

# **PineApp™ Archive-SeCure™**

## **User Manual**

**3000/5000 series**

October 2008

© 2001-2008 PineApp Ltd. All Rights Reserved.

The information in this guide is furnished for informational use only, and is subject to change without notice and should not be construed as a commitment by PineApp Ltd. PineApp Ltd. 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 PineApp Ltd., as long as this copyright notice remains intact and unchanged on all copies.

PineApp Ltd. and Archive-SeCure are trademarks of PineApp Ltd. All other names and trademarks are the property of their respective owners.

**PineApp International**

8, Hata'asia Street

Nesher, 36601

Israel

Tel. +972 4 8212 321

Fax. +972 4 8203 676

<http://www.PineApp.com>

support@pineapp.com

## **Table of contents:**

<b>Chapter 1 Introduction .....</b>	<b>1-1</b>
Accessing Archive-Secure™ Via A Web-Browser .....	1-2
<b>Chapter 2 Configuration.....</b>	<b>2-1</b>
<b>Server Tab .....</b>	<b>2-2</b>
Time Zone.....	2-2
Hostname .....	2-2
Adding A New DNS Server.....	2-2
Adding A New Mount Point.....	2-3
<b>Domains Tab .....</b>	<b>2-4</b>
Adding A New Domain .....	2-4
Editing An Existing Domain.....	2-4
Deleting An Existing Domain.....	2-4
<b>Login Tab.....</b>	<b>2-5</b>
<b>Volumes Tab.....</b>	<b>2-6</b>
Email Encryption Password .....	2-6
Automatically Create And Rollover To New Volumes.....	2-6
Adding A New Volume .....	2-7
Volume Status Table .....	2-7
<b>Journal Accounts Tab .....</b>	<b>2-8</b>
Pre Installation Exchange Server Configuration .....	2-8
Archive-SeCure's Exchange Features .....	2-9
Creating A Journal Account.....	2-9
Enable Journaling On Microsoft Exchange.....	2-9
Enable Envelope Journaling .....	2-10
Adding A Journal Account Connection .....	2-10
<b>Archive Rules Tab .....</b>	<b>2-11</b>
Adding A New Archive Rule .....	2-12
Deleting An Archive Rule .....	2-12
<b>Retention Tab .....</b>	<b>2-13</b>
<b>Listeners Tab.....</b>	<b>2-14</b>
Listen For Incoming Exchange/SMTP Requests.....	2-14
Exchange/SMTP Port.....	2-14
Bind IP Address.....	2-14
Restrict Incoming Connections.....	2-14
<b>Roles Tab.....</b>	<b>2-15</b>
Built-In Role Permissions .....	2-15
<b>General Tab.....</b>	<b>2-17</b>
Archive Settings.....	2-17
Recover Emails .....	2-17
Index Settings .....	2-17
Mail Server SMTP Connection Settings.....	2-18
Viewing Log's Contents .....	2-19
<b>Status Reports Tab .....</b>	<b>2-23</b>
Send Status Reports To Administrator At Regular Intervals.....	2-23
Admin Email .....	2-23
Send Report .....	2-23
<b>About Tab .....</b>	<b>2-24</b>
Updating The Appliance's License.....	2-24
<b>Chapter 3 Search .....</b>	<b>3-1</b>
Search Queries.....	3-1
<b>Appendix A: Status Report Delivery Example</b>	

# CHAPTER 1

## Introduction

Archive-SeCure™ is an easy-to-use, yet feature-rich, email archiving system. It works in conjunction with popular mail systems such as Microsoft Exchange to archive all incoming, outgoing and internal emails. It enables you to enforce strict email retention, monitoring and compliance policies throughout your organization.

In many jurisdictions around the world, the law requires that company emails are kept for up to seven years. Archive-SeCure is designed to help you comply with legislation such as the Sarbanes Oxley act (SOX), Gramm-Leach Bliley act (GLBA) and the Freedom of information act (FOIA).

