

CYBONET



PineApp Mail Secure

5.1 User Manual



January 20, 2016

The information in this guide is furnished for informational use only, is subject to change without notice and should not be construed as a commitment by CYBONET. CYBONET assumes no responsibility or liability for any errors or inaccuracies that may appear in this guide.

This publication may not be reproduced, stored in a retrieval system, or transmitted, in any form or by any means -- electronic, mechanical, recording, or otherwise without the prior written permission of CYBONET as long as this copyright notice remains intact and unchanged on all copies.

CYBONET is trademarks of CYBONET. All other names and trademarks are the property of their respective owners.

CYBONET

Matam, Building 23,

P.O.B. 15102

Haifa

Israel

Tel +972 4 8212 321

Fax +972 4 8203 676

<http://cybonet.com/en/>



Table of Contents

INTRODUCTION.....	6
Before You Start.....	6
Accessing PineApp Mail Secure via Web Browser.....	6
System.....	8
General Information.....	8
Main Panel.....	8
Dashboard Tab.....	9
Disk Usage.....	10
Licensing Tab.....	11
Installing License Key.....	11
SMS Provider Tab.....	12
User Management Tab.....	12
Connectors Tab.....	16
Configuring OpenLDAP.....	18
SSL Certificate Tab.....	19
Generating a Self Signed Certificate.....	19
Generating & Installing a Third-Party License.....	19
Date and Time Tab.....	20
Advanced Tab.....	21
Backup Configuration Tab.....	21
Backup Instructions.....	22
Backing-Up PineApp Mail Secure Configuration (SAMBA protocol).....	22
Backing-Up PineApp Mail Secure Configuration (FTP Protocol).....	22
Restore Instructions.....	22
Alerts & Monitoring Tab.....	23
Remote Access Tab.....	24
CLI over SSH Settings.....	24
Logs Tab.....	25
Networking.....	26
General Tab.....	26
Add Static Route.....	27
Tools & Information Tab.....	28
Mail System.....	29



Basic MTA Settings.....	29
Advanced MTA Settings.....	31
SMTP Authentication Settings	32
MTA Plug-in Settings.....	33
Local Domains	34
Add Domain	34
Relay Networks.....	35
Logs	36
Mail Retriever	37
Activating and Configuring the Mail Retriever	38
Queue Info	38
Mail Policy.....	40
General Tab.....	40
Mail Policy Rules Tab	41
Add Group.....	43
Understanding Policy Modules.....	44
SPAM Rules	44
Attachment Rules.....	47
General rules.....	49
Black & White Rules	51
Disabling, Enabling and Deleting Rules.....	53
Content Rules.....	53
HTML Tags Rules	55
Mail Traffic Management Tab.....	57
Understanding Information Window.....	58
Zone Management Tab.....	59
File Types Tab.....	61
Footnotes Tab	62
Content Filtering Tab	64
DHA Protection Tab	67
Notification Templates Tab.....	68
Creating a Template.....	69
HTML Tags Tab.....	70
Creating tag groups.....	70



Deleting tag groups.....	71
Managing tag-groups.....	71
Deleting tags	71
Archive	73
General Tab.....	73
Archived Emails Tab	73
Daily Report Policy	74
Email Branding	77
Create a Template.....	77
Add a New Branding Rule	78
Big Email Data	79
Anti-Virus Tab	80
Anti-Spam.....	81
Control Tab.....	81
RBL Tab.....	83
Recipients and Block Networks Tab.....	84
Statistics	85
Summary Tab	85
Tops Tab.....	86
Statistics & Report Tab.....	86
Connections & Emails Report Tab.....	87
Domains, Groups & Users Report Tab	87
Managed Services	89
Customers & Units Allocation Tab	89
Settings.....	90
Personalize Tab	90
CONFIGURING THE FIREWALL.....	90



INTRODUCTION

Before You Start

PineApp Mail Secure is a leading security appliance that protects organizations of all sizes from both targeted and non-targeted threats. PineApp Mail Secure's improved scanning capabilities enable better content control.

All email traffic is scanned and the internal network is protected from known and unknown threats such as Viruses, Worms, Trojan Horses, Backscatter, Macros and Spam. PineApp 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.

PineApp 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 PineApp 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 PineApp Mail Secure via Web Browser

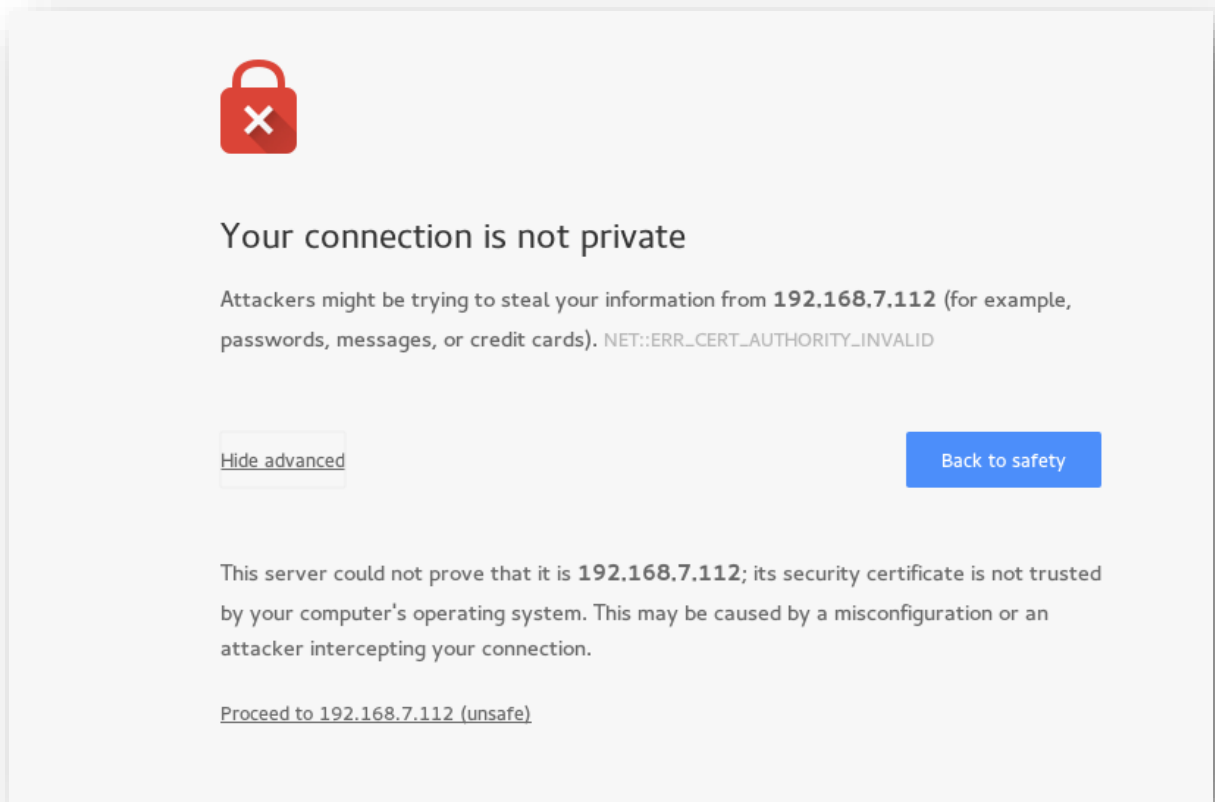
PineApp Mail Secure is accessed easily using any common web browser.

Connect the appliance to your internal network (port 1 on the appliance). Open any web-browser.

To access PineApp 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** or **http://192.168.24.24:7080** . If you are having trouble connecting, check your firewall setting and be certain that it is configured for this IP range.

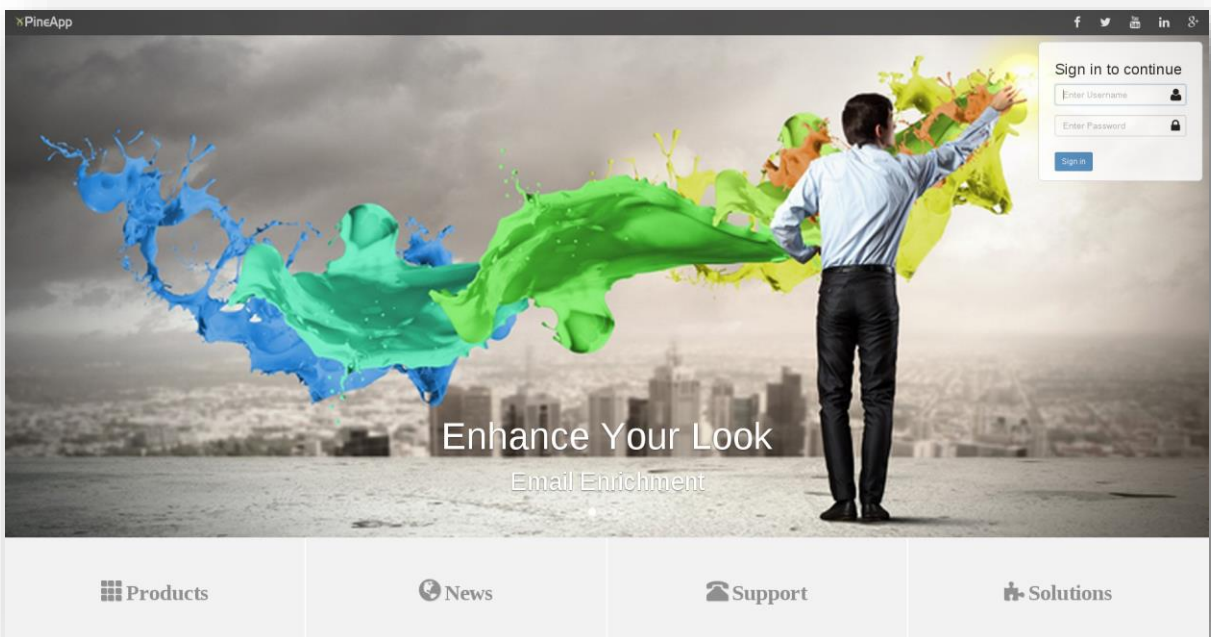
To access your appliance without having to make changes to your firewall settings, you can simply create a static route to the device in your firewall. Once you have logged into the device you can change the IP address.

A security alert message will appear when using **https**. Click OK to continue. In IE 7.0, an error page will be displayed. Click on **“Continue to this website (not recommended)”** or **“Proceed to 192.168.24.24 (unsafe)”** like in the screenshot below.



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 PineApp 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.

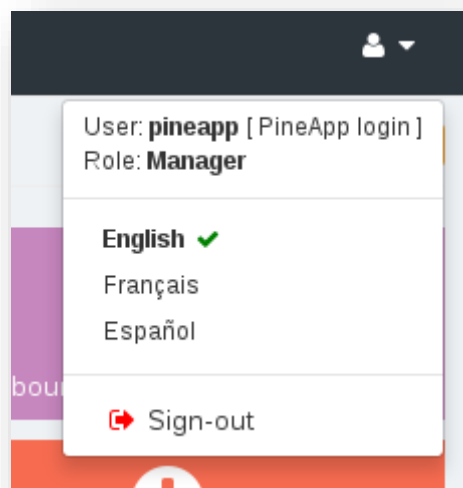
System

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.

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



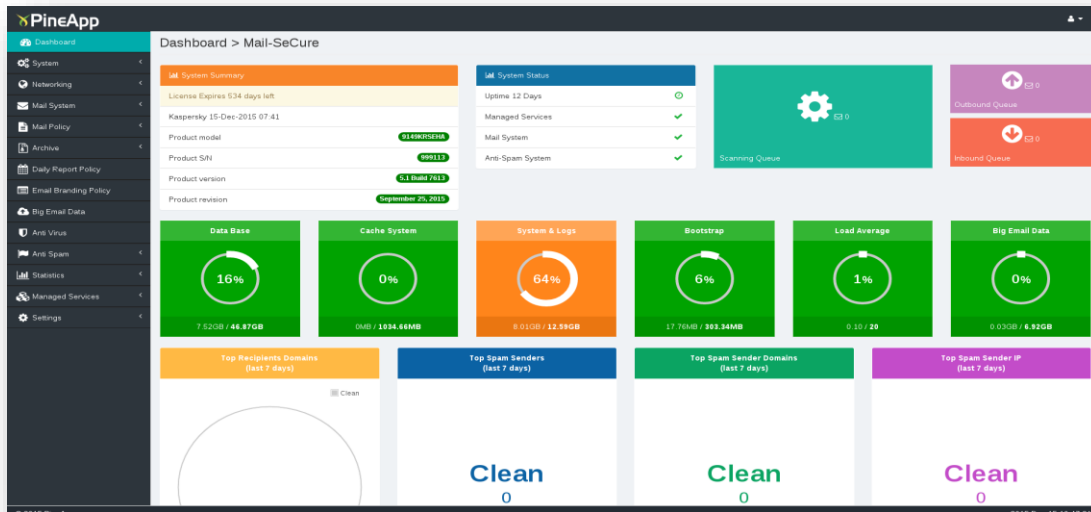
2. **Who's logged in** - Clicking on the *person icon on the top right corner* link will show you the users currently logged into the unit.
3. **Quick links** - Quick links are a shortcut to the most commonly used tabs. this option is configurable according to user's preferences simply by clicking on the hollow STAR in the headers of each tab.

Main Panel

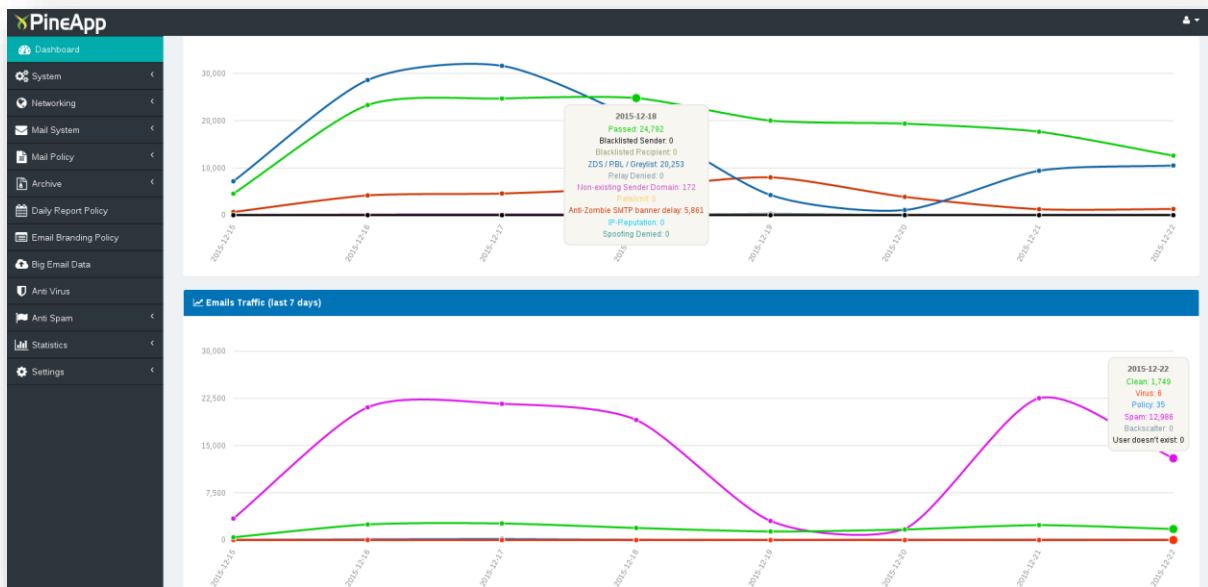


Clicking on different options in the left panel will open different options in the subpanel. Follow the instructions of this user guide in order to understand the different functionalities of the system.

Dashboard Tab



This is the first pane that appears after logging in.



Scrolling down shows more options

The screen provides the most important and essential information regarding the system. This pane contains System Summary, Network Usage, System Status and Disk Usage. It also shows the mail queue status and some spam statistics.



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.

Traffic Usage

This pane provides traffic information such as smtp connections and email traffic for last 7 days

System Status

This table is divided into three sections:

1. This provides information on Uptime of the unit and shows if engines are on or off
2. Scanning, inbound and outbound queue status.

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 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.

3. Disk status according to partitions and important folders.

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

Advanced Anti-Spam System - This section shows whether PineApp Mail Secure's Anti-Spam system, in charge of all perimeter & content inspections, is Operational/Down/Disabled (**Green** - **OK**, **Red** - **Down** , **Gray** - **Disabled**)

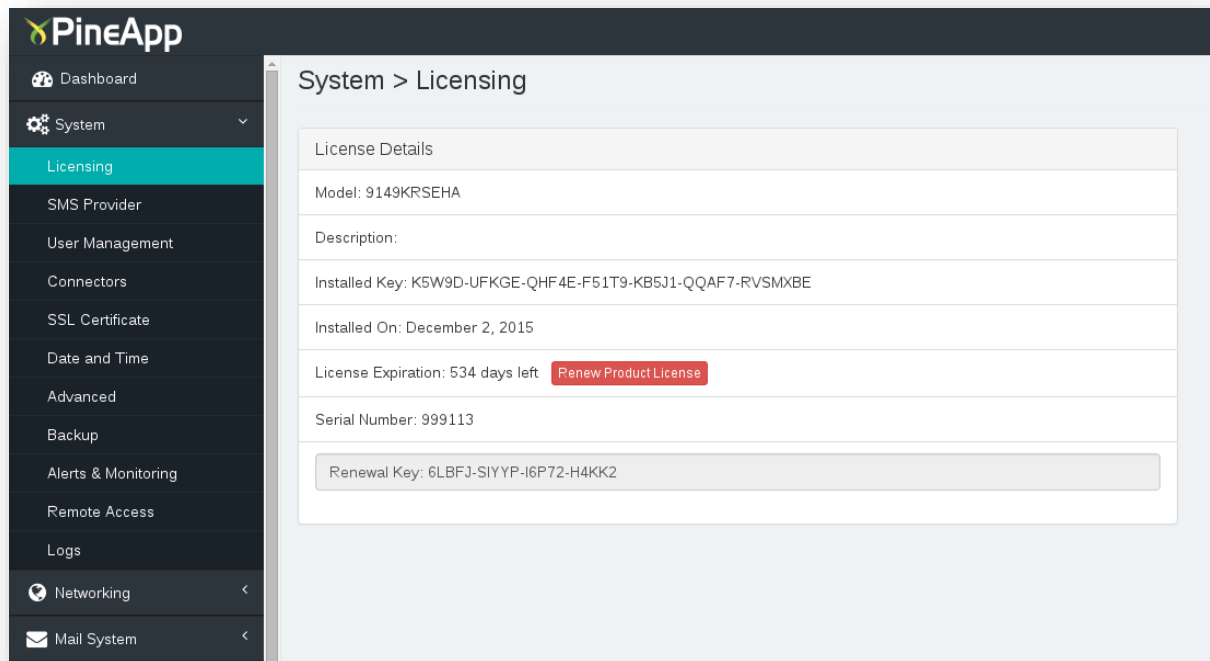
Disk Usage

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 7days - This section provides graphic statistical analysis for the traffic that has arrived the system during the last 7 days.



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.

