slave" for all added records	Choose "Slave" for all added Scanner units. When adding the Director unit records, choose "Master"	
RSA Key	Copy RSA key from the unit currently being added		
Load balance	Check the box for all added records	Check the box for all added Scanner units. When adding the Director unit record, leave unchecked	
Weight	Configure weight according to the configured weight in load balancing settings.		
Action	Click on **Add** for button once finished, in order to add the new record		

OPSEC Tab

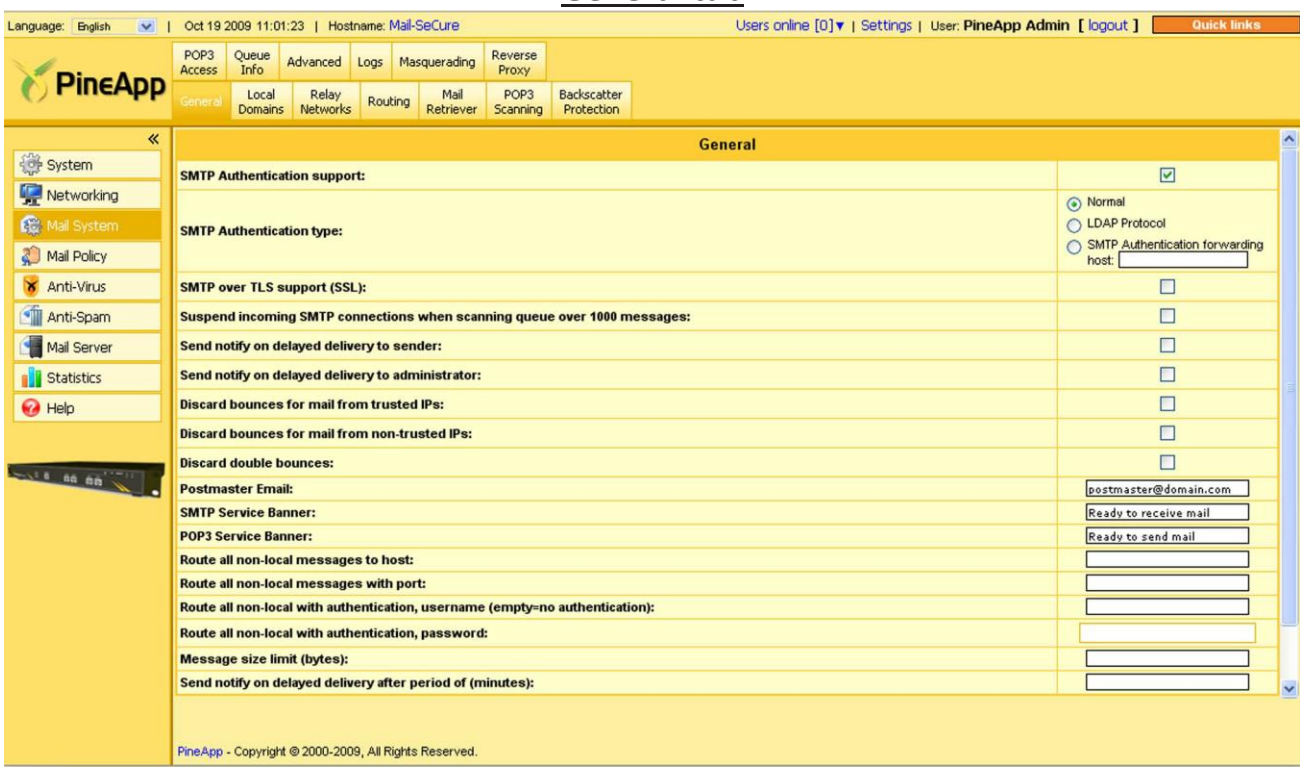


PineApp Mail-SeCure V3.7 Is an OPSEC certified product. It can interconnect with Checkpoint's Firewall-1 and provide IP Reputation services to the Firewall.

CHAPTER 4

MAIL SYSTEM

General tab



In the General tab, all general information regarding the Mail-SeCure MTA engine is configured.

SMTP Authentication support - This feature enables activating SMTP authentication. This feature will allow users, while out of the office, to send mail using the Mail-SeCure without changing the outgoing mail server in the local Email client.

SMTP Authentication type - Mail-SeCure has three methods of authenticating SMTP connections:
1. **Normal -** when checked, Mail-SeCure will authenticate the users with the usernames and passwords as configured in the User management tab.
2. **Authenticate using LDAP Protocol** – when checked, Mail-SeCure will authenticate the users with the usernames and passwords as configured in the LDAP server after the Mail-SeCure has synchronized with the LDAP server.
3. **SMTP Authentication forwarding** – when checked, an IP of an authentication server must be entered. Usually it will be the local mail server. Make sure that the SMTP Authentication is enabled on that server.

SMTP over TLS support (SSL) - This tab enables sending and receiving using a secure SMTP connection.

Suspend incoming SMTP connections when scanning queue over 1000 messages - When checked, if the scanning queue exceeds 1000 emails (usually caused due to a Virus or Spam attack), the system will not accept anymore SMTP connections until the queue drops under 1000.

Send notify on delayed delivery to sender - If the system, for any reason, is unable to send the mail within a given period of time, it generates a notification message. Checking this box will cause the sender to receive the notification message.

Send notify on delayed delivery to administrator - Mail-SeCure system performs deliayed delivery checks once an hour. If the system, for any reason, is unable to send the mail within that given period of time, it generates an error message. Checking this box will cause the administrator to receive the notification message.

Discard Bounces for mail from trusted IPs - When checked, Mail-SeCure will not generate NRD's for emails originated from trusted IPs (from within the organization) (default - unchecked).

Discard Bounces for mail from non-trusted IPs - When checked, Mail-SeCure will not generate NRD's for emails originated from non-trusted IPs (from outside the organization) (default - checked).

Discard double Bounces - When checked, Mail-SeCure will not relay double email bounces. This usually happens when a non-existing user sends an email to another non-existing user (default - checked).

Postmaster Email - It is essential to enter the Postmaster's correct email. This email will receive notifications regarding mail delivery, license, policy and virus issues.

Route all non-local messages to host - All outgoing mail will be sent using the host defined in this field. It is most common to use the ISP's mail server as the "mail-delivery server" to save bandwidth and to avoid connection timeouts (Default: empty).

Route all non-local messages with port - If this field is defined, it is possible to define the port in which the mail will be forwarded (Default: 25).

Route all non-local with authentication, username - If the external host requires authentication, define the username (default: empty), no authentication required.

Route all non-local with authentication, password - If the external host requires authentication, define the password.

Encryption service type – this section contains 3 available delivery methods for encryption-designated emails, according to the customer encryption server's type and location.

1. On –demand SeCure Email – Checking this option will deliver all outgoing mail designated for encryption (in a secure copy form) to PineApp SeCure On-Demand Encryption Center.

2. In-LAN SeCure e-mail host – Checking this option, in addition to typing the destination's IP address, will route all outgoing mails designated for encryption (in a secure copy form) to the SeCure Encryption Center located in the organization's Local network.

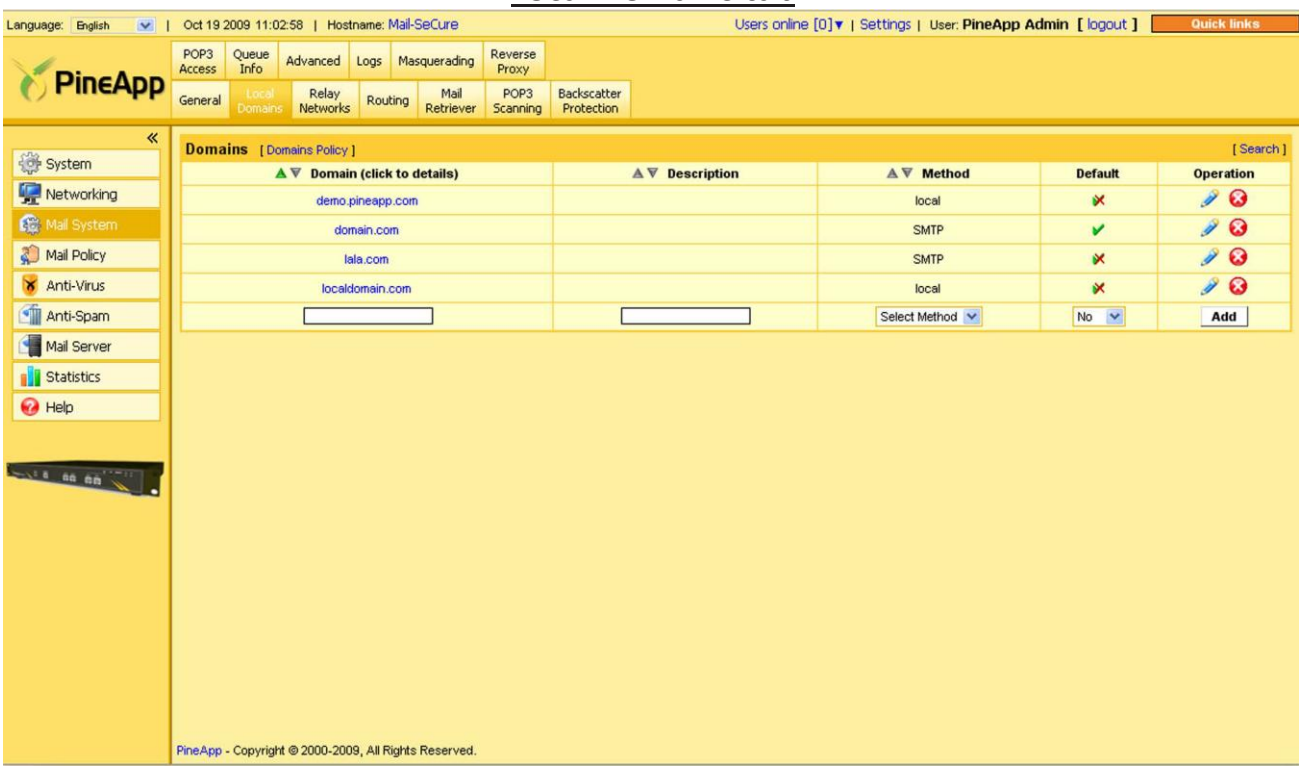
3. SMTP Encryption forwarding host - checking this option will re-route all outgoing mail designated for

encryption to a third party e-mail encryption server.

Message size limit (bytes) - The maximum size of message in bytes; if left empty - unlimited size. Message size limit effects both incoming and outgoing mail (Default: Unlimited).

Send notify on delayed delivery after period of (minutes) - As mentioned above, if an email can't be sent to the recipient, after a certain time, a notification is generated. In this field, the time until the error message can be configured (If left empty – 240 minutes).

Local Domains tab



The local domains tab contains a list of all the domains, which are handled by the Mail-SeCure.

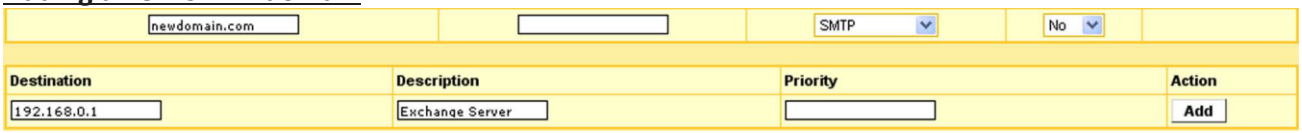
Delivery Methods

LOCAL - All mail sent to the domain will be stored locally on the Mail-SeCure (when acting as a mail server).

POP3 - All mail sent to the domain will be stored in ONE local mailbox. The mail can be retrieved using third party software as POPBeamer or EFS. Please refer to page 4-19 in order to learn how to install POP3 Mail retrievers.

SMTP - All mail sent to the domain will be forwarded to the local mail server.

Adding a new SMTP domain



A) Type the domain name and its description (optional) in the empty fields.

B) Choose the SMTP method for the specific domain from the dropdown menu.

C) As soon as the method is chosen, a new field will appear, containing 3 text fields. Type the destination mail server's IP address, and add a short description of it (not mandatory). To finalize your action, click on the **Add** button (marked in a red square in the picture above).

D) Several destination mail servers can be defined per one domain. You can control mail flow between those servers by using the priority field*.

E) Define the newly configured domain that will be the default domain, instead of the localdomain.com's existing record, by clicking on the V next to it. One domain has to be defined as default at any time.

F) Delete the localdomain.com record, by clicking on the X icon next to it.

Adding a new POP3 domain

A) Type the domain name and its description (optional) in the empty fields.
B) Choose POP3 from the dropdown menu.
C) Type the name of the Mailbox and the password.
D) Click on **Add** button to finalize your action.

Adding a new local domain

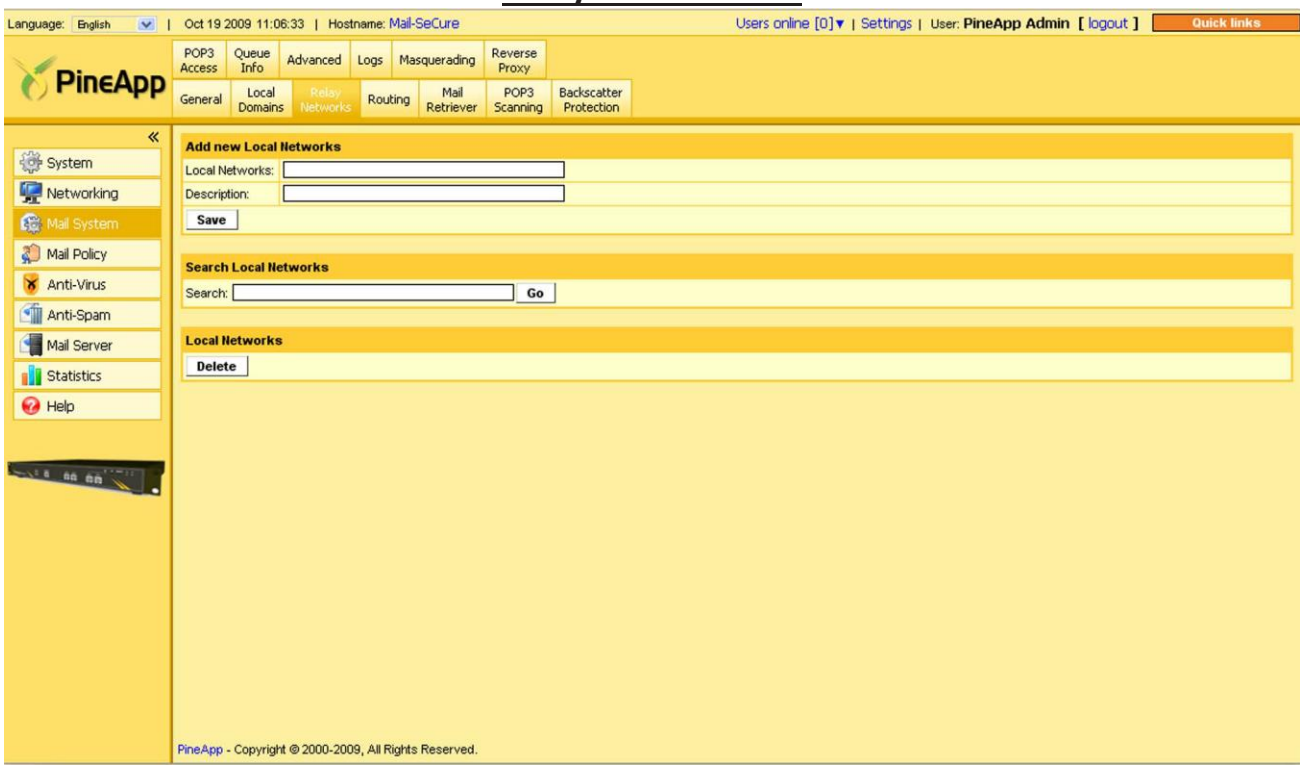
A) Type in the empty fields the new domain name and its description.
B) Click on the **Add** button.

*The destination mail server's priority should be configured in case there is more than one destination mail server for the specific domain (External Servers may also be configured).

In case different priorities are configured, the mail will always be sent to the domain with the higher priority score.
If, for any reason, the server isn't responding, the mail will be delivered to the next server in priority.

In the Mail-SeCure 1000 series there is a limitation of 5 domains that can be configured. In all the other series - no limitation exists.

Relay networks tab



The networks and IPs configured in Relay Networks tab will be authorized to send mail via the Mail-SeCure.

All IP connections to Mail-SeCure from listed IPs will be identified as trusted outgoing connections or outgoing mail.
The networks and/or hosts defined in this tab will be considered trusted networks in all of the Mail-SeCure's inspections, and won't be subject for Spam inspections.
It is possible to configure single hosts, complete network subnets or specific IP ranges to be trusted.

Examples: For network 192.168.24.0 with subnet mask 255.255.255.0, type in: 192.168.24. (Including the dot); for network 209.88.177.64 with subnet mask 255.255.255.192, type in: 209.88.177.64-127

Adding a new entry

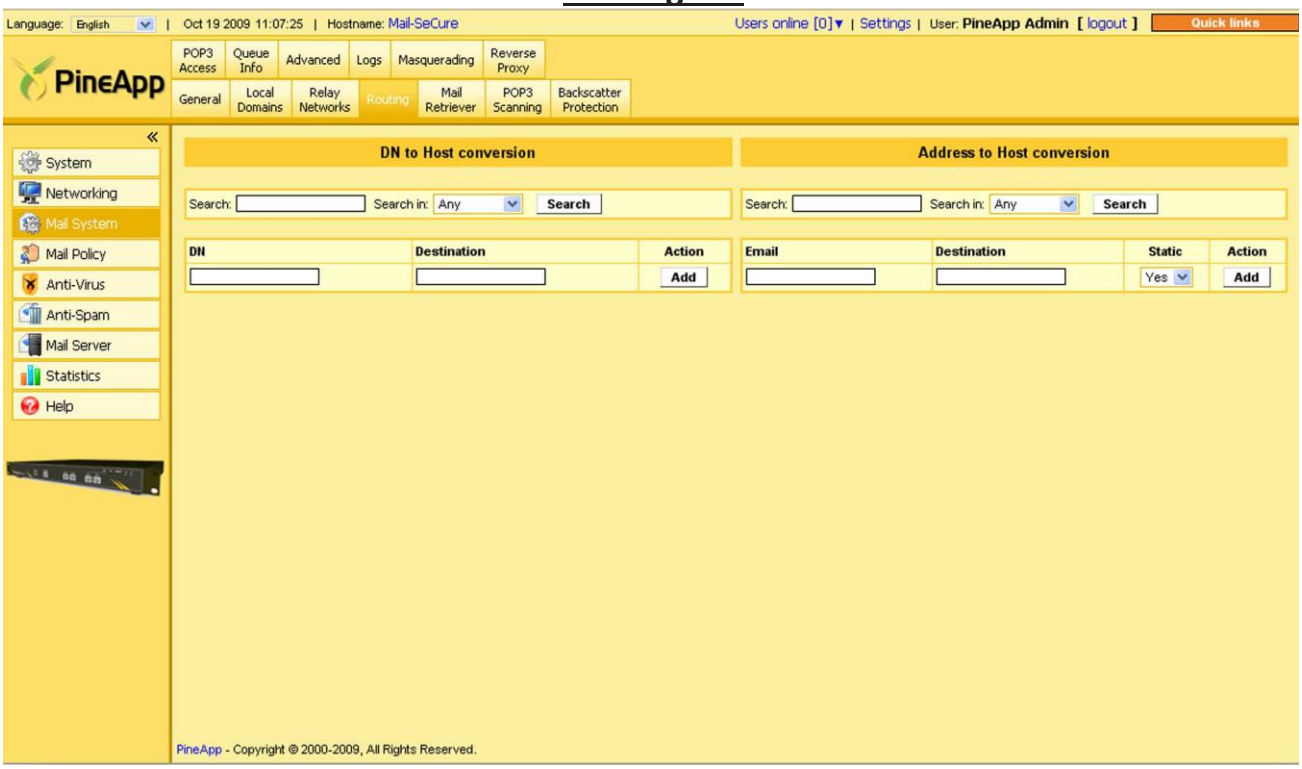
A) Type the IP address and/or range into the **Local Networks** empty field.
B) Click the **Save** button.

Removing an entry

Check the box next to the entry you wish to delete and click on the **Delete** button.

Misconfiguration of these fields may cause the system to become an open relay. That can lead to multiple entries in RBLs.

Routing tab



Mail-SeCure supports advanced email-routing features, which can be configured in this tab.

DN to Host conversion

It is possible to configure the LDAP server to route different emails based on their address and/or domain affiliation to different servers. In other words, the system can retrieve and route mail based on its configuration in the LDAP server.

Adding a new DN-based Route

A) Type the specified branch you wish to synchronize in the **DN** text input field.
The syntax is as follows: **DN=group, Domain=domain.com**
B) Type in the destination mail server's IP address in the **Destination** text input field.
C) Click on the **Add** button. Users are supposed to be automatically added under the **Address to host conversion** section.
D) Click on **Apply Changes.**

Address to Host conversion

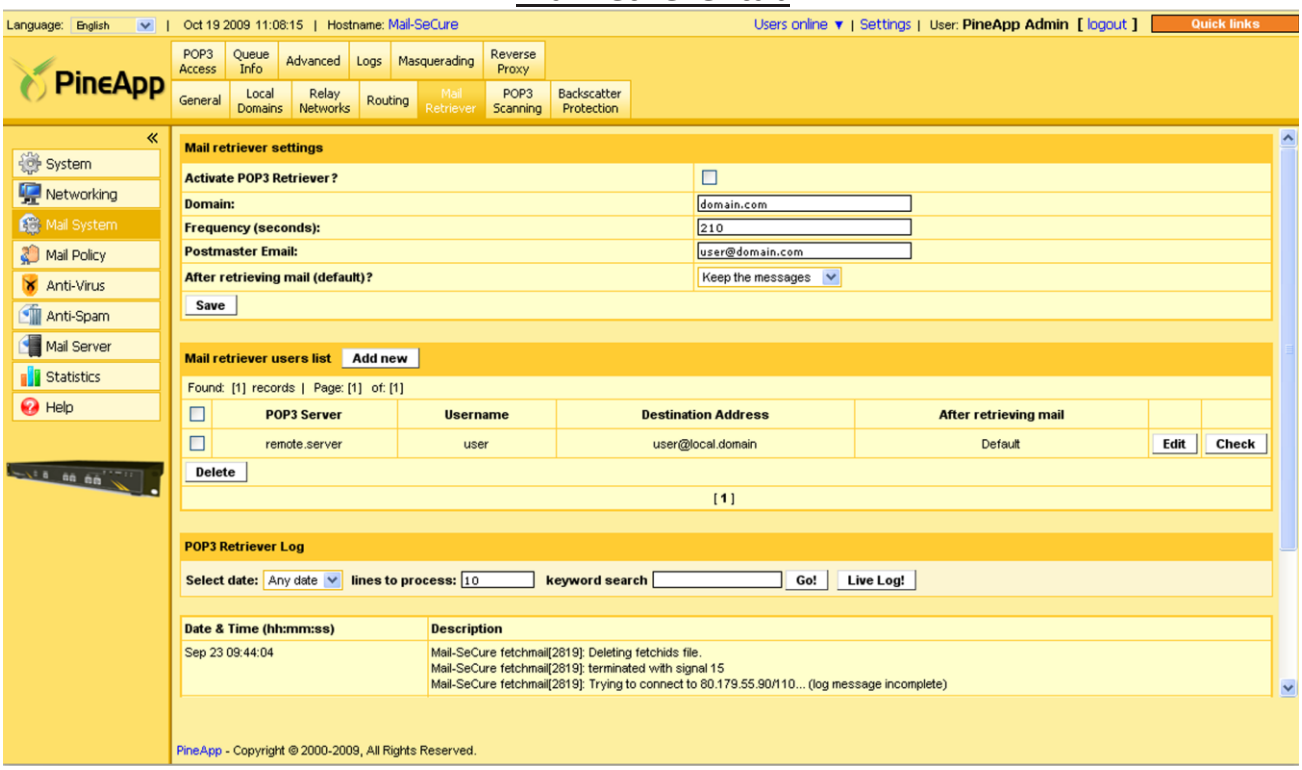
It is also possible to route singular mail addresses to different mail servers using manual configuration.

Adding a new address-based Route

A) Type the specified email address you wish to route in the Address input text field.
B) Type in the destination mail server's IP address in the **Destination** text input field.
C) Click on the **Add** button.

This feature is not available in Mail-SeCure 1000 series.

Mail retriever tab



In “Mail Retriever” tab, external POP3 Mailboxes can be retrieved and then “injected” into the system. This feature prevents users from accessing their personal POP3 mailboxes and bypassing the Anti-Virus and the content-filtering engine.
Their mail is retrieved by Mail-SeCure, processed and then forwarded to their mailbox, thus preventing contamination of the network.

All retrieved mail is handled as regular incoming mail; it is scanned, cleaned and then delivered.

Activating and configuring the Mail Retriever

A) Check the **Activate POP3 Retriever** checkbox to activate the retriever engine
(Default: off).
B) Domain - Type the default domain in this field.
C) Frequency - Type the time interval in seconds between each mail check interval (Default: 210 seconds).
D) Postmaster’s Email - Type the Postmaster’s email address.
E) After retrieving mail - Select whether the mail should be kept or deleted from the external mailboxes after retrieval in the “” field (Default: keep).

Adding a new entry

For each mailbox:
A) Click on the **Add new** Button. A new table will appear.
B) Enter the POP3 mail server, username, password and the local user who will receive the mail in the corresponding fields. If a name is entered without a domain, Mail-SeCure will append the default domain.
C) Choose whether you want the mail to be deleted or kept on the external mail server. Default refers to the global setting in the upper part of the configuration menu.
E) After clicking the **Save** button, it is recommended that you click the **Check** button to verify

the configuration (username and password against the defined POP3 server).
In addition, generated system logs can be viewed at the bottom of this screen.

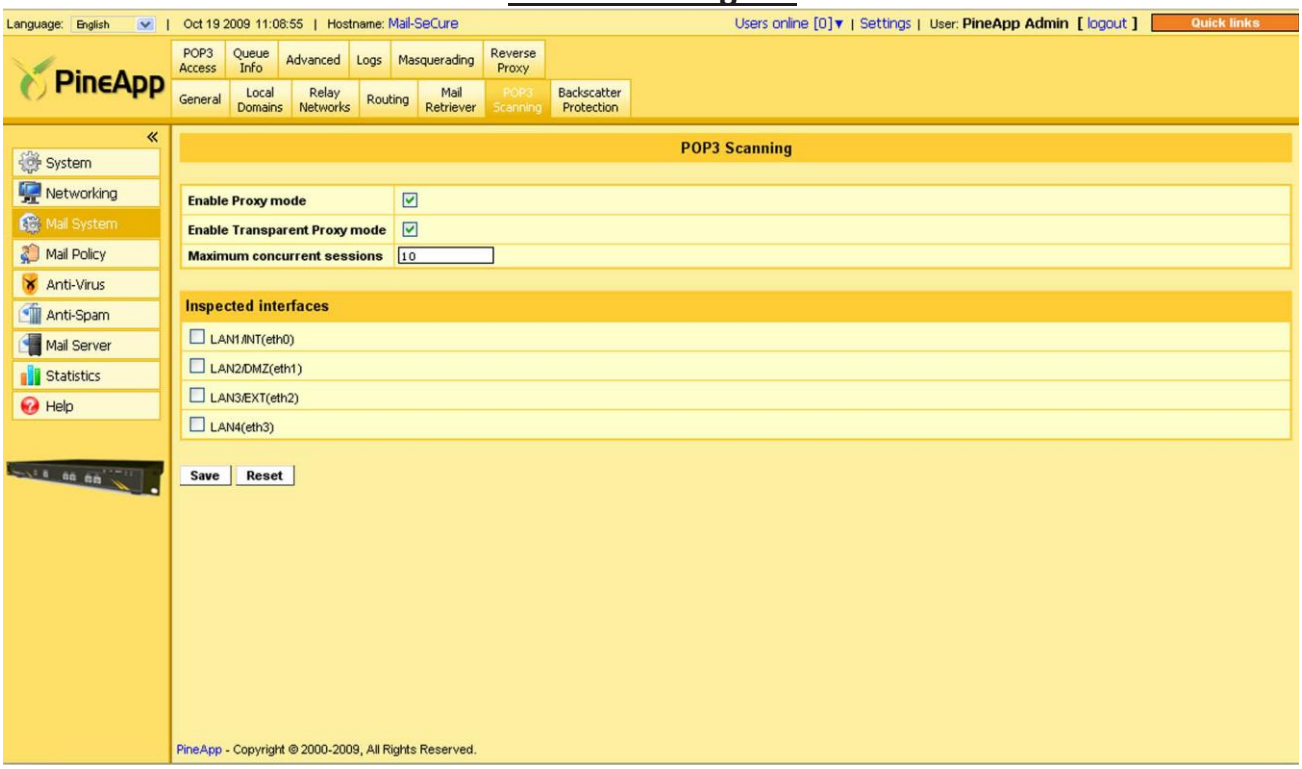
Modifying an entry

A) Click on the **edit** button for the relevant user you would like to edit information for.
B) Change any relevant details in the appropriate fields.
C) Hit the **save** button to save your changes.