Archive-SeCure employs highly scalable search engine technology. A Google-like web interface is provided, enabling auditors and employees to search through tens of millions of emails at the click of a button.

In contrast to many other email archiving systems, Archive-SeCure stores emails directly on the file system. This design allows you to avoid the pitfalls associated with storing information in a database; namely: high maintenance costs, size restrictions, backup complexity and increased potential for total data loss.

Archive-SeCure stores your email in standard Internet mail format (RFC822). RFC822 is the standard format for storing and transporting email messages on the Internet. Thus, Archive-SeCure ensures that your information will remain accessible over the long-run.

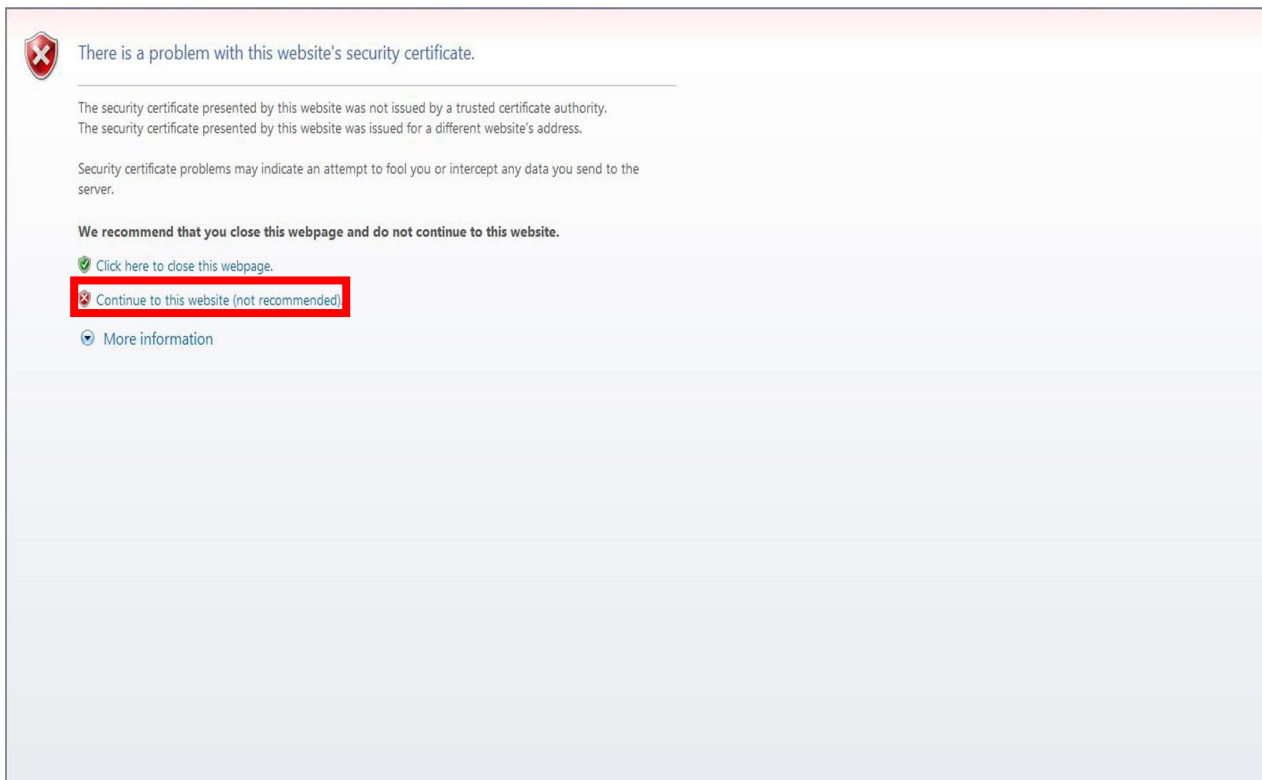
## **Accessing Archive-SeCure™ via a web-browser**

Archive-SeCure™ is accessed easily using any common web browser.