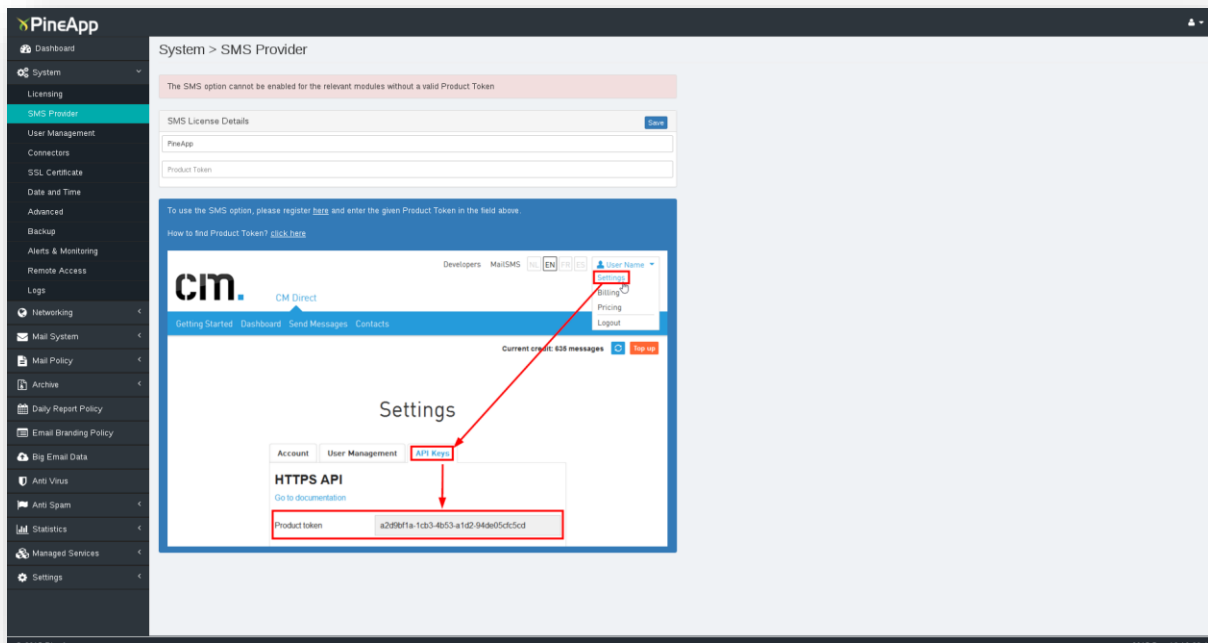
Installing License Key

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

* 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.



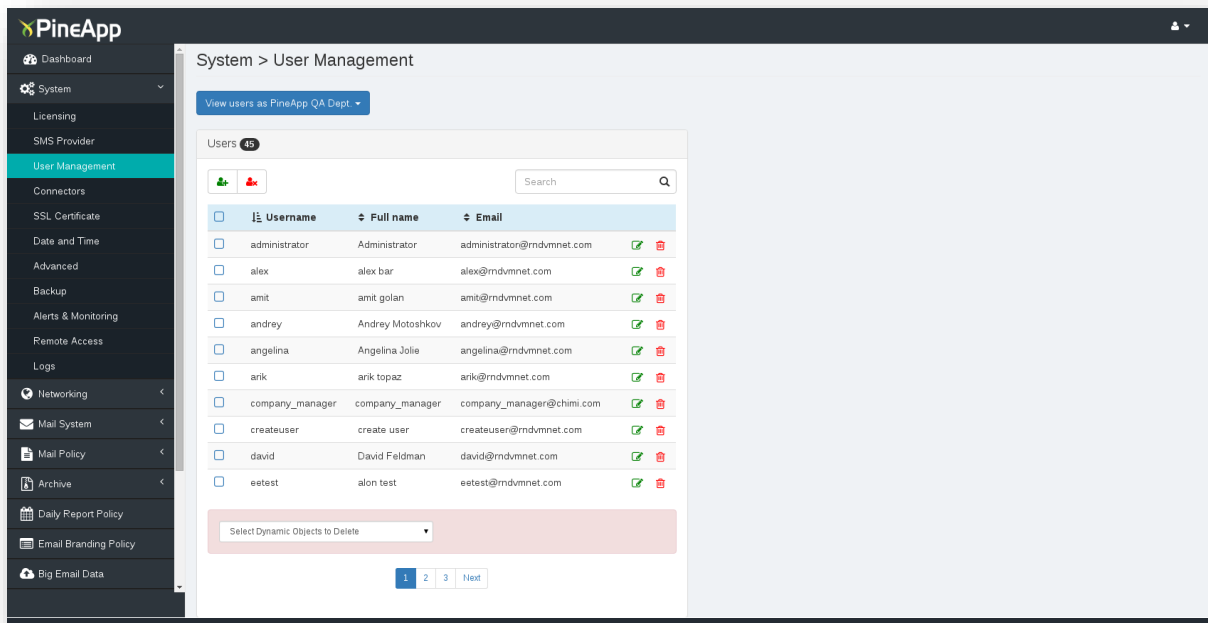
SMS Provider Tab



This section is related to our feature called Big Email Data, which will be discussed later on.

To Enable the “send password by SMS” option you will need to register to the provider according to the instruction in the tab.

User Management Tab



User management tab allows configuration and adjustments for new and existing users.

There are three methods for configuring users: (screenshots below)



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 password 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 were 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. **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

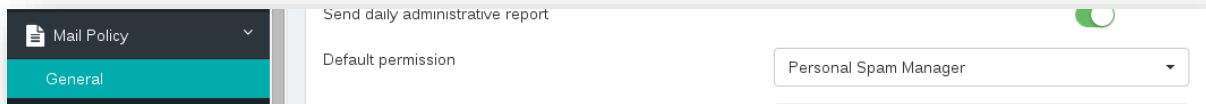
The screenshot shows a modal window titled "Add User" with the following fields and options:

- Username:
- Full name:
- Password: Confirm Password:
- Email: @
- Permission:
- Queue Priority:
- LDAP Sync:

Buttons at the bottom:

Click on the [Add new user](#) link. A new panel will pop-up (as seen above).

Default - When creating a new user (manually or by synchronizing to an LDAP server), the user will receive the "Default" permission. If the option in [Mail Policy > General](#)



In the fields, fill in the account information, enter a user name, full name (optional), email (It is possible to add more than one email).

After each mail we need to press “Add Email”

Use the dropdown menu to pick the domain. The domains are configured in the [Mail System> Local Domains](#) tab.

Click on the **Save** button to finalize the procedure.

Once added, the user will appear in the user list: By default, the order of the list is by username - 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 line or the Edit button, the window will pop-up again for editing. All modifications can be made – including changing the password. (note that when the user is ldap synced, changing the password is irrelevant.) When we finish changing the password, we will click the **SAVE** button.

Deleting Users

In order to delete users which were created manually, click on the red Trashcan icon. if you wish to delete multiple users, Mark all the needed checkboxes next to the user and click the red “person” icon

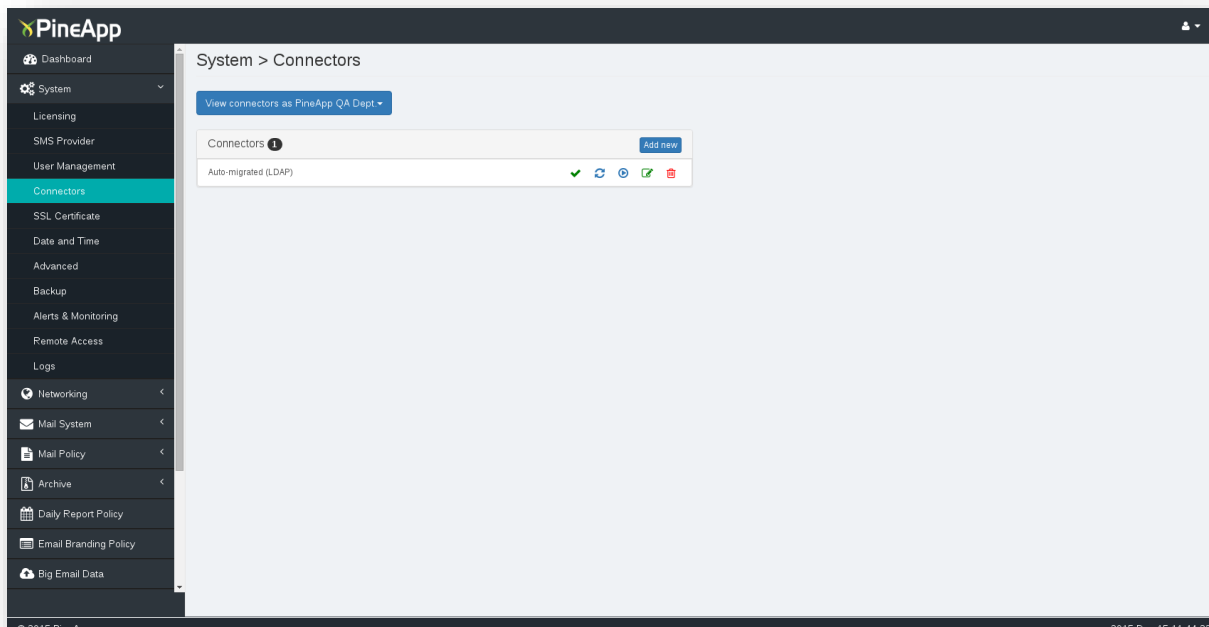


In order to delete users which are synchronized from the organization’s LDAP server, Select “Delete All Dynamic Objects” from the drop down menu below.

Delete 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.

Connectors Tab



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

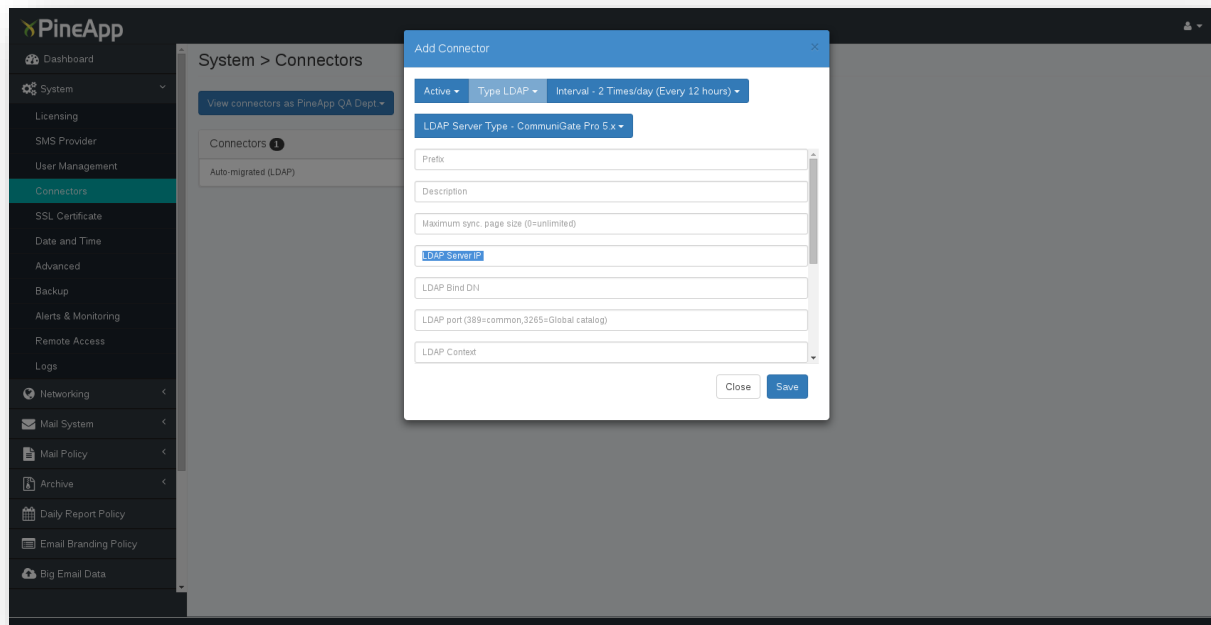
The system supports the following LDAP servers: Exchange 5.5, Windows 2000, Windows 2003, Communicate pro 5.x, Lotus Notes and Open LDAP.

This feature provides the ability to authenticate SMTP connections to CYBONET. 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. (if this is the 1st time, a demo connector will be presented, you can simple edit it, delete it and create a new connector or just ignore it)

Active - Check box to Enable / Disable the connector.

Type - At this stage, PineApp 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 4 times per day. 2 is more than enough. we can always sync manually in case a new user is added to the Active Directory.

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 (optional).

Description - Describe the LDAP connector (optional).

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 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 PineApp Mail Secure (Default: Checked).

Do not perform database queries (LDAP Only) - When checked, the PineApp 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 PineApp Mail Secure will Sync the data - but will not perform queries.

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%20assistance> Please contact support for further assistance.

<mailto:Support%40pineapp.com?subject=Open%20LDAP%20assistance>

<mailto:Support%40pineapp.com?subject=Open%20LDAP%20assistance>

If 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 PineApp 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 independently (CYBONET'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:

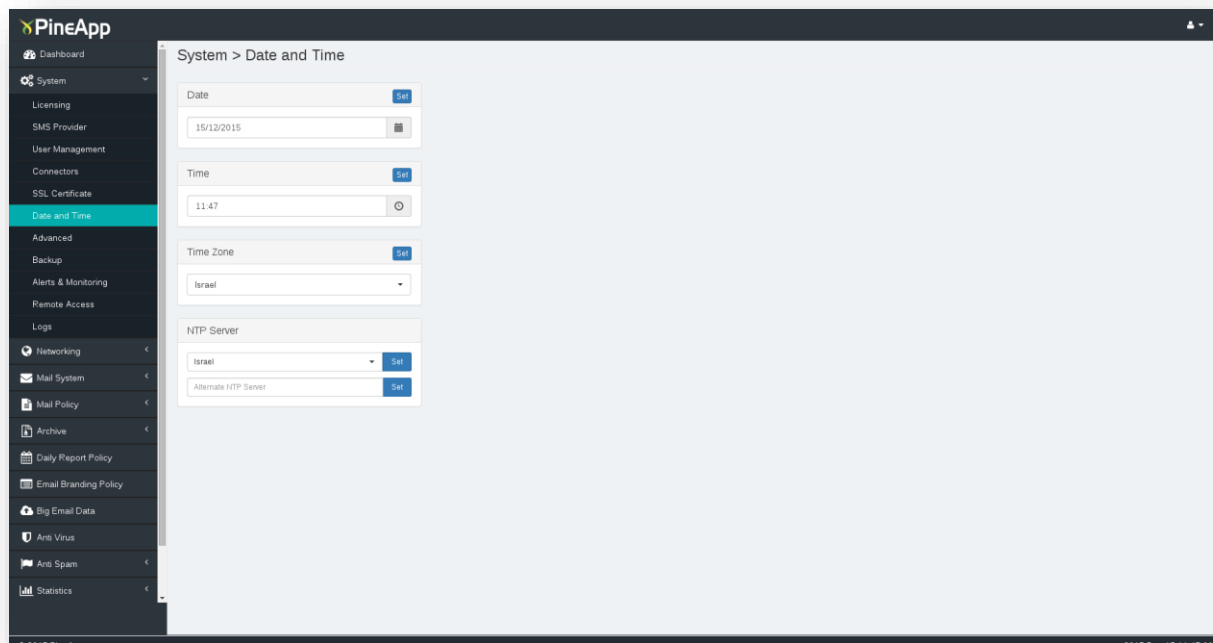
- A) **Country** - Choose the country of your company's location (initials) from the dropdown menu
- B) **State/Province** - Type the state/province of your company's location
- C) **Locality/City** - Type your company's full city name
- D) **Organization/Company** - Type your company's full name
- E) **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.
- H) Click on **Save Changes & Apply Settings**
- I) 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

Date and Time 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.

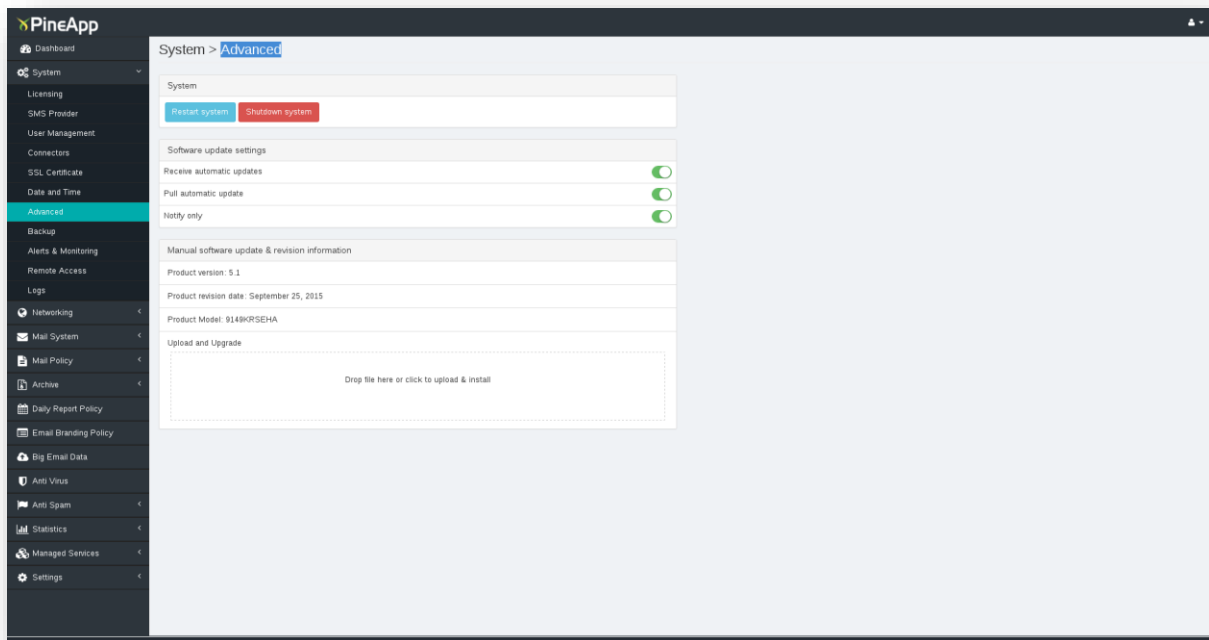
Using the NTP is simply done by choosing your country from the dropdown NTP menu and clicking on the **Set** button or by manually entering the IP of the NTP server and clicking on the **Set** button.

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

After “apply changes” is done, refresh the page.

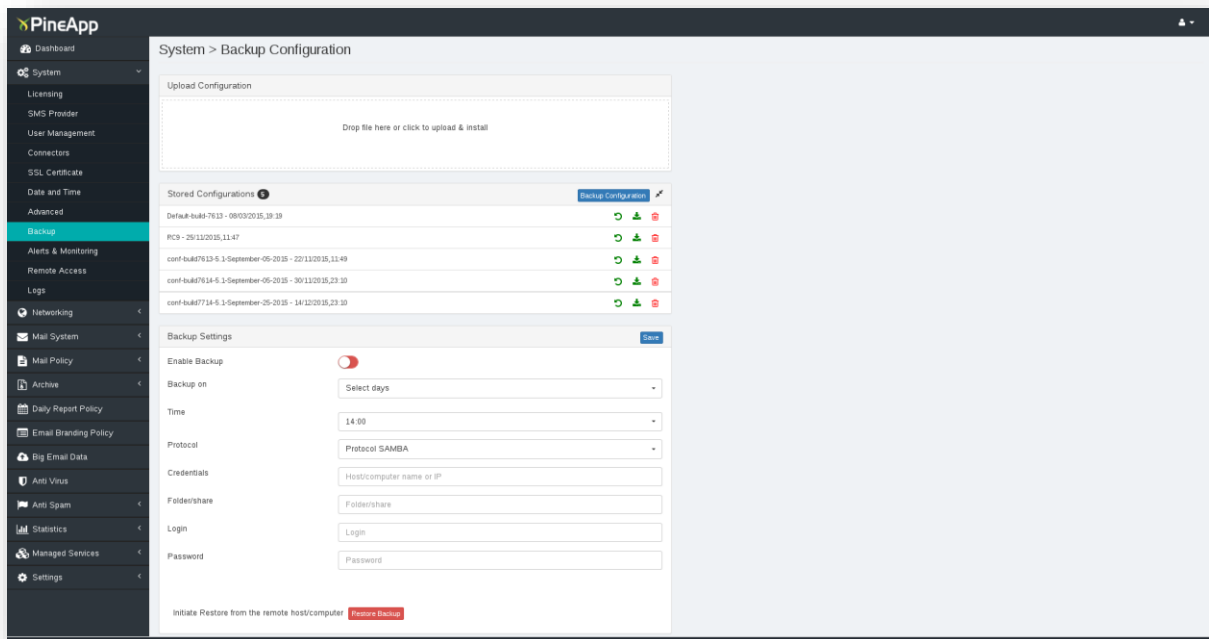
Advanced Tab



In the Advanced tab, manual restart or shutdown to the PineApp 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 PineApp Mail Secure system using these buttons only.