Removing an entry

Check the entry you wish to delete and hit the **delete** button.

POP3 scanning tab



PineApp Mail-SeCure models can also act as a transparent POP3 proxy. In other words, it can scan external POP3 mailboxes. The users do **not** need to change anything in their configuration.

To activate the service, check both boxes and determine the concurrent sessions (at least the number of users who will be using this service). Check the Inspected Interface, usually LAN1 (eth0).

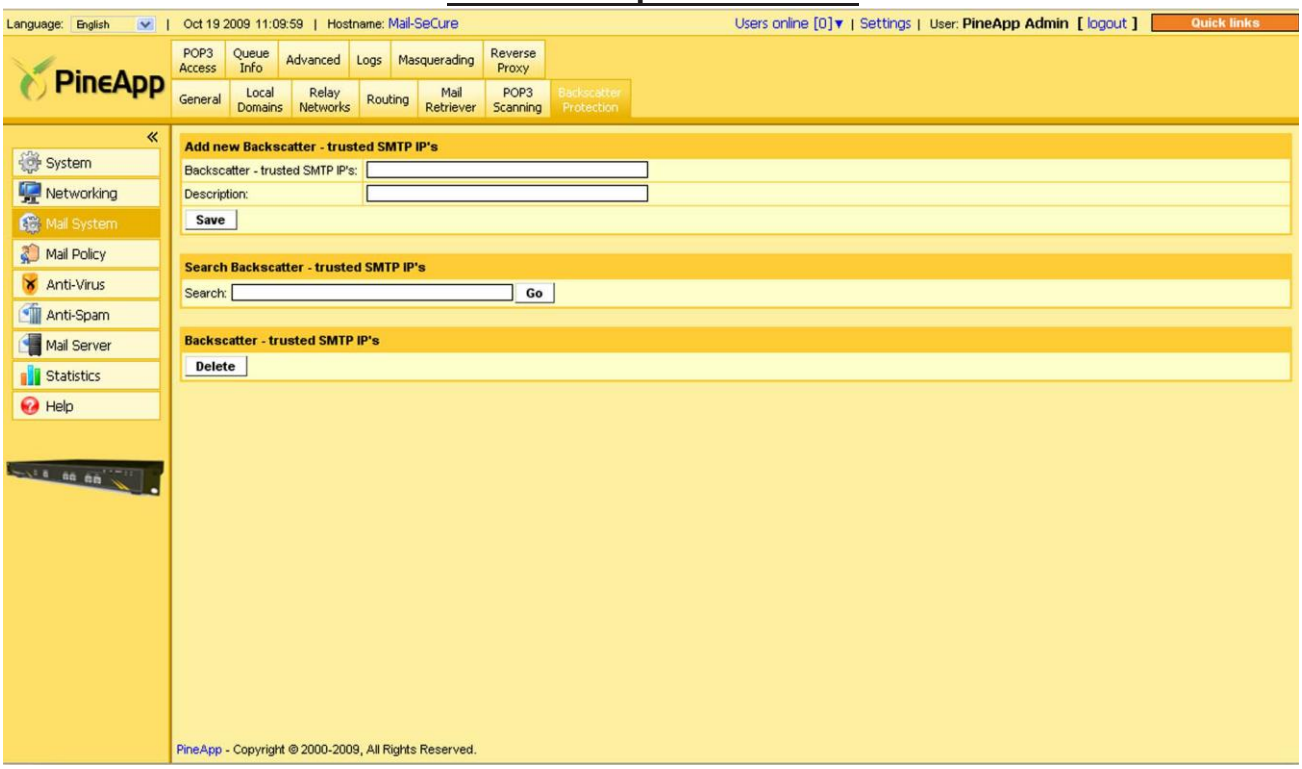
When working in a proxy mode, the following settings need to be configured on the end users' email clients:

1. Default port for email retrieval is 7110.

2. SMTP Authentication should be checked, with the remote account's username and password credentials.

3. Incoming & outgoing mail server addresses should be the Mail-SeCure's address.

Backscatter protection tab



PineApp has developed a unique solution for Backscattered mail.
In order to reduce Backscatter, enter the external SMTP IP of the organization.
The external SMTP IP can be located in the header of a mail received from a recipient in that domain.

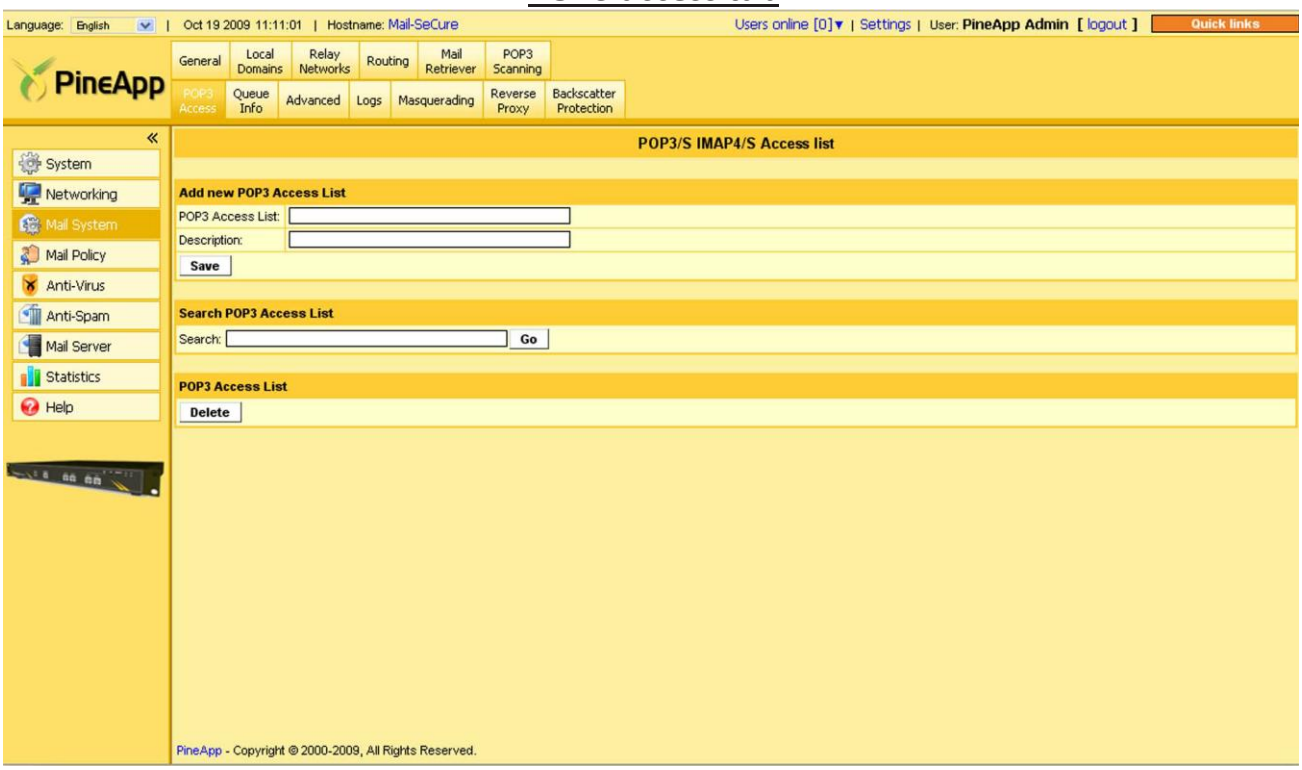
Adding a new entry

A) Type the SMTP server's IP address in the **Backscatter - trusted SMTP IP's** text field.
B) click on the **Save** button.

Removing an entry

Check the box next to the entry you wish to delete and click **Delete**.

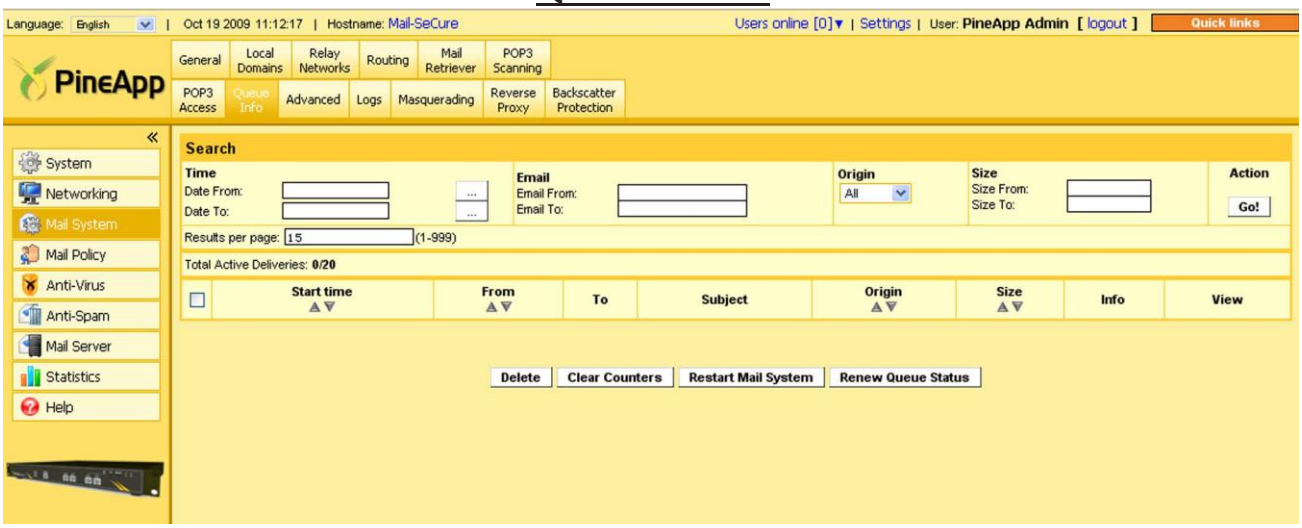
POP3 access tab



If the selected delivery method is Local, restrict networks and IPs from accessing the POP3 service in the Mail-SeCure device. (Default: none defined).
When no entries are defined, POP3 protocol is open to everyone.

Examples: For network 192.168.24.0 with subnet mask 255.255.255.0, type: 192.168.24. (Including the dot); for network 209.88.177.64 with subnet mask 255.255.255.192, type: 209.88.177.64-127.

Queue Info tab



In the Queue Info tab, it is possible to view all mail that is waiting for delivery or mail that is in the process of delivery.

Mail can be delayed in queue for the following reasons:
• Mail is in the process of being delivered (large email, multiple recipients etc.). When mail is in the process of been delivered, the line will be in blue.
• Problems at the recipient side. There are many kinds of problems that may cause mail not to be sent. For example:
• Domain expiration
• Bandwidth problems
• Unable to resolve domains due to DNS problems
• Non-existing users
• Mail servers rejecting mail due to size limits or any other rejection reason
• Temporary connectivity problems
The system will try to send the mail for 2 days (configurable; “Mail System > Advanced > Maximum message lifetime” (seconds).

Other possible reasons include:
• Timeouts caused by heavy bandwidth to and from the WAN.
• Problems with the internal mail server. If, for some reason, the internal mail server stops accepting SMTP connections, the incoming mail will be queued until the problem with the mail server is solved.

Each mail in the Queue Info can be viewed by clicking the **View** button.
Clicking the **Info** button will result in a pop-up window with more information regarding the mail.

This information contains the following: Start and end time of the email, to whom it was sent, status (failure, success or deferral), description of the status (reasons for failure or deferral) and the sessions (R - Remote, L- Local).

*In addition, it is possible to del*ete messages and to clear the counter. After a few sending attempts, the intervals between every sending attempt grows longer.
Clearing the counter restarts the intervals as they were in the beginning.

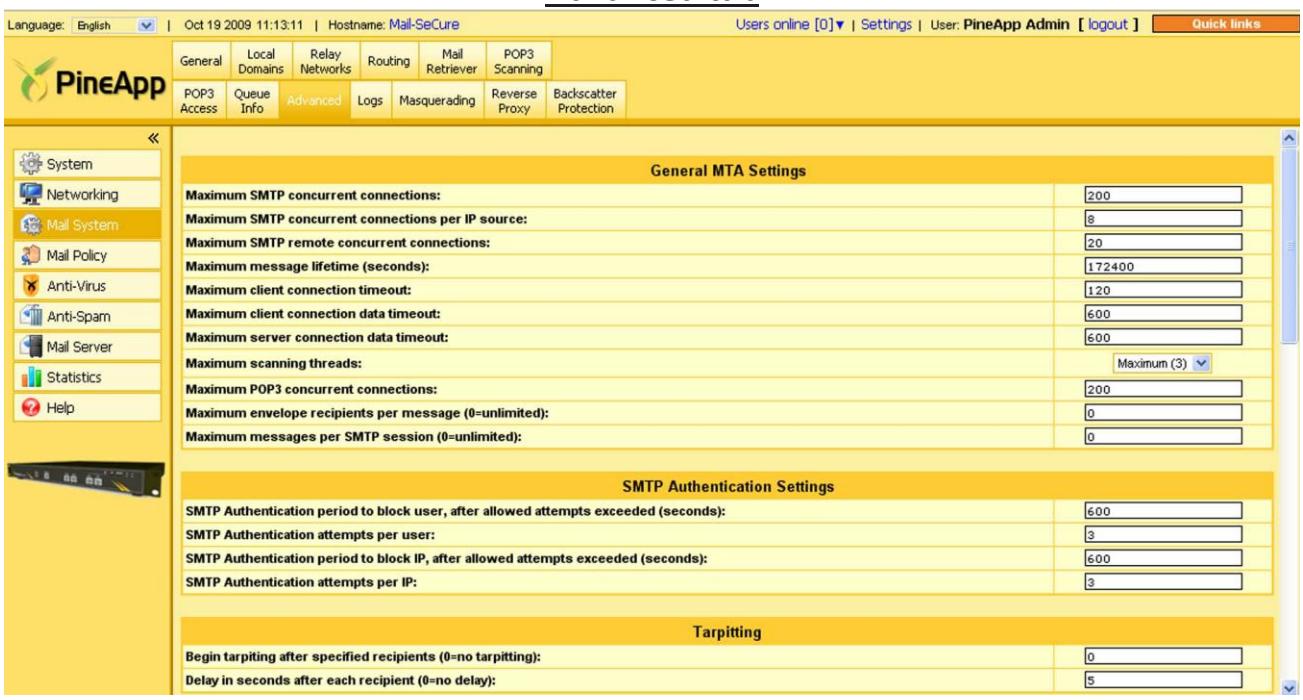
Blue Mail - Mail in transaction. If the sent mail is large and/or has many recipients, it may take a while until it is sent (especially if the upload of the organization is low). As long as the mail is bold, it is in the process of being sent.
Green Mail - After mail is successfully sent, it will not appear in the queue info any more. However, if a mail with multiple recipients is sent and at least one of the recipients has a problem, all successful mail will be in green, except the problematic one.
Red Mail - Mail that failed to be sent due to one of the reasons mentioned above. At first, the system will try to re-send it in short intervals. As time passes, the time between intervals will grow longer. The system will delete the mail after one week (configurable, Mail System > Advanced > Maximum message lifetime [seconds]) and the sender will receive a notification that the mail was not sent to the recipient and it was deleted from the system.
Purple Mail - If the recipient mail server returns a temporary error message
(4XX SMTP error message), the system will try to send the mail again later.

Search options
Searching for information in the different queues and logs was never easier and simpler than it is today. It is not mandatory to fill all fields. Empty fields are regarded as “all”.

When finished filling in the various fields, click the **Go!** button and the results will appear beneath the search fields.

Time - Type the time frame for searching (format: yyyy-mm-dd hh:mm) or click on the “…” button and a calendar will appear. Choose the desired date and time.
Email - Type the mail (or part of it) in the preferable field. It is possible to use wildcards (*).
Origin - Choose the direction: trusted (outgoing mail), Internet (incoming mail) or both.
Size - Type the size limit in bytes (1,000,000 ~ 1MB).

Advanced tab



In this tab, you can set some of the advanced features of Mail-SeCure. We recommend, however, leaving these features unchanged.

Maximum SMTP concurrent connections - Define the number of maximum SMTP connections (default: 200).

Maximum SMTP concurrent connections per IP source - This DoS (Denial of Service) feature determines the maximum SMTP concurrent connections per IP.
This feature protects Mail-SeCure from mail bombing by harmful servers. When more than 8 (default) concurrent connections from the same IP are established, the system refuses any more connections from that IP.

Maximum SMTP remote concurrent connections - This number is the maximum concurrent SMTP connections established by Mail-SeCure when sending mail.

Maximum message lifetime (seconds) - If a sent mail doesn't leave the system for any reason (recipient server is down, remote server doesn't exist etc.), the system will try and send the message for 172,800 seconds (default) - 2 days. Changing the length of time in which the system will continue trying to send these messages is possible.

Maximum client connection time-out - This figure refers to the time-out (in seconds) of the envelope session when connecting to the Mail-SeCure.

Maximum client connection data time-out - This figure is the time-out (in seconds) of the data session when connecting to Mail-SeCure.

Maximum server connection data time-out - This figure refers to the time-out (in seconds) of the data session when Mail-SeCure connects to external mail servers (outgoing traffic).

Maximum scanning threads - This value represents the number of scanning threads processed by the system for incoming mail. This value is determined by the license of the unit.

Maximum POP3 concurrent connections - This number refers to the maximum concurrent POP3 connections established to Mail-SeCure. This is relevant especially when the system is a mail server.

Maximum envelope recipients per message (0=unlimited) - Determines the number of envelope recipients per message. Defining this field may result in limiting the number of recipients in a single mail

Maximum messages per SMTP session (0=unlimited) - Defining any other number except 0 will limit the number of messages in a single SMTP session.

SMTP Authentication Settings

In order to prevent brute-force attacks by hackers, the system is configured to limit SMTP authentication requests and time-outs.

SMTP Authentication period to block user, after allowed attempts exceeded (seconds) - This defines the number of seconds after which the user is blocked after attempting to authenticate his SMTP session with wrong credentials. The number of allowed attempts before blocking is defined below (Default:600).

SMTP Authentication attempts per user - The number of attempts allowed per user before blocking (see above) - default: 3 attempts.

SMTP Authentication period to block IP, after allowed attempts exceeded (seconds) - This defines the number of seconds after which the IP is blocked after attempting to authenticate a SMTP session with wrong credentials. The number of allowed attempts before blocking is defined below (Default:600).

SMTP Authentication attempts per IP - The number of attempts allowed per IP before blocking (see above) - default: 3 attempts.

Begin Tarpitting after specified recipients (0=no tarpitting). In order to activate this feature, change the value. Tarpitting will start after X number of recipients within the envelope (default - 0).

Tarpitting - When activated, Tarpitting can increase the delay between recipients within the same envelope (Rcpt-to). The more recipients within the envelope, the bigger the delay is. The purpose of Tarpitting is to decrease mail from spammers who very often use many recipients in one envelope. Creating the delay will suppress such attacks.

Example: Putting 10 and 5 respectively will activate Tarpitting. If an Email with more than 10 recipients is received by the device, from the eleventh recipient, there will be a delay of 5 seconds between each recipient.

SMTP Banner Delay - This feature is based on the fact that most spammers (through Zombies) will not establish an SMTP connection with a server that will not respond the request within a few seconds. This feature artificially creates such delay in order to drive out such Spam attacks.

Delay in seconds after each recipient (0=no delay) - This is the delay (in seconds) that will be activated between the recipients (default - 5).

IP rate limit settings - The system allows you to limit maximum messages and sessions per IP within Day/Hour/Minute (Default - unlimited).

Domain Rate Limit Settings for specified domains - The system allows you to limit maximum messages and sessions per Domain within Day/Hour/Minute (Default - unlimited). The list of domains that will be affected by activating this feature can be listed below.

Enable Anti-Zombie fake SMTP delay - Enables the SMTP delay.

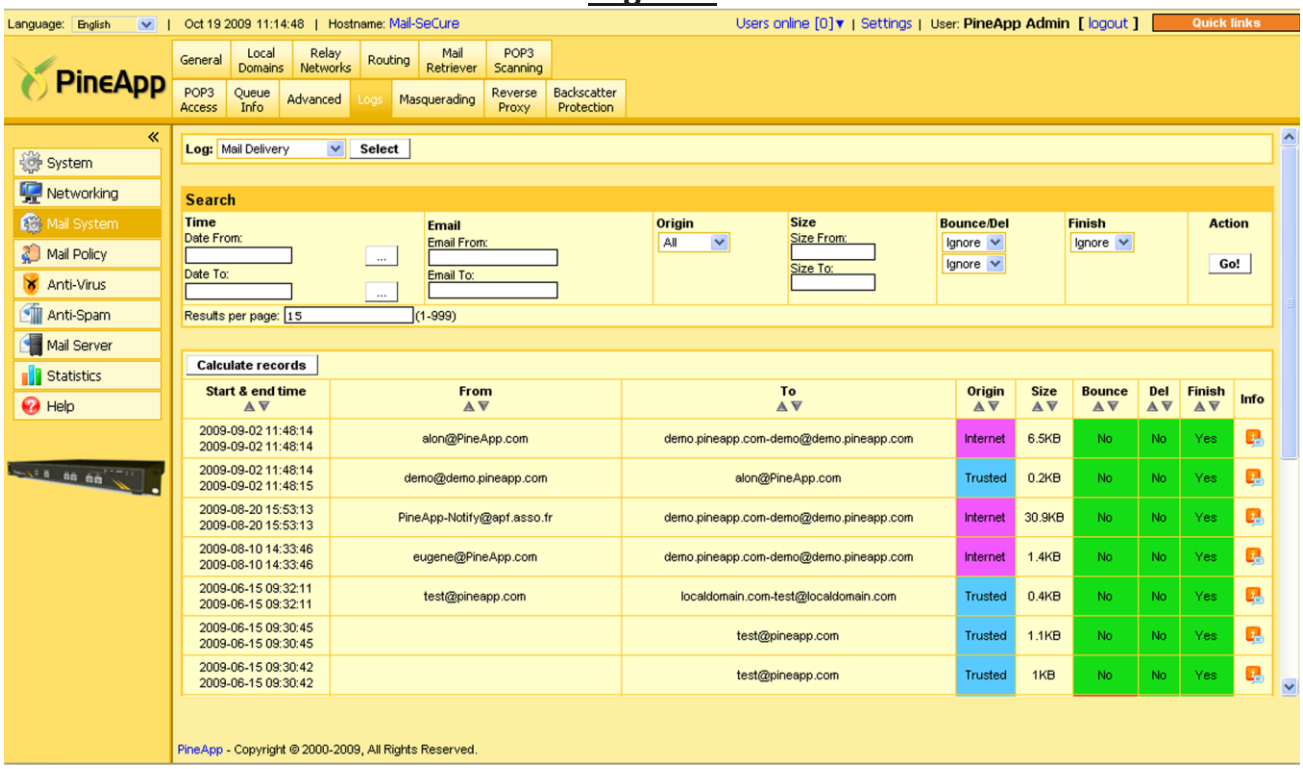
Delay to use for hosts with non-dynamic-looking reverse-DNS (x.x seconds) - This is the delay (in seconds) for traffic originated from non-dynamic-looking reverse-DNS hosts (default: 1).

Delay to use for hosts with dynamic-looking reverse-DNS (x.x seconds) - This is the delay (in seconds) for traffic originated from dynamic-looking reverse-DNS hosts (default: 18).

Delay to use for hosts with no reverse-DNS - This is the delay (in seconds) for traffic originated from no reverse-DNS hosts (default: 26).

Probability for which IPs with no reverse-DNS should be rejected with temporary error (percentage, 0=none, 100=all) - When traffic arrives from a no reverse-DNS host, it is possible to define what percentage of it will be delayed. This will increase the chance that legitimate “second attempts” will be successful (default: 10)

Logs tab



In this tab, logs regarding mail delivery and logs regarding traffic of protocol are generated. First, from the combo menu, the desired log is chosen: For each mail log, the start and end time can be viewed: Sender, recipients, origin, size, whether the mail bounced, whether the mail was deleted and if the delivery was successfully finished. If there is an unusual event, it will be painted in red.
All log events can be viewed by clicking the **Info** button. As in the queue info, the info window provides more details regarding the mail.
The search engine is activated as in Queue Info.

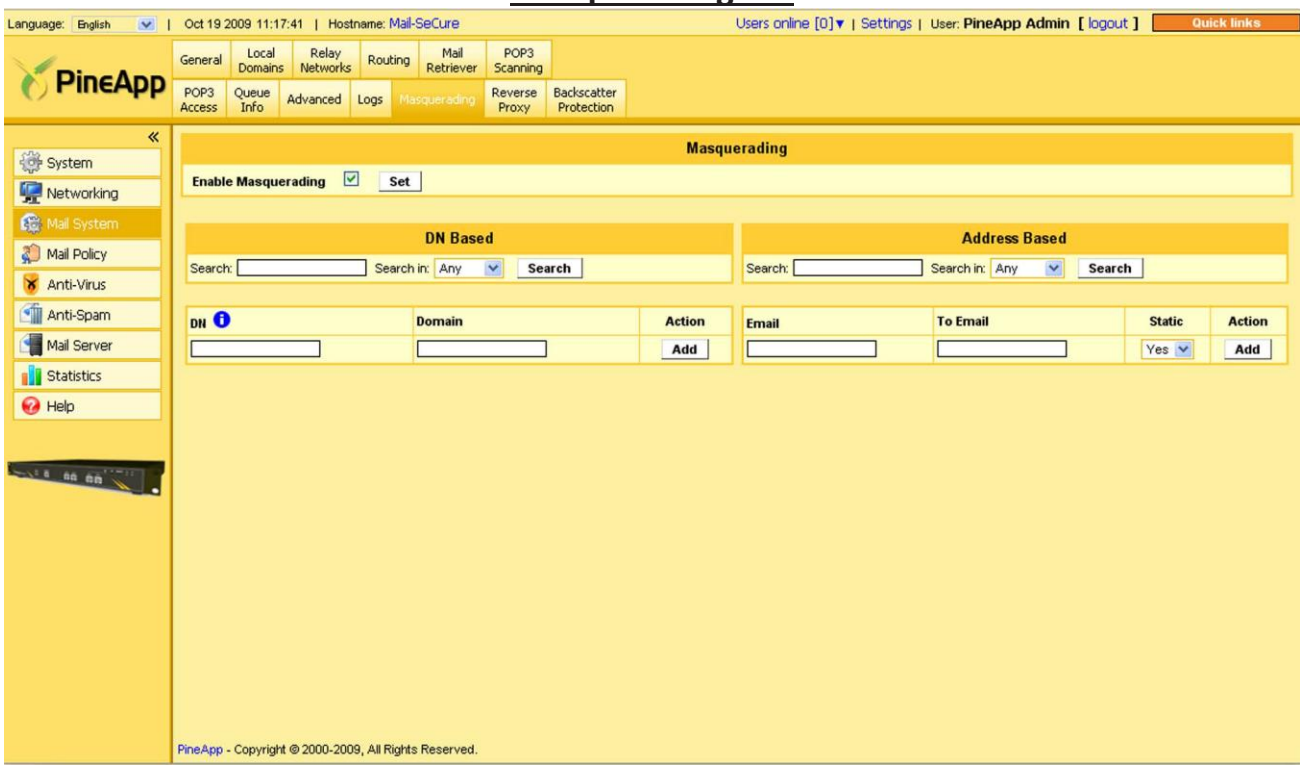
Mail Delivery - All traffic concerning the final email delivery phase (incoming and outgoing) is logged in the menu. Mail server responses can be viewed from this menu.