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

To access Archive-SeCure for the first time you need to type the default IP address of your appliance which is <https://192.168.24.26:7443>. If you have any trouble connecting, check your firewall setting and be certain that it is configured for this IP range. To access your appliance without having to make changes to your firewall settings, you can simply create a static route to the device in your firewall. Once you have logged into the device you can change the IP address.

A security alert message will appear. Click **OK** to continue. In IE 7.0, an error page will be displayed (as seen in the picture below).



Click on **"Continue to this website (not recommended)"** (marked in a red square in the picture above) in order to continue.

The following login window will be displayed.



Log into the system, using the default username (**pineapp**) and the default password (**password**).

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

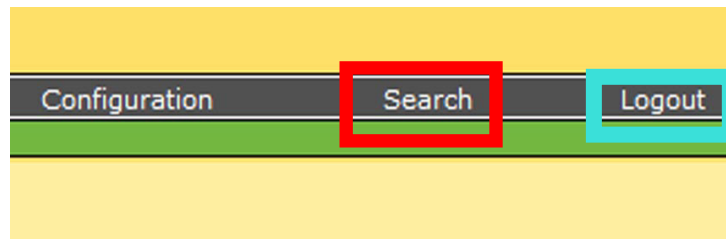
Upon entry, the System Information pane will be displayed.

# 2

## CHAPTER

### Configuration

The Archive-SeCure web interface is divided into two main sections, Configuration & Search. The configuration section is divided into 13 tabs, each one concerns different aspects of the appliance's settings' adjustment and configuration.