Backup Configuration Tab



This feature enables you to back up the system's configuration on a daily basis.



First, check the **Enable backup**. Choose the days and times for the backup to be performed.

[Backup Instructions](#)

[Backing-Up PineApp 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 PineApp 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 PineApp 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.

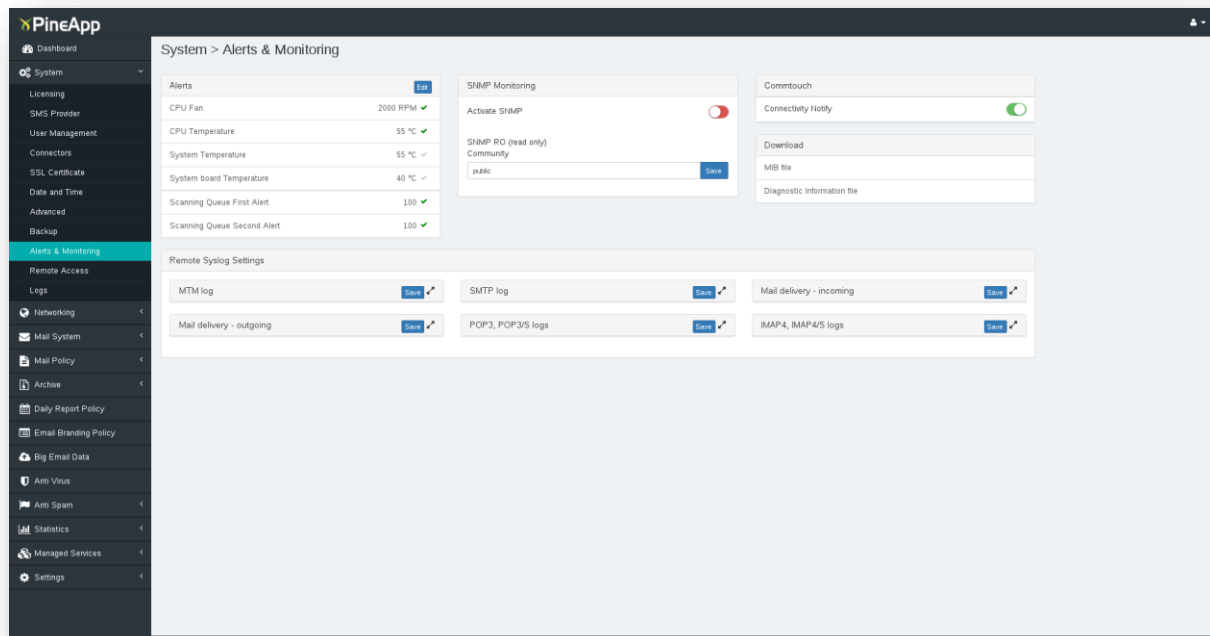
[Restore Instructions](#)

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 CYBONET 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 PineApp Mail Secure's functionality from the unit. Sending the downloaded file to CYBONET's support (support@pineapp.com), will help us troubleshoot problems.

Configuring Remote Syslog Settings

PineApp Mail Secure support Syslog. It is possible to remotely log the PineApp Mail Secure activities such as: SMTP logs, Incoming and Outgoing mail delivery, POP3, IMAP4 and mail traffic logs.

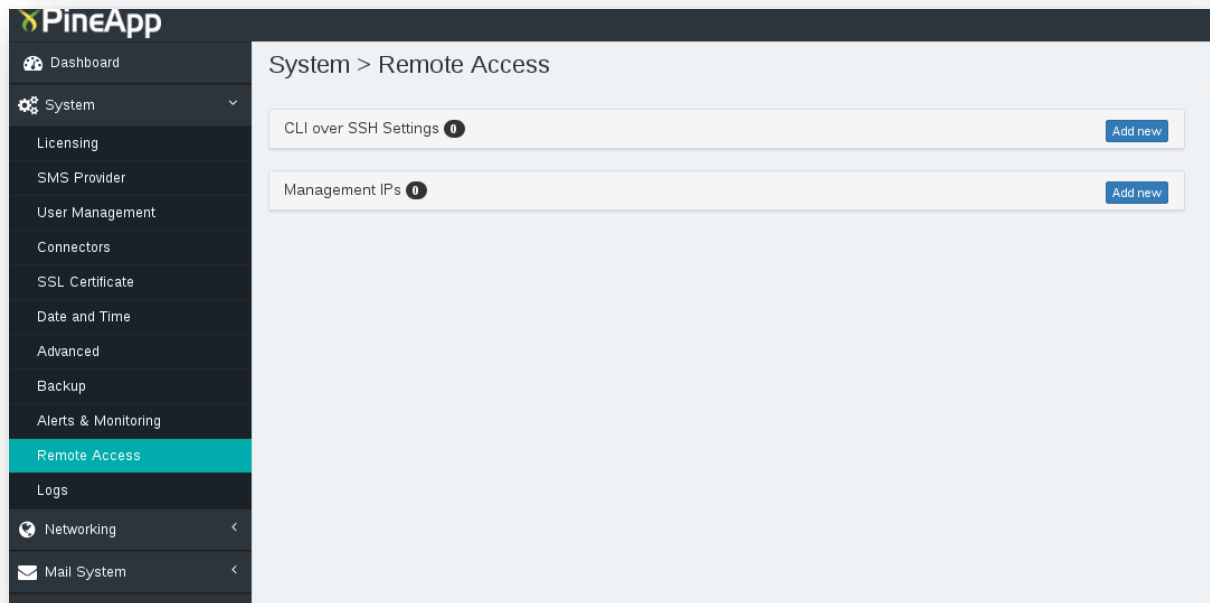
Setting up Remote Syslog

- 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 PineApp 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.

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.



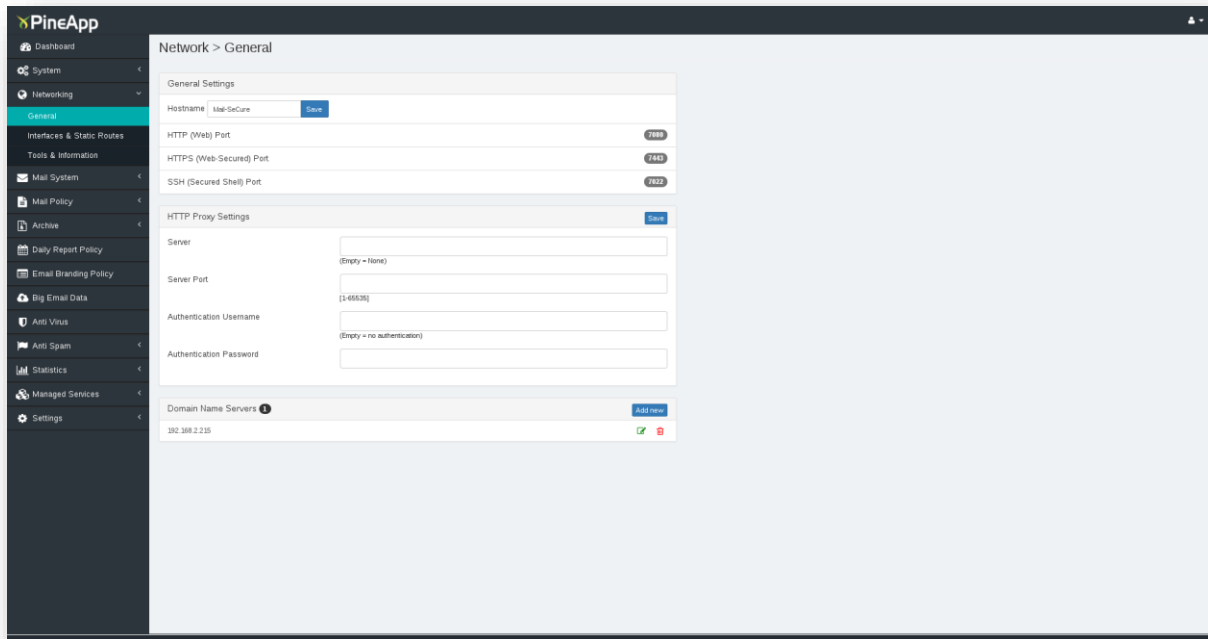
Logs Tab

The screenshot displays the PineApp interface with the 'Logs' tab selected. The main content area is titled 'System > Logs' and contains three log sections:

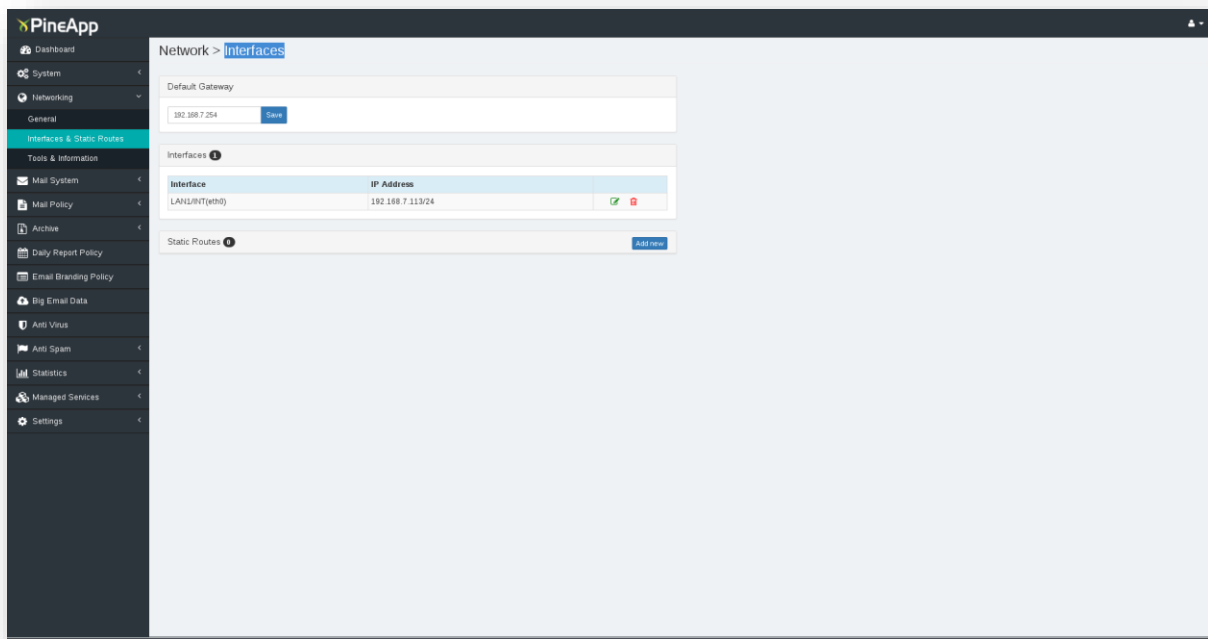
- Software Update Log:** Shows a table with columns for Release Date, Install Date, Description, and Info. The install date is November 30, 2015 at 14:23. Below the table are filters for 'Select date' (Any date), 'Line to process' (10), and a 'Keyword search' field. Buttons for 'Go' and 'Clear log' are present.
- System Log:** Shows a table with columns for Date and Time and Description. It contains two entries from Dec 15, 2015, detailing Mail-Secure virus scanning activities and warnings.
- POP3 Retriever Log:** Similar to the other logs, it has filters for 'Select date', 'Line to process', and 'Keyword search', along with 'Go' and 'Clear log' buttons.



Networking General Tab




Interfaces Tab




Adding an Interface

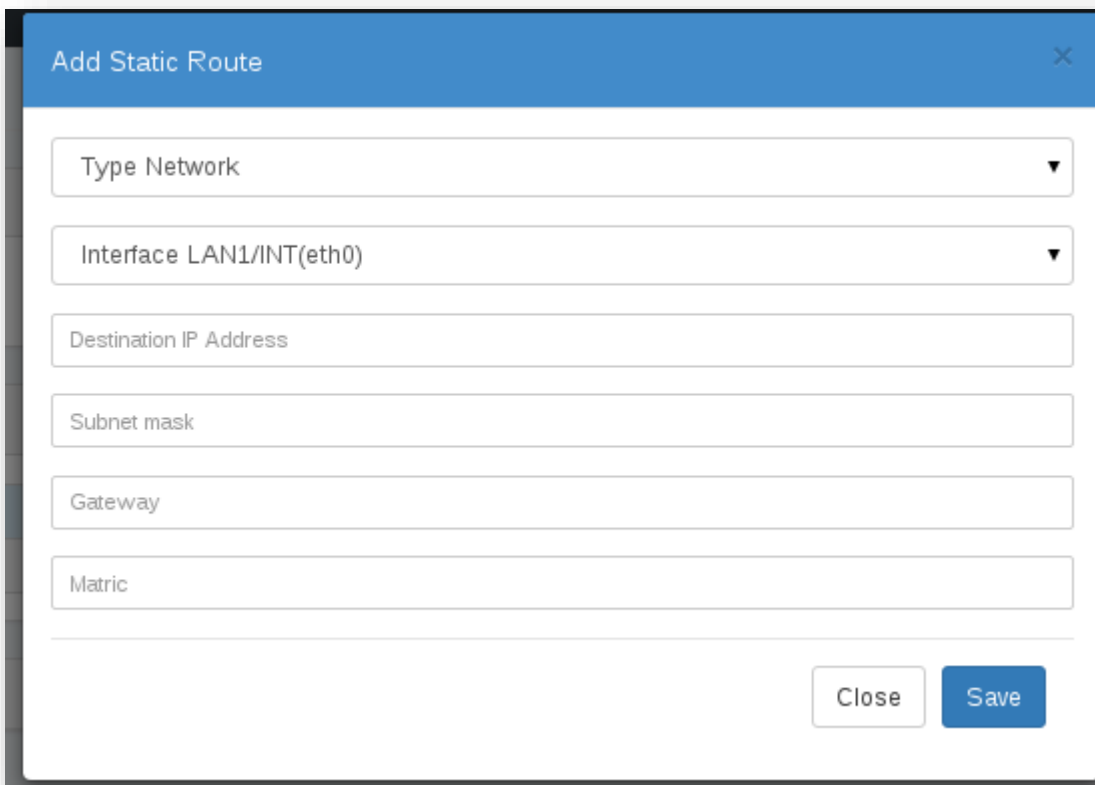
- A) Click on the [Add new Interface](#) link
- B) Choose the relevant interface from the drop-down menu.
- C) Type the desired IP address and Subnet mask in their corresponding fields.
- D) It is possible to define the interface's speed and MTU (Maximum Transmission Unit). If unknown, leave on defaults (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.

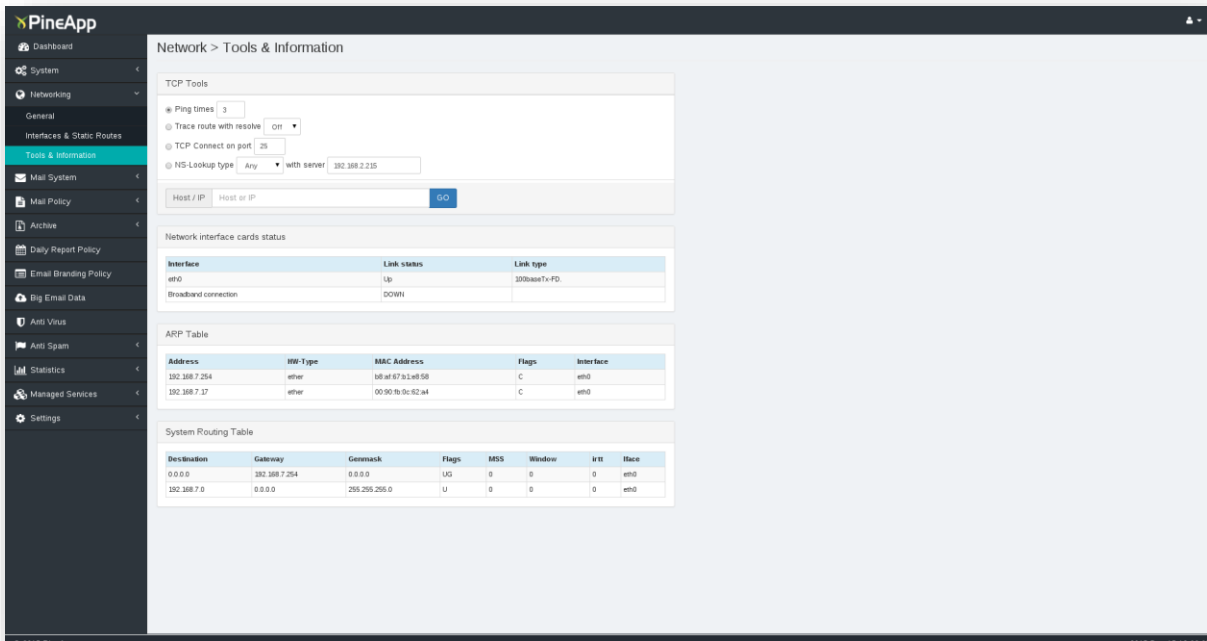
Add Static Route



Adding a New Static Route

- A) **Type** – Choose whether you would 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

Tools & Information Tab



The screenshot displays the PineApp interface for the 'Tools & Information' tab under the 'Network' section. It features several diagnostic tools and status tables:

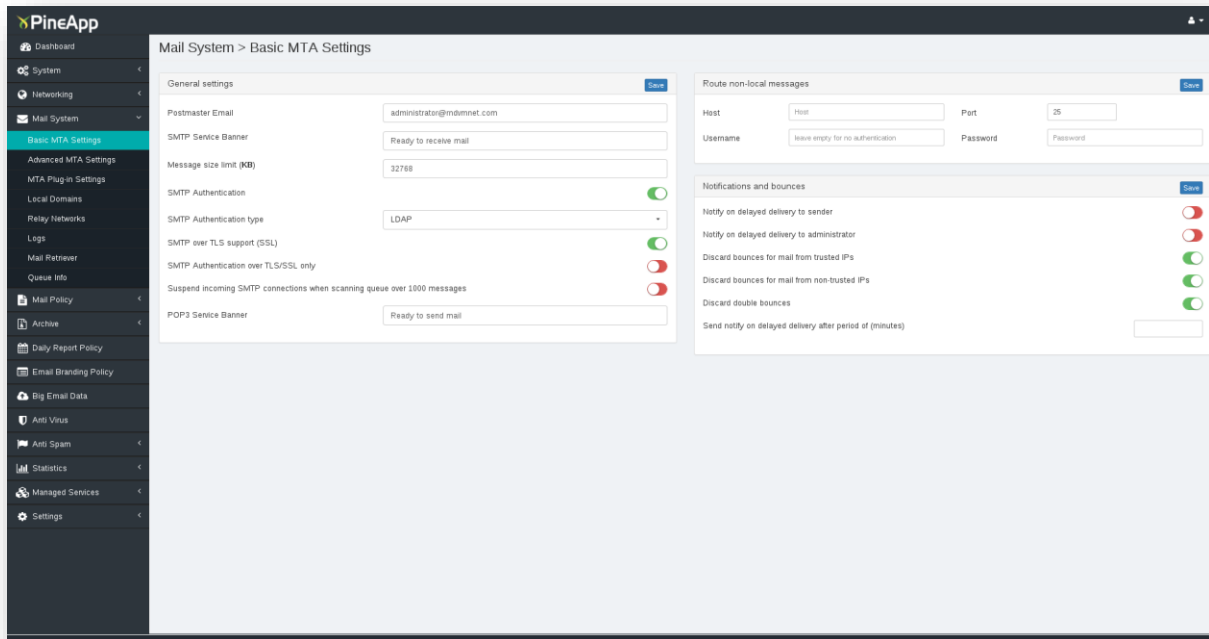
- TCP Tools:** Includes fields for Ping times (3), Trace route with resolve (on), TCP Connect on port (28), and NS-Lookup type (Any) with server (192.168.2.215). A 'GO' button is present.
- Network interface cards status:** A table showing the status of network interfaces.
- ARP Table:** A table listing IP addresses, HW-Types, MAC addresses, flags, and interfaces.
- System Routing Table:** A table showing destination, gateway, netmask, flags, MSS, window, IRT, and Iface.