SMTP sessions - All incoming SMTP sessions' results are shown in this menu, including detailed error status etc.

POP3 sessions - All POP3 traffic sessions' results are shown in this menu.

IMAP4 sessions - All IMAP4 traffic sessions' results arre shown in this menu.

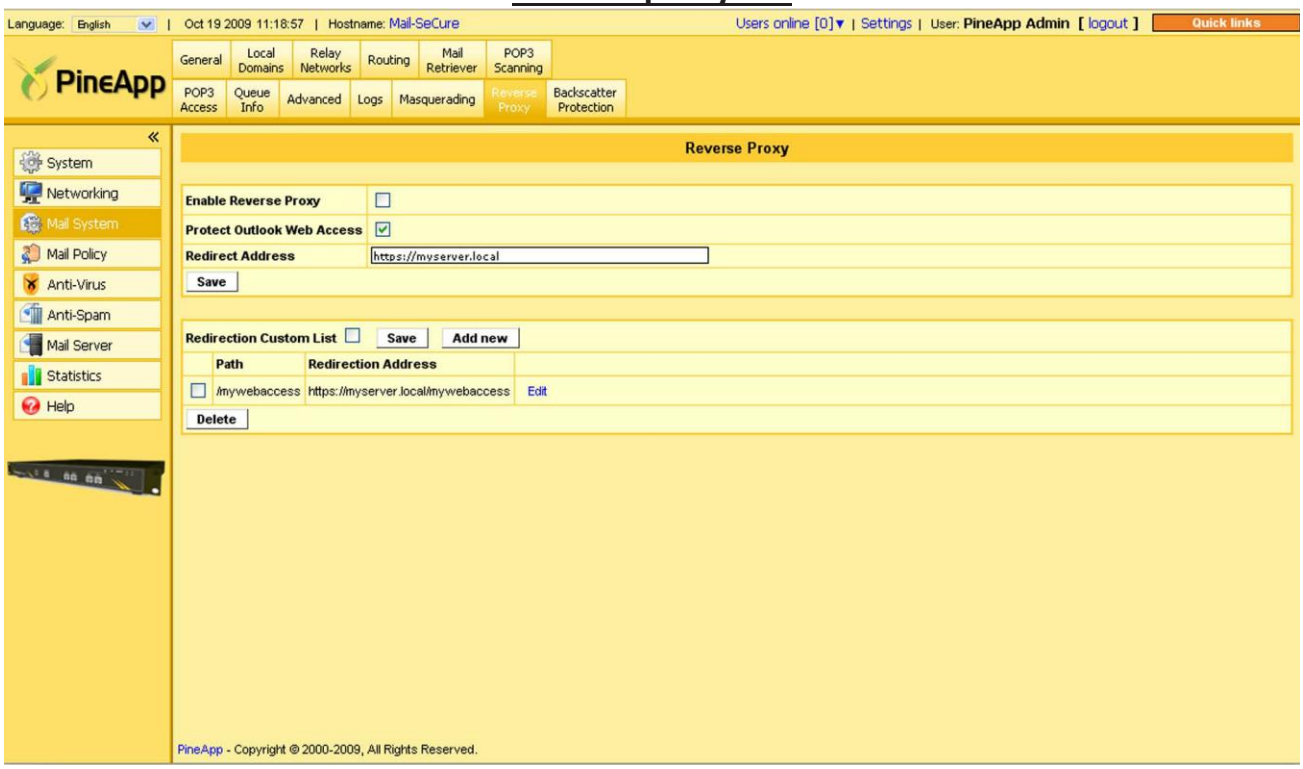
Masquerading tab



In this tab, it is possible to masquerade incoming mail. For example, mail sent to admin@domainA.com will be routed to the recipient admin@domainB.net.
First, make sure that the Masquerading feature is enabled.

On the left column - DN based, it is possible to fetch an existing group from the LDAP server. Make sure the system is synchronized with the LDAP server (System > LDAP). If configured properly, a list of the emails of the ou group will appear in the right pane.
Syntax:
DN > ou=europe,
Domain > pineapp.com
The list of emails on the right pane can be retrieved from the LDAP server or
can be manually configured. Manually configured emails should be static while the imported ones get a non static status.
Example: A user called mike in the pineapp.fr domain will have an email:
mike@pineapp.fr. After configuring the system, mail sent to mike@pineapp.fr will be presented to him as mike@pineapp.com
Note This feature is not available in Mail-SeCure 1000 series.

Reverse proxy tab



Reverse Proxy provides the ability to act as a proxy server near an email web access application such as Microsoft Outlook Web Access. It acts as a gateway to a mail server by acting as the final IP address for requests from outside.
Activating the reverse proxy is done by checking the **Enable Reverse Proxy** box

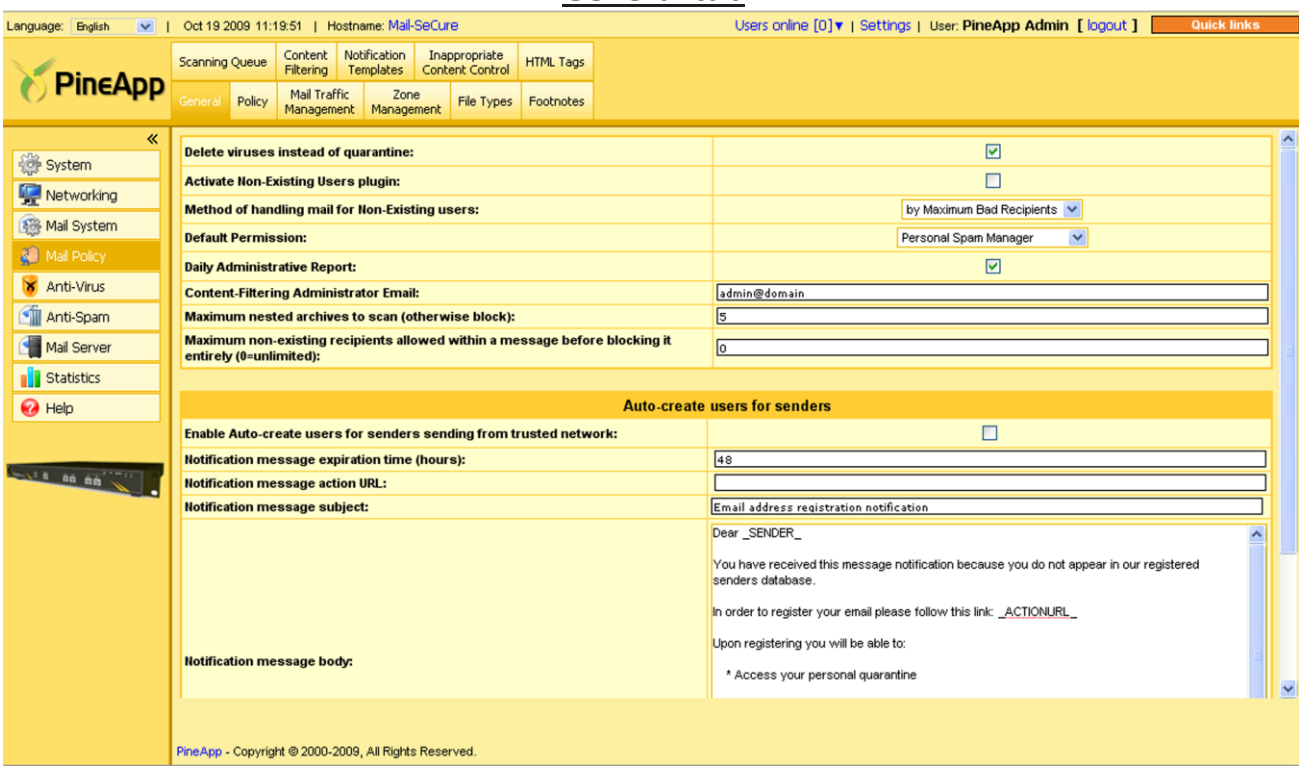
Check the next box if the device will be proxying an Microsoft Web Access.
Define the address of the re-directed device.
If there are more than one redirected devices in the organization, it is possible to create a custom redirect list.
Click on the **edit** button, and create the redirection: When done, click the **Save** button.
It is possible to create more than one redirection.

CHAPTER 5

MAIL POLICY

In this window, the Mail-SeCure's mail policy is configured and managed.

General tab



Delete viruses instead of quarantine - Define whether viruses will be deleted instead of sent to quarantine, where they may be viewed but not managed or downloaded (default - checked).

Activate non-existing users plug-in - After synchronizing Mail-SeCure with an LDAP server, the system can treat mail to nonexistent users in several different methods. Checking this box will activate the module.

Method of handling mail for non-existent users - After checking the box above, you will need to choose from the dropdown menu which method should be taken in order to treat mail for non-existing users:

1. **By maximum bad recipients -** mail message that exceeds the allowed number of non-existing recipients within one mail message will be blocked. Once choosing .
2. **Move to low priority queue** - This will always give mail to existing users higher priority in the scanning queue.
3. **Auto-Quarantine** - all mail to non-existing users will be quarantined.
4. **Auto-Delete -** all mail to non-existing users will be deleted.

Default Permission - Define the permission new users receive when created on the system,

whether manually (System > User management), or by synchronizing to an LDAP server (System > Connectors).

Daily Administrative Report - Once checking this box, the administrator's email address, configured in Mail System > General tab will receive a daily report that summarizes the system's daily traffic.

Content-Filtering Administrator Email - The email defined in this field will receive all administrator notifications that are configured in the policy rules.

Maximum non-existing recipients allowed within a message before blocking it entirely (0=unlimited) - Set a parameter of Maximum non-existing recipients allowed within one mail message. If an email message will be delivered with a higher nyumber of non-existing recipients from the configured number, it will be automatically quarantined.

Notice that *Special handling of mail to non-existing users* must be activated in order for this feature to work (default - 0).

Maximum nested archives to scan (otherwise block) - Define how deep in the archive the system must scan. The deeper the scan, the longer it takes. If there are more nested files than defined, the system will treat the mail as infected (default - 5).

Auto-create users for senders

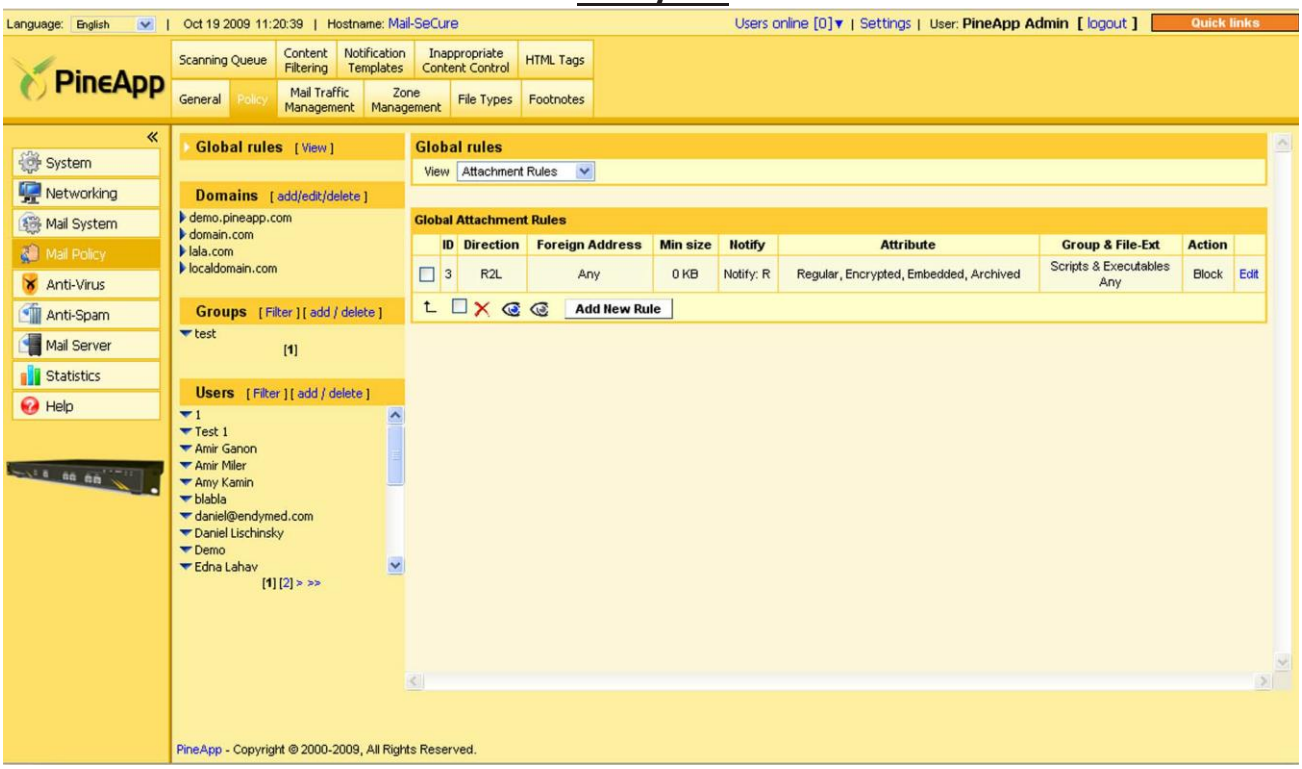
This section contains service provides features for automatic registration. Upon delivering an email using a local domain from a trusted network, customer will receive a notification message, containing an activation URL. Once clicking on the action URL, sender will be automatically registered on the system, and will be added as a user in User Management tab.

Enable Auto-create users for senders sending from trusted network- by checking this option, the Auto-user creation feature will be activated.

Notification Message expiration time – This field contains a numerical parameter (the default value is 48), representing the notification link's lifetime: after the given number of hours listed in this text field, the link will expire and will not redirect the customer to Mail-SeCure for registration.

Notification message action URL – In this text field, fills in Mail-SeCure's URL address, to which all registration requests will be redirected.

Policy tab



In this tab, all Global/Domain/Group/User policies are configured in corresponding tiers:
When entering this tab for the first time, the above window is displayed.

Policy Tiers Description

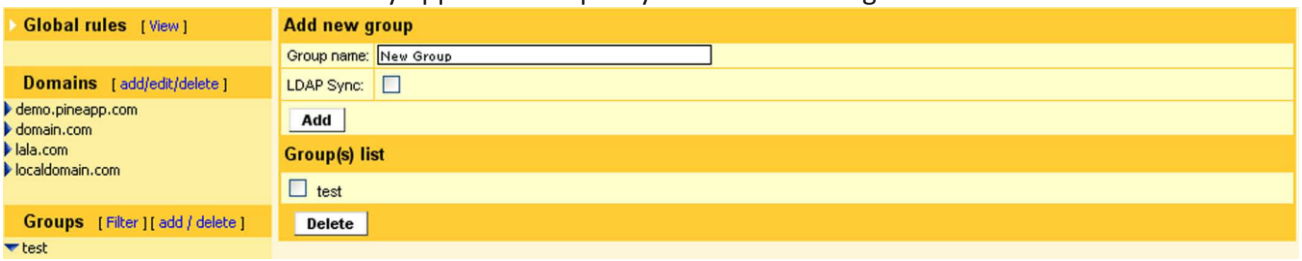
Global Policies effect the whole organization.
Domains Policies effect the defined domain only.
Groups Policies effect the defined group members only.
Users Policies effect specific users only.

Creating new users

Creating and managing users is done through the User Management tab.

Creating new domains

New domains will automatically appear in the policy tab after creating them in the **Local Domains** tab.

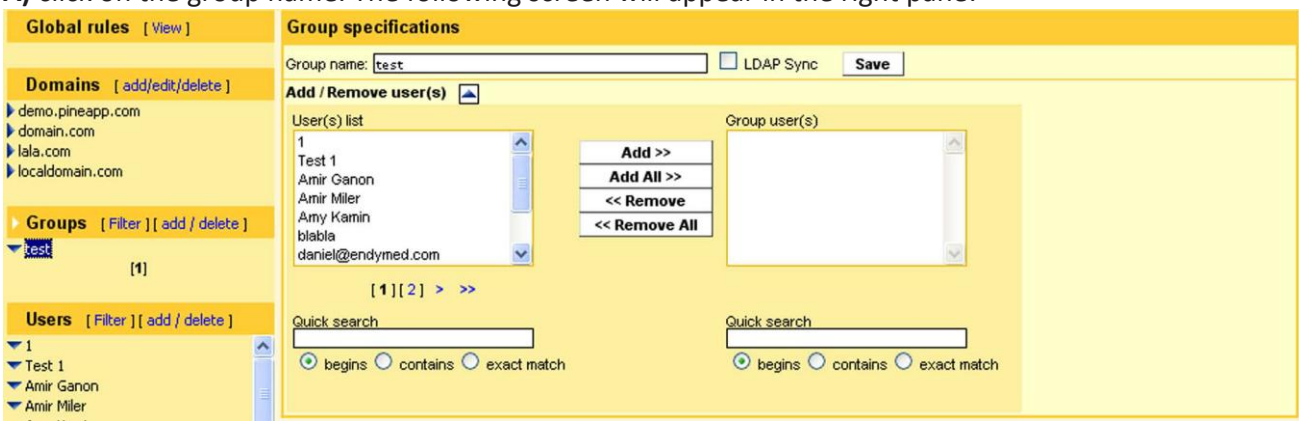


Creating new groups

A) In the Groups tier in the left pane, click on the add link (indicated in a red square in the picture above).
B) In the Group name field, type the name of the group you wish to create and check **LDAP sync** option, in case you want to synchronize its users from an existing LDAP group under the same name.
C) Click on the **Add** button (marked in a blue square in the picture above). A new group will be created and added to the column on the left.

Adding/Removing new group users

A) click on the group name. The following screen will appear in the right pane:



B) Click on the user that you wish to add/remove, and click on the **Add/Remove** button.
You can also add all users/remove them from the group by clicking on **Add all/Remove all** button. In case you wish to make up the members in the specific group.
C) When done, click on the **Save** button.

Modifying groups

A) Select the group you wish to modify by clicking on it.
B) The group will appear in the right pane with its list of members. It is possible to add and remove members, as described above in the **Creating new groups** section.
C) Rename the group by typing the new name. When done, click on the **Save** button.

Deleting groups

A) Before deleting a group, ensure that all members of that group are removed.
To do this, select the group you wish to delete by clicking on it. In the right pane, click to remove all members and then click **Save.**
B) In the Group tier in the left pane click **add/delete**. A list of all groups will appear in the right pane. Select the groups you wish to delete by checking the box next to them and then click **delete**.

Understanding policy modules

Mail-SeCure offers a four-tier policy management tool (Global/Domain/Group/User). For each tier a different set of rules can be configured from the different modules - Attachment, Spam or Content Filtering, HTML Tags and General policy rules.

The rule hierarchy states that the lower the tier (Global > Domain > Group >User), the "stronger" the rule. Rules given to groups will override global rules even if they contradict them. Rules given to users will override their group or global rules, even if they contradict them.
In addition, if contradicting rules are given to two different groups that contain the same users, the severe rules will override the other rules.
Note In Mail-SeCure 1000 series it is only possible to create global rules

Attachment Rules - In this module define attachment rules. It is possible to define rules for incoming and outgoing mail, extension types, notifications and actions.

Spam Rules - In this module define Spam rules. It is possible to set Anti-Spam threshold scores, notifications and more.

General Rules - In this module define general rules such as forwarding, notifications and footnotes.

Black & White rules - These rules define the Black and White lists for each tier. The lists refer **only** to the Spam rules.

Content Rules - Rules set in this module define content filtering rules. It is possible to create rules based on keywords within a message's subject, body and attachments. This module supports almost 300 types of attachments.

HTML tags Rules - In this module define HTML tag rules. It is possible to create rules based on HTML tags. Tags are created under the Policy > HTML Tags tab.

Attachment Rules

The first step in creating an attachment rule is to determine which tier the rule will effect.

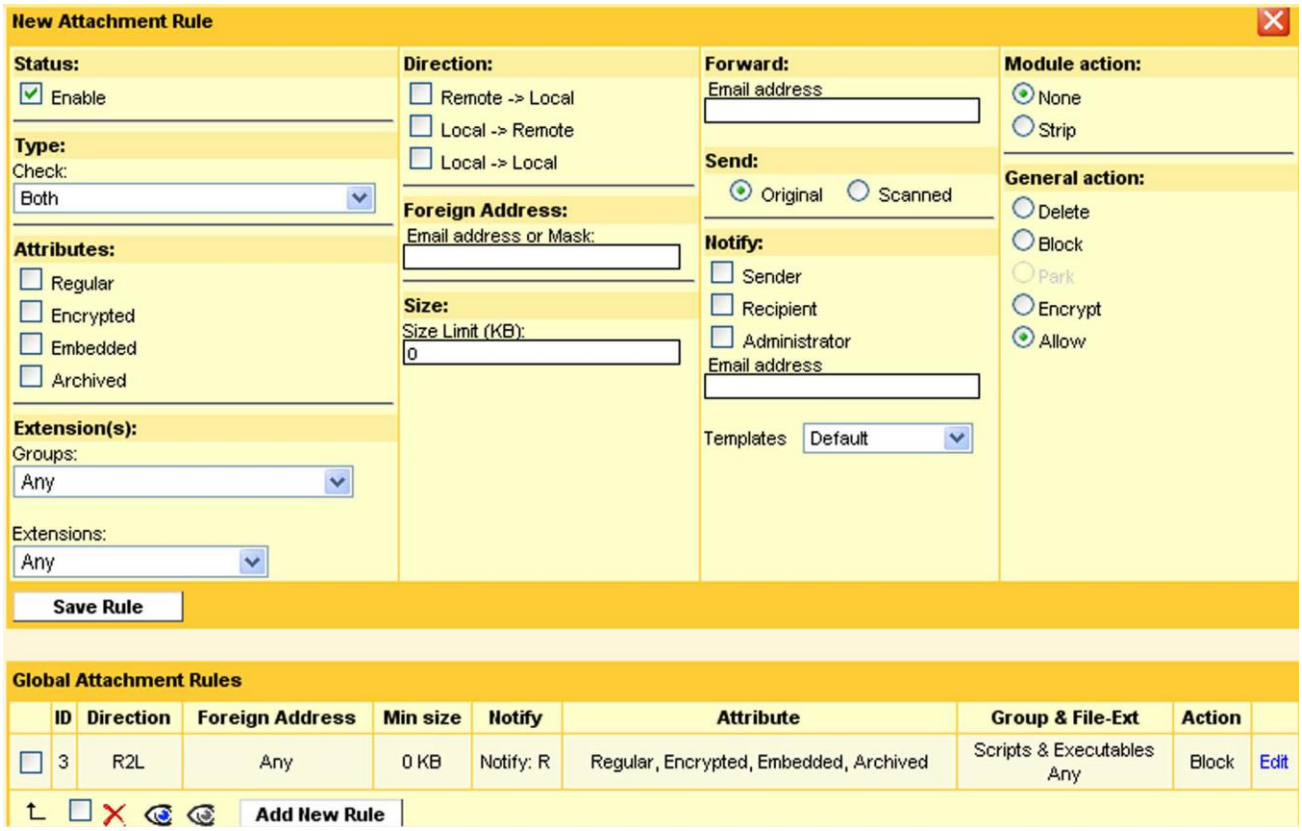
Choosing a policy Tier for rule creation:

Global - In the Global rules section in the left pane, click on the *View* link. A summary of all global rules will appear in the right pane.
Domain - Select the domain you wish to create rules for by double clicking on the domain from the list in the left pane, and click on it.
Group - Select the group you wish to create rules for by double clicking on the group from the list in the left pane. The details of that group will appear in the right pane.
User - Select the user you wish to create rules for by clicking on the user from the list in the left pane.

Make sure that the Attachment rules menu is chosen from the dropdown menu

Adding a new attachment rule

After clicking on the **Add new rule** button (whether for Global, Domain, Group or User), under attachment rules menu, the following screen will appear in the right pane:



Status

In case the box next to "Enable" is unchecked, the rule will be disabled and won't apply.

Type

From this dropdown list, select the blockage type:
File type - The file is examined only by its header.
Example: If a sender renames an EXE file XXX, the system will still identify it as an EXE file.
Extension - The file is examined only by its extension.
Example: If a sender renames an EXE file XXX, the system will identify the file as XXX file.
Both - The file is identified by its type or its extension (default).

Attributes

Select the file attributes the rule will apply to (more than one can be selected).
Regular - Ordinary files sent as they are (default).
Encrypted - Encrypted files.
Embedded - Files that are embedded in other files**. Example**: An EXE file that is embedded into a DOC file.
Archived - Archived Files that are compressed into files such as ZIP, ARJ and RAR.
Extension(s) - In this menu, the groups and extensions that the rule will apply to are selected (see File Types Tab for detail on groups and extension management). As soon as a group is selected, only the extensions related to that group will appear in the menu. It is possible to select specific groups and specific extensions from within the group.

Direction

In this section, select the direction of the mail for which the rule will apply by checking the box next to it (it is possible to check more than one):

Local -> Remote All outgoing mail.
Remote -> Local All incoming mail.
Local -> Local All internal mail (when acting as a mail server).
Foreign address - If the rule applies to a specific address or domain, the address or domain must be written in the Foreign address field. Wildcards are accepted (*). It is not possible to add more than one domain/address per rule.

Size - To configure a file size limit, enter the file size (in KB). This will activate the limitation (the default is 0 = no limit).

Forward - In this section, it is possible to enter a defined recipient's email address for the system to send email copies. If "Original" is checked (default), the email will be forwarded as it was sent to the system. If "Scanned" is checked, the system will first scan the email for any rules that may apply and take relevant action.

Notify - In this section, notifications are configured (see **Notification Templates** Tab for information on how templates are created and managed).
First, select the notification recipient (more than one recipient can be selected).
It is possible to add specific email addresses to receive notification.

Then, select the notification template for a specific rule from the **Template** dropdown list.

Module action

In this menu, the email's attached files fate is decided:

None - Do not perform any action on the email's attached files.
Strip - When checked, the email with the attachment will be stripped so the recipient receives the original email stripped of its attachments. Once this option is checked, it is not possible to delete or block the email.

General action

In this menu, the action for each rule is configured:

Delete - The message will be deleted and a copy of the email will not be sent to quarantine.
Block - The message will be blocked and sent to quarantine.
See "Zone Management Tab" for information on creating and managing quarantine zones.
Park - The mail will be parked in a specific zone. As soon as the Park action is selected, different zone options become available.
See "Zone Management Tab" for information on creating and managing parking zones.
Encrypt – the email will be forwarded to the encryption server for content encryption

Allow - The email will reach its recipient.

Once finished, click on the **Save Rule** button.

Some basic rules:
• There is no limit to the number of rules that can be applied to groups and users.
• If there is a conflict between the rules, User rules override Group rules, and Group rules override Global rules.
• If there are rules that contradict each other, the stricter rule will override.

Modifying rules
Click on the rule to display its current settings.
To modify a rule, click the **edit** link next to it.
After modifying the rule, click on the **Save** button.

Modifying rules is done the same way, as described above, for all policy modules.

SPAM Rules

In general, Spam rules work like Attachment rules.