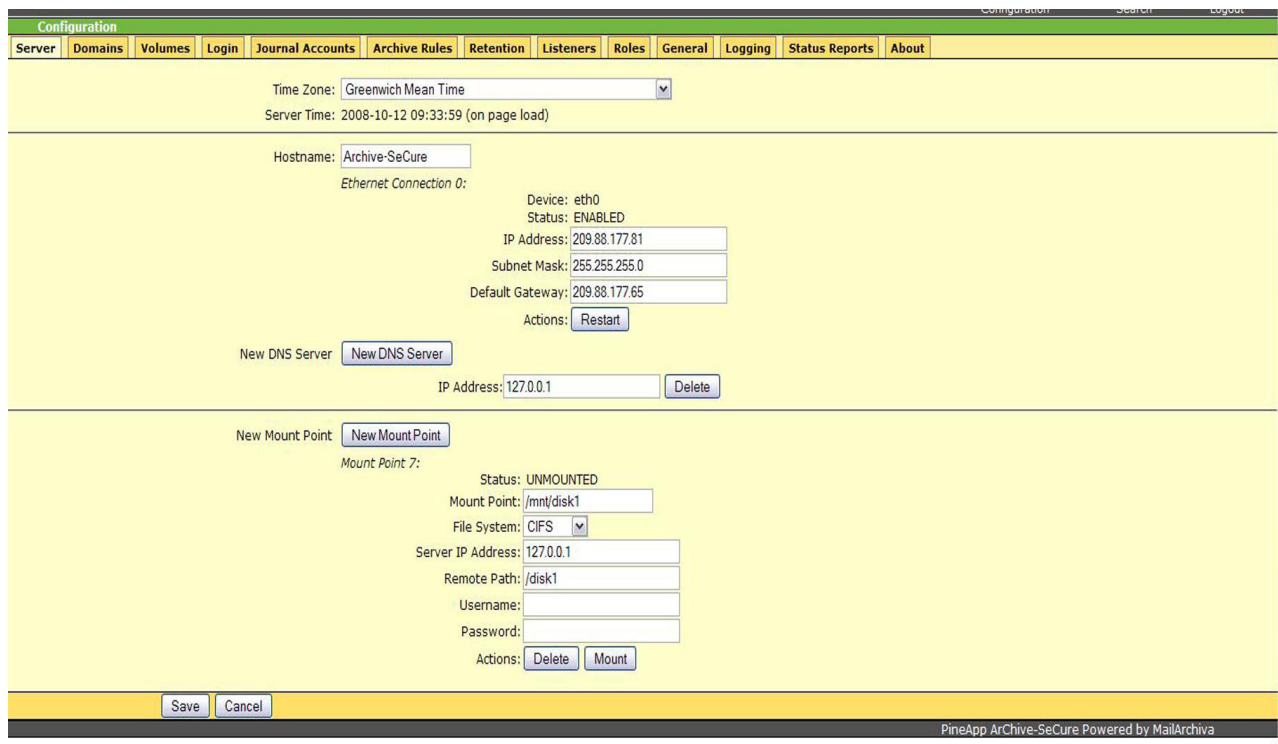


In order to enter the Configuration section, simply click on the **Configuration** link (marked in a red square in the picture above).

In order to log out of the appliance appropriately, click on the **Logout** link, next to the Configuration and Search links (Marked in a light blue square in the picture above).

## Server Tab

The Server tab contains networking related configuration settings, along with additional system settings.



The screenshot shows the PineApp configuration interface for the Server tab. At the top, there is a navigation bar with tabs: Configuration, Domains, Volumes, Login, Journal Accounts, Archive Rules, Retention, Listeners, Roles, General, Logging, Status Reports, and About. The Configuration tab is active. Below the navigation bar, the interface is divided into several sections. The first section contains a Time Zone dropdown menu set to 'Greenwich Mean Time' and a Server Time display showing '2008-10-12 09:33:59 (on page load)'. The second section is for Hostname configuration, showing 'Archive-SeCure' as the current hostname. Below this, it lists Ethernet Connection 0 details: Device: eth0, Status: ENABLED, IP Address: 209.88.177.81, Subnet Mask: 255.255.255.0, and Default Gateway: 209.88.177.65. There is a Restart button for this connection. The third section is for New DNS Server configuration, showing a text field for IP Address set to '127.0.0.1' and a Delete button. The fourth section is for New Mount Point configuration, showing a text field for Mount Point set to '/mnt/disk1', File System set to 'CIFS', Server IP Address set to '127.0.0.1', Remote Path set to '/disk1', and fields for Username and Password. There are Delete and Mount buttons for this mount point. At the bottom, there are Save and Cancel buttons. The footer of the interface reads 'PineApp Archive-SeCure Powered by MailArchiva'.

**Time Zone** – the appliance’s clock can be adjusted using the Time Zone from the dropdown menu (city, country, region or GMT time zone based choice).

**Hostname** – This text field determines the canonical hostname (network identifier) of the device (Archive-SeCure by default).

The appliance’s assigned interfaces are listed below the Hostname field, according to their interface name (ETH0, ETH1 etc.)

To change the settings of an existing and functioning interface, edit the IP address, subnet mask & default gateway fields accordingly, and click on the Restart button.

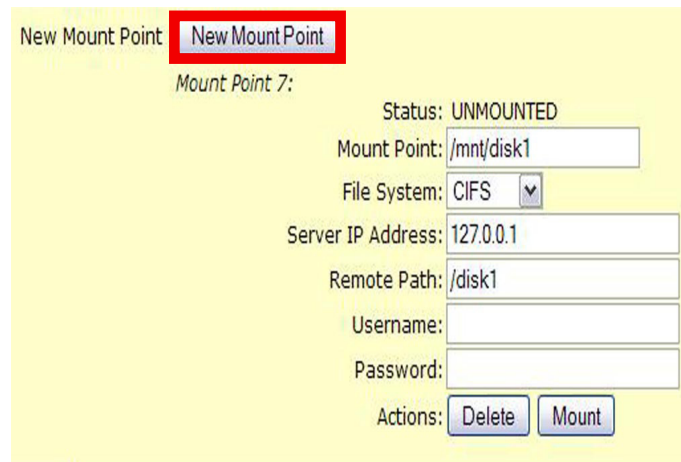
**Adding a new DNS server** – To add a new domain name server, simply type it in the text field under the **New DNS Server** section.