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.

Mail System Basic MTA Settings



In the Basic MTA tab, all general information regarding the PineApp 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 PineApp Mail Secure without changing the outgoing mail server in the local Email client.

SMTP Authentication type – PineApp Mail Secure has three methods of authenticating SMTP connections:

1. **Normal** - when checked, PineApp 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, PineApp Mail Secure will authenticate the users with the usernames and passwords as configured in the LDAP server after the PineApp 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 any more 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 – PineApp Mail Secure system performs delayed 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, PineApp Mail Secure will not generate NDR's for emails originated from trusted IPs (from within the organization) (default - unchecked).

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

Discard double Bounces - When checked, PineApp 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.

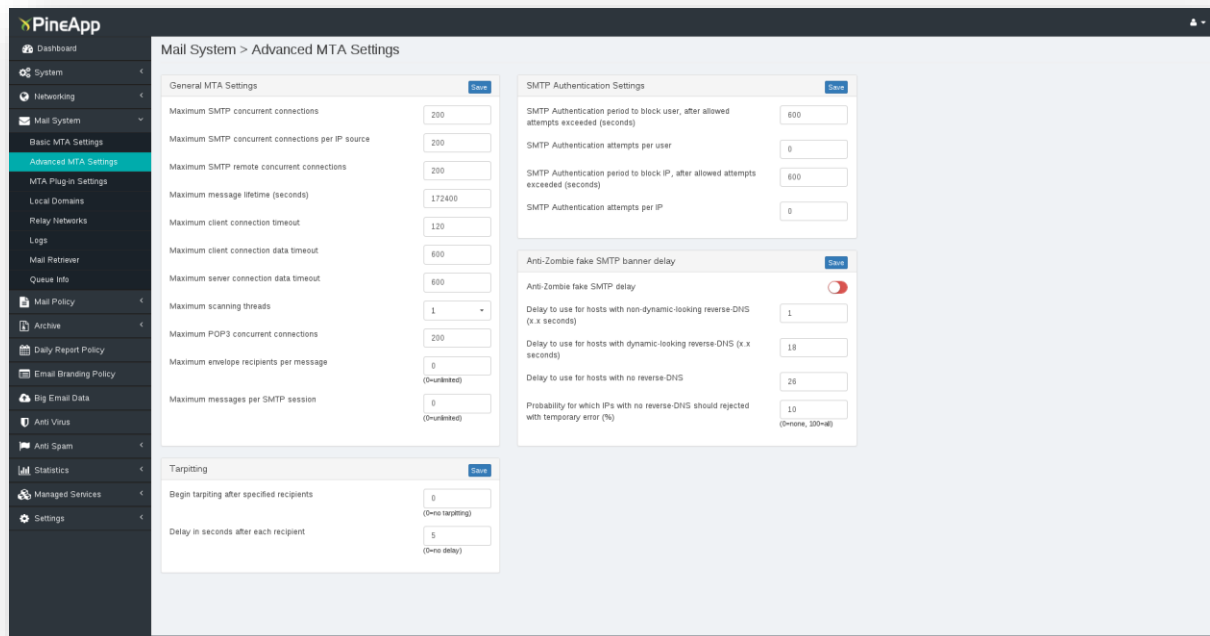
Route all non-local with authentication, password - If the external host requires authentication, define the password.

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).



Advanced MTA Settings



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 PineApp 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 PineApp 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 PineApp Mail Secure.

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

Maximum server connection data time-out - This figure refers to the time-out (in seconds) of the data session when PineApp 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 PineApp 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.

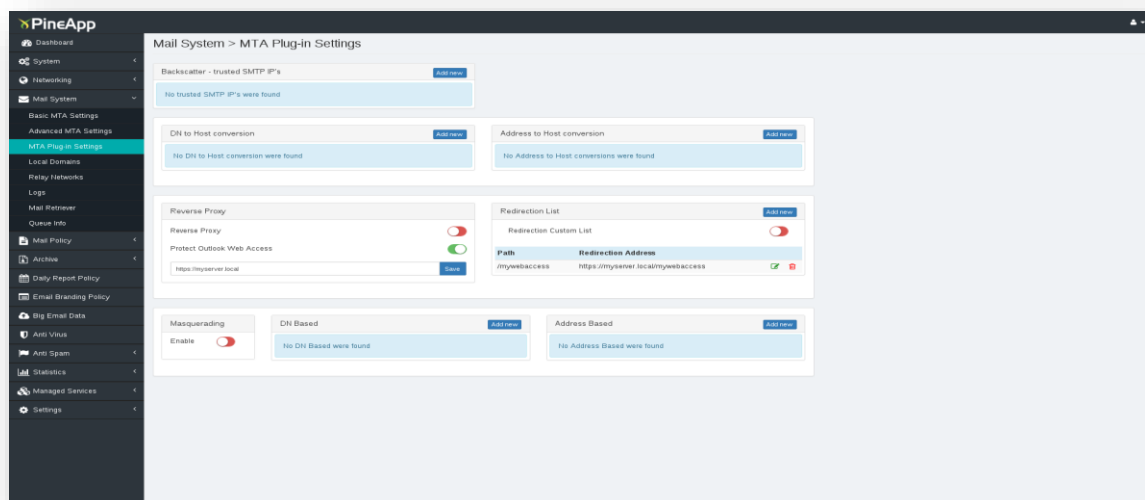
Delay to use for hosts with non-dynamic-looking reverse-DNS (x.x seconds) - This is the delay (in seconds) for traffic originated from non-dynamic-looking reverse-DNS hosts (default: 1).

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).

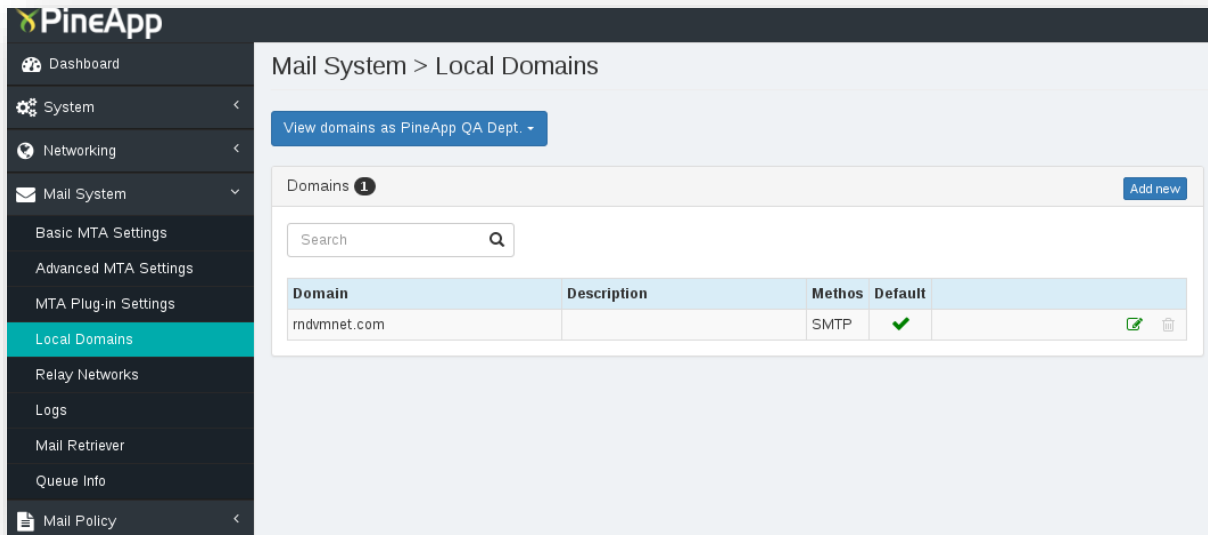
Probability for which IPs with no reverse-DNS should be rejected with temporary error (percentage, 0=none, 100=all) - When traffic arrives from a no reverse-DNS host, it is possible to define what percentage of it will be delayed. This will increase the chance that legitimate “second attempts” will be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

MTA Plug-in Settings





Local Domains



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

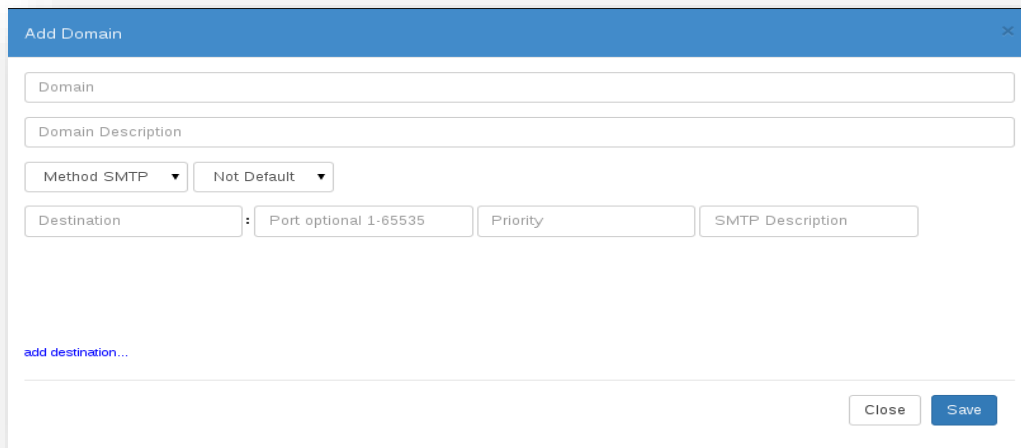
Delivery Methods

LOCAL - All mail sent to the domain will be stored locally on the PineApp 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.

Add 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
- F) localdomain.com's existing record, by clicking on the V next to it. One domain has to be defined as default at any time
- G) 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

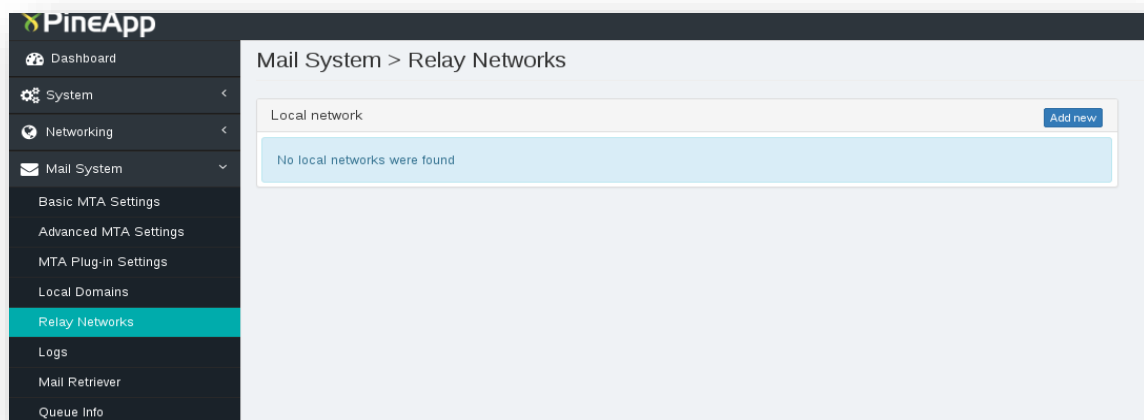
- A) Type in the empty fields the new domain name and its description.
- B) Click on the **Add** button.

*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.

Relay Networks



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

All IP connections to PineApp 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 PineApp 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

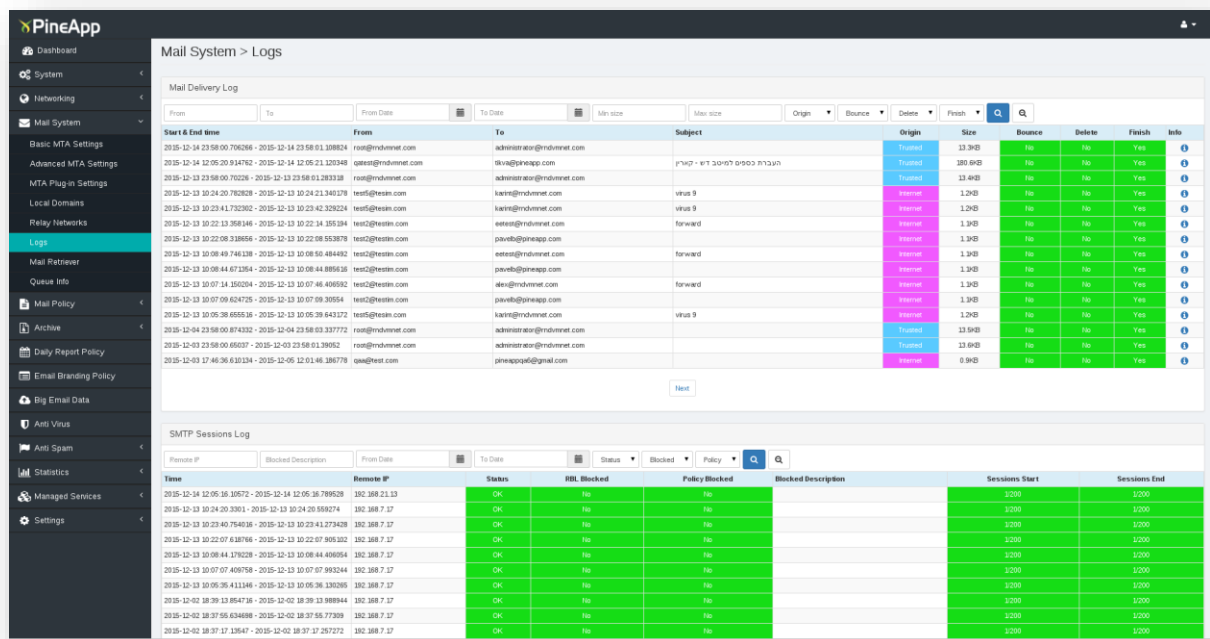
Adding a New Entry

- 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.

Logs



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.

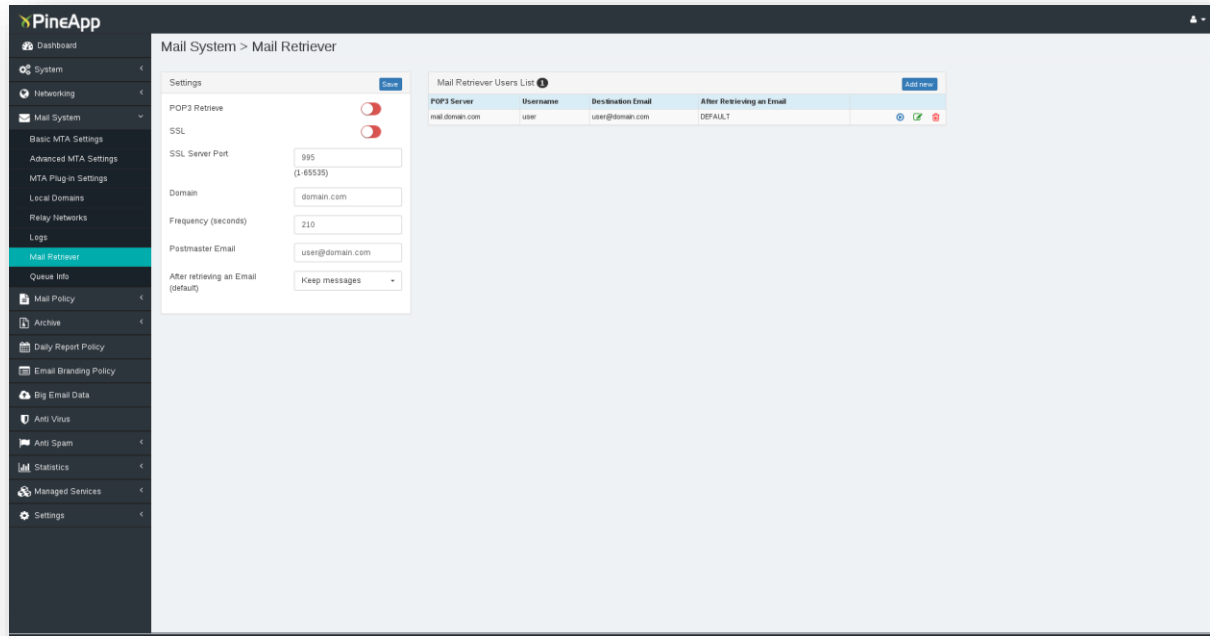
Mail Delivery - All traffic concerning the final email delivery phase (incoming and outgoing) is logged in the menu. Mail server responses can be viewed from this menu.

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 are shown in this menu.

Mail Retriever



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 PineApp 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
- B) (Default: off)
- C) **Domain** - Type the default domain in this field
- D) **Frequency** - Type the time interval in seconds between each mail check interval (Default: 210 seconds)
- E) **Postmaster's Email** - Type the Postmaster's email address
- F) **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:

Click on the **Add new** Button. A new table will appear.

- A) 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, PineApp Mail Secure will append the default domain.
- B) 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.
- C) 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).
- D) In addition, generated system logs can be viewed at the bottom of this screen.

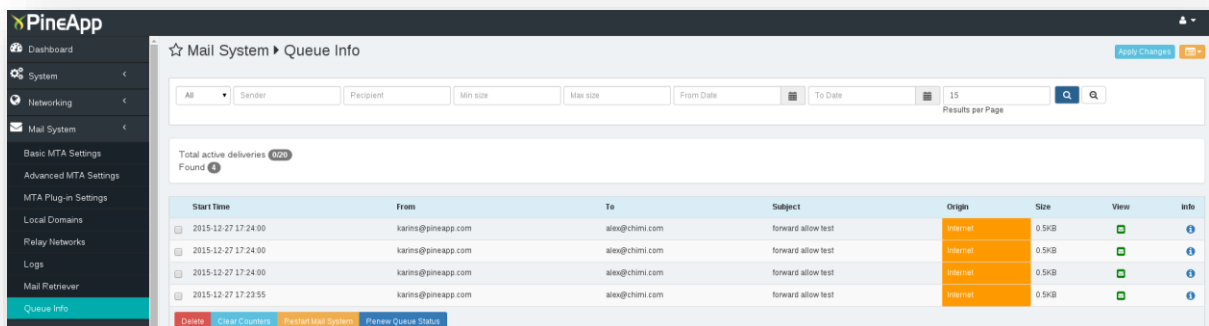
Modifying an Entry

- 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.

Queue Info



Start Time	From	To	Subject	Origin	Size	View	Info
2015-12-27 17:24:00	karims@pineapp.com	alex@chimi.com	forward allow test	Internet	0.5KB	<input type="checkbox"/>	i
2015-12-27 17:24:00	karims@pineapp.com	alex@chimi.com	forward allow test	Internet	0.5KB	<input type="checkbox"/>	i
2015-12-27 17:24:00	karims@pineapp.com	alex@chimi.com	forward allow test	Internet	0.5KB	<input type="checkbox"/>	i
2015-12-27 17:23:55	karims@pineapp.com	alex@chimi.com	forward allow test	Internet	0.5KB	<input type="checkbox"/>	i

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 delete 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.

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  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 (*).