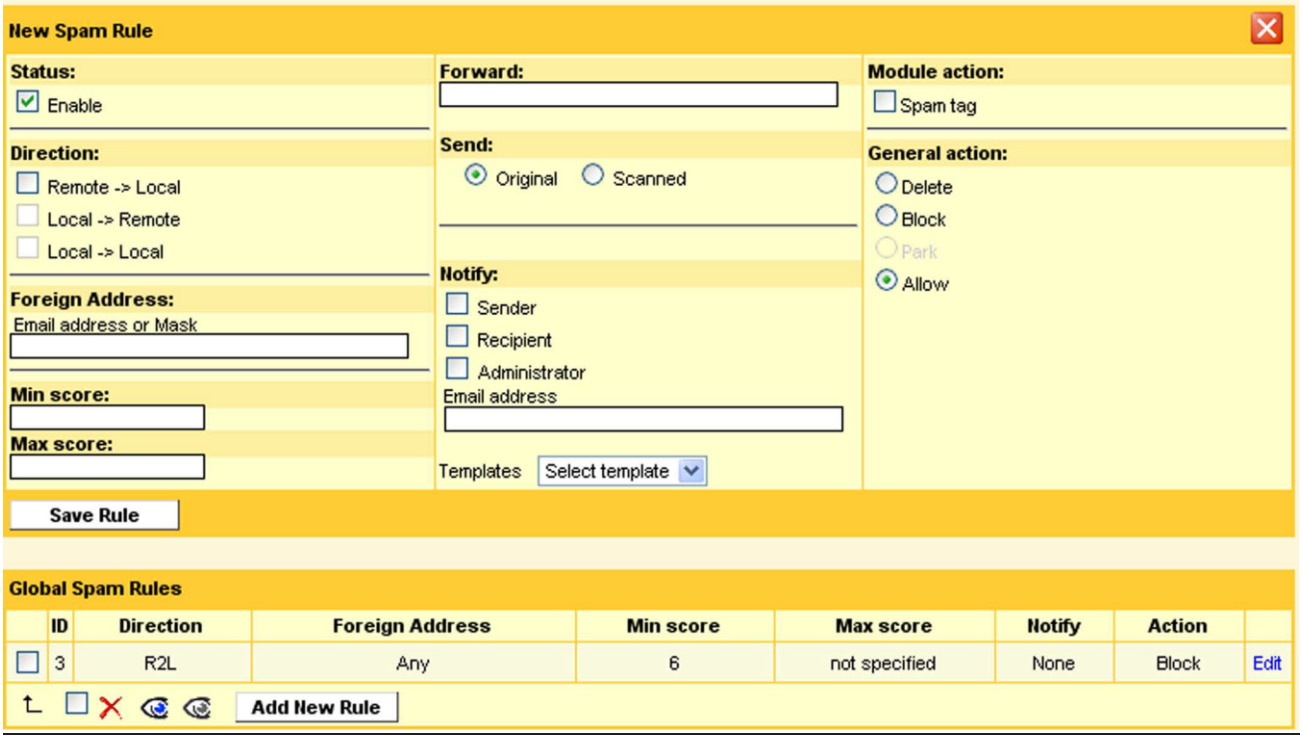
Choosing a policy Tier for spam rule creation:
Global - In the Global rules section in the left pane, click on the *View* link. A summary of all global rules will appear in the right pane.

Make sure that the Spam rules menu is chosen from the dropdown menu

Domain - Select the domain you wish to create rules for by double clicking on the domain from the list in the left pane, and click on it.
Group - Select the group you wish to create rules for by double clicking on the group from the list in the left pane. The details of that group will appear in the right pane.
User - Select the user you wish to create rules for by clicking on the user from the list in the left pane.

Adding a new SPAM rule

Select the tier to create the rule for, as mentioned above, under Spam Rules menu, and click on the **Add new rule** button (indicated in a red square in the picture below).



The following options are displayed in the right pane:

Status

In case the box next to "Enable" is unchecked, the rule will be disabled and won't apply.

Direction

In this section, select the direction of the mail to which the rule will apply by checking the box next to it.
Remote -> Local - Incoming mail
Local -> Remote - N/A
Local -> Local - N/A

Foreign address - If the rule must apply to a specific address or domain, the address or domain must be entered here. Wildcards are accepted (*). It is not possible to add more than one domain/address per rule.

MIN score / MAX score - These values define the sensitivity of the Anti-Spam engine. The two sets of scores (min and max) enable the system to be more flexible. It is possible to enter values in either fields or both. The example on page 5-20 explains the functionality of the scoring.

Forward - In this section it is possible to enter a defined recipient's email address for the system to send email copies. If "Original" is checked (default), the mail will be forwarded as it was sent to the system. If "Scanned" is checked, the system will first scan the email for any rules that may apply and take relevant action.

Notify - In this section, notifications are configured (see Notification Templates Tab for information on

how templates are created and managed).
First, select the notification recipient (more than one recipient can be selected).
It is possible to add specific email addresses to receive notification.
Then, select the notification template for a specific rule from the dropdown list.

Module action

SPAM Tag - When checked, emails identified as Spam will be tagged as Spam and then either sent to the recipient or parked. The user will receive the email with ***Spam*** added to the subject (Configurable - see page 7-4).
Please remember that the mail will be tagged only if the score it received falls within the defined score in the rule.

General action

In this menu, the action for each rule is defined:
Note When finished configuring the rule, don't forget to save.
Delete The message will be deleted and a copy of the email will not be sent to quarantine.
Block - The message will be blocked and sent to quarantine.
See **Zone Managemen**t Tab for information on creating and managing quarantine zones.
Park - The mail will be parked in a specific zone. As soon as the Park action is selected, different zone options become available.
See **Zone Management** Tab for information on creating and managing Parking zones.
Allow - The message will go through to the recipient. This is useful if an email notification is required.
Once finished, click on the **Save Rule** button.

General rules

The General rules deal with rules that apply to all clean incoming and/or outgoing mail.

Choosing a policy Tier for General rule creation:

Global - In the Global rules section in the left pane, click on the *View* link. A summary of all global rules will appear in the right pane.

Domain - Select the domain you wish to create rules for by double clicking on the domain from the list in the left pane, and click on it.

Group - Select the group you wish to create rules for by double clicking on the group from the list in the left pane. The details of that group will appear in the right pane.

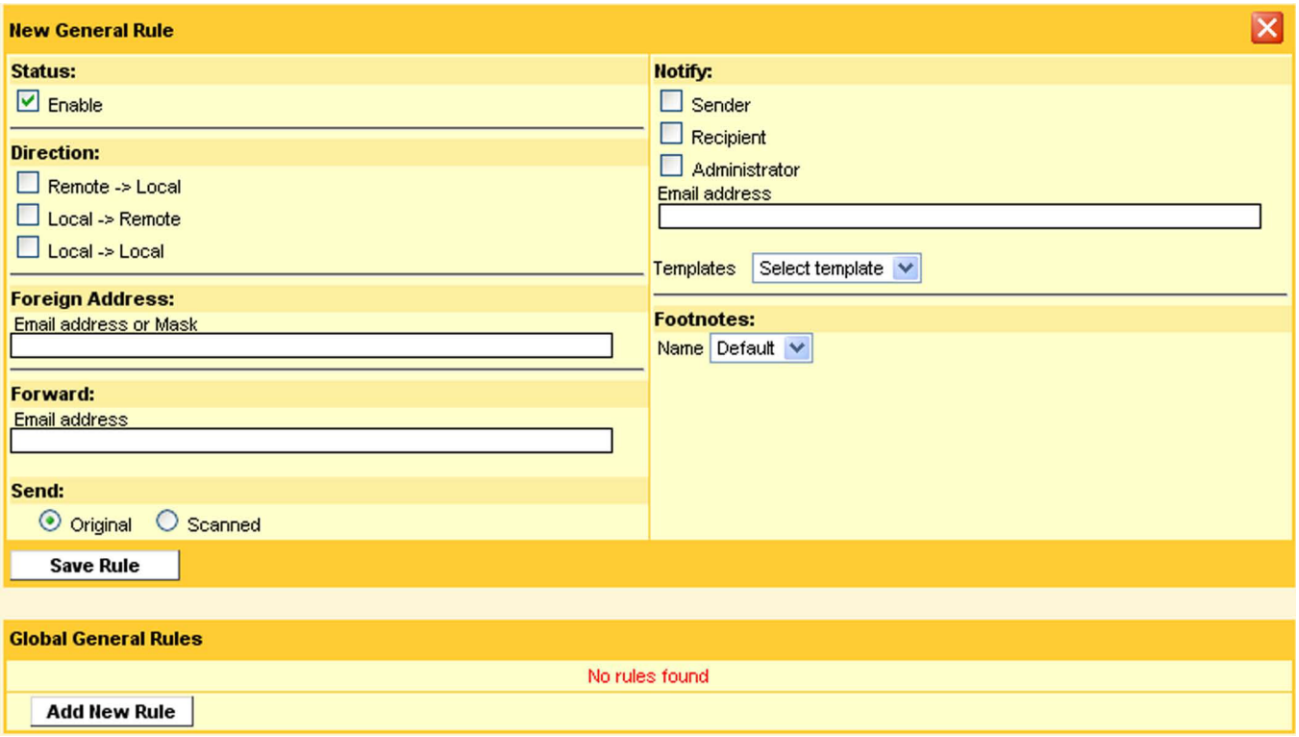
User - Select the user you wish to create rules for by clicking on the user from the list in the left pane.

Make sure that the General rules menu is chosen from the dropdown menu

Adding a new general rule

Select the tier to create the rule for, as mentioned in the beginning of Attachment rules section, and under Global General Rules, make sure that the Spam rules option is chosen from the drop-down menu. click on the **Add new rule** button (indicated in a red square in the picture below).

The following screen will appear in the right pane:



Status

In case the box next to “Enable” is unchecked, the rule will be disabled and won’t apply.

Direction

In this section, select the direction of the mail for which the rule will apply to by checking the box next to it (it is possible to check more than one):

Local -> Remote - All outgoing mail
Remote -> Local - All incoming mail
Local -> Local - All internal mail (when acting as a mail server)

Foreign Address - If the rule applies to a specific address or domain, the address or domain must be written in the Foreign Address field. Wildcards are accepted (*). It is not possible to add more than one domain/address per rule.

Forward - In this section it is possible to enter a defined recipient's email address for the system to send email copies to. If "Original" is checked (default), the mail will be forwarded as it was sent to the system. If "Scanned" is checked, the system will first scan the email for any rules that may apply and take relevant action. In any case, the original mail will be sent to the original recipient.
Notify - In this section, notifications are configured (see **Notification Templates** Tab for information on how templates are created and managed).
First, select the notification recipient (more than one recipient can be selected).
It is possible to add specific email addresses to receive notification.
Then, select the notification template for a specific rule from the dropdown list.

Footnote - Select the footnote that will be attached to the email.

Additional Footnotes are created and modified in the Mail Policy > Footnotes tab (see page 5-46.)

Black & White rules

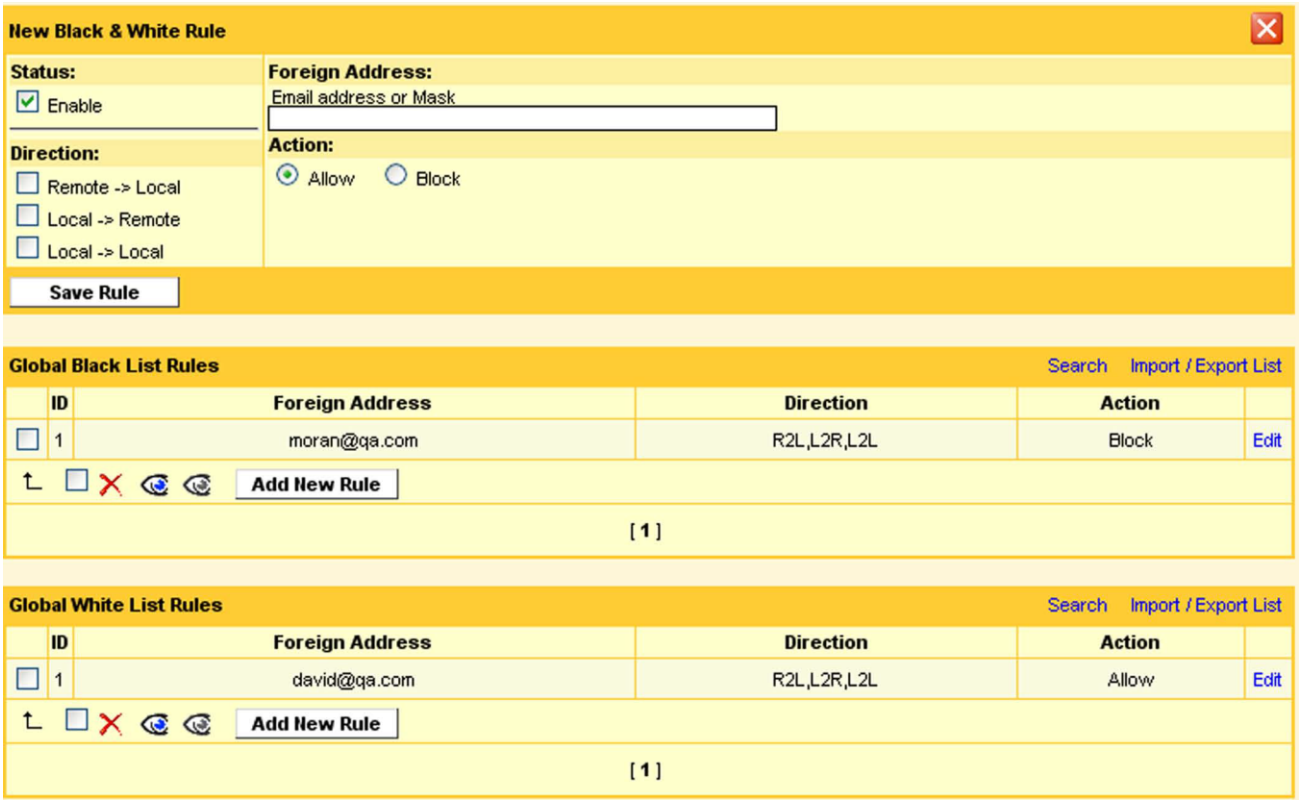
It is possible to create Black & White list to apply to one of the three policy management tiers.
Choosing a policy Tier for Black & White rule creation:
Global - In the Global rules section in the left pane, click on the *View* link. A summary of all global rules will appear in the right pane.
Domain - Select the domain you wish to create rules for by double clicking on the domain from the list in the left pane, and click on it.
Group - Select the group you wish to create rules for by double clicking on the group from the list in the left pane. The details of that group will appear in the right pane.
User - Select the user you wish to create rules for by clicking on the user from the list in the left pane.
It is also possible to create Black & White lists for specific domains, groups and users.
Black & White lists for groups - Click on a group to select it and then select **Black &White rules** from the *View Rules* dropdown list. This will enable you to manage the group's lists.
Repeat the instructions described for adding lists to the Global tier.
Black & White lists for users - There are two ways the Black & White lists can be updated for the users:
1. The administrator can use the GUI to manage the user's list (same as the Global and Group tiers).
2. By using Black & White listing options in the Daily Report.

Make sure that the Black & White rules menu is chosen from the dropdown menu

When importing a text file using the Auto-detect, the list will be imported as all blocked. However, if the list is listed with the action tag (BLOCK or ALLOW) next to each record, the import will know what to block and what to allow:
spam@pineapp.com, BLOCKED; test@pineapp.com, BLOCKED;*@pineapp.net, ALLOW

Adding a new Black & White list rule

To add a new entry, click on the Add New Rule button (marked in a red square in the picture below).
The following screen will appear:



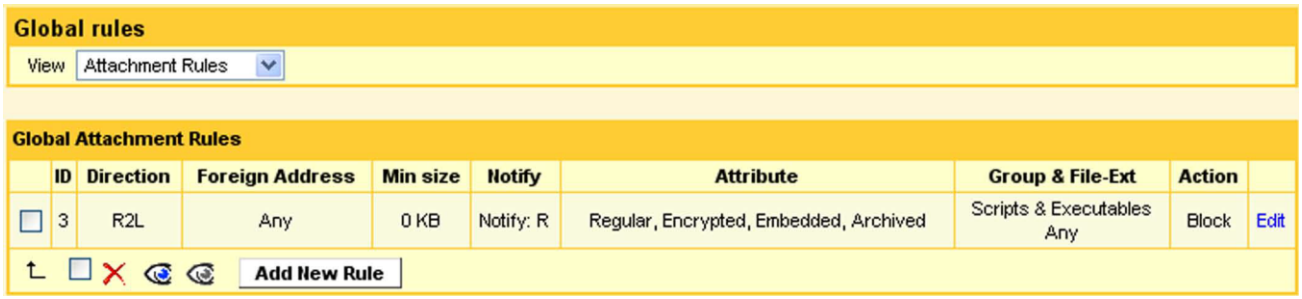
A) Type the email address or domain that you wish to block/allow access to.
To blacklist/whitelist a single email address, simply type it (example: john@pineapp.net).
To blacklist/whitelist an entire domain, type the wildcard character (*) and the domain name afterwards (example: *@pineapp.net).
B) Pick **Allow** or **Block** from the **Action** section, below the address field.
C) Click on the **Save new rule** button

It is also possible to create Black & White lists for specific domains, groups and users.

Black & White lists for groups - Click on a group to select it and then select **Black &White rules** from the **View Rules** dropdown list. This will enable you to manage the group's lists.

Some basic rules:
• User entries will always override Global & Group entries.
• Entries configured in the GUI for the user by the administrator will override global or group entries.

Disabling, enabling and deleting rules
If, for any reason, a rule needs to be disabled for a short period of time, there is no need to delete the rule and recreate it.



Clicking on the Disable icon (marked red in the picture above) will disable the rule and the rule will turn grey.

In order to enable the rule, click on the **Enable** icon (marked green in the picture above) and the rule will become active again.

By clicking on the **Delete** icon (marked blue in the picture above), the rule can be deleted all together.

Exporting a Black/Whitelist file

A) Check the type of list(s) you wish to export to your local hard drive from the Export Action section (All, Block and Allow).
B) Check the requested file format you wish to receive the file in the Export List section (Excel CSV file or a simple txt file).
C) Click on the **Export** button (marked in an orange square in the above picture).

Importing a black/whitelist file to the system

A) Choose the location where the file is placed on the local hard drive, by clicking on the **Browse** button (marked in a blue square in the picture above).
B) Upload the file to the system by clicking on the **Import** button (marked in a green square in the picture above)

It is also possible to create Black and White lists for specific domains, groups and users.

Black & white lists for groups - Click on a group to select it and then select **Black &White rules** from the **View Rules** dropdown list. This will enable you to manage the group's lists. Repeat the instructions described for adding lists to the Global tier.

Black & white lists for users - There are two ways the Black and White lists can be updated for the users:
1. The administrator can use the GUI to manage the user's list (same as the Global and Group tiers).

Content rules

Before creating the content filtering rules, please refer to the **content filtering** tab and activate the groups that the rules will use.

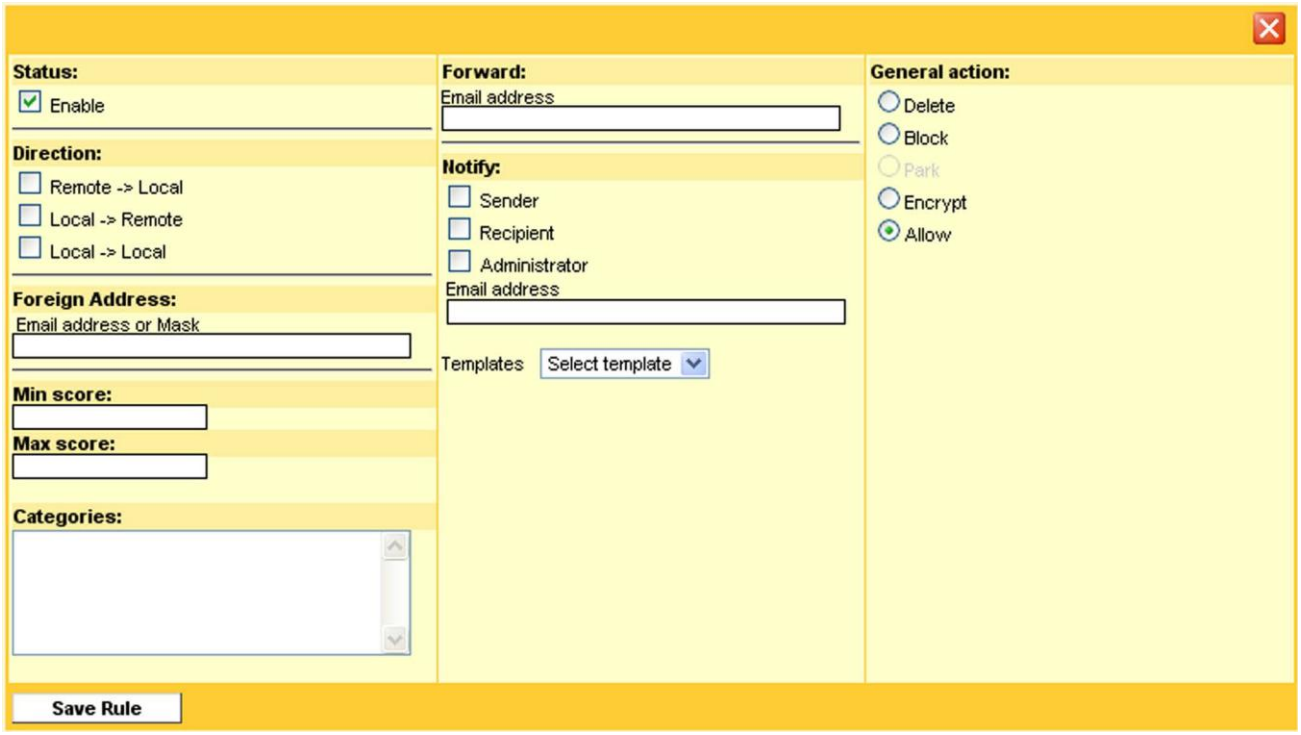
Choosing a policy Tier for General rule creation:

Global - In the Global rules section in the left pane, click on the *View* link. A summary of all global rules will appear in the right pane.
Domain - Select the domain you wish to create rules for by double clicking on the domain from the list in the left pane, and click on it.
Group - Select the group you wish to create rules for by double clicking on the group from the list in the left pane. The details of that group will appear in the right pane.
User - Select the user you wish to create rules for by clicking on the user from the list in the left pane.

Adding a content rule

Select the tier you wish to create the rule for, and make sure that the Content rules menu is chosen from the View drop-down menu. Click on the **Add new rule** button.

The following screen will appear in the right pane:



Status

In case the box next to “Enable” is unchecked, the rule will be disabled and won’t apply.

Directions

Remote -> Local - Incoming mail
Local -> Remote - Outgoing mail
Local -> Local - When acting as a mail server, all mail delivered between local users

Foreign address - If the rule must apply to a specific address or domain, the address or domain must be entered here. Wildcards are accepted (*). It is not possible to add more than one domain/address per rule.

MIN Score/ MAX Score - These values define the threshold of the content scores. As soon as the threshold score exceeds the minimum score, the rule will be activated.

Categories - From within the table, the categories that the rule effects are chosen. Only categories that have been activated will appear (Mail Policy > Content Filtering). Choose the categories by clicking on the desired category. More than one category can be chosen by pressing the **Ctrl** button and clicking on the desired category.

Forward - In this section it is possible to enter a defined recipient's email address for the system to send email copies. If "Original" is checked (default), the mail will be forwarded as it was sent to the system. If "Scanned" is checked, the system will first scan the email for any rules that may apply and take relevant action.

Notify - In this section, notifications are configured (see **Notification Template**s Tab for information on how templates are created and managed).
First, select the notification recipient (more than one recipient can be selected).
It is possible to add specific email addresses to receive notifications.
Then, select the notification template for a specific rule from the drop-down list.

General action
In this menu, the action for each rule is defined:
Delete - The message will be deleted and a copy of the email will not be sent to quarantine.
Block - The message will be blocked and sent to quarantine.
See Zone Management Tab for information on creating and managing quarantine zones.
Park - The mail will be parked in a specific zone. As soon as the Park action is selected, different zone options become available.
See Zone Management Tab for information on creating and managing Parking zones.
Encrypt – the email will be forwarded to the encryption server for content encryption

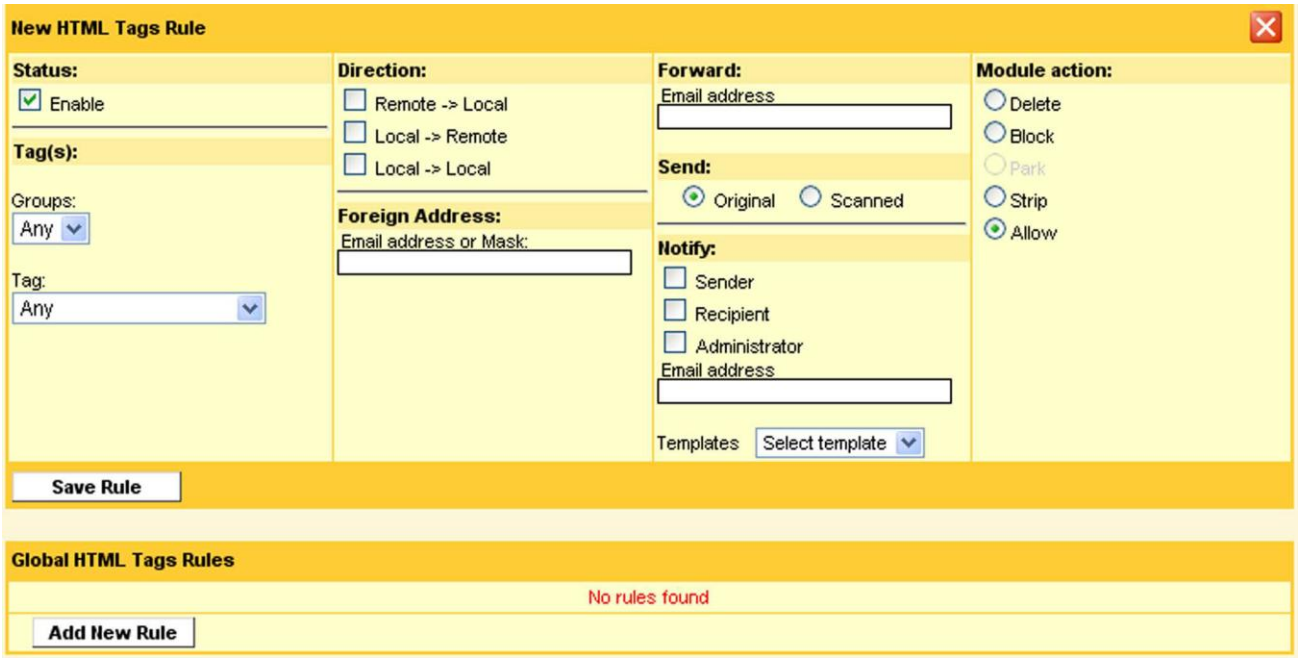
Allow - The message will go through to the recipient. This is useful if an email notification is required.

HTML Tags rules

HTML Tags rules provide the system manager the capability to block HTML emails based on HTML tags. In order to create HTML Tag rules, first you will need to define the HTML Tags that will be affected. This is done in the HTML Tags tab (Policy > HTML Tags) see page 5-56. Once created, it will be possible to create these rules.
Like the rest of the rules, it is possible to create global, domain, group and per user rules.

Adding a new HTML Tags' rule

Select the tier you wish to create the rule for, and under Global Rules, make sure that the HTML Tags rules is chosen from the drop-down menu. Click on the Add new rule button (marked in a red square in the following picture). The following screen will appear in the right pane:



Status - Define the status of the rule by checking or unchecking the checkbox.

Tags - After created in the **HTML Tag**s tabs, the groups and specific tags will appear in the drop-down menu. From the drop-down menu, choose the desired group or specific tag that the rule will affect.

Directions
Remote -> Local - Incoming mail
Local -> Remote - Outgoing mail
Local -> Local - When acting as a mail server, all mail delivered between local users

Foreign address - If the rule must apply to a specific address or domain, the address or domain must be entered here. Wildcards are accepted (*). It is not possible to add more than one domain/address per rule.

Forward - In this section it is possible to enter a defined recipient's email address for the system to send email copies. If "Original" is checked (default), the mail will be forwarded as it was sent to the system.

If "Scanned" is checked, the system will first scan the email for any rules that may apply and take relevant action.

Notify - In this section, notifications are configured (see **Notification Templates** Tab for information on how templates are created and managed).

First, select the notification recipient (more than one recipient can be selected).

It is possible to add specific email addresses to receive notifications.

Then, select the notification template for a specific rule from the drop-down list.

General action - In this menu, the action for each rule is defined:

Note! When finished configuring the rule, don't forget to save.

Delete - The message will be deleted and a copy of the email will not be sent to quarantine.

Block - The message will be blocked and sent to quarantine.