\*Archive-SeCure has an internal DNS-Cache system. If you wish to use it (127.0.0.1), please confirm that port 53 (TCP and UDP) is open from Archive-SeCure to the world on your organization’s firewall. If you wish to use a different DNS server, please confirm that it is properly configured.

To delete a certain record, click on the **Delete** button on the DNS record’s right side.



**Adding a New Mount Point** - In case you're using an external storage device, you need to configure a local mount point for it as follows:



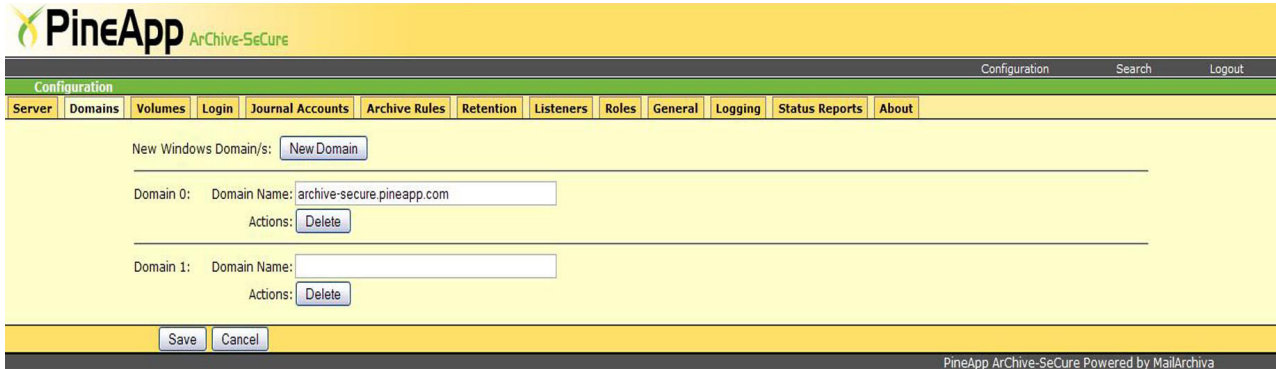
- a. Click on **New Mount Point** (marked in a red square in the picture above).
- b. Type the local mount folder path in the **Mount Point** field. It is recommended to leave the mount point's default setting (/mnt).
- c. Choose your storage point's file system method from the **File System** dropdown menu.
- d. Type the remote server's IP address in the **Server IP address** field.
- e. Type the detailed remote storage folder path in the **Remote Path** field.
- f. Type in the remote server's authentication credentials (**username & password**) in the corresponding fields.
- g. To finish, click on **Mount**.

Note:

Do not forget to save any change made to your settings, using the **Save** button at the bottom of the screen.

## Domains Tab

The Domains tab contains a list of all the appliance's handled domains.



When configuring Archive-SeCure for the first time, you need to add one or more of your organization's domains.

### **Adding a new domain -**

- a. Click on the **New Domain** button.
- b. Type the domain name ("company.com" or "company.local", for example).

**Editing an existing domain** – in order to edit an existing domain's name, simply retype the desired name in the text field where the old domain name is written, and click on the **Save** button at the bottom of the page.

**Deleting an existing domain** – in order to delete an existing domain, simply click on the **Delete** button underneath the text field where its name is written.