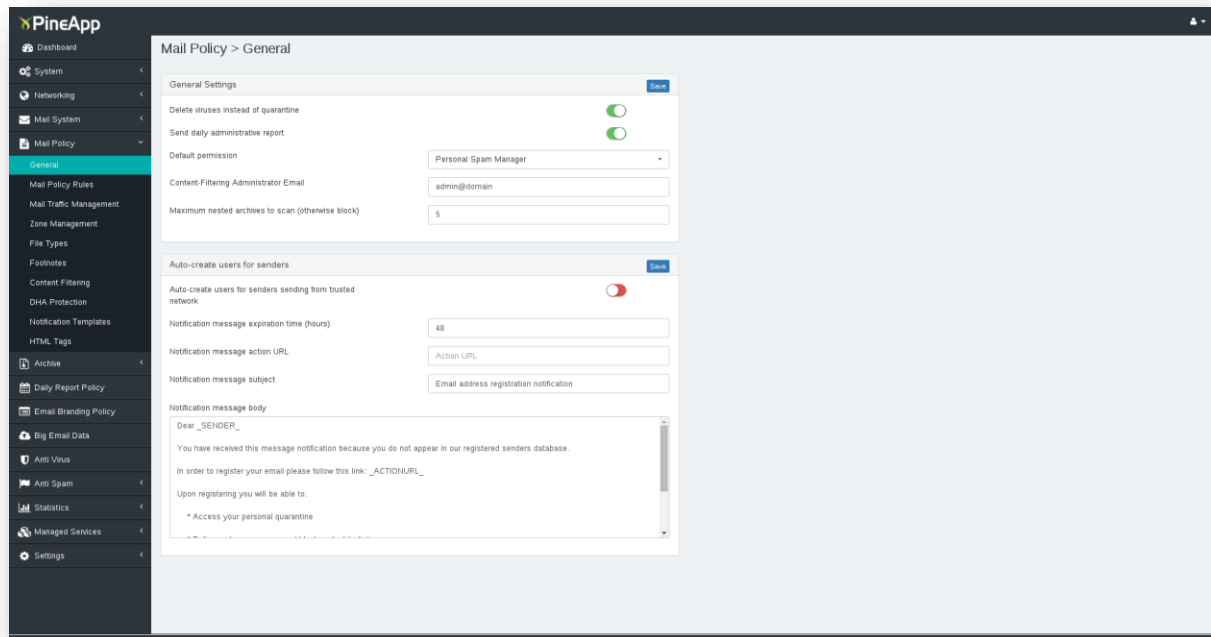
Origin - Choose the direction: trusted (outgoing mail), Internet (incoming mail) or both.

Size - Type the size limit in bytes (1,000,000 ~ 1MB).

Mail Policy

In this window, the PineApp 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 PineApp 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 number 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

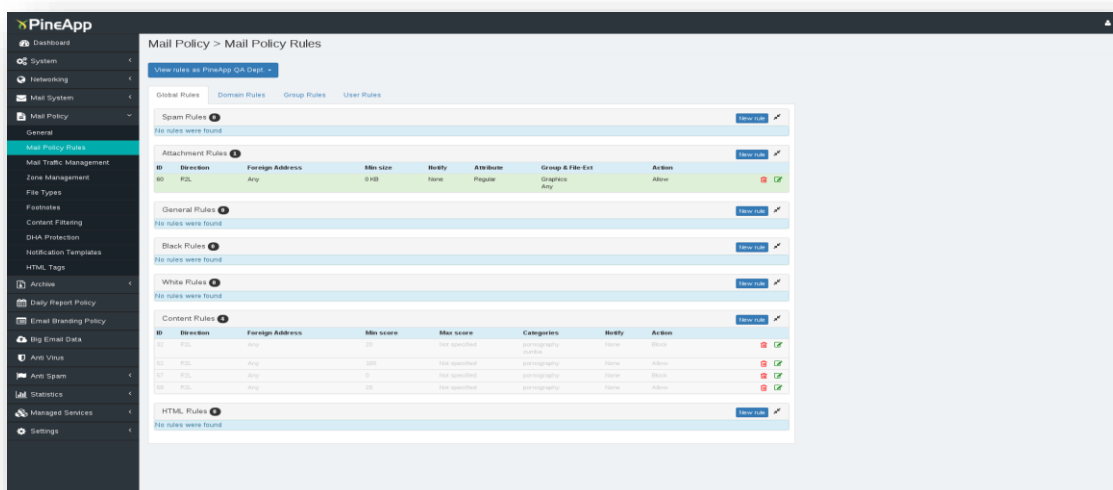
This section contains service provides features for automatic registration. Upon delivering an email using a local domain from a trusted network, customer will receive a notification message, containing an activation URL. Once clicking on the action URL, sender will be automatically registered on the 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 PineApp Mail Secure’s URL address, to which all registration requests will be redirected.

Mail Policy Rules 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.

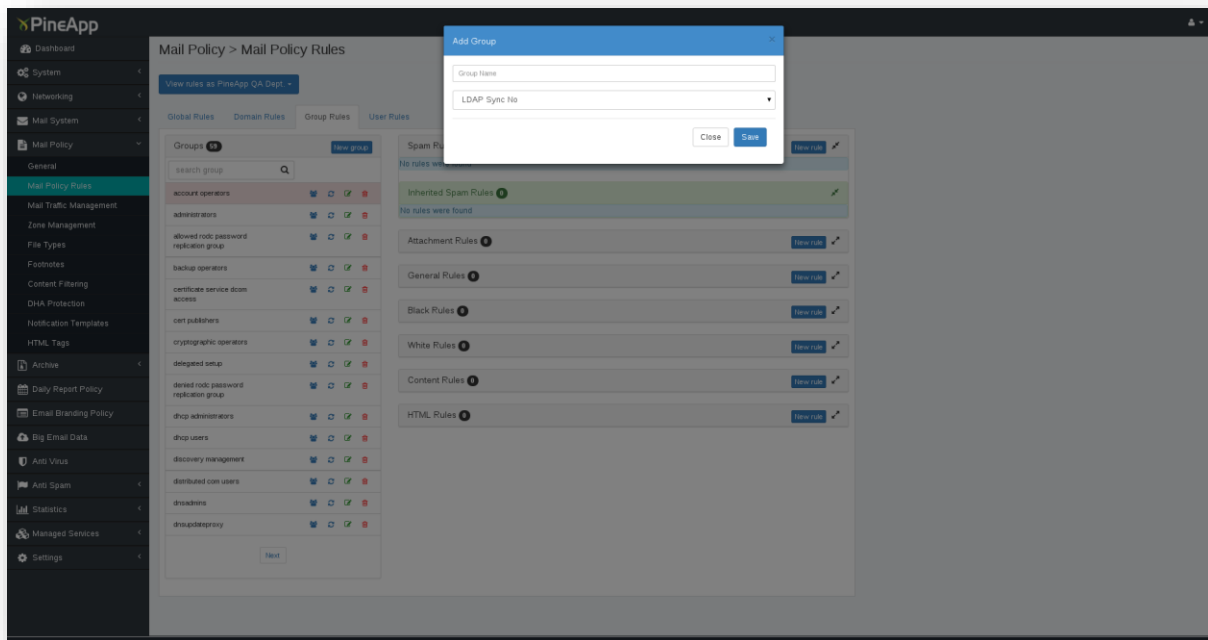
Creating new users

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.

Add Group

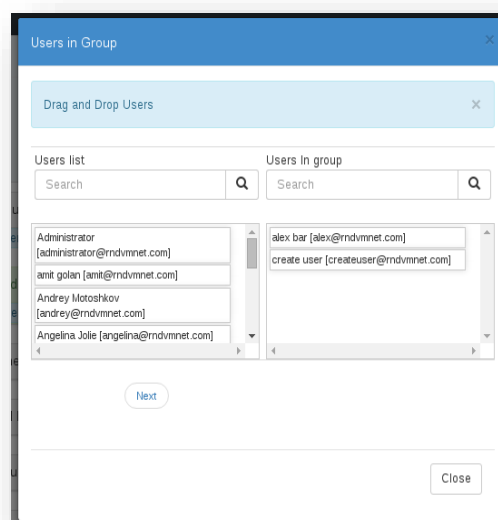


Creating new groups

- A) In the Groups tier in the left pane, click on the add link
- 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 **Save** button. 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:




- B) Drag and drop the user that you wish to add/remove, and click on the **Close** button when done.




C) Clicking on the group after it was saved will show us the information of the group.

Modifying Groups

- A) Edit the group by clicking on the green edit icon next to the group().
- B) Rename the group by typing the new name. When done, click on the **Save** button.
- C) The group will appear in the left pane with its list of Rules in the right pane.

It is possible to add / remove members, as described above by pressing the Blue icon ()

Deleting Groups

We can delete any group by pressing the red Trashcan icon (), this will automatically discard all users and rules related to the group and delete the group.

Understanding Policy Modules

PineApp 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 PineApp 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.

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.

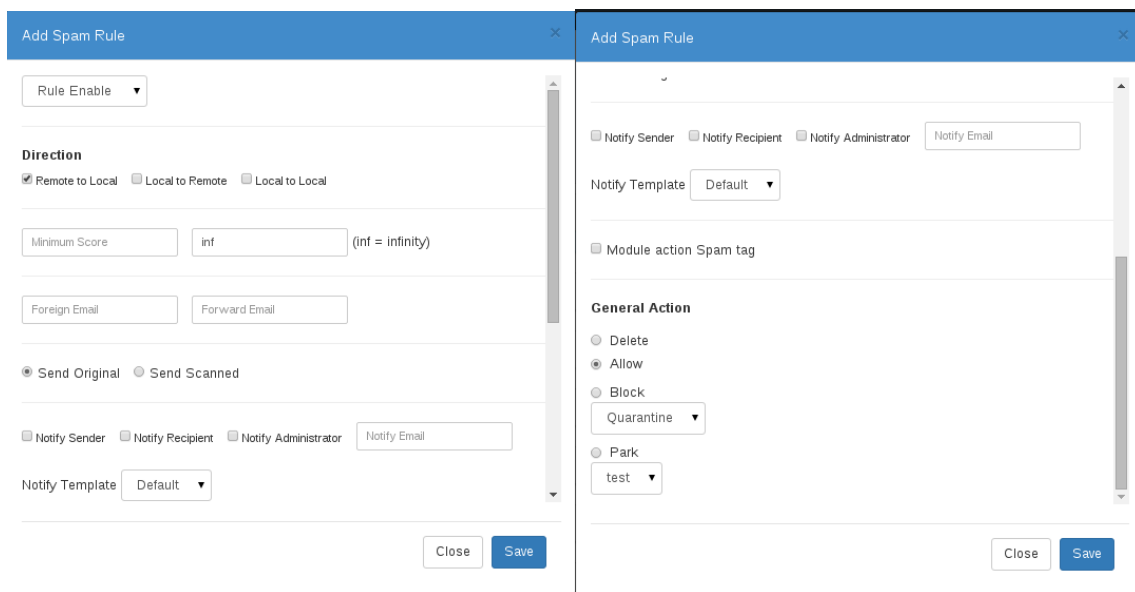
Domain - Select the domain you wish to create rules for by double clicking on the domain from the list in the left pane, and click on it.

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 screenshot shows two side-by-side views of the 'Add Spam Rule' dialog box. The left view shows the 'Direction' section with 'Remote to Local' selected, and the 'General Action' section with 'Block' selected and 'Quarantine' as the action. The right view shows the 'General Action' section with 'Delete' selected and 'test' as the action.

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 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.

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.



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.

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.

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.

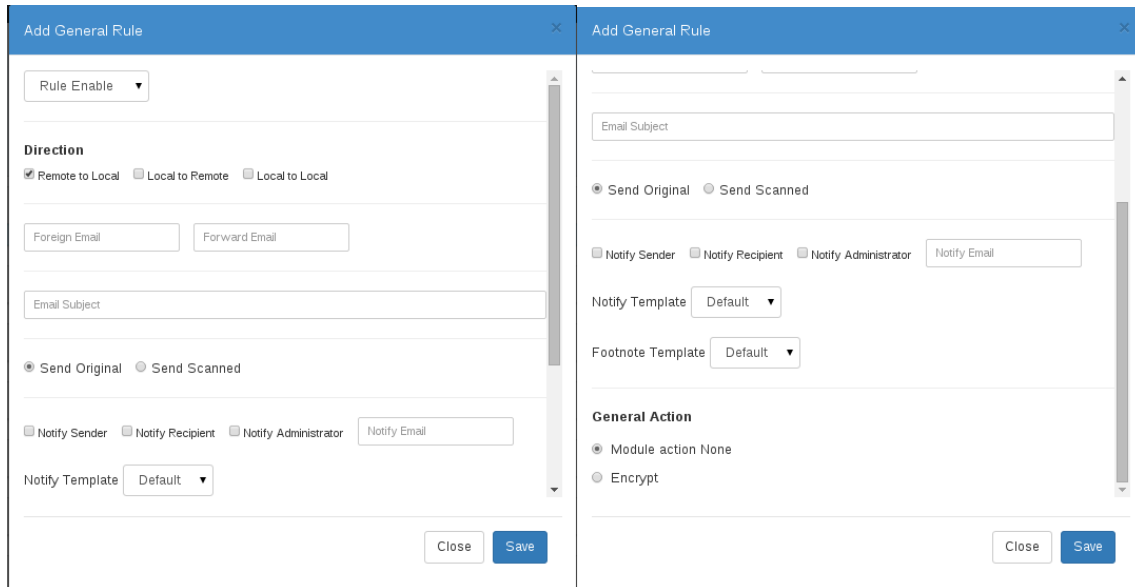
Group - Select the group you wish to create rules for by double clicking on the group from the list in the left pane. The details of that group will appear in the right pane.

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

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:



The image shows two side-by-side screenshots of the 'Add General Rule' dialog box. Both screenshots show a 'Rule Enable' dropdown set to 'Rule Enable'. The left screenshot shows the 'Direction' section with three radio buttons: 'Remote to Local' (checked), 'Local to Remote', and 'Local to Local'. Below this are two text input fields: 'Foreign Email' and 'Forward Email'. The 'Email Subject' field is empty. The 'Send Original' radio button is selected. The 'Notify Sender', 'Notify Recipient', and 'Notify Administrator' checkboxes are unchecked, with a 'Notify Email' text input field. The 'Notify Template' dropdown is set to 'Default'. The right screenshot shows the 'Email Subject' field with some text. The 'Send Scanned' radio button is selected. The 'Notify Sender', 'Notify Recipient', and 'Notify Administrator' checkboxes are unchecked, with a 'Notify Email' text input field. The 'Notify Template' dropdown is set to 'Default'. The 'Footnote Template' dropdown is set to 'Default'. The 'General Action' section has 'Module action None' selected and 'Encrypt' is also visible. Both screenshots have 'Close' and 'Save' buttons at the bottom right.

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

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.

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. The following screen will appear:

Add Black List Rule



Add White List Rule

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 () , the rule can be deleted all together.

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 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:



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 Tags** 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.

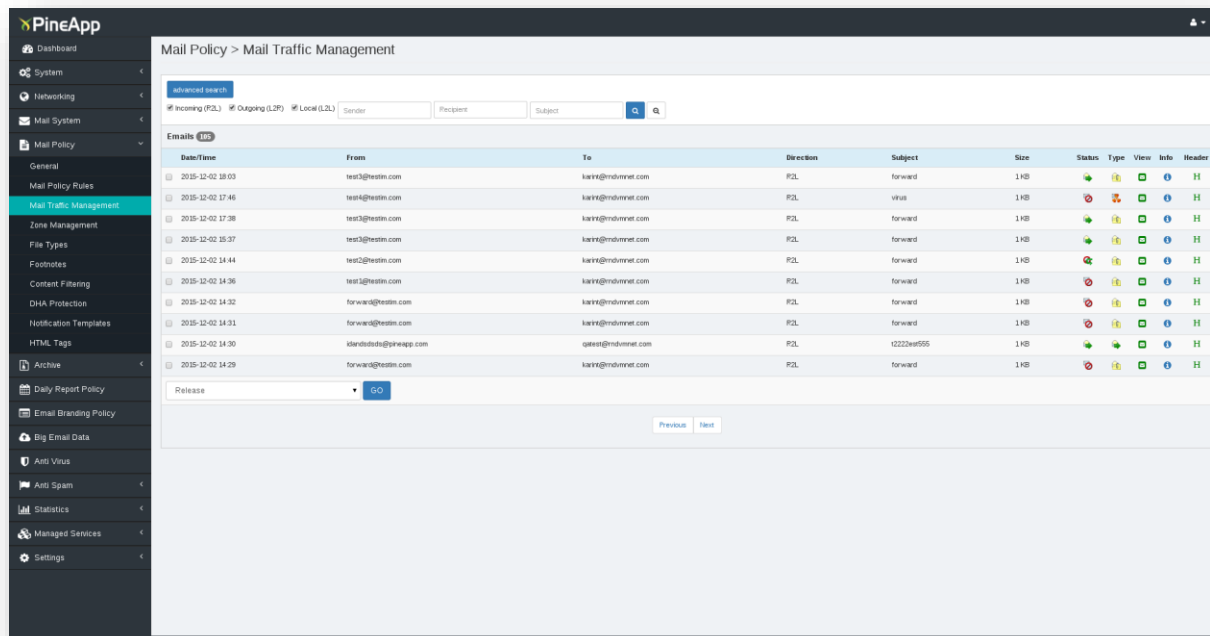
See **Zone Management** Tab for information on creating and managing Parking zones.

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

Messages 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.

The screenshot shows a window titled "Information" with the following details:

- Message ID: 9000000000000089268
- Rule ID: 0
- Source IP: 192.168.7.17/32
- Virus: No virus found
- Spam: Score: 5.5
- Advanced Anti-Spam: No Commtouch match found
- Policy: No Policy match found
- Mail Delivery:

Start & End Time	Status	Description
2015-12-02 14:30:22.623295	success	192.168.17.4_accepted_message./Remote_host_said:_250_2.6.0__[InternalId=162965]_Queued_ma
2015-12-02 14:30:22.484838		

A "Close" button is located at the bottom right of the window.

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).



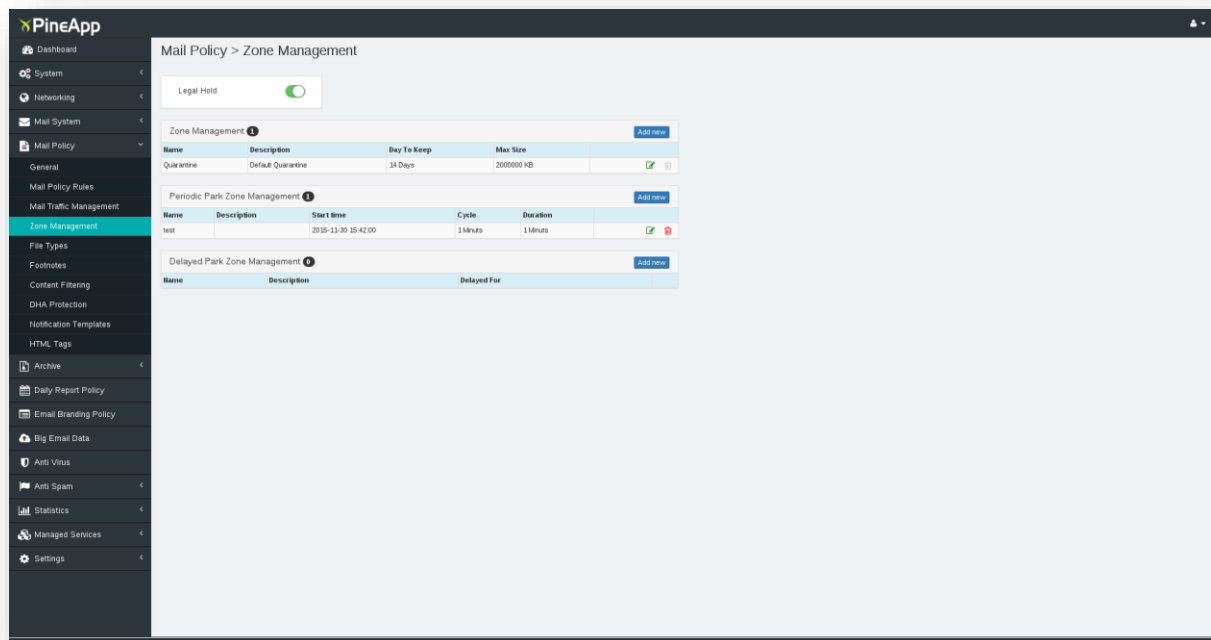
Spam - If an email was blocked because it was deemed as Spam, the score will be displayed.

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 PineApp 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

Click on the **Add new** link, right next to the Zone Management section.

Type in the new quarantine zone's name, the requested maximum number of days to keep quarantine items, and its maximum size.

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.

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.