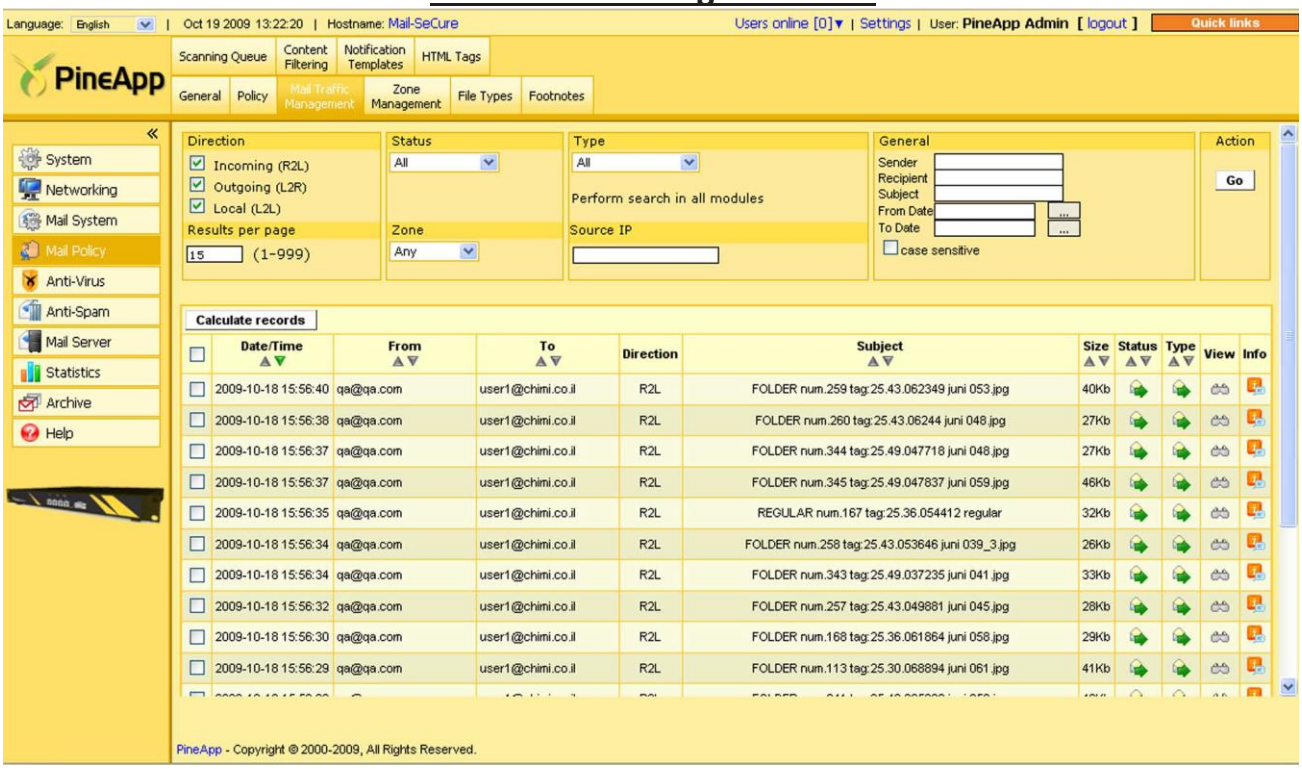
See **Zone Management** Tab for information on creating and managing quarantine zones.

Park - The mail will be parked in a specific zone. As soon as the Park action is selected, different zone options become available.
See **Zone Management** Tab for information on creating and managing Parking zones.

Strip - The message will go through to the recipient. stripped from its HTML code.

Allow - The message will go through to the recipient. This is useful if an email notification is required.

Mail traffic management tab



In this tab, mail traffic is managed. It is possible to search and locate any email that passed the system or was quarantined for any reason. It is also possible to release, view, download and perform other manageable tasks.

When viewing this tab, the following window will be displayed:

Locating an email is done by entering its direction, status, zone (see **Zone Management** Tab) and type, or by entering information such as sender, recipient and date.
It is possible to use any one or more of these fields. Wildcards are accepted (*).
After entering the search requirements, click on the **Go** button. The results of the query will be displayed.

All quarantined mail can be inspected and managed. To delete, release, or add to Black or White lists, select the specific mail and choose the action from the Combo menu located on the bottom left side of the screen.

Only quarantined mail can be managed, while the clean or tagged mail cannot. It is only possible to view the "info" popup.

Massages can also be managed by right clicking on the desired row. Once clicked, a list of available actions for the pointed mail appears. In order to reach the common windows commands, right click while holding the Ctrl button.

To view a message, click **View** next to the specific mail. The details of the email will open in a new browser window.

Release - Release the quarantined mail to its recipient.

Release and add sender to White list - Mail will be released and the sender will be added to the global White list.

Release and add sender to recipient White list - Mail will be released and the sender will be added to the recipient's White list.

Add sender to White list - Add sender to global White list without releasing the mail.

Add sender to Black list - Add sender to global Black list.

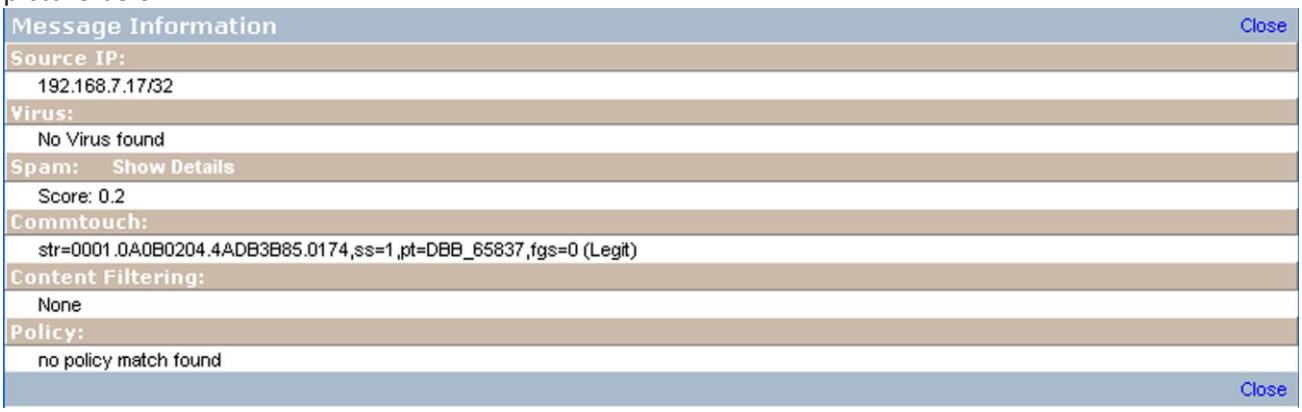
Add sender to recipient White list - Sender will be added to the recipient's White list. Mail will not be released.
Add sender to recipient Black list - Sender will be added to the recipient's Black list.

Download - Download mail that has been inspected as eml files archived in a ZIP file.

Delete - Delete inspected mail from quarantine.

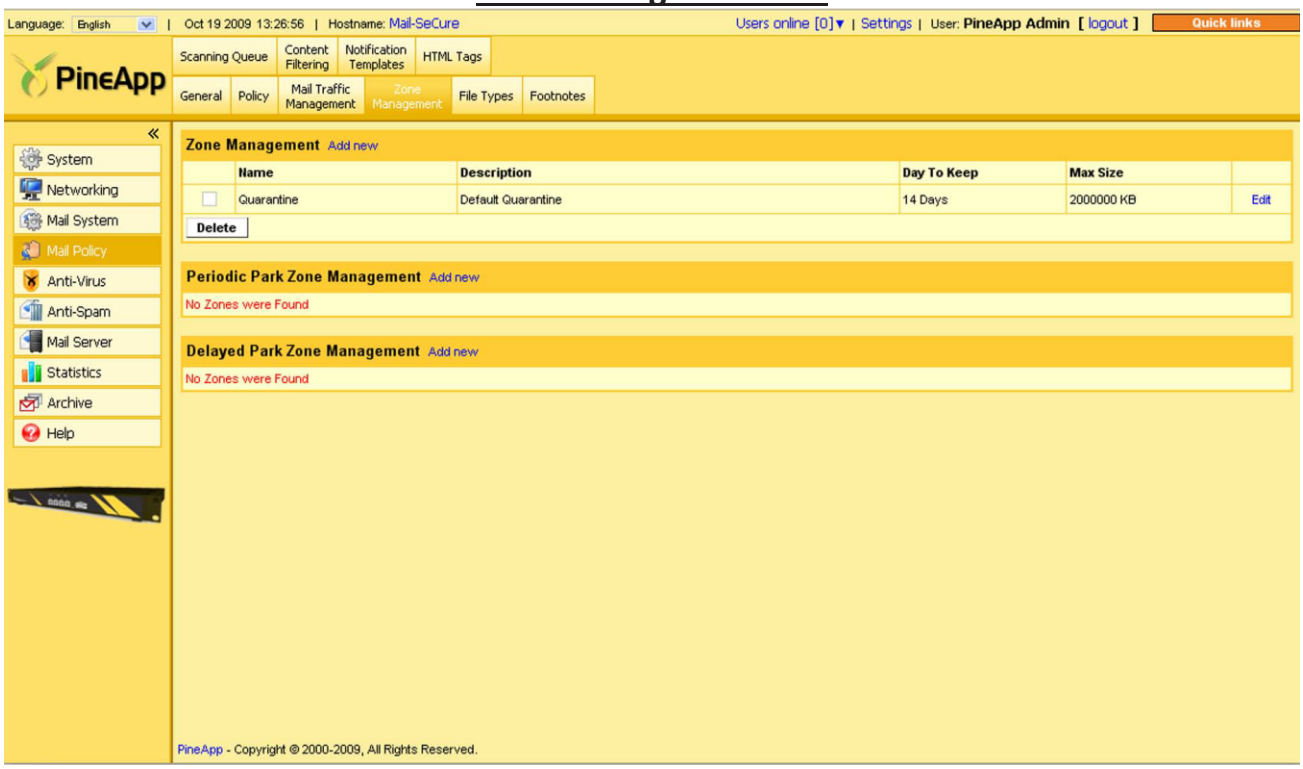
Understanding Information window

By clicking on the icon next to each message, a new window pops-up, displaying score and policy inspection details with additional information as to why the email was quarantined, as shown in the picture below.



Source IP - Shows the source IP of the message.
Virus - Shows if the email was quarantined because it was identified as a Virus (if so, the name of the Virus will be displayed).
Spam - If an email was blocked because it was deemed as Spam, the score will be displayed.
Click Show details (marked in a red square in the picture above) to see why the message received this score. **Commtouch** - Every email that enters the system receives a Commtouch ID.
This information is useful when reporting false positives.
Policy - If an email was blocked due to a policy breach, this will be indicated with the rule that caused the message to be blocked.

Zone management tab



In this tab, all zones are managed. Zones are configurable "folders", on which quarantined and parked emails are stored, according to various conditions.
When viewing this tab, the following will be displayed:
There are three different zones that the system manages: Zone Management, Periodic Park Zone and Delayed Park Zone.

Zone Description

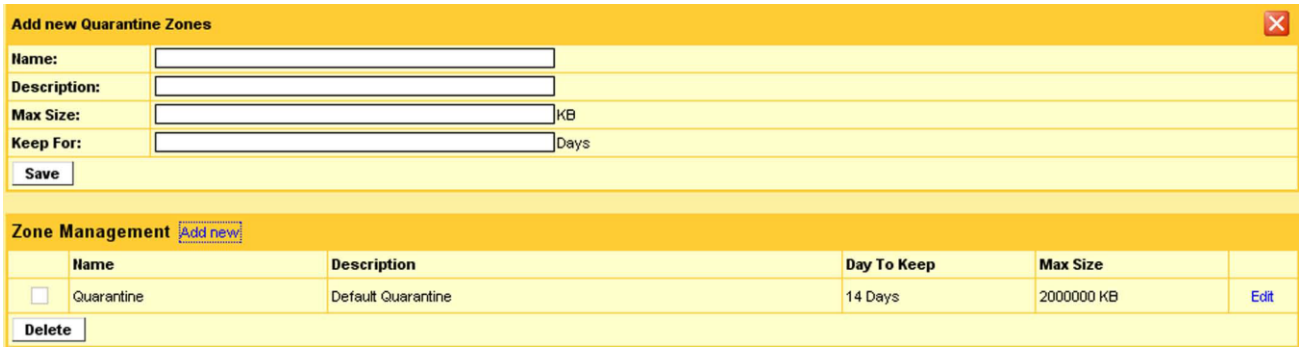
Zone Management Different quarantine zones.

Quarantine zones

The Mail-SeCure system has default settings defined for the default quarantine zone (14 days and 2GB max size). Information older than the days defined or larger than the max size defined is deleted.
The default quarantine zone can be edited, but not deleted.
After changing the settings, click on the **Save** button.

Adding a new quarantine zone

A) Click on the **Add new** link, right next to the Zone Management section.
B) Type in the new quarantine zone's name, the requested maximum number of days to keep quarantine items, and it's maximum size.
C) To finalize your action, click on the **Save** button (marked in a blue square in the picture above)



Periodic parking zones - These zones release the mail sent to them at defined time intervals during the day.

Adding a new Periodic Parking zone

A) Click on the **Add new** button.

B) Enter a name and description for the specific zone.

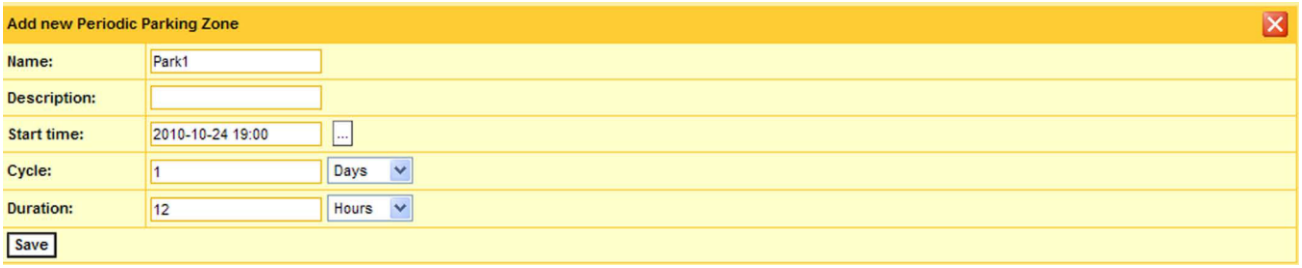
C) Start date (click for a calendar) – this value represents the date and time from which the rule will apply.

D) Cycle – this value represents the time frame when the parking rule should be operated in (calculated in minutes, hours or days).

E) Duration – this value represents the actual amount of time during which mail will be released from the parking zone.

F) After adding all the above information, click on the **Save** button.

EXAMPLE:



In this example, a parking zone called “Park1” is created. It will be active from October 24th at 19:00. Then, every one day (cycle = 1 day) for 12 hours (duration = 12 hours) the system will release all mail in this parking zone. After 12 hours, at 07:00, mail will no longer be released and will park in this zone until 19:00 that day

Delayed parking zones - These zones release mail sent at a defined time. Unlike the above rule, there is no reference for the time of day or specified release periods.

Each mail that arrives to the park zone is delayed in an equal amount of time, and delivered once the decided delayed period is over, regardless to the delivery hour.

Adding a new Delayed Parking zone

A) Click on the **Add new button** under the **Delayed parking zone** section

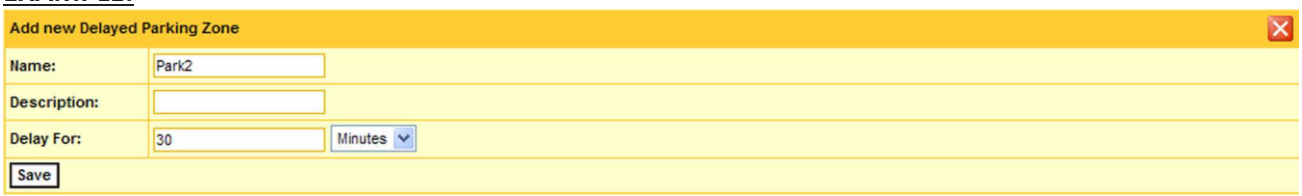
B) Enter a name and description for the specific zone.

C) Type in the numeric value for the requested delay, and pick the relevant time unit from the dropdown menu.

D) Once finished, click on the **Save** button.

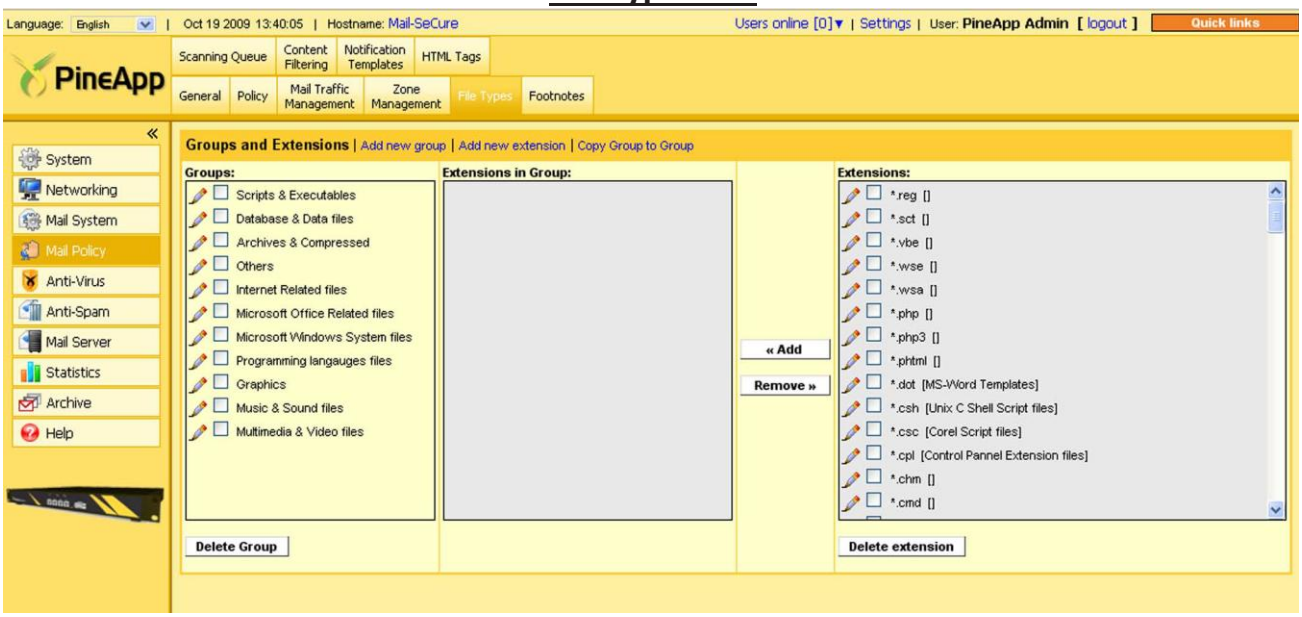
Each zone can be edited or deleted.

EXAMPLE:



In this example, a parking zone called “Park2” is created. It will delay mail for 30 minutes before sending it.

File types tab



In this tab, the file types are managed. It is possible to create new extension groups and extensions, edit existing groups and delete extensions.

The system has built-in groups and extensions. However, it is possible to create new extensions and groups.

Creating new groups and extensions

A) To add a new group, click **add new group**.
B) Type the name and description of the new group and click on **add new group.**
The new group will be added to the list of groups in the left pane. The same procedure is done with extensions;
C) Click on the add *new extension* link and type the new extension in the proper fields. the syntax will be simply typing the extension's name (for example: psd of pdf) with no additional characters.

Adding and removing extensions from groups

Select the group you wish to add extensions to by clicking on it.
Three panes will appear (from left to right): The group, the existing extensions within the group and the list of available extensions.
Managing the extensions within a group is done by checking the desired extension and adding or removing it using the appropriate buttons.

Deleting extensions

In order to delete an extension, simply check the box next to the desired extension and click on **Delete Extension** button.

Deleting groups

To delete a group it is first necessary to remove all its extensions. Next, check the box next to the group you wish to delete and click on the **Delete Group** button.

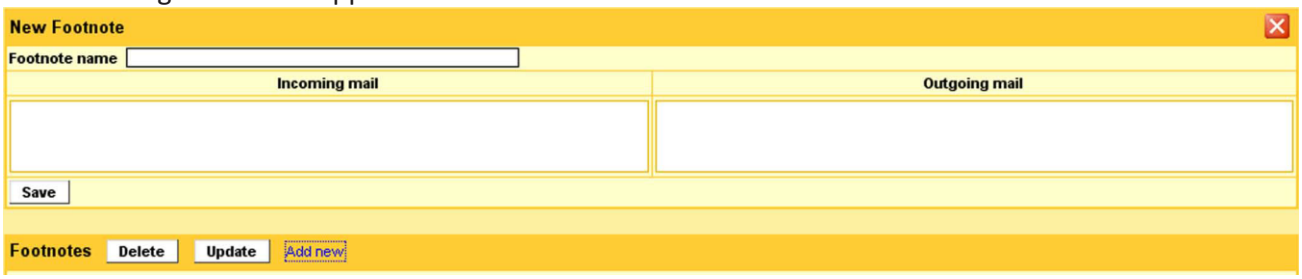
Footnotes tab

In this tab, a custom disclaimer can be defined. It is possible to create numerous footnotes and attach them to specific rules. At this stage, it is possible to only text based footnotes (HTML format is not supported yet).
The Mail-SeCure system comes with a default pre-configured footnote which can be disabled:
This mail was scanned by PineApp.com

****
This footnote confirms that this email message has been scanned by
PineApp Mail-SeCure for the presence of malicious code, vandals & computer
viruses.
****

Adding footnotes

A) Click on the **add new** link (marked in a red square in the picture below).
The following screen will appear:



B) Name the footnote and type the relevant text for incoming and outgoing mail.
C) After adding the information, click on the **Save** button.

Modifying footnotes:

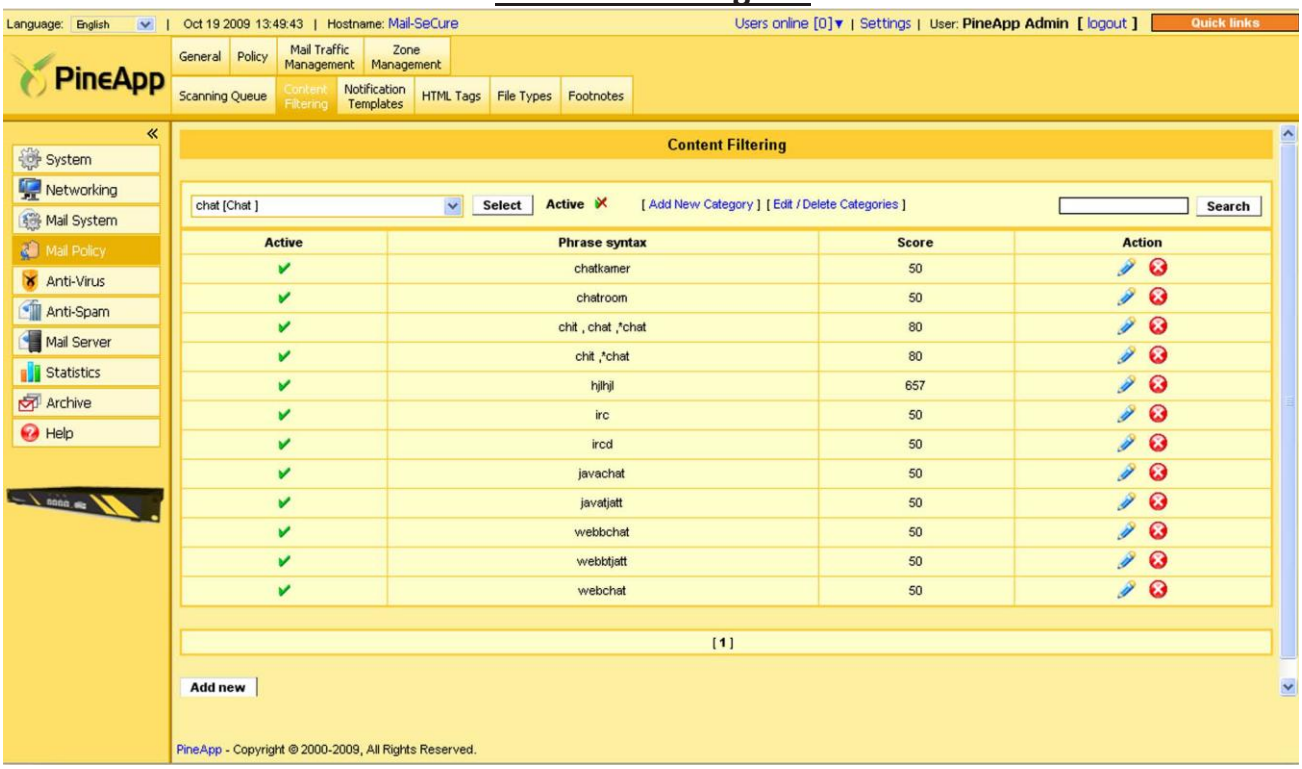
A) Select the footnote you wish to modify and click on the **edit** link.
The following screen will open:

B) Make the required changes in the incoming and/or outgoing footnote's text body.
C) Click on the **update** button (marked in a blue square in the picture above).

Deleting footnotes

A) Select the footnote you wish to delete by checking the box next to it.
B) Click on the **delete** button (marked in a green square in the picture above).

Content filtering tab



In this tab, the content filtering is configured. The content filtering feature allows the system to scan incoming or outgoing mail and detect mail based on keywords, thus providing the ability to prevent information leakage from within the organization and prevent incoming mail with certain words. The system can detect words from within the body or subject of the email. It can also extract words from within over 300 file types.
The following table describes the types of files that are supported:

File types

Email Files - Outlook Express, Eudora, MBOX, EML - Sender, Recipient, Subject
Outlook items and MSG files (Sender, Recipient, Subject, contact fields - StreetAddress, CompanyName, etc.)
Microsoft Word, Excel, PowerPoint Document summary information fields – all versions
OpenOffice/Open Document Format
Document properties fields
HTML META tags; <TITLE> is indexed as HtmlTitle field; <H1>, <H2>, <H3> are indexed as HtmlH1, HtmlH2, HtmlH3, etc.
XML All fields
DBF All fields
CSV All fields (CSV, or comma-separated values, files must have a csv extension, a list of field names in the first line, and must use tab, comma, or semicolon delimiters)
PDF files
Document Properties
WordPerfect Document summary information fields
MP3 All metadata fields
JPG, TIFF EXIF and IPTC metadata fields; XMP (Vista) metadata supported in version 7.40
ASF, WMA, WMV All metadata fields

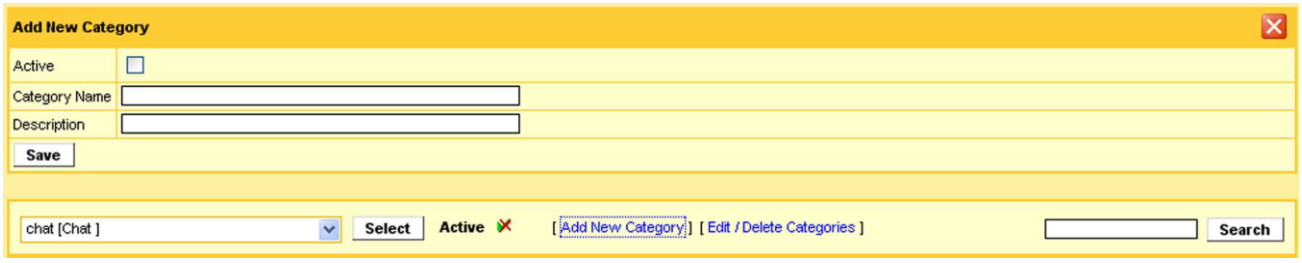
The Content Filtering mechanism is divided into two:
1. Configuring the categories and words in which the content rules will be applied. It is possible to use the pre-configured categories and words or customize new or existing ones.
2. Creating the per user/group/domain/global rules.
In the **Content Filtering** tab the configuration of the categories and words are done.

Managing Categories

Mail-SeCure features 16 pre-configured categories. In order to activate a category, choose from within the drop-down menu the desired category and activate it by clicking on the **activate** button (marked in a red square in the picture above).
The gif will change to activated.