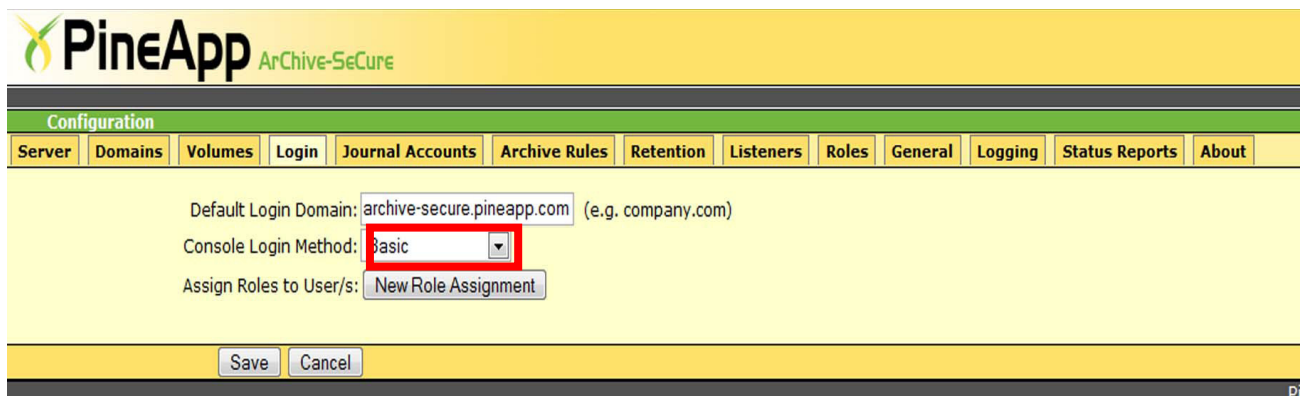
The entered domains are used by the server to assess whether the origin and destination of emails are internal or external to your organization. When applying archive rules, the server will match the domain of a given email address with all of the domains entered here.

### Please note

If your organization has an internal domain called "company.local" and an external one called "company.com", you need to include both these domains in your configuration.

## Login Tab

The login tab contains assigned user's manual creation and automatic synchronization (from all existing library server brands) features.



**Default login domain** - this text field contains the organization's default domain name (for example: company.com).

### Adding a new assigned user (role)

There are a few available methods for assigning roles on the organization's users. The preferred method can be chosen from the dropdown menu (marked in a red square in the above picture).

**Basic** – Choose this option for registering and manually assigning new roles.

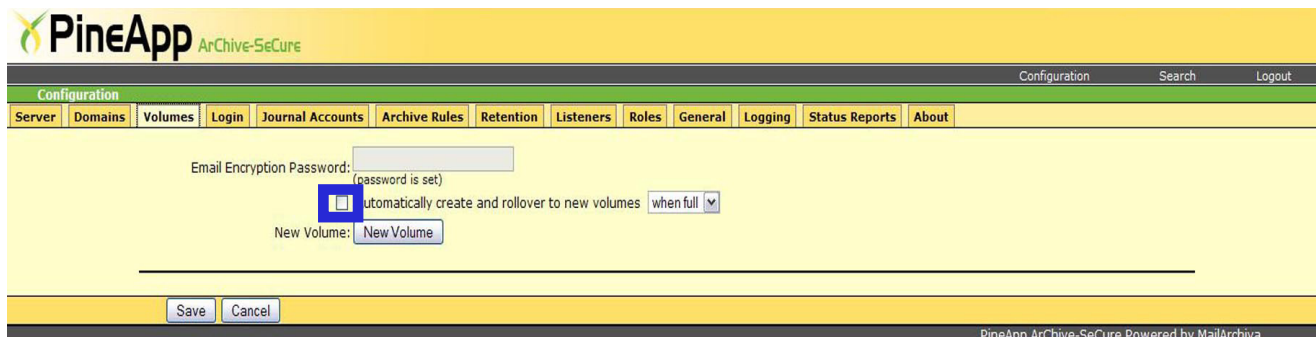
**Active Directory** – Choose this option for synchronizing and importing all of the organization's users automatically (including automatic default role assignment), from any Microsoft based server (Exchange, Windows 2003 etc.).

**LDAP** – Choose this option for synchronizing and importing all of the organization's users automatically (including automatic default role assignment), from all other non-Microsoft based servers (Lotus Notes