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**.
- C) The new group will be added to the list of groups in the left pane. The same procedure is done with extensions;
- D) 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 or 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.

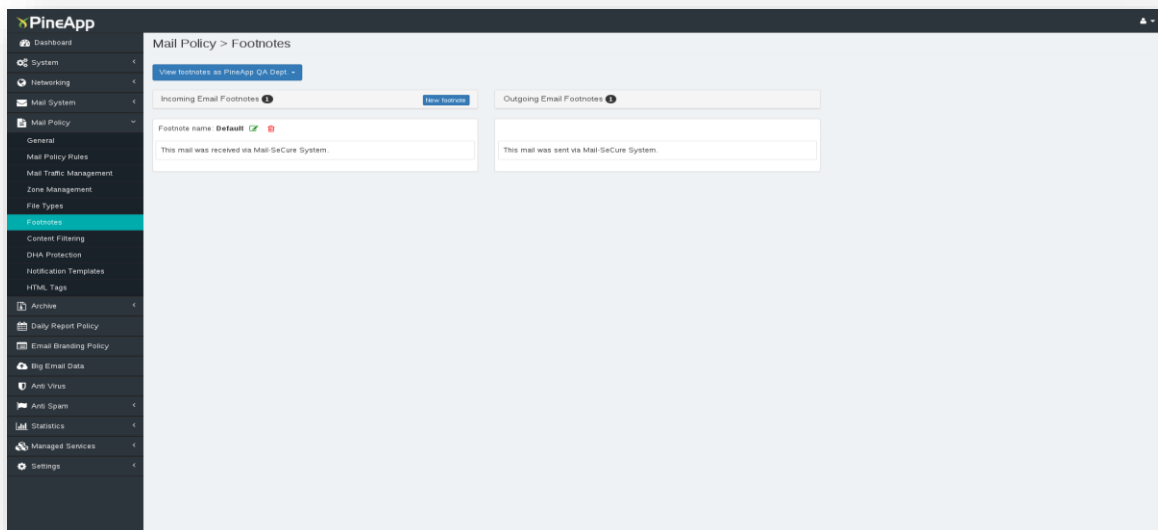
Deleting extensions

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).

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:

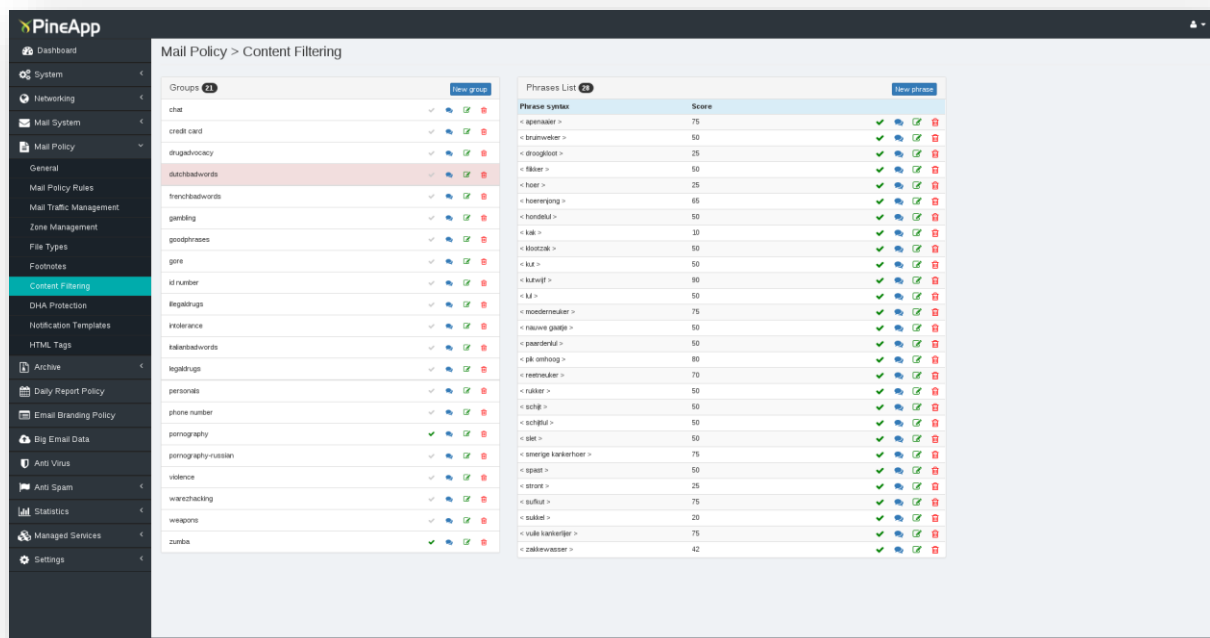
- A) Select the footnote you wish to modify and click on the **edit** link.
 B) Make the required changes in the incoming and/or outgoing footnote's text body.
 C) Click on the **update** button (marked in a blue square in the picture above).

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

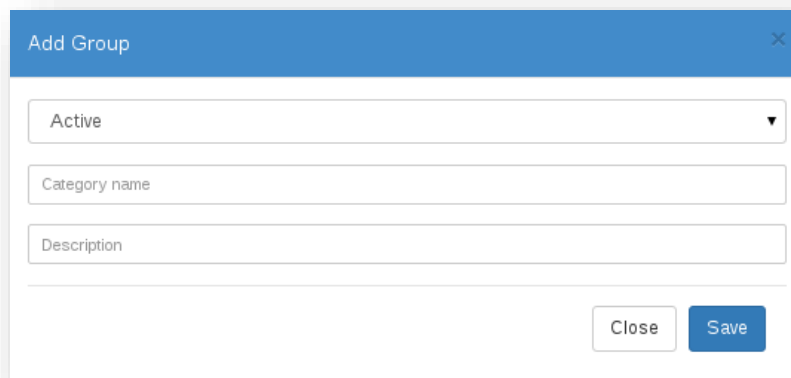
PineApp Mail Secure features 16 pre-configured categories. In order to activate a category, choose from within the drop-down menu the desired category and activate it by clicking on the **activate** button (marked in a red square in the picture above).

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:

Add a Phrase

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).

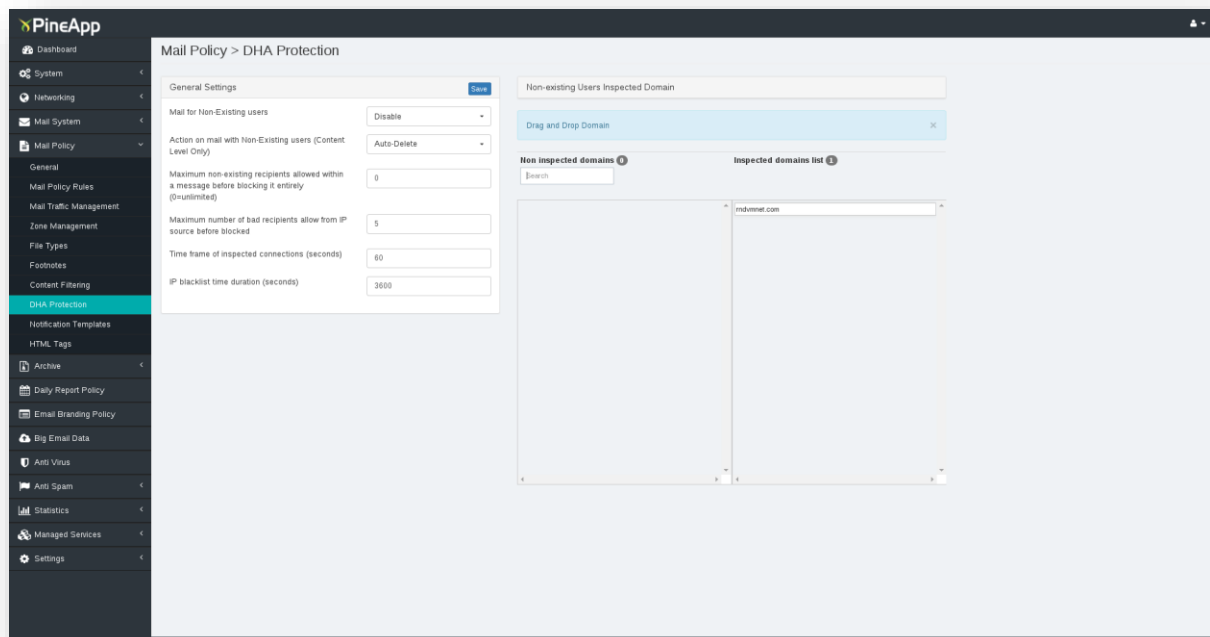
Edit a Phrase



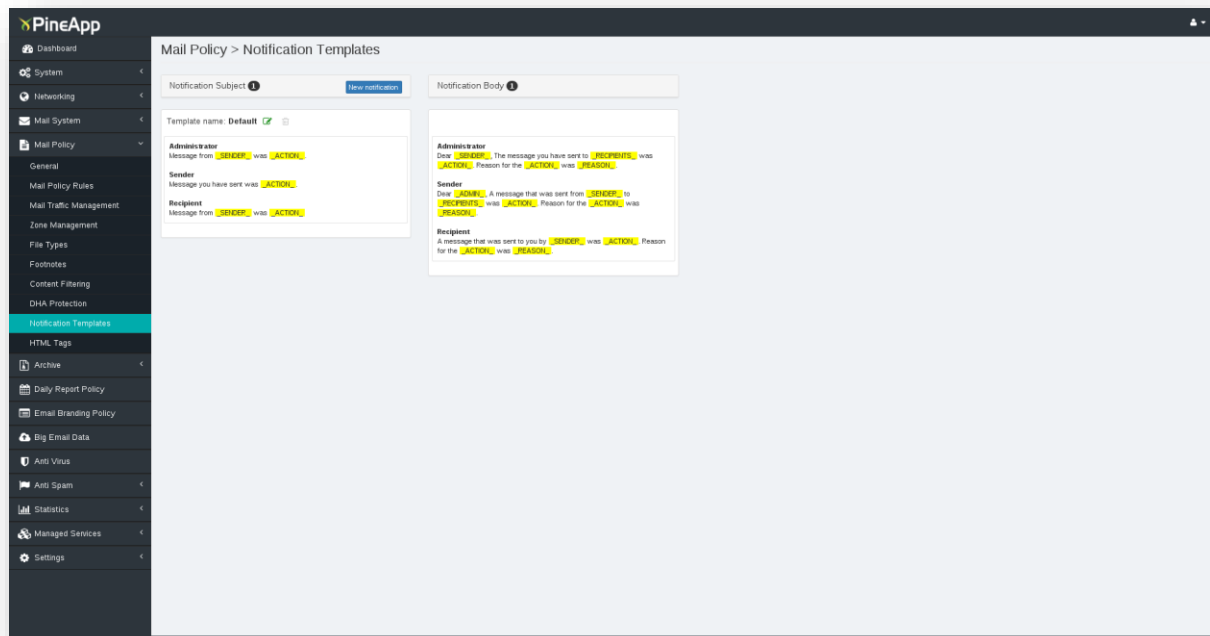
The Scoring System

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.

DHA Protection Tab



Notification Templates Tab



In this tab, notification templates can be defined and assigned to rules.

The PineApp 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

Add Notification
✕

(Subject) Administrator

(Subject) Sender

(Subject) Recipient

(Body) Administrator

(Body) Sender

(Body) Recipient

- 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.

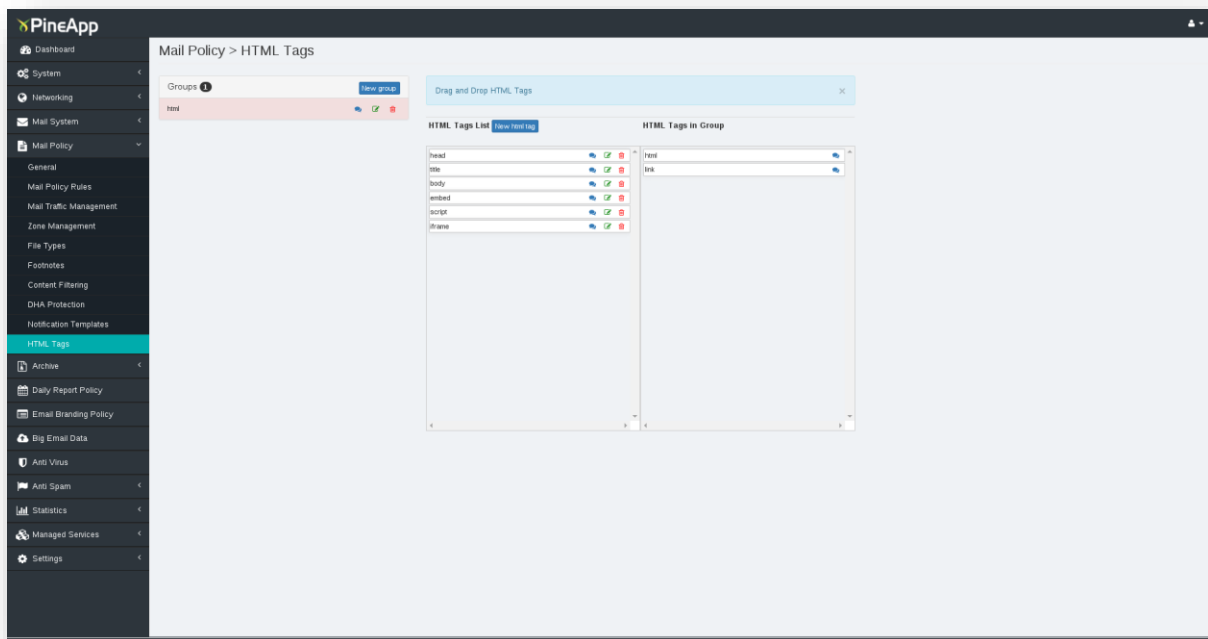
Viewing pre-defined keywords

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

HTML Tags Tab

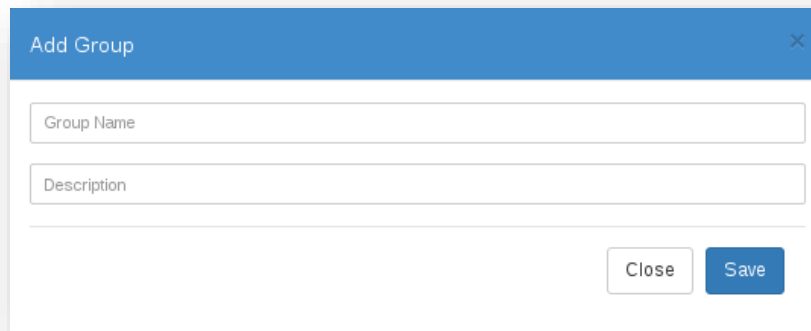


In this tab, HTML tags (groups or specific tags) can be defined in order to assign them to the relevant rule.

Creating tag groups

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

Create HTML Group



- 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).

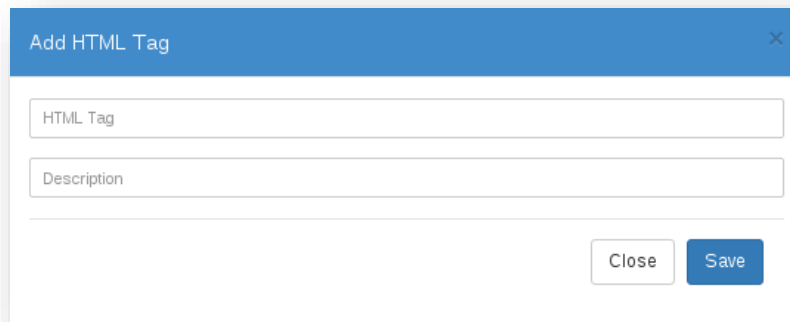
Editing tags

- 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.

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.

Create HTML Tag

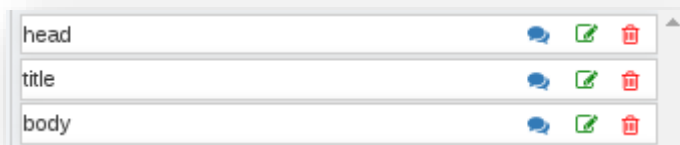











A dialog box titled "Add HTML Tag" with a close button (X) in the top right corner. It contains two text input fields: "HTML Tag" and "Description". At the bottom right, there are two buttons: "Close" and "Save".

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.