Adding new categories

A) Click on the *Add new category* link (marked in a blue square in the picture below).
The following fields will appear:



B) Enter the desired name for the Category and a description (not mandatory)
C) Hit the **save** button (marked in a red square in the picture above).
The new category will be added to the list of existing categories.

Editing/Deleting categories

A) Click on the *Edit/Delete Categories* link. The list of categories will appear.
B) Choose the category for editing or deleting and perform the action.

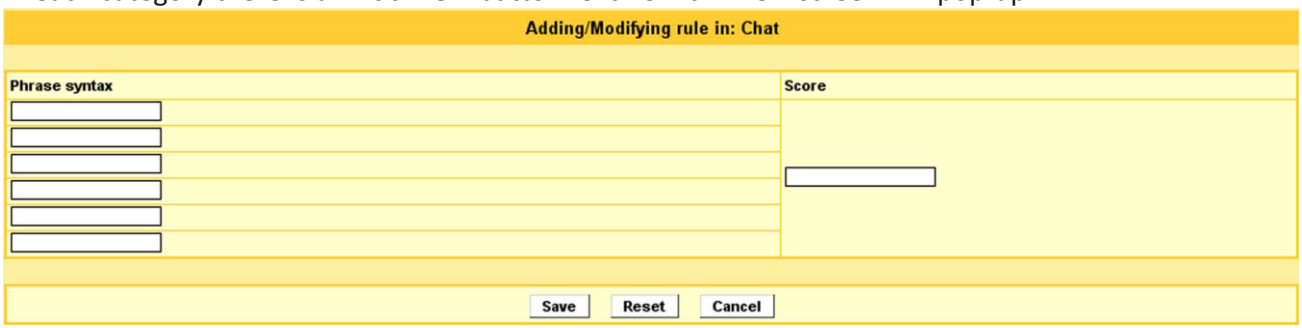
Managing Keywords

For every category (whether pre-configured or customized), there is a list of pre-configured keywords. Each keyword, can be activated or de-activated.
Please make sure that the category is activated, as shown above.

New keywords can be added to any category.

Adding new Keywords

In each category there is an **Add New** button. Click on it. A new screen will pop-up:



The keywords are entered in the left pane. The system supports wildcards (*) and it is possible to put more than one word in each field. If more than one word is added, the system will check if all words appear in the email and only then will activate the phrase score. The score of the keywords is entered in the right pane. When done, click on the **Save** button.
When the user receives an email, it doesn't matter if the phrase appears once or many times.

As soon as the word appears at least once, he will get the score that was assigned to it. If the score passes the threshold defined in the policy rule, the rule will be activated. For example, if the word "sex" appears once, the score will be 50. If it appears 10 times, the score will also be
50.

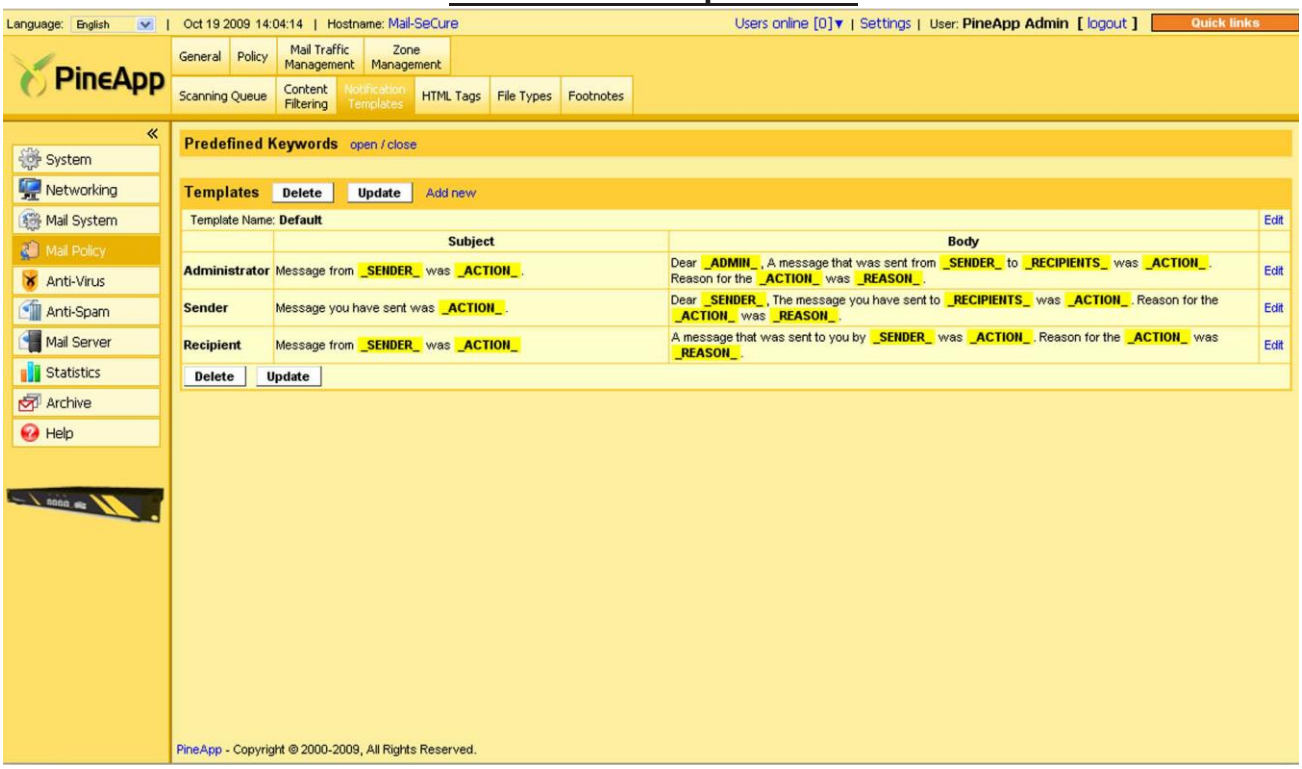
Editing/Deleting keywords

Choose a certain category from within the categories dropdown menu and click on the **Select** button (marked in a red square in the picture below), in order to delete or edit its affiliated keywords.
Editing keywords can be done by using the **Edit** link (marked in a green square in the below picture), while deleting them can be achieved by checking the box next to the keyword(s) and hitting the **Delete** button (marked in a blue square in the picture below).

The Scoring System

As noticed, each keyword or set of keywords gets a score. When creating the content Filtering rules, these scores are used to determine whether the rule is breached or not. Like the Spam rules, if the accumulated score breaches the configured threshold, the rule will be activated.

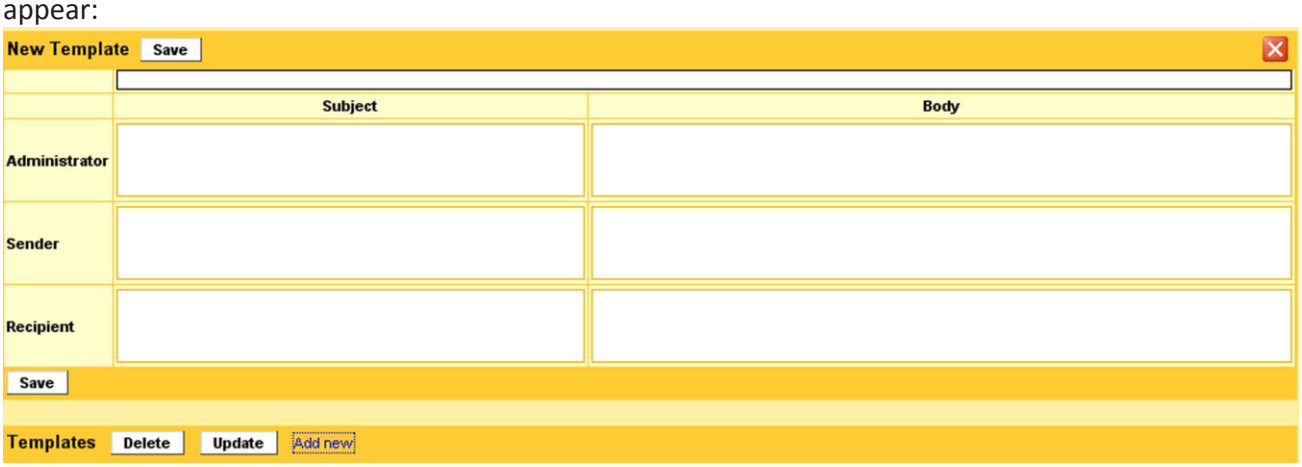
Notification templates tab



In this tab, notification templates can be defined and assigned to rules.
The Mail-SeCure system comes with default, pre-configured notification messages that are sent to senders, recipients or administrators when a rule is breached.
It is also possible to create new notifications and assign existing and new ones to any rule.

Creating a template

A) click on the *add new* link (marked in a blue square in the picture below). The following window will appear:



B) Type the messages to be received by the sender, recipient or administrator, in their corresponding fields.
C) When done, click on the Save button (marked in a red square in the picture above).
When done, the new notification will be added.

It is possible to edit every field by clicking **edit** located to the right hand side of every field.

Viewing pre-defined keywords

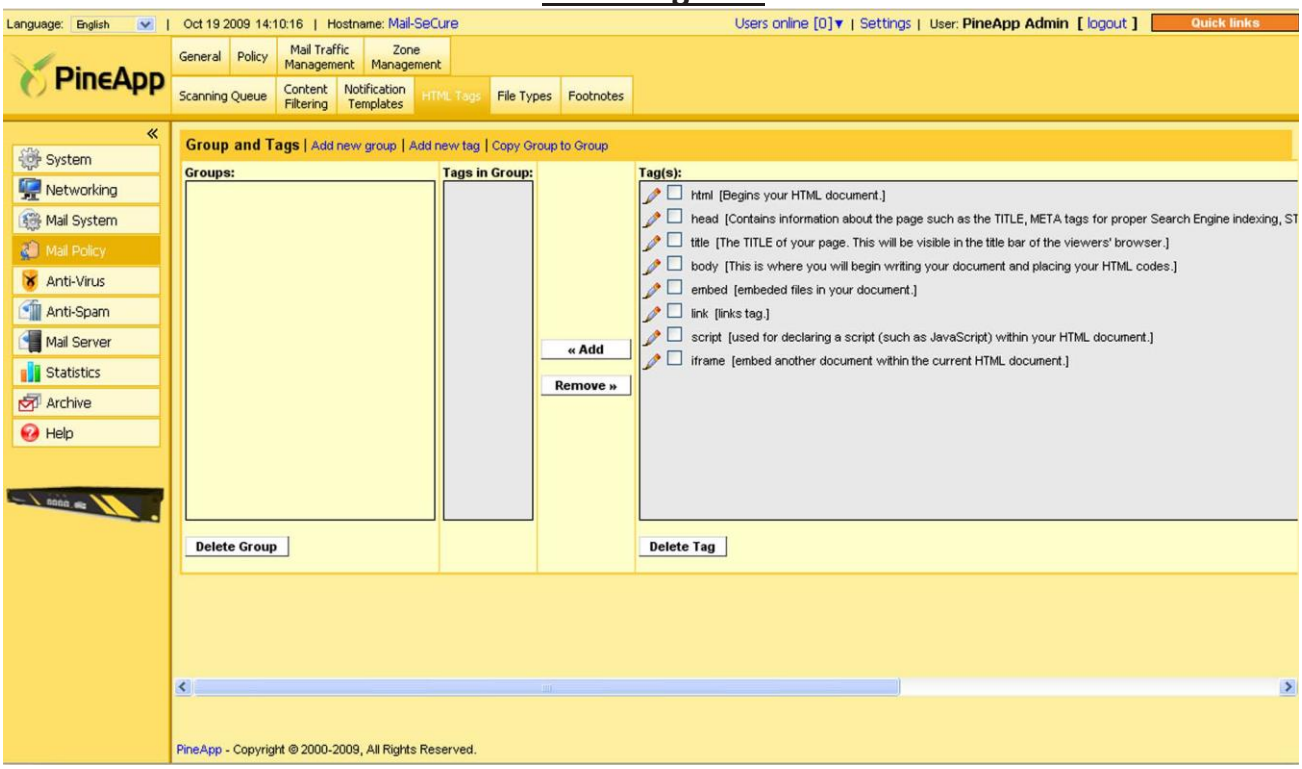
It is possible to use pre-defined wildcards. Click **open/close** link and a list of the pre-defined keywords will appear:

Keywords Types

SENDER - The sender of the message
ADMIN - The postmaster's email address
(example: postmaster@pineapp.com)
RECIPIENTS - The recipients email addresses
(example: first@pineapp.com; second@pineapp.com)
ACTION - The action applied to the message
MSGSIZE - The message byte size
EFFSIZE - The effective size of the message
(mestizos * number of recipients)
SUBJECT - The message subject
REASON - The reason for the action

Editing groups can be done in the same way, by clicking on the pencil icon next to the group's name.

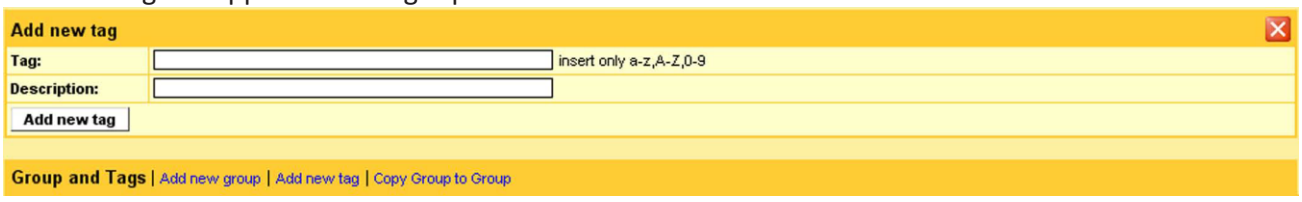
HTML tags tab



In this tab, HTML tags (groups or specific tags) can be defined in order to assign them to the relevant rule.

Creating tags

A) Click on the *Add new tag* link (marked in a red square in the picture below).
B) Type the desired tag (example: Iframe) and a description (optional).
C) Hit the **Add new Tag** button (marked in a blue square in the picture below) in order to save the tag.
The new tag will appear in the right pane.

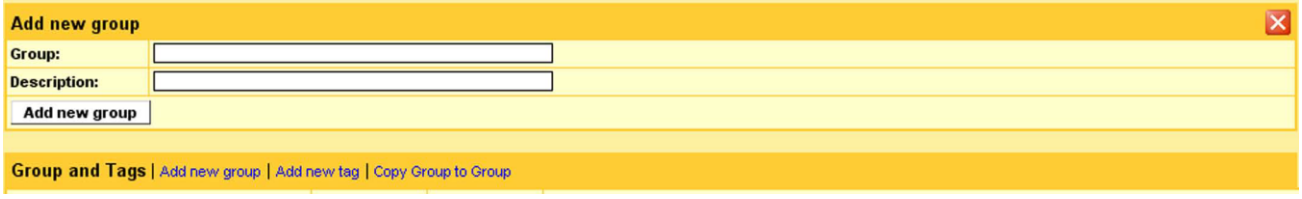


Editing tags

A) Click on the Pencil icon next to the tag you wish to edit.
B) Edit the Tag and/or its description as you wish.
C) Once finished, hit the **Update** button.

Creating tag groups

A) Click on the *Add new group* link (marked red in the picture below);
The following table will open up:



B) Type the desired group name (example: group2) and a description (optional).
C) Hit the **Add new group** button in order to save the tag. The new group will appear in the left pane (marked blue in the picture below);

Deleting tag groups

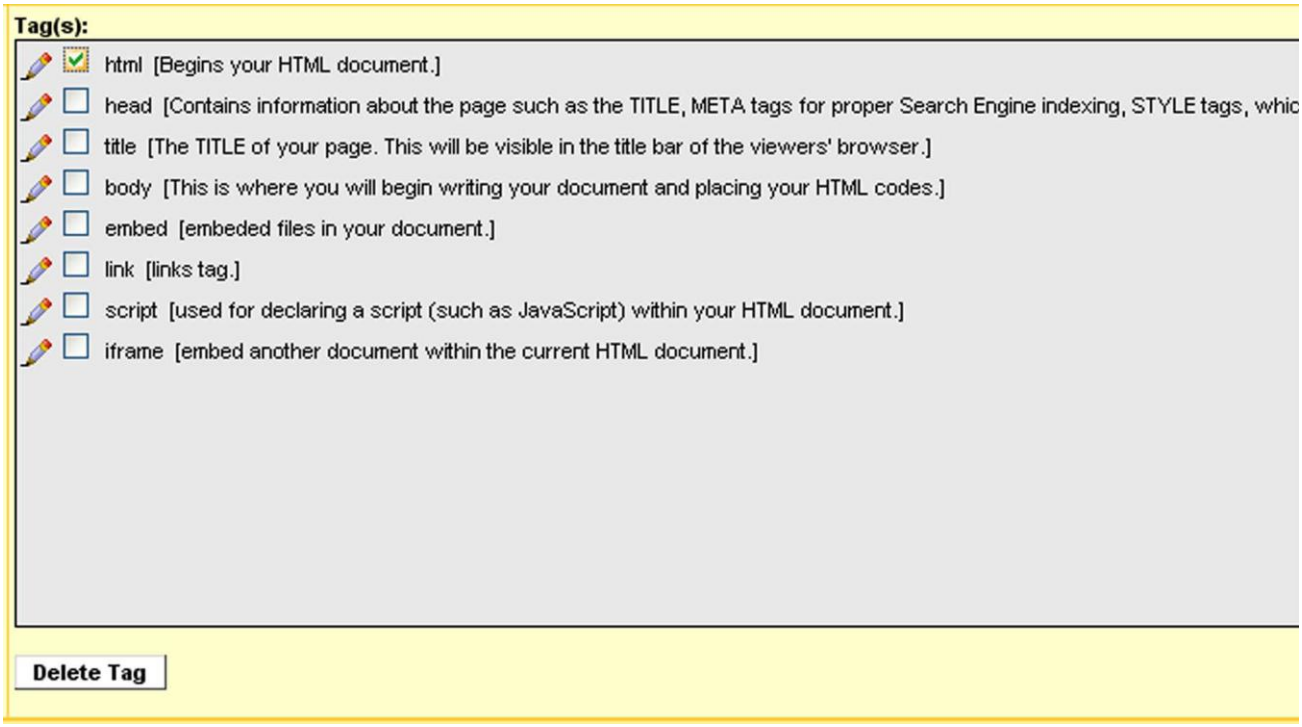
Deleting groups is done by checking the desired group and hitting the **Delete tag** button

Managing tag-groups

Managing groups is done by clicking on the desired group, then transferring specific tags from the available list (right pane) to the tags in the group left pane.
Transferring the tags is done by choosing the tag (it is possible to choose more than one) and hitting the **Add** button. Removing tags is done by choosing the tags from the group and hitting the **Remove** button.

Deleting tags

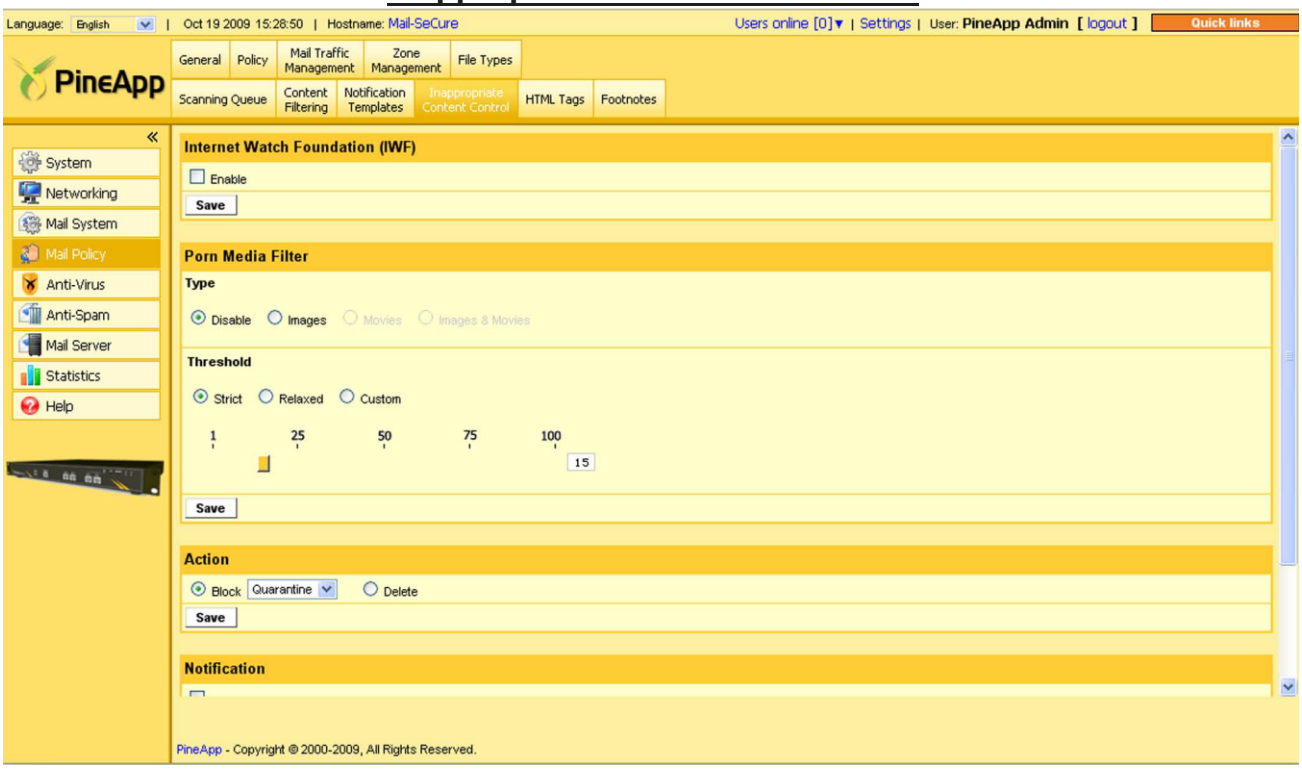
Deleting tags is done by checking the desired tag and hitting the **Delete tag** button (marked in a red square in the picture below).



Editing tags

A) Click on the Pencil icon next to the tag you wish to edit.
B) Edit the Tag and/or its description as you wish.
C) Once finished, hit the **Update** button.

Inappropriate Content Control tab



This tab will only be visible if you purchased the ICC (Inappropriate Content Control) Pack.

This tab allows to activate the IWF (Internet Watch Foundation) and to set up the sensitivity of the Porn Mega Filter.

Activating the IWF

When activated, the system will be able to detect and report child pornography material. The system interconnects to the IWF database and notifies the administrator on every violation.

More info can be found at: http://www.iwf.org.uk/
Activating the feature is done by checking the **Enable** box. Define an email address that will receive notifications of each violation.

Porn Media Filter

When activated, this feature enables the system to scan incoming images and movies (in a later version) for pornographic image content. Once detected, the system can either quarantine or delete the mail.
The image scanning is done after the Anti-Spam engines scan the email, thus only non Spam emails will be scanned for inappropriate content. The system can scan archived files (ZIP, ARG, RAR etc.) as well.
In order to activate the module, check the type of content that will be scanned (images, movies or both). Then, check the threshold.

Porn Media Filter rates images on a 0 – 100 scale – 0 being Clean, while 100 indicates a strict Pornographic content. The threshold settings allow the user to define at what value images are

classified as Clean or Porn. The higher the setting, the engine will be less sensitive. In other words, the chance that a porn picture will "slip" through the engine is higher.
After defining the desired score, hit the **Save** button.

Threshold Levels

Strict - The strict setting is set to 15. This setting is recommended for organizations that require a higher detection rate on account of a higher false positive ratio
(Legitimate picture identified as Porn).
Relaxed - The relaxed setting is set to 70. This setting is recommended for organizations that require a lower detection rate on account of a higher false negative ratio (the chance for a porn picture to slip through the system is higher).
Custom - When checked, it will be possible to toggle between the settings.

Notifications

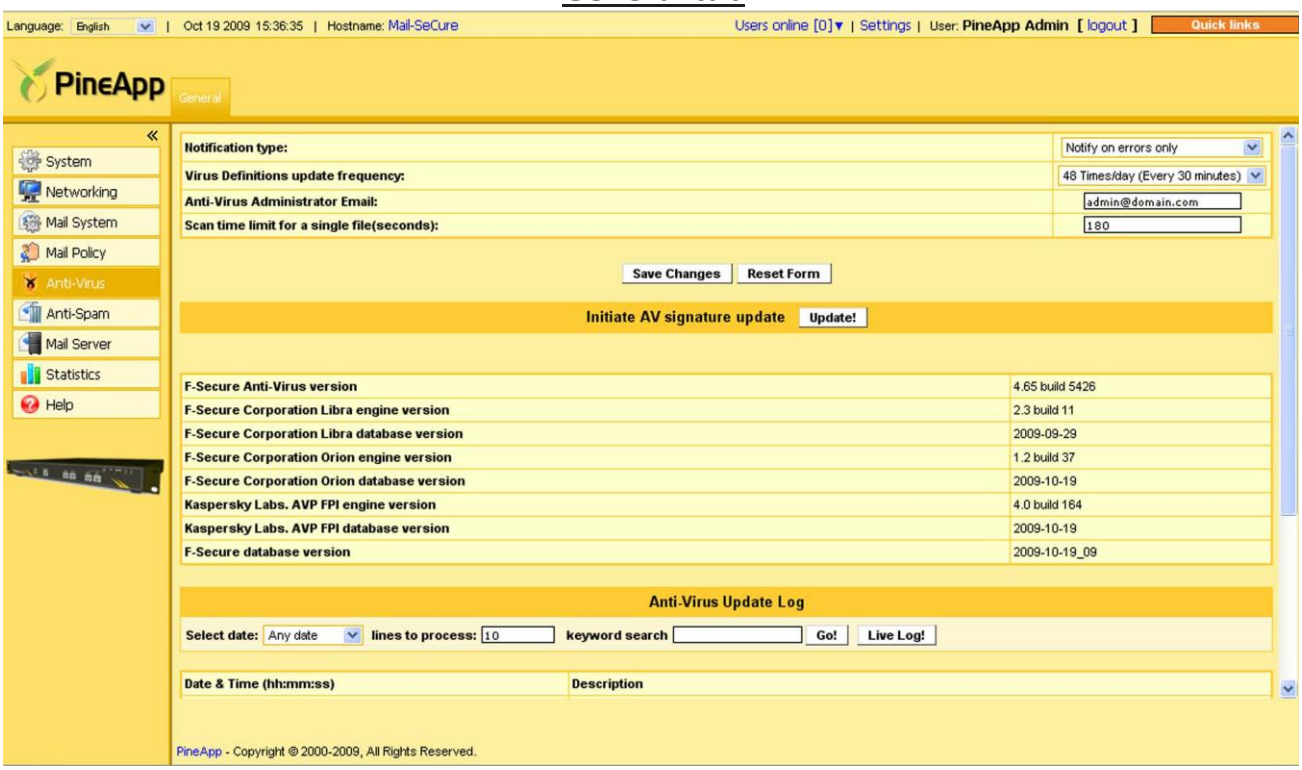
Once detected, the system can either notify the sender and/or the recipient and/or the administrator (or none at all). You can also attach the appropriate notification to the notifying message (Mail-Policy > Notification templates).
There are two Admin emails available: Administrator which is the Postmaster's email and the IWF Admin which can be defined separately.

CHAPTER 6

ANTI-VIRUS

The Anti-Virus menu allows managing and monitoring the Anti-Virus updates.

General tab



From within the General tab, the following can be done:

Notification Level - Select the type of notification received on a Virus signature's update (Default: Only Errors).

Virus Definitions update frequency - Defines how often Mail-SeCure should check for new Virus signatures (Default: 48 times a day).

Anti-Virus Administrator Email - Type-in the administrator's email address.

Important - A virus signature update can be initiated at any time by clicking the **Update!** button.

In addition, full information regarding the various AV engines and their latest update can be observed on this screen.

Logs of the latest updates are generated and can be viewed at the end of this screen.

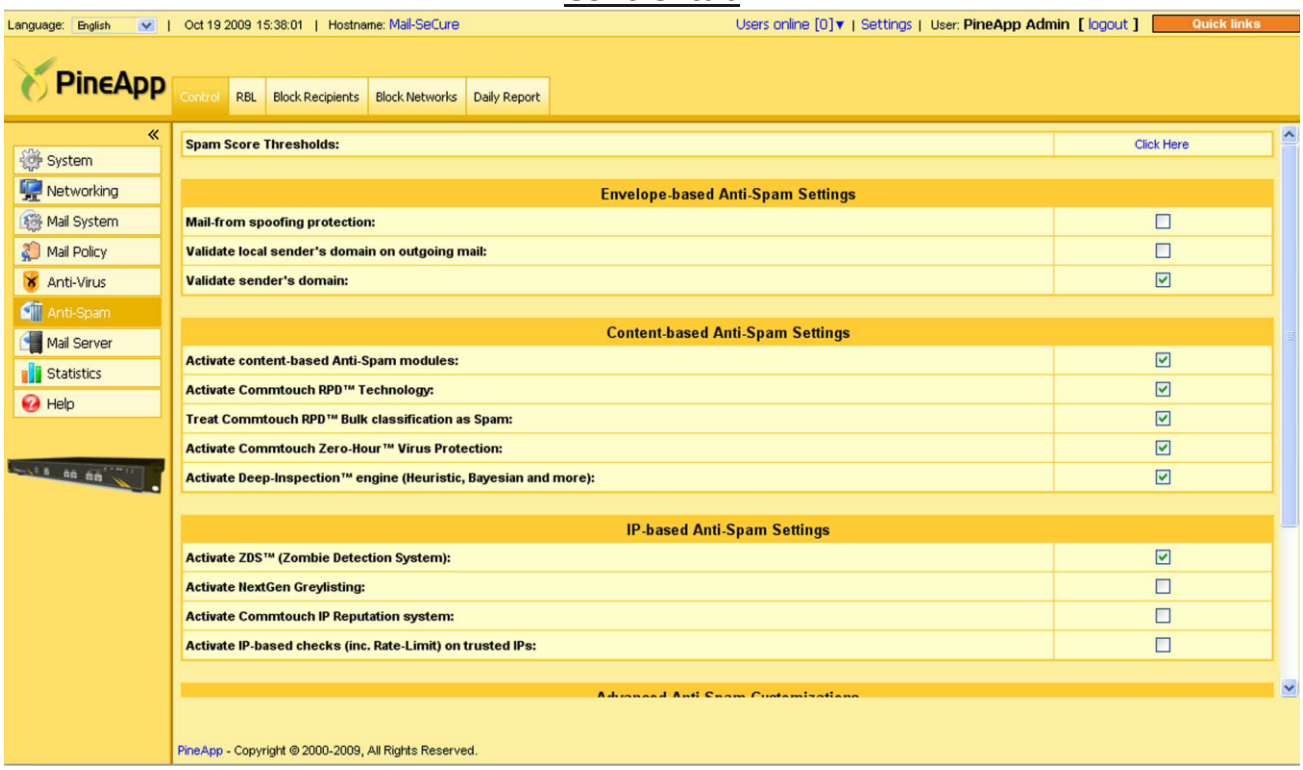
Scan time limit for a single file (seconds) - For some very large files, the scanning time may be relatively long. Usually such files are very suspicious and may contain Viruses. If the scanning time exceeds the value in the field, the scanning will stop and the system will regard the file as infected (Default 300 seconds).

CHAPTER 7

ANTI-SPAM

The Anti-Spam menu allows the user to manage and monitor the Anti-Spam modules.

Control tab



Spam Score Thresholds *Click here* - will open the Anti-Spam rules within the *Policy Management* tab. For further information refer to Creating, Deleting and Modifying Spam Rules.

Mail-from spoofing protection - Prevents impersonators from sending mail into the organization on behalf of your domain. This is a useful tool when fighting Spam, as many spammers use your email as the sender when sending Spam.

However, if there are "legal" users that send mail on behalf of your domain from the external network, do not activate this feature as this may cause those users to receive a spoofing error message when trying to send mail to the organization (default - disabled).

In order to solve this possible challenge, it is recommended to use SMTP authentication.

Validate local sender's domain on outgoing mail - When checked, users sending mail through Mail-SeCure must be identified with their local domain.

Users whose email domain is not configured on Mail-SeCure will not be able to send mail (default - unchecked).

Validate sender's domain - When checked, Mail-SeCure will validate the sender's domain. Mail sent from an invalid domain will be rejected (default - enabled).

Activate Advanced Anti-Spam module - When checked, Mail-SeCure's advanced Anti-Spam module, the most important feature in the system, is activated.

Activate Commtouch RPD™ technology - When checked, the Commtouch Recurrent Pattern Detection (RPD™) technology database lookups are activated (default - checked).

RPD technology analyzes large volumes of email traffic in real time, and is able to detect new Spam and Malware outbreaks as soon as they emerge, as well as mail sent from Zombies (language independent!). These are all recorded in the Commtouch Detection Center. (For more information see: www.commtouch.com).

Treat Commtouch RPD™ Bulk classification as Spam - When checked, bulk mail (mail with a large number of recipients) will be treated as Spam. By checking this box, the Spam detection rate will grow (default - unchecked).

Activate Commtouch Zero-Hour™ Virus Protection - When checked, this technology can identify and quarantine new-born Virus outbursts. This module also uses Commtouch technology (default - unchecked).

Activate Deep-inspection Engine - When checked, PineApp's Anti-Spam built-in Heuristic and Bayesian engines are activated (default - checked).

Activate PineApp ZDS™ (Zombie Detection System) - When checked, real-time verification of remote IP against PineApp's unique Zombie database is activated (default - checked).

Activate PineApp NextGen Greylisting - Greylisting is a methodology that helps the system battle large amounts of Spam. When an Email from an unknown IP is sent to the system - it is rejected with a "try again message". In most cases, Spammers will not send the Spam again while most legal servers will (default - unchecked).

Activate Commtouch IP Reputation system - This engine uses Commtouch's technology to detect and block Spam originated from Zombies (estimated at 90% of all Spam) at the SMTP session level.

Activate IP based checks on trusted IP's - When checked, mail originated from trusted IP's (relay networks) will be checked by the IP-based Anti Spam engines. This is efficient against outbound zombies and spammers. If the system is also the mail server, you will need to add it to the White list located in the RBL tab.

Automatically white-list foreign recipients - When checked, all external recipients wil automatically be added to the sender's white list. For example, if user@pineapp.com send an email to user@domain.com, user@domain.com will be added to user@pineapp.com's white list (default - unchecked).

Encapsulate Spam message as attachment – When using the system as a POP3 transparent proxy and when checked, mail identified as Spam will arrive as an attachment rather than as an email (default - unchecked).

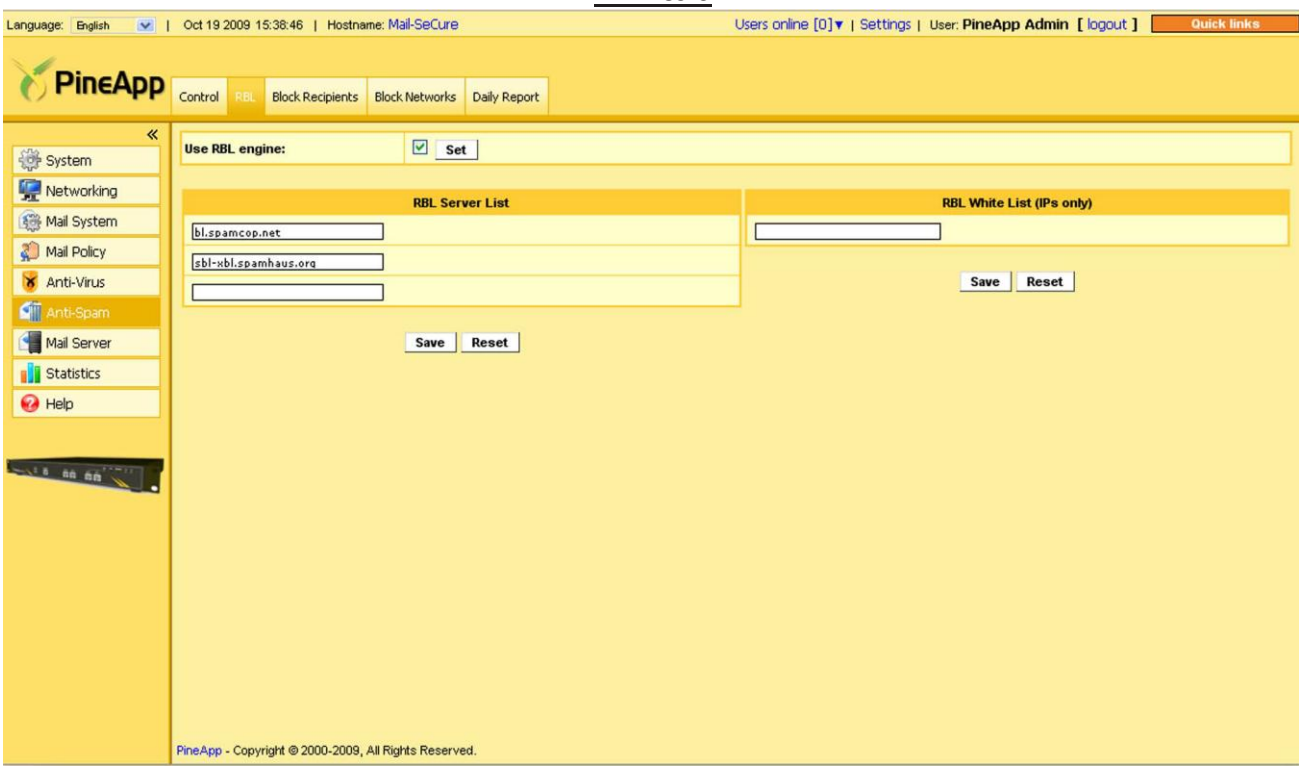
Use full report - When checked, a full report will be generated for every email identified as Spam. This will only work if the tagging option is activated, as seen in *Creating, Deleting and Modifying*

Spam Rules (default - unchecked).

Use Spam module on POP3-Proxy connections - When checked, incoming mail will pass Anti-Spam filtering, even if the transparent POP3 proxy is activated (default - unchecked).

Tagging String - When the tagging Spam feature is configured (Mail Policy > Policy) it is possible to configure the Tagging String Default: ***SPAM***.

RBL tab



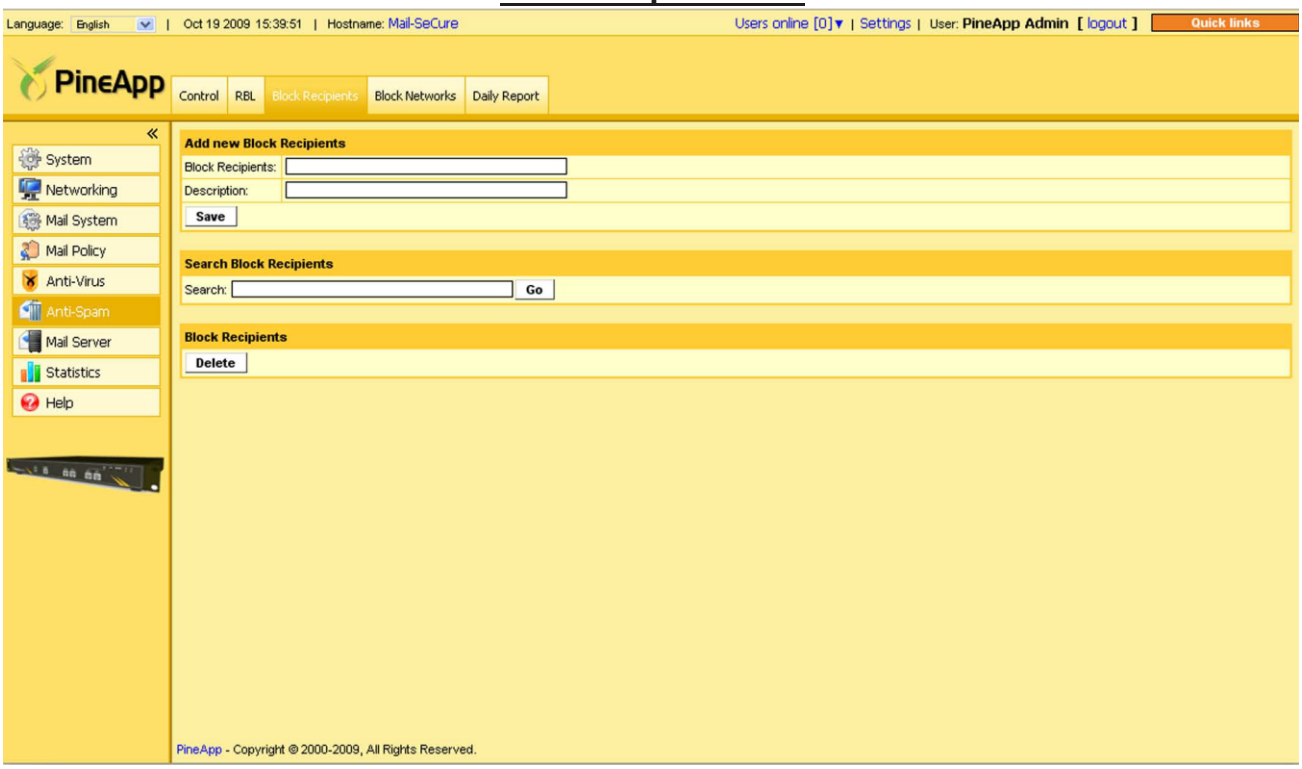
RBL (Real-time Blackhole Lists) engines are external servers that maintain a list of banned mail servers. Most servers are banned because they were identified as spammers. When activated, the system checks the IP address of the session before the mail is accepted by Mail-SeCure and rejects mail that originated from those servers.

Use RBL engine - Check the box to use the RBL engine (default - disabled).

RBL Server list - These servers hold the databases of known spammers.
Mail-SeCure features two pre-configured RBL servers.

RBL White list - If you wish to receive mail from black-listed servers, enter the server's IP address in the column on the right.

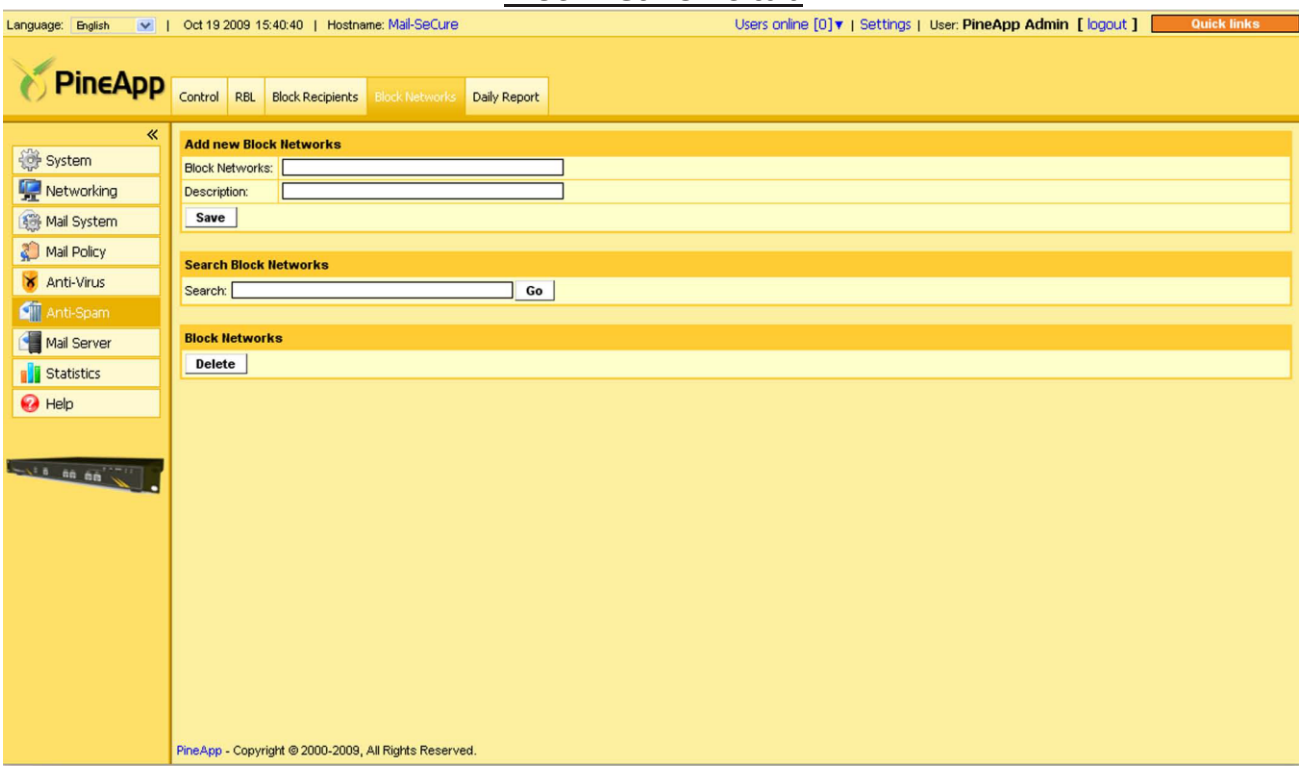
Block recipients tab



In the Block Recipients tab, specific recipients can be blocked. This feature is useful when employees leave an organization but still receive mail.

The syntax for adding new blocked recipients is: user@domain.com

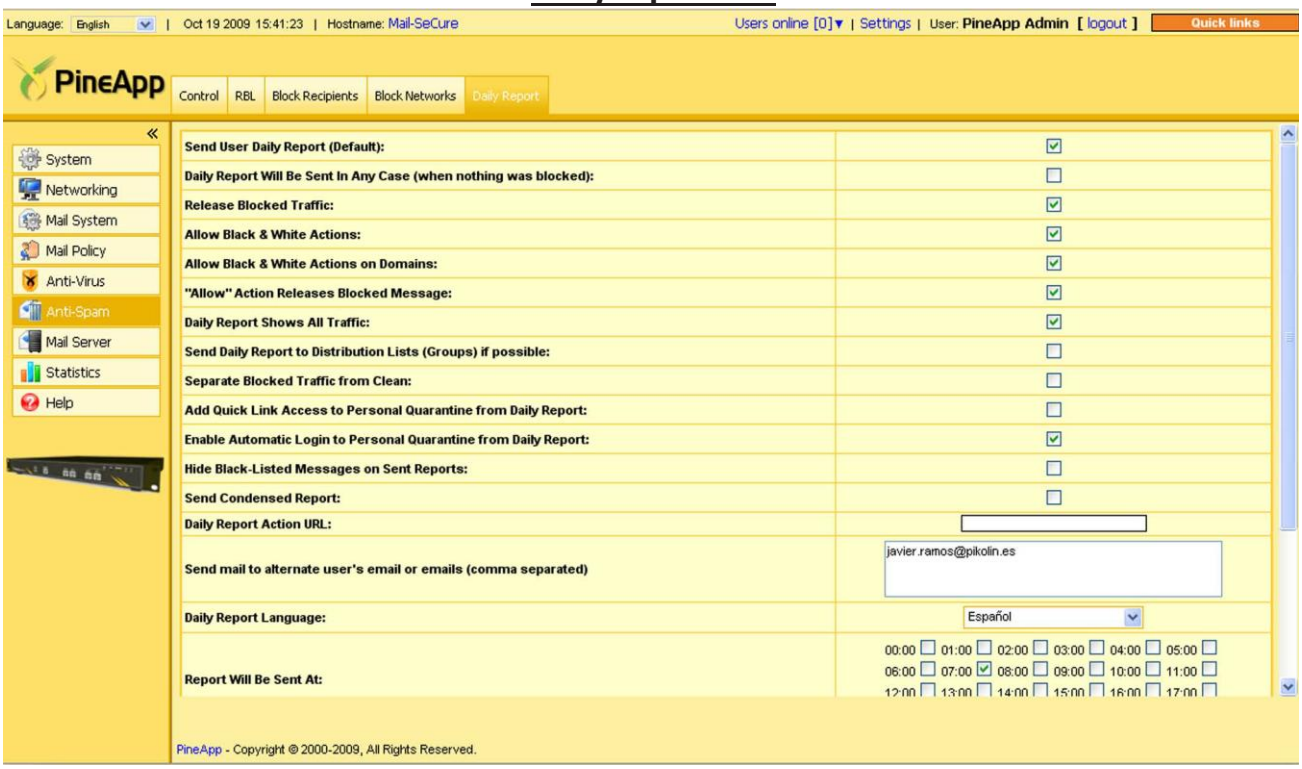
Block networks tab



In the Block Networks tab, IPs and networks can be blocked.

Examples of methods for blocking networks: For network 192.168.24.0 with subnet mask 255.255.255.0, type in: 192.168.24. (Including the dot). For network 209.88.177.64 with subnet mask 255.255.255.192, type in: 209.88.177.64-127.

Daily report tab



Mail-SeCure allows the system to send daily reports to the users configured in the user management screen (page 2-6).
The daily report is an HTML email that is sent to the users. It contains information about the user's email traffic, what was quarantined and the reason.

From within the report, users can release quarantined Spam, add senders or domains to their Black & White lists. The characteristics of the daily report can be configured from within this tab. Further information about managing Spam can be found in PineApp's Managing Spam Manual.

Send User Daily Report - When checked, users with the default settings (System > User Management) will receive the daily report.
When unchecked, they will not receive it unless they are configured to YES (see page 2-8) (default - Unchecked).

Daily Report will be sent in any case - As default, when no email was blocked within 24 hours, he will not receive a daily report.
When checked, the user will receive his daily report in any case (default - unchecked).

Allow Black & White Actions - By default, the daily report will allow users to manage their own Black & White lists from within the HTML email. However, if the system administrator wishes the users to receive their daily report without them being able to manage their Black & White lists, he should uncheck this box (default - checked).

Allow Black & White Actions on domains - By default, users can allow or block domains and specific emails. When unchecked, users can only allow or block specific emails (default - checked).

"Allow" action releases blocked message - When checked, when the user clicks on the allow

button in the daily report, the email is added to the White list AND released (default - unchecked).

Daily Report shows all traffic - When checked, the daily report will show all the traffic that passed in the last 24 hours. The report will show all passed mail and quarantined mail. If unchecked, the daily report will only show the quarantined mail.

Send Daily Report to Distribution Lists (Groups) if possible - If checked, mailing lists which where synchronized with the system (LDAP) will receive the daily report.

Separate blocked traffic from clean - If checked, the information in the daily report will be separated into two blocks: Blocked and Passed.

Add Quick Link Access to Personal Quarantine from Daily Report - When checked, a link to the GUI management will be added to the acknowledgment messages when performing actions in the daily report.

Send Condensed Report – Check this box if users use low resolution desktops and their report doesn't present properly.

Daily Report Action URL - As the system is based on mail correspondence, the administrator must open access from the workstations (whether located in the LAN or WAN) to Mail- SeCure. The default ports open to Mail-SeCure are 7443 and 7080. When there is no entry in this field (default), the system will take the internal IP from the interfaces and the administrator must ensure that all users are able to access the unit through port 7443 or 7080.
However, if the administrator decides to open a different port or wishes to grant access using another port, or if users will need to access the module from the WAN, a URL (or IP) must be defined.

Example: http://192.168.2.220:7004 (192.168.2.220 – internal IP) - Users from within the LAN will communicate with the system using port 7004 (defined in the firewall).
https://mail.pineapp.com:7443 (mail.pineapp.com – enter full qualified domain name) - Users from anywhere will be able to communicate with the system. Note that the firewall permits access from anywhere to Mail-SeCure through port 7443 and that the DNS translates mail.pineapp.com to the internal IP for local users.

Language - Choose the language of the daily report.

Report will be sent at - Choose the hour in which the daily report will be sent. It is possible to check more than one box.

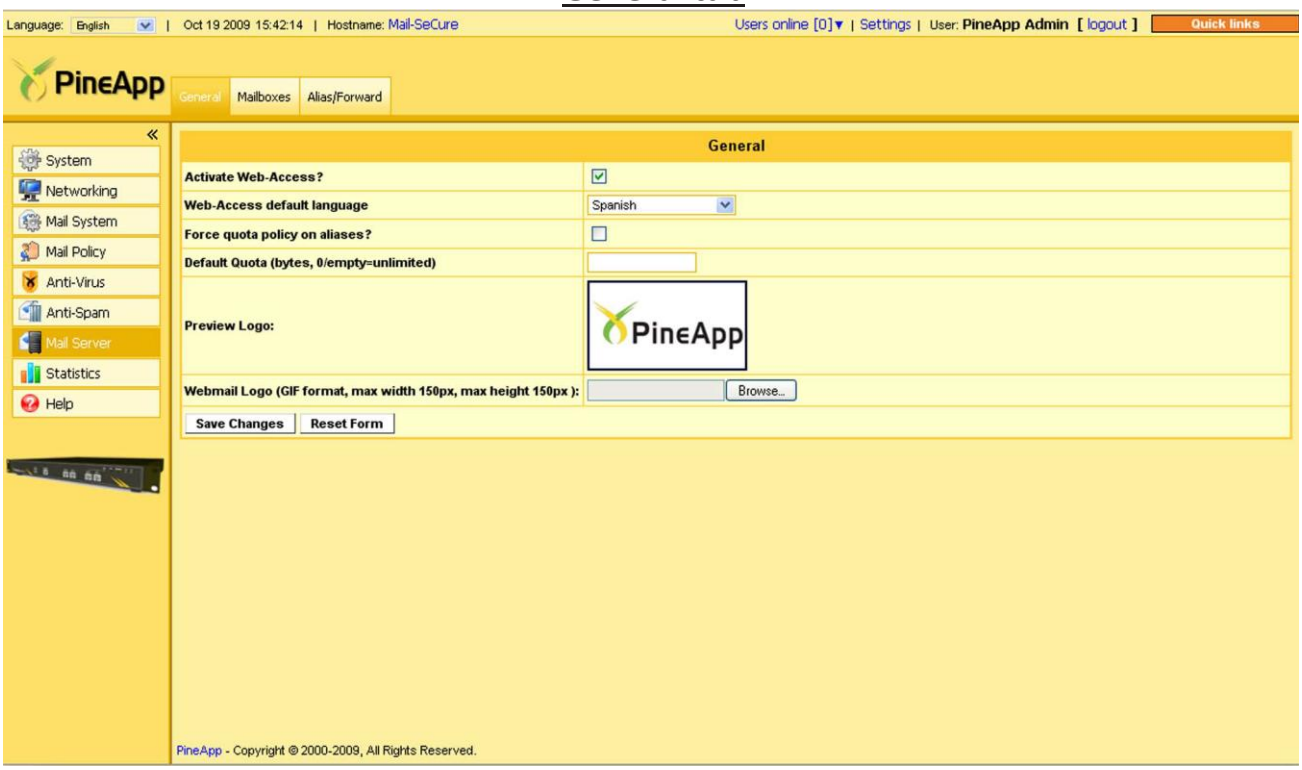
Logo - As default, all daily reports arrive with PineApp's logo on the top left page of the email. It is possible to replace the logo with the organization's one.

CHAPTER 8

MAIL SERVER

This tab is available only in systems that act as a mail server and have purchased the mail server feature

General tab



In the General tab, activating the Web-Access, forcing quota policy on aliases and determining the default quota is carried out.

Activate Web-Access - When checked, users will be able to access their mailbox using their browser. In order to allow users to access from outside the LAN, please make sure port 443 tcp is open

Web-Access default language - From within the drop-down menu, please choose the default language of the web-access

Force quota policy on aliases - When checked, this feature forces the quota policy on aliases. If a mailbox is part of an alias and a mail that exceeds the quota limit is sent to that alias, an error message will be sent to the sender. Please notice that the error message will be sent from the specific mailbox and not from the alias. Therefore, if you do not want to reveal the mailboxes behind the alias, do not activate this feature (default: checked).

Default quota **- Define the default quota for all mailboxes. The value entered here is in bytes (5000000 = 5MB).**

Leaving it empty or with 0 means there is no limit.

Webmail Logo - Changing the company's logo in Web-Access can be done by browsing and choosing the graphic image file (GIF) you wish to upload, using the **Browse** button. Please note, that the replaced logo's size should be 300x300 pixels, in GIF for

Using web-access

Using the Web-Access feature is very simple and doesn't require additional modules or installation.
First, activate Web-Access (in the General tab under the Mail Server menu).
Each mailbox that is open in the mailboxes tab automatically gets access to a Web-Access mailbox.

In order to use the Web-Access feature, port 443 must be open (for service https) from the WAN to the Mail-SeCure unit.

Accessing web access

It is possible to access mailboxes from anywhere (as long as there is connection to the internet and any standard web browser).

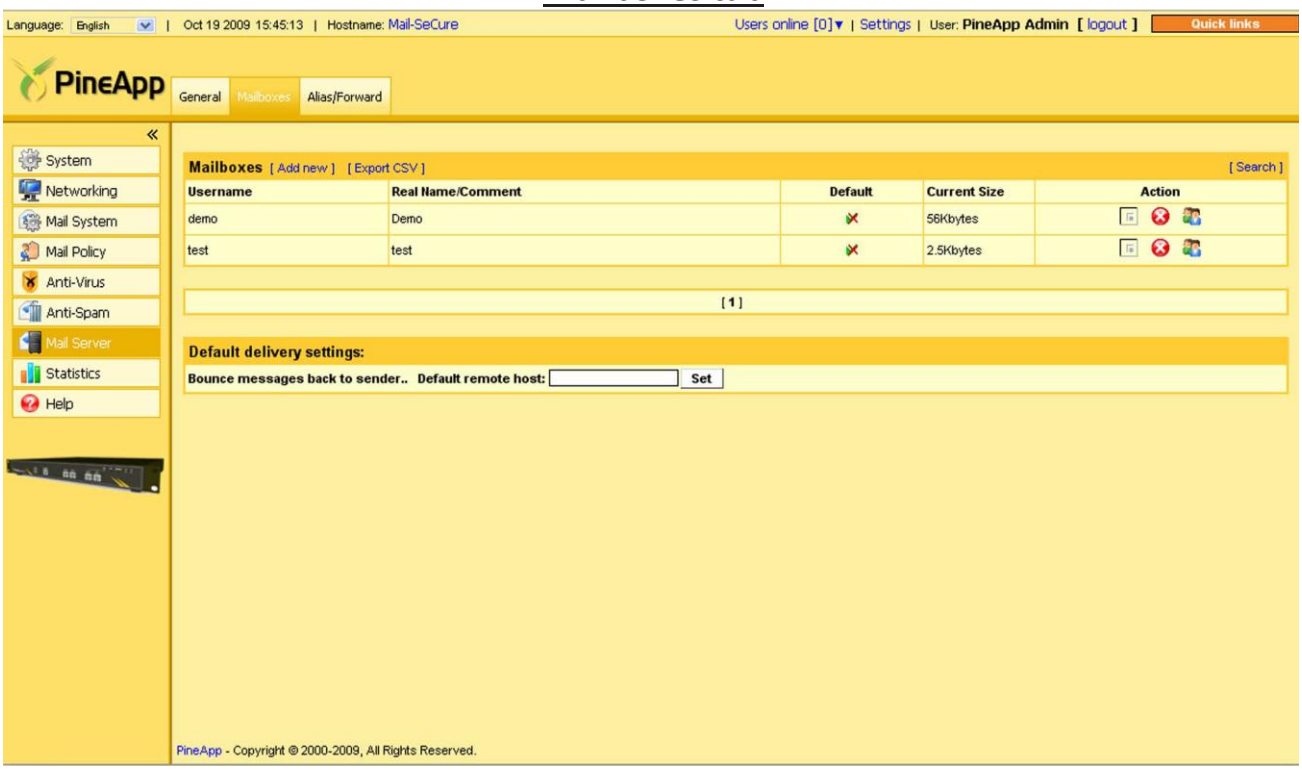
1. Open the web-browser.

2. Enter the following address: **https://ip-address or https://mail.domain.com** (for example: **https://mail.pineapp.com**).

3. Username and password are required: Enter the username and password. The username is the mailbox name and the password is the mailbox password.

Web-Access contains all common mailbox management features such as Folder management, Address books, forwarding and many options so the users can customize their Web-Access.

Mailboxes tab



In the Mailboxes tab all user management is handled. Here you can define new mailboxes, modify and delete mailboxes.
In this screen, define which mailbox will be the default. The default mailbox will receive mail that is sent to a domain that no user exists to receive it. If you do not wish for that to happen, you can decide that such mail will bounce back to the sender (by clicking the **Bounce All** button).
If there is an internal mail server or another mail server that will gather the bounced mail, enter its IP in the **Default remote host** field.

Modifying entries

There is no need to click “Apply changes” after creating users or modifying passwords. Pressing the **Save Changes** and **Change Password** button is enough.

Creating a new mailbox

A) Click on the **Add new** link.
The same screen will appear when modifying an existing mailbox.
The mailboxes in the mail server interconnect with the user management list (system > user management). It is possible to fetch existing users from the user management into the mail server.
B) Choose from the combo menu the user you want to fetch (Current users menu) and click the **Add current** button. The user will be added to the mail server.
C) If you are creating a new user from scratch, type the mailbox name, real name and an alias for the relevant domain.

This will allow you to create the same usernames for different domains. In order to configure the same user for different domains, create a mail box (all mailboxes must receive different names). Enter the real name and give an alias for the wanted domain.

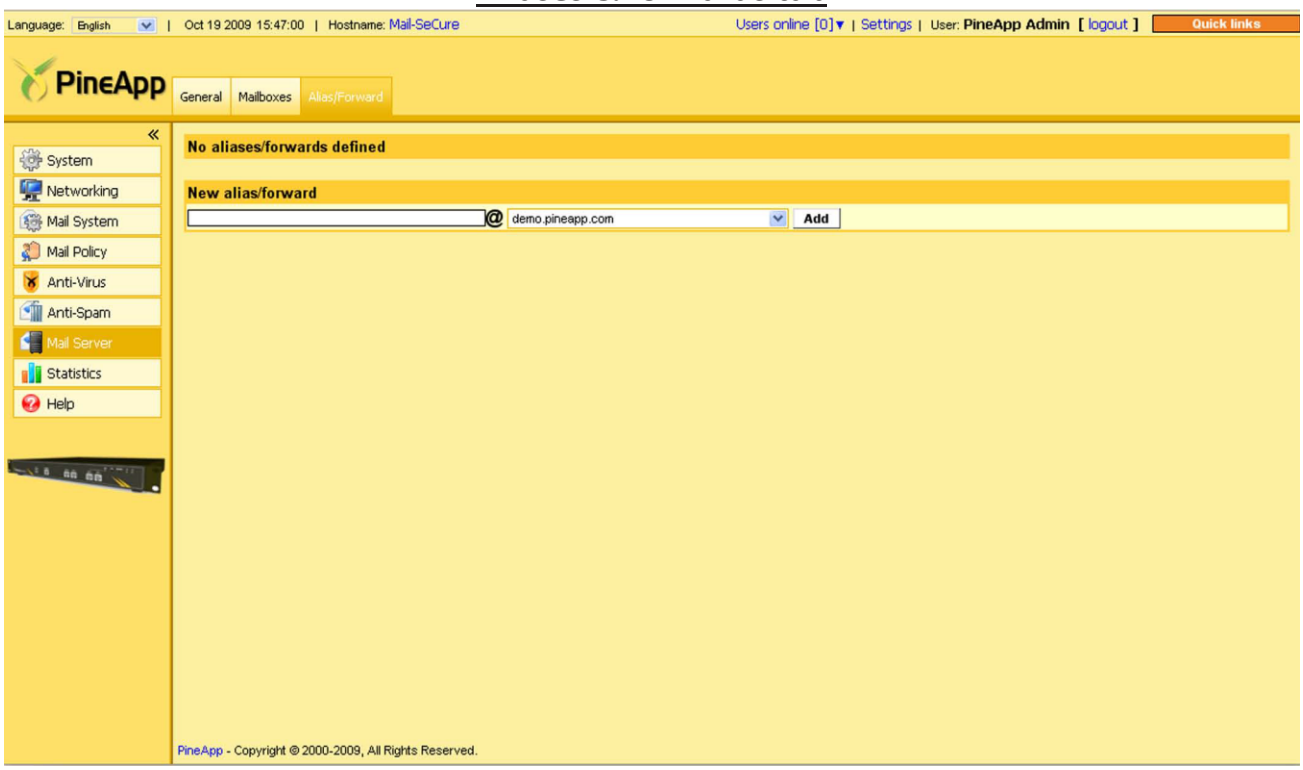
Defining a quota per mailbox is done by typing the size in the relevant field. Leaving the field empty means the user does not have any quota limitations.
If the default quota was defined in the general tab, whatever is defined here will overtake the default quota. If left empty, the default quota is the limit. If a value in numbers is given (the value entered in the quota field is in bytes: 5000000 = 5MB), this will be the quota. If there is a default value and 0 is entered, this specific mailbox will have no limit.

There is an option to determine whether mail will be forwarded to other recipients (local or external) and whether to save a copy of the message in the local mailbox.
Enable Vacation - In case the mailbox owner is on vacation, this screen enables an "auto response". Enable the feature and type the automated message the senders will receive.

After setting the mailbox, click the **Password** button to set the password:
The following pane will be displayed:
Type and retype the password and click the **Change password** button.

When deleting a mailbox, the user created in the user management is **not** deleted. It is necessary to delete it manually.

Aliases & forwards tab



In this tab, defining mailing lists and aliases is possible.
First, create a new alias/forward group. Then, add the members to the group.
The members can be local (chosen from the menu) or external users added manually.

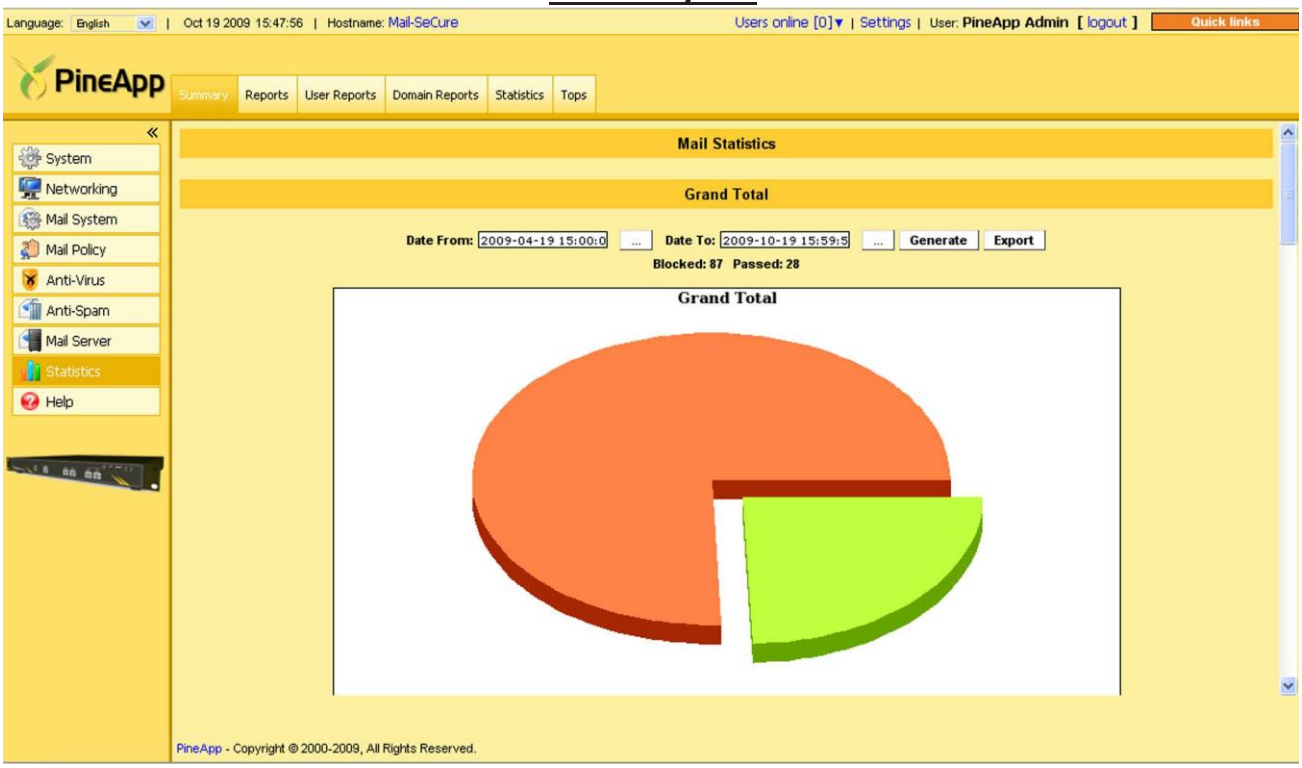
Do not create aliases with the same name as the mailboxes. In the case of Identical names, both the alias and mailbox will not receive any mail.

The details in the summary tab are generated once an hour and include Spam blocked by the RBL engine.

CHAPTER 9

STATISTICS

Summary tab

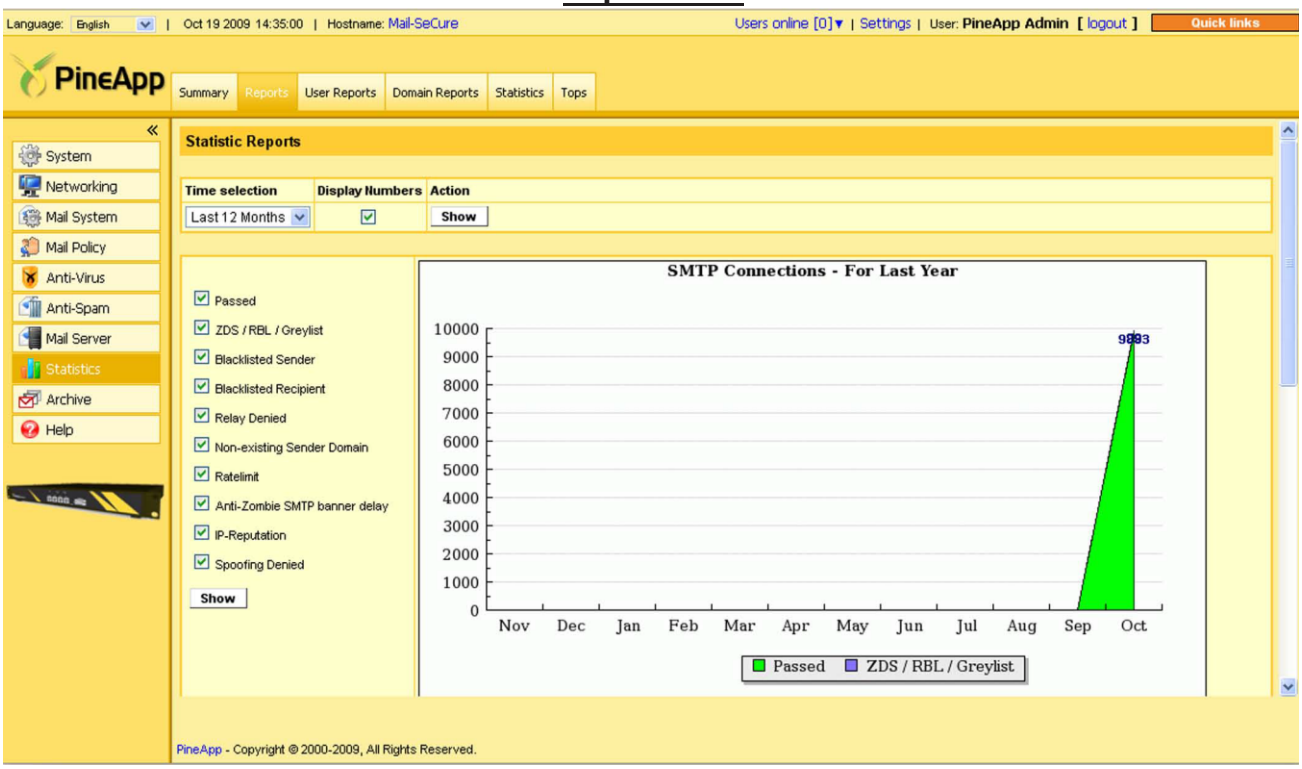


From within the summary tab, general statistics can be viewed.

In the summary tab only general information regarding the whole system is generated. Statistics can be queried by dates (using the date query on top) and can be viewed as Grand Total, SMTP Connections, Content Analysis, Incoming and Outgoing pies.

The statistics can be exported to a CSV file (which can be opened by Excel).

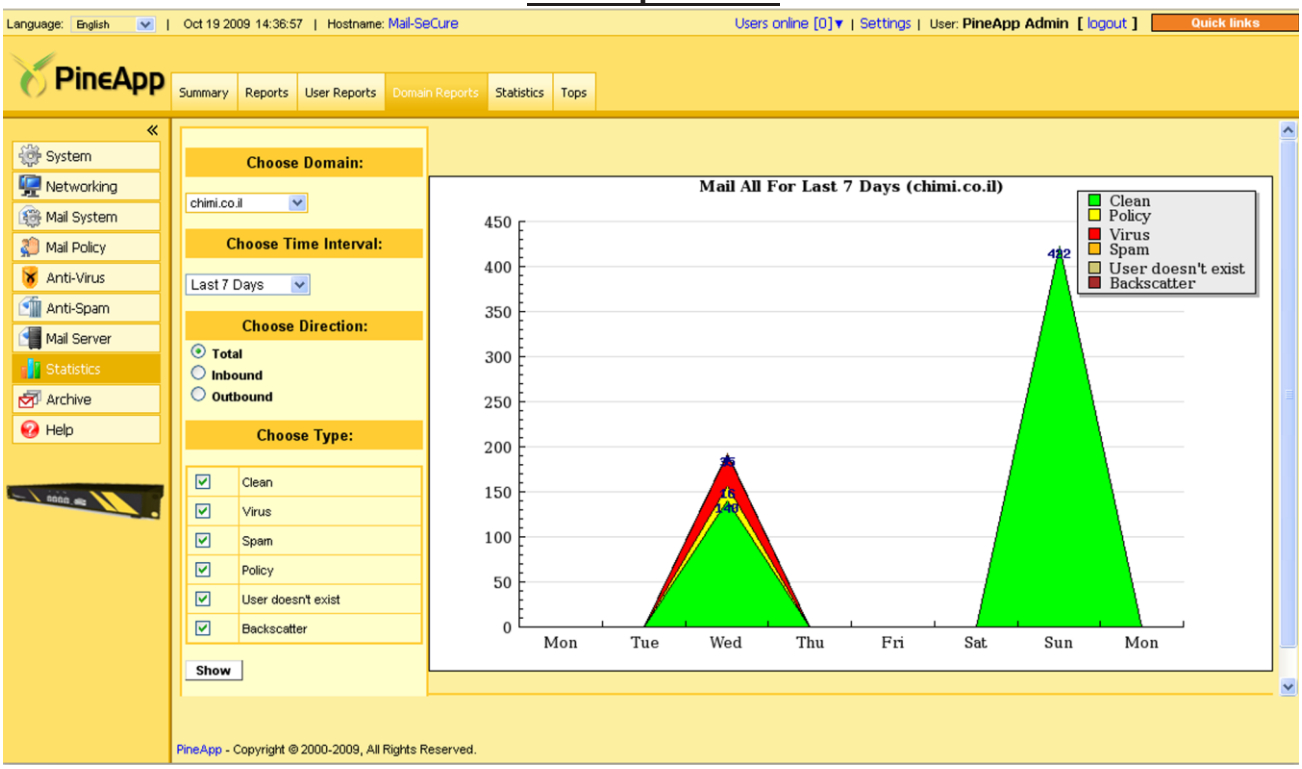
Reports tab



In the reports tab, more detailed statistics can be retrieved.
By choosing the type and time frame, it is possible to generate the required information.
The statistics can be exported to a CSV file (which can be opened by Excel) or downloaded as a gif file.

The details in the reports tab are generated once an hour and include Spam blocked by the RBL engine.

User reports tab



The user reports tab displays graphic statistics per user.

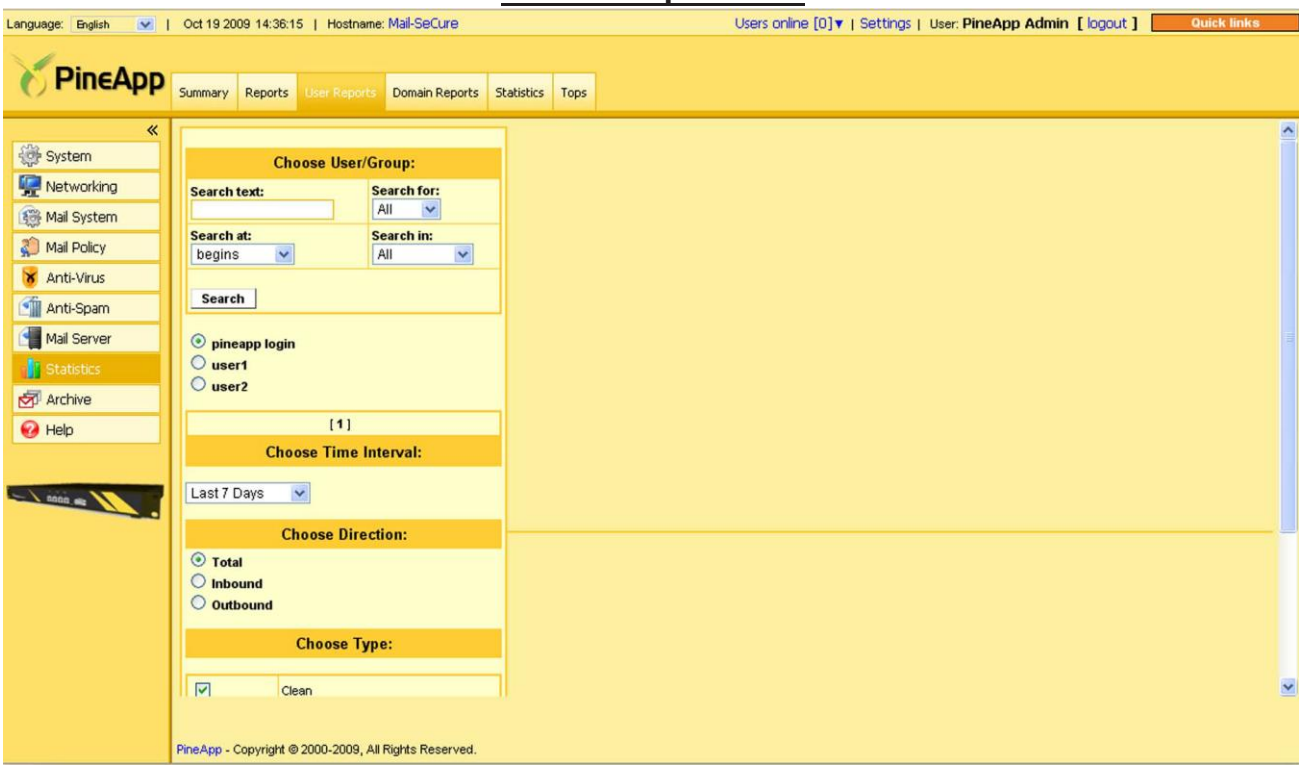
As soon as a user is defined (System > User management), the user will automatically be added to the scroll-down menu. Choose a user (or group) from the menu, time frame, direction and type and show the statistics.

The statistics can be exported to a CSV file (which can be opened by Excel).

The details in the User reports tab are generated once every 24 hours and include Spam blocked by the RBL engine.

This feature is not available in Mail-SeCure 1000 series.

Domain reports tab

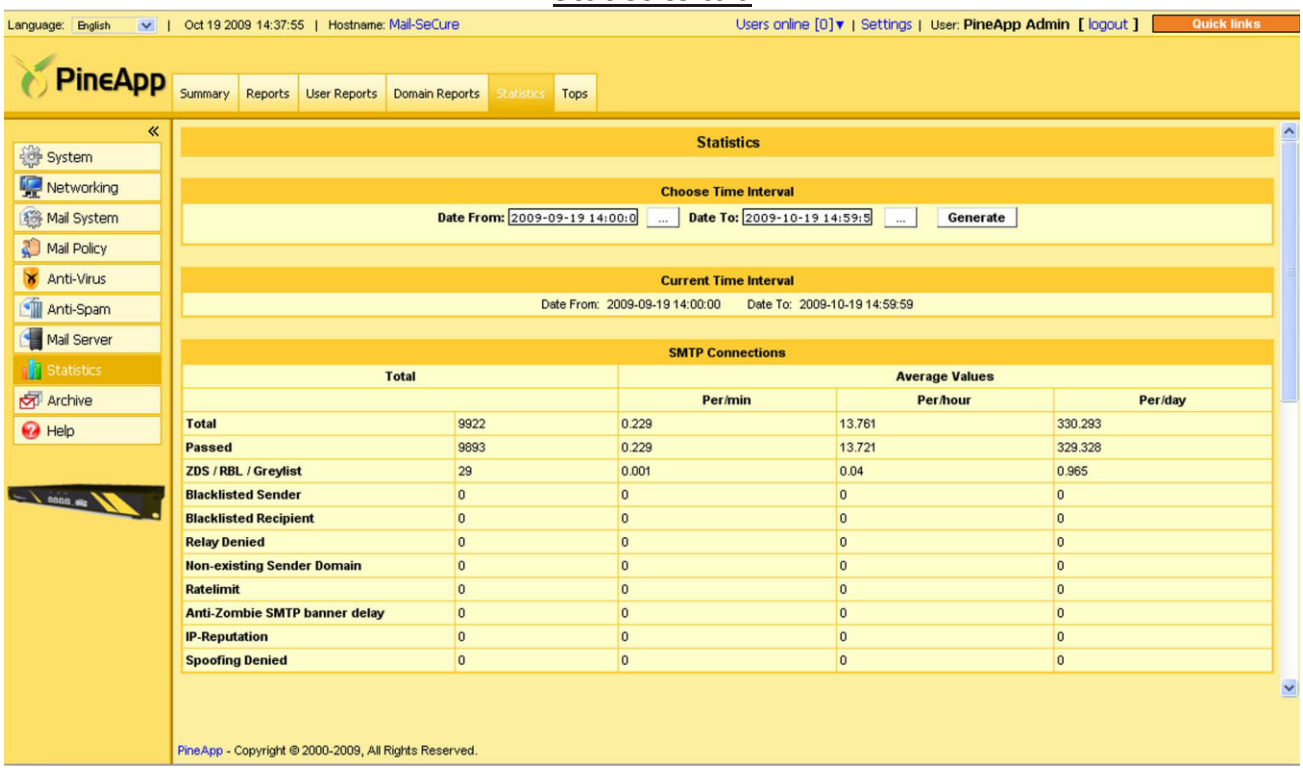


The domain reports tab displays graphic statistics per domain.
As soon as a domain is defined (Mail System > Local domains), the domain will automatically be added to the scroll-down menu. Choose a domain from the menu, time frame, direction and type and show the statistics.
The statistics can be exported to a CSV file (which can be opened by Excel).

The details in the User reports tab are generated once every 24 hours and include Spam blocked by the RBL engine.

This feature is not available in Mail-SeCure 1000 series.

Statistics tab



The statistics tab displays various textual statistics.
This tab provides additional information and helps to complete the information needed for the administrator.

The details in the User reports tab are generated once every 24 hours and include Spam blocked by the RBL engine.

Tops tab

In this tab, top statistics for different parameters can be displayed. For example: Top Spam senders, Top Virus senders, Top clean senders. The information can be displayed by domains, IPs or specific emails.
Choose the desired report from the drop-down menu and press "*go*".
Each report can be downloaded as a gif file.

CHAPTER 10

CONFIGURING THE FIREWALL

When installing PineApp Mail-SeCure, some configuration must be done on the local Firewall.

Ports from the world (WAN) to Mail-SeCure
SMTP (25/tcp and udp)
SSH (7022/tcp)
HTTPS (7443/tcp)
Web-Access (443/tcp and udp) - When the unit acts as a mail server
POP3 (110/tcp) - When the unit acts as a mail server

Ports from Mail-SeCure to the world (WAN)
SMTP (25/tcp)
DNS (53/tcp and udp)
HTTP (80/tcp)
POP3 (110/tcp) - When the unit acts as a mail server