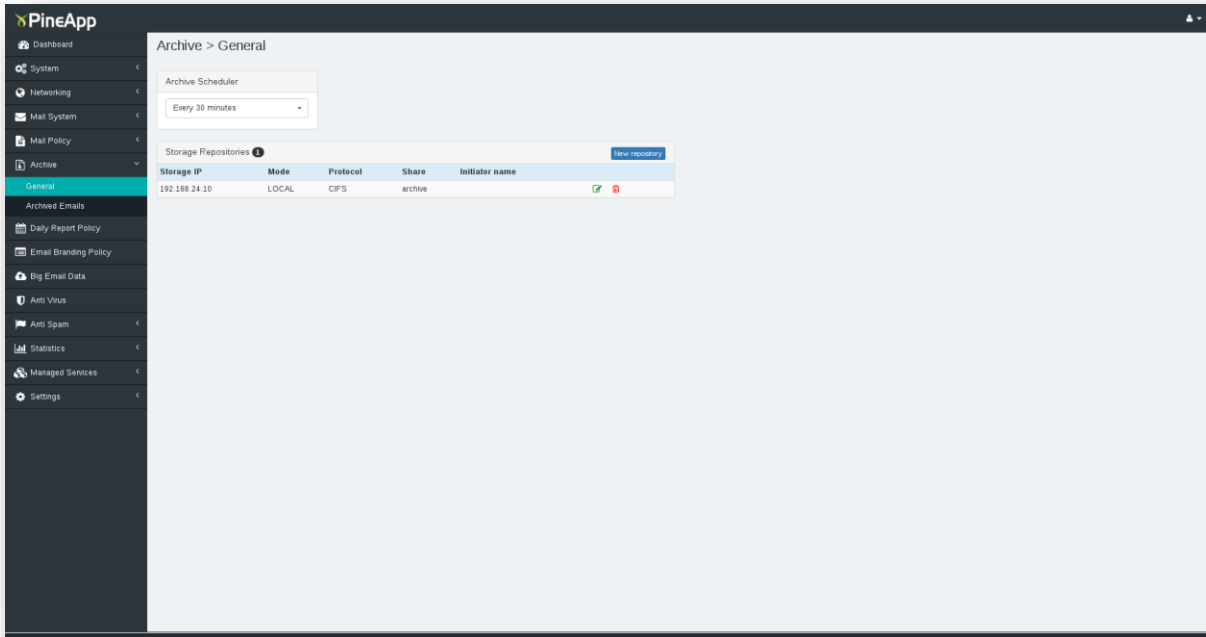
Delete HTML Tag



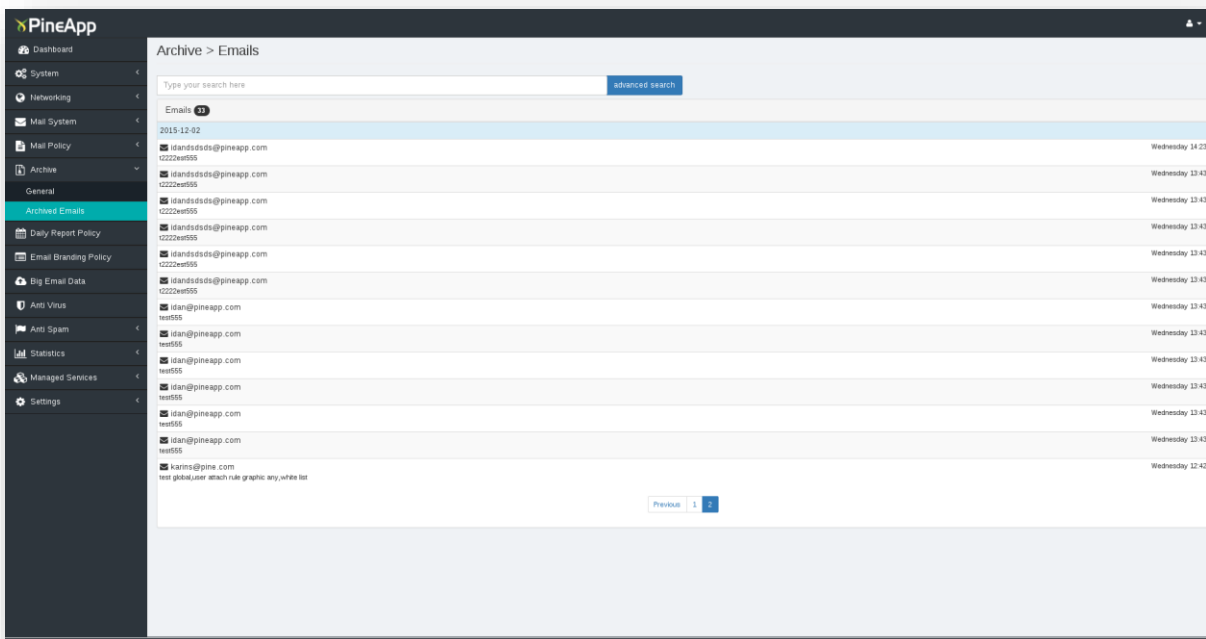
head			
title			
body			



Archive General Tab



Archived Emails Tab

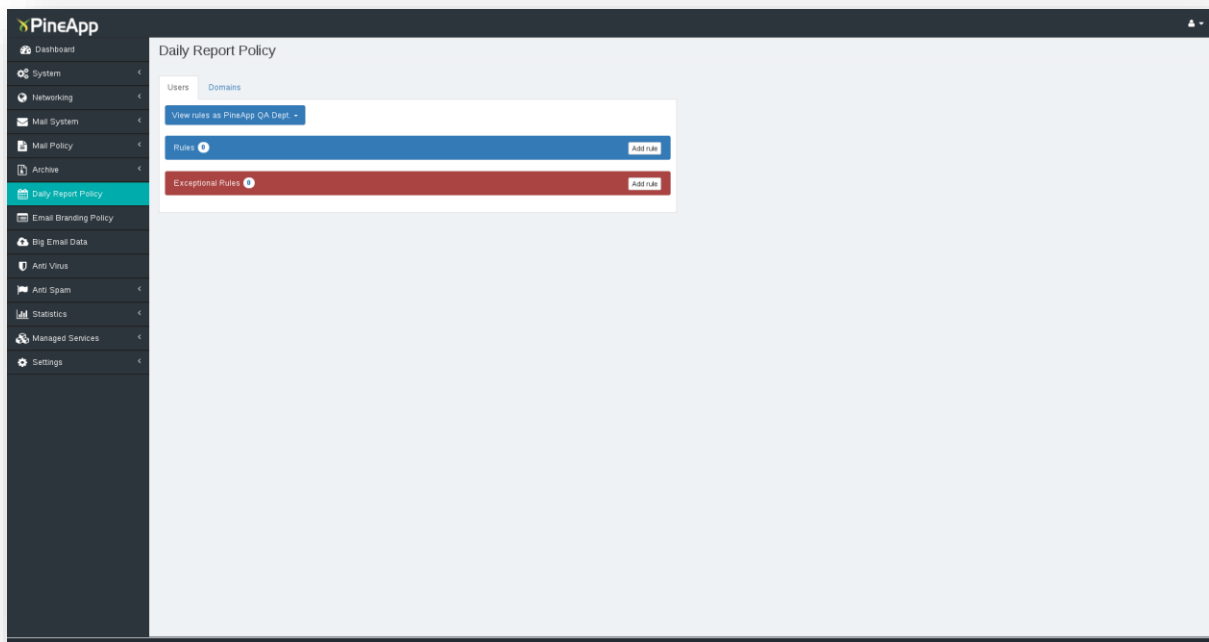




Daily Report Policy

OBJ:OBJ:OBJ:OBJ:

Daily Report Policy Tab



PineApp 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 CYBONET's Managing Spam Manual.

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).

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 were 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.

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 PineApp Mail Secure. The default ports open to PineApp 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 PineApp 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 CYBONET's logo on the top left page of the email. It is possible to replace the logo with the organization's one.



Add Daily Report Rule

Add Daily Report Rule ✕

Time send ▾ English ▾ Enable ▾

Rule name Rule description (optional)

Email address

Users 44

search user

pineapp (pineapp login)	
pavel (pavel)	
vpnt (vpnt)	
eladj (Elad Jochanan)	
createuser (create user)	

Next

Close Save

Add Exceptional Rule

Add Daily Report Rule ✕

Time dismiss ▾ Enable ▾

Rule name

Rule description (optional)

Users 44

search user

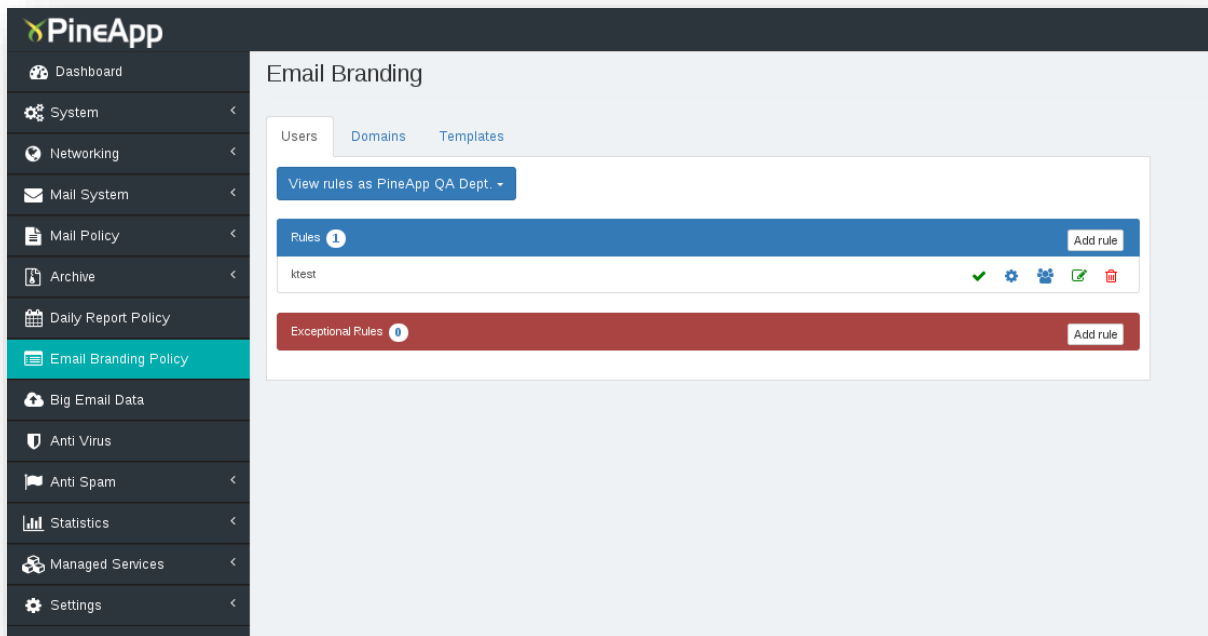
pineapp (pineapp login)	
pavel (pavel)	
vpnt (vpnt)	
eladj (Elad Jochanan)	
createuser (create user)	

Next

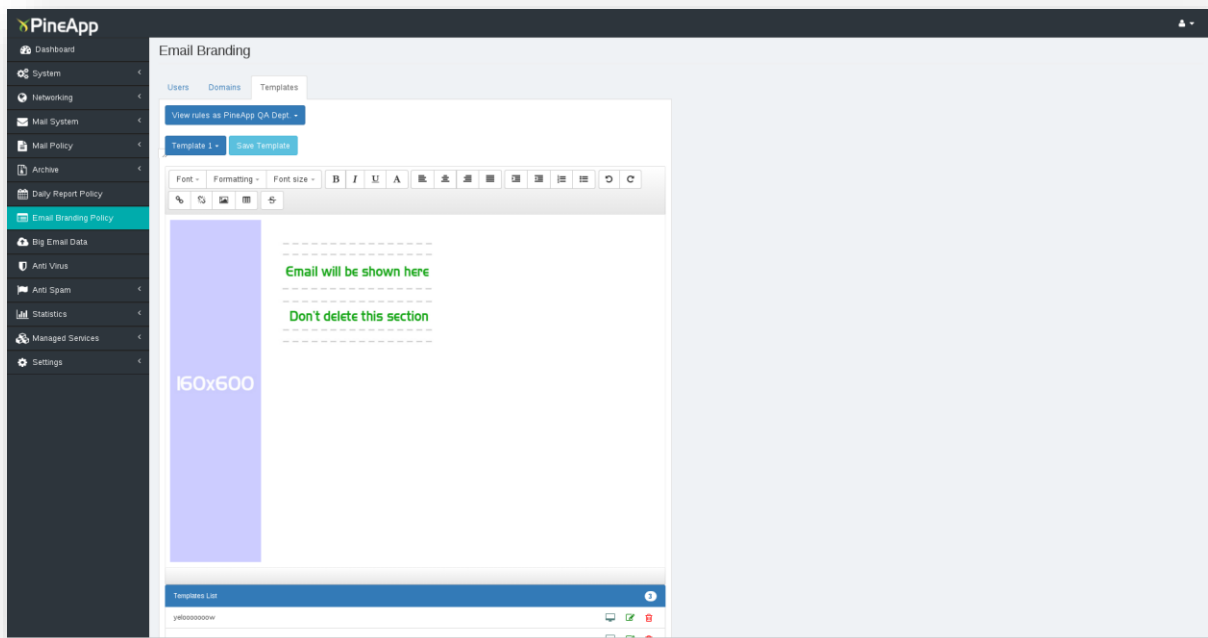
Close Save



Email Branding



Create a Template





Add a New Branding Rule

Add Template Rule ✕

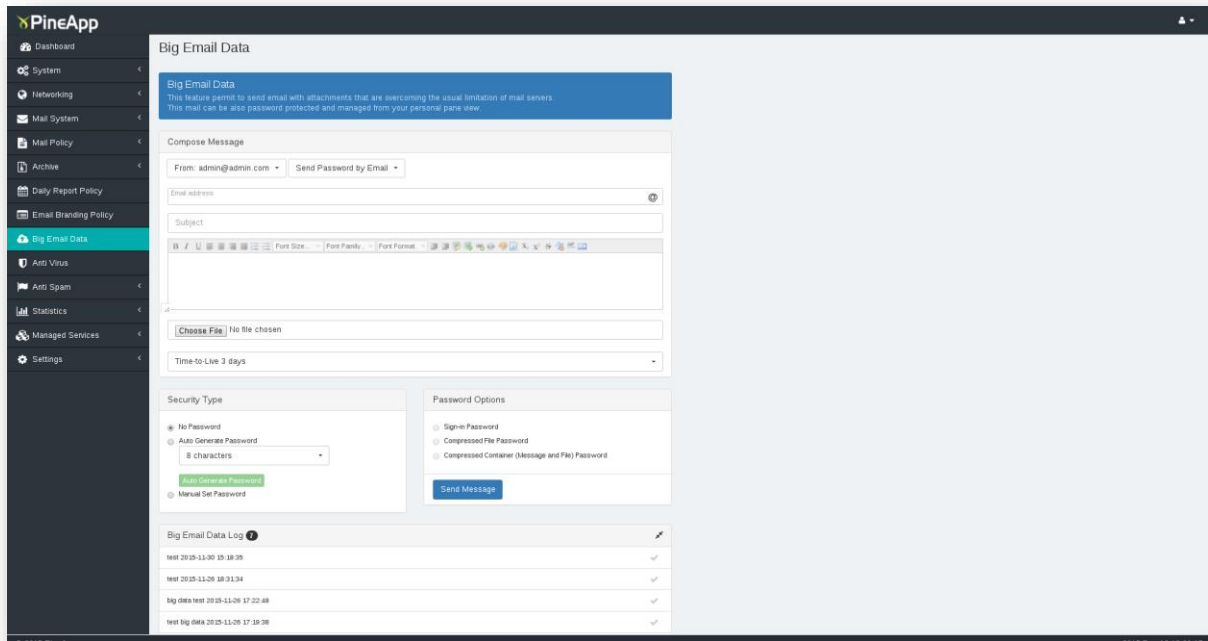
Enable ▾ **Template** ▾

Users 44

pineapp (pineapp login)	
pavel (pavel)	
vpnt (vpnt)	
eladj (Elad Jochanan)	
createuser (create user)	

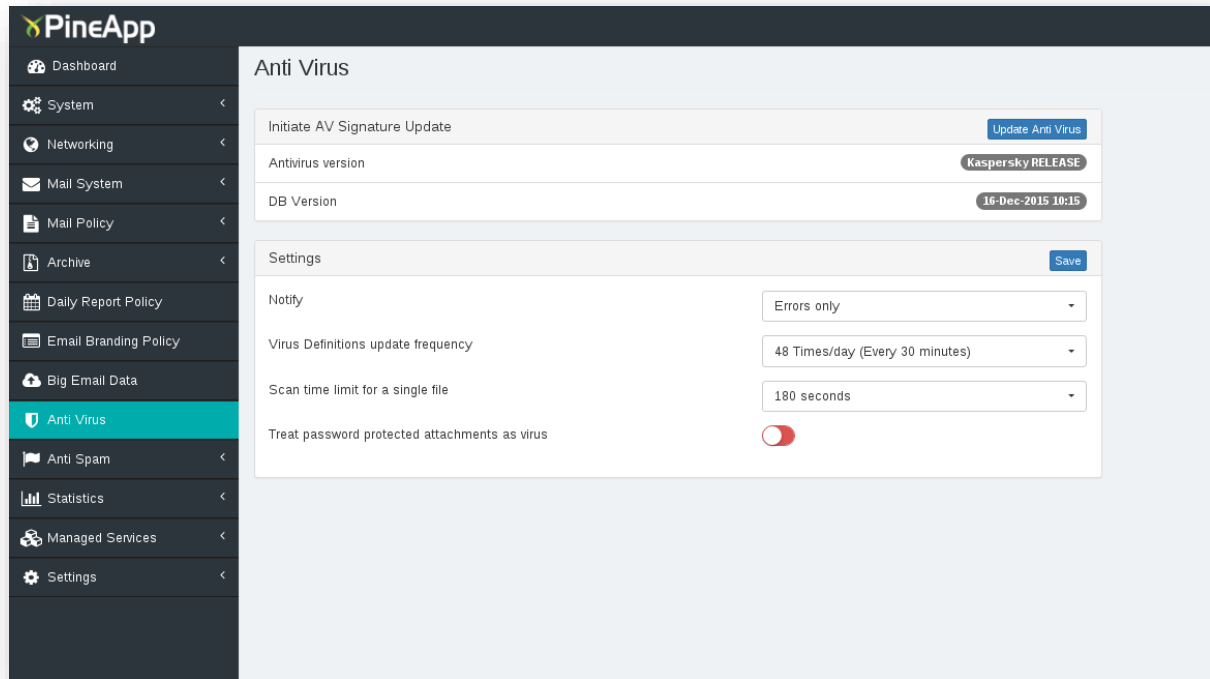


Big Email Data



Anti-Virus Tab

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



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 PineApp 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.

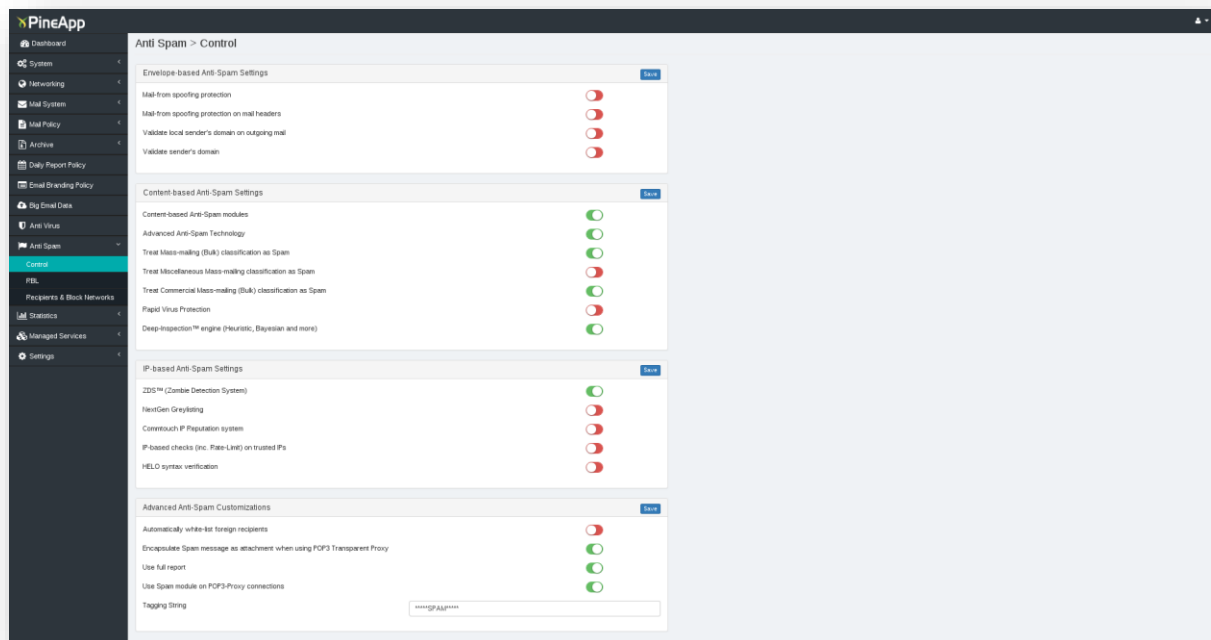
Scan time limit for a single file (seconds) - For some very large files, the scanning time may be relatively long. Usually such files are very suspicious and may contain Viruses. If the scanning time exceeds the value in the field, the scanning will stop and the system will regard the file as infected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



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 PineApp Mail Secure must be identified with their local domain.

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

Validate sender’s domain - When checked, PineApp 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, PineApp 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, CYBONET'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 CYBONET'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 will 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*

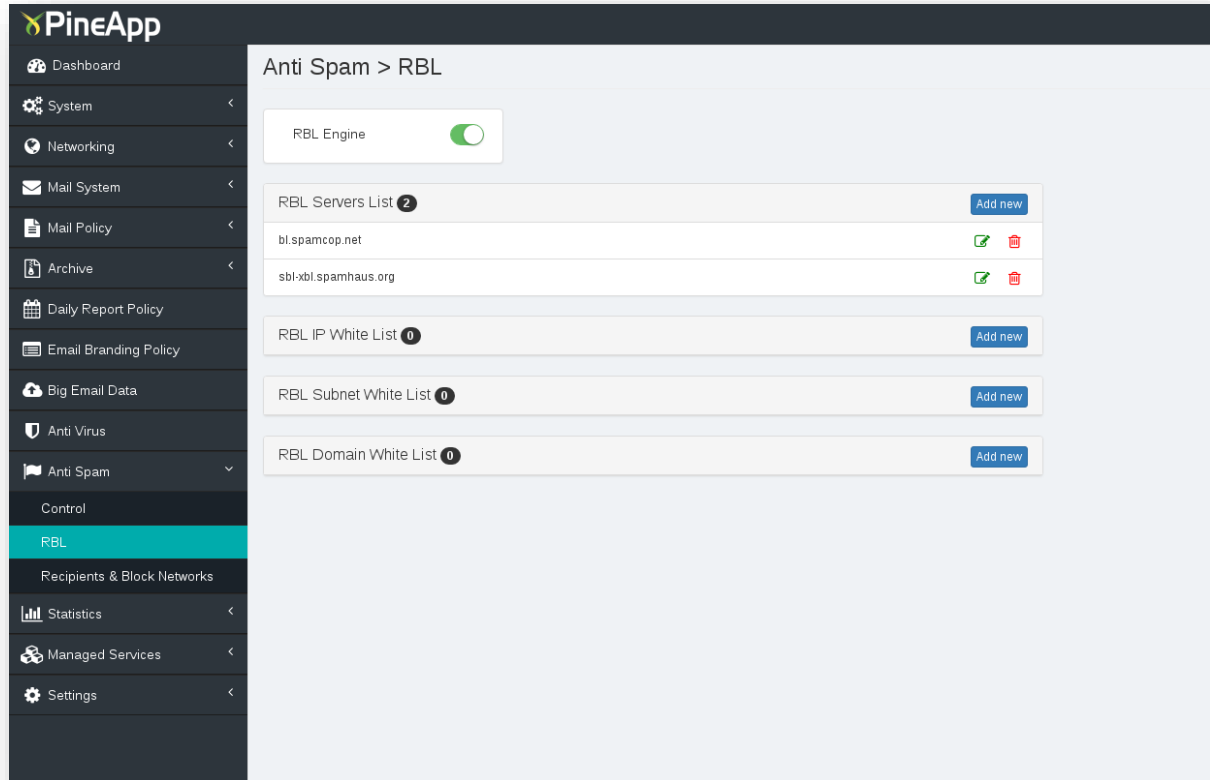
Spam Rules (default - unchecked).

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



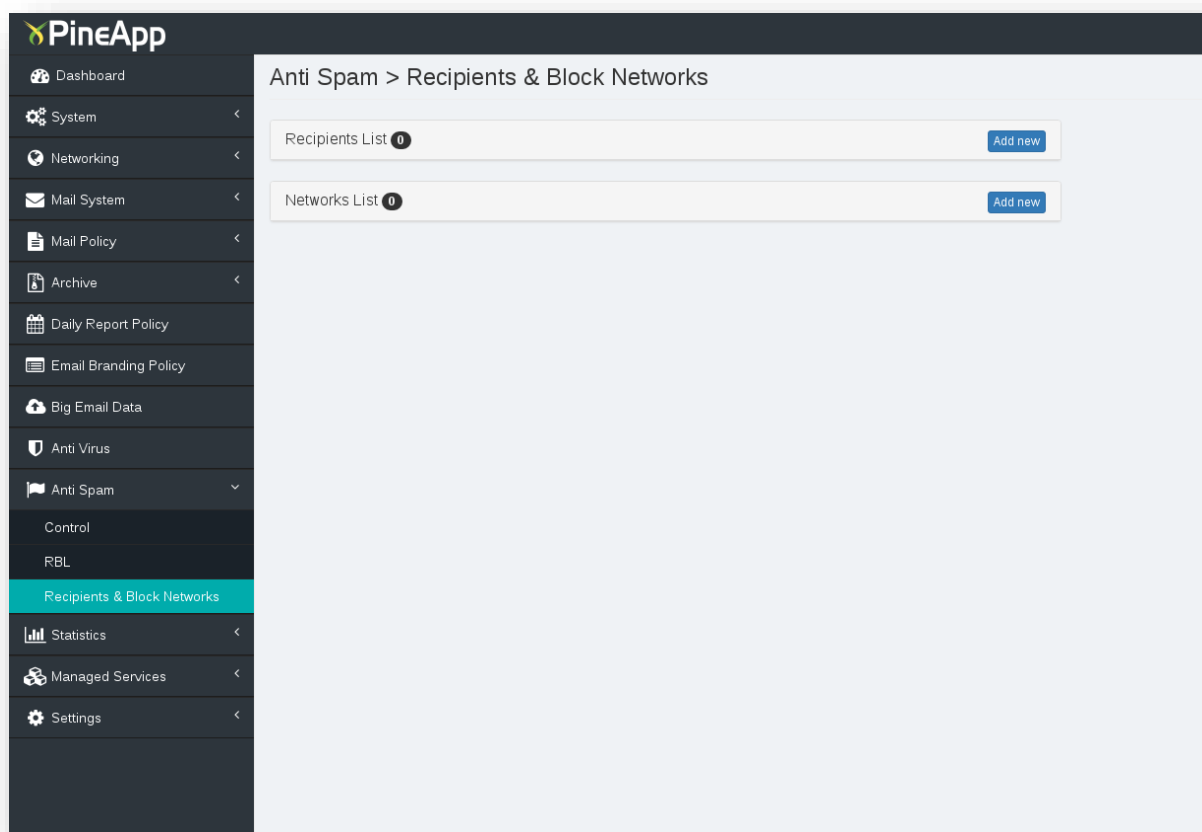
RBL (Real-time Blackhole Lists) engines are external servers that maintain a list of banned mail servers. Most servers are banned because they were identified as spammers. When activated, the system checks the IP address of the session before the mail is accepted by PineApp Mail Secure and rejects mail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

Recipients and Block Networks Tab



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

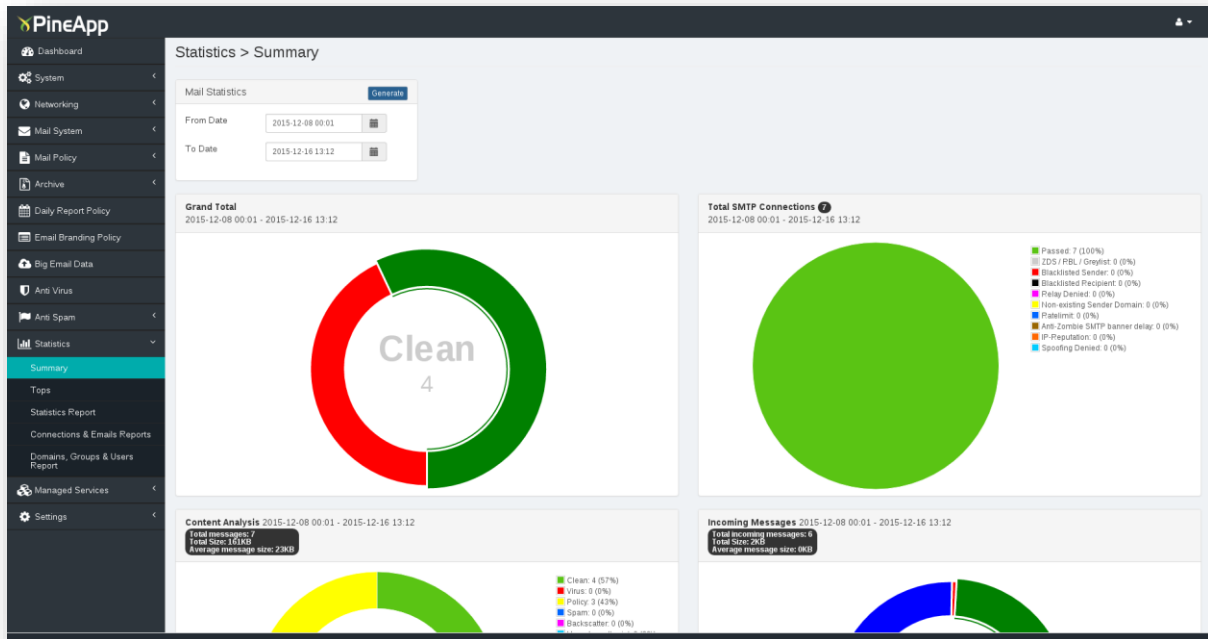
The syntax for adding new blocked recipients is: `user@domain.com`

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.



Statistics Summary Tab



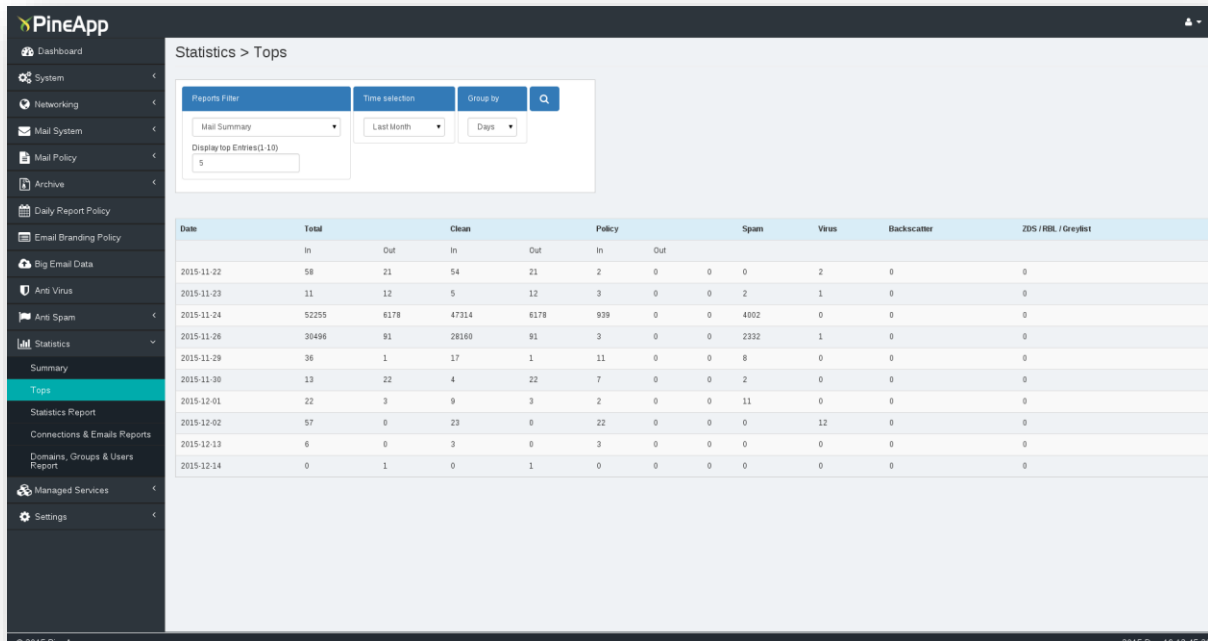
From within the summary tab, general statistics can be viewed.

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).



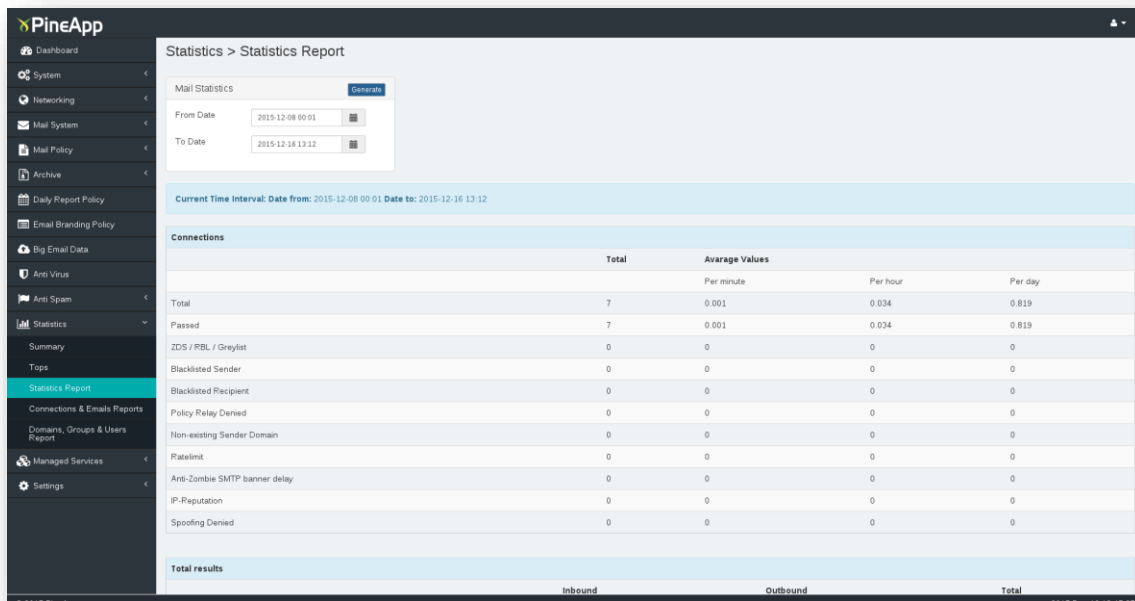
Tops Tab



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.

Statistics & Report Tab

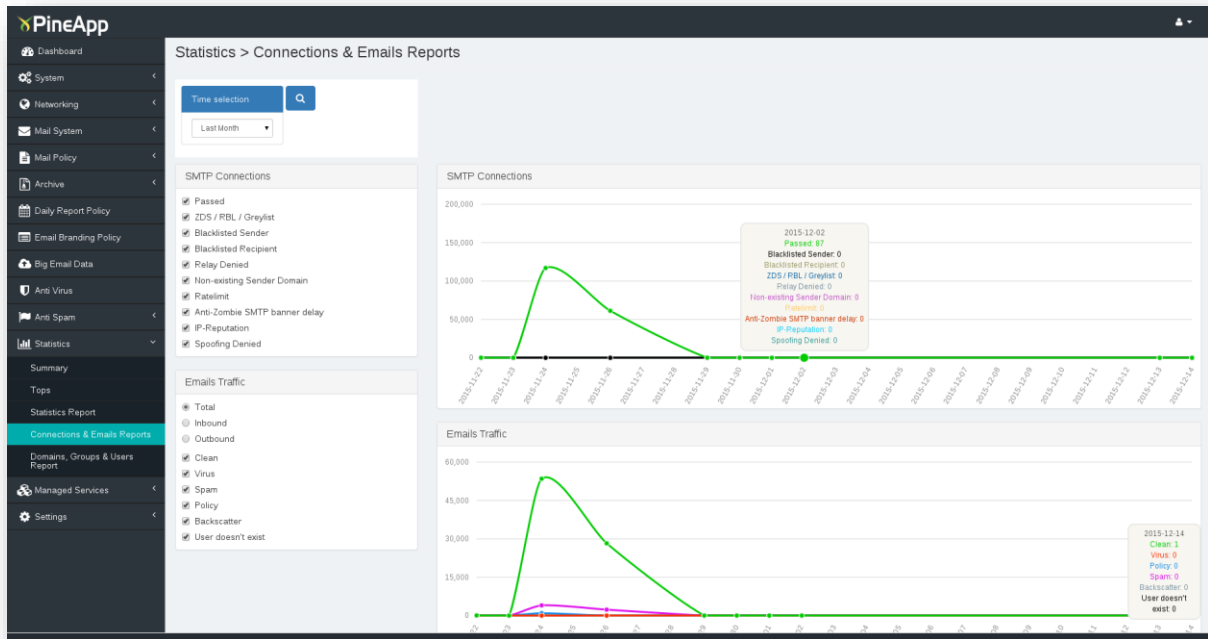


The statistics tab displays various textual statistics.



This tab provides additional information and helps to complete the information needed for the administrator

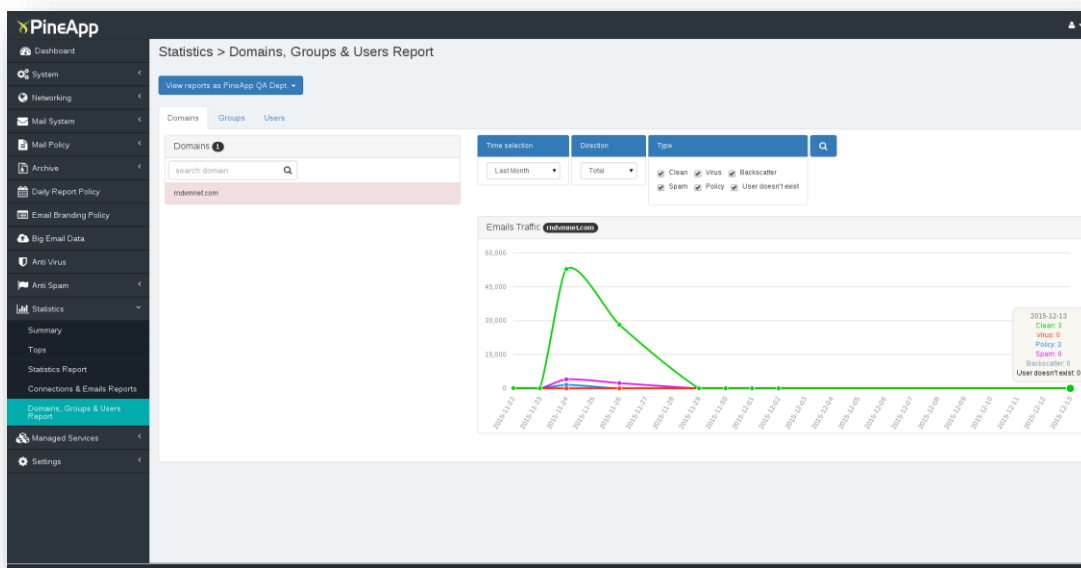
Connections & Emails Report Tab



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.

Domains, Groups & Users Report 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 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).



Managed Services Customers & Units Allocation Tab

PineApp
🔔

- Dashboard
- System
- Networking
- Mail System
- Mail Policy
- Archive
- Daily Report Policy
- Email Branding Policy
- Big Email Data
- Anti Virus
- Anti Spam
- Statistics
- Managed Services
 - Customers & Units Allocation
 - Settings

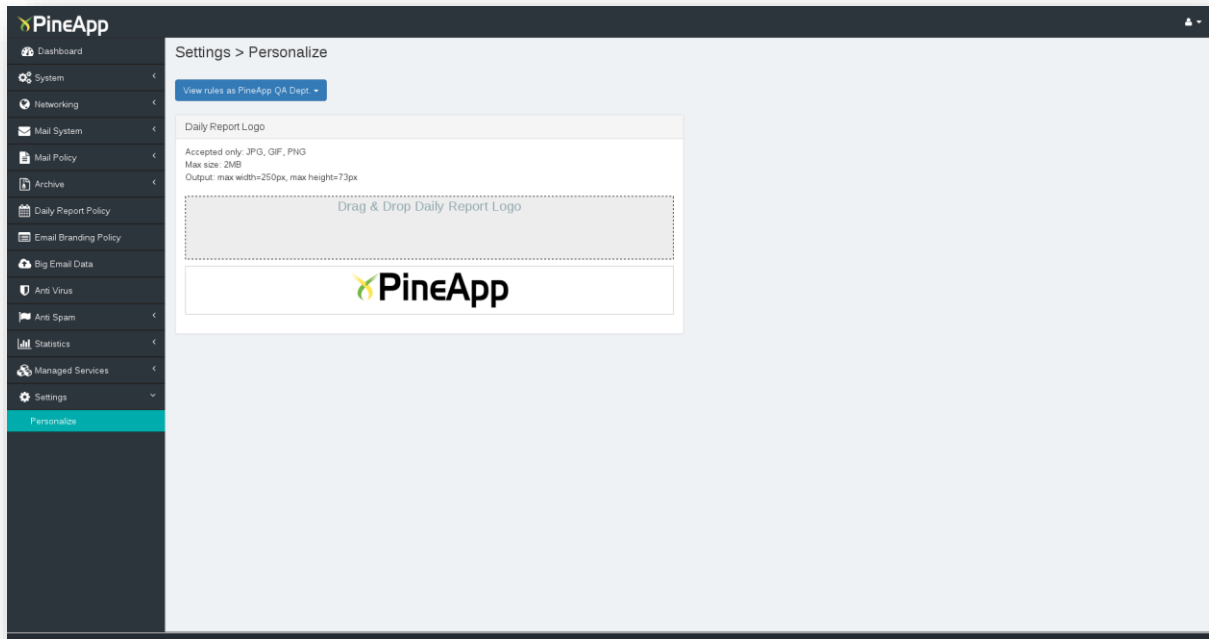
Managed Services > Customers & Units Allocation
🔍

View customers as PineApp QA Dept. +

Customers
Units Allocation
New customer

Customer Name	Active	Type	Allow Allocate	Email	Phone	Configure by Owner	Amount of Users	Amount of Domains	Allocations	Actual Use	Remained
PineApp QA Dept.	✔	ISP	✔	solution@owner.com	11-1111111	-	50000	1000	-	-	✔
test	✔	Customer	✔	karina@pineapp.com	111	✔	10	2	Users: 0 Domains: 0 Connectors: 0	Users: 0 Domains: 0	Users: 10 Domains: 2 ✔

Settings Personalize Tab



CONFIGURING THE FIREWALL

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

Ports from the world (WAN) to PineApp 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 PineApp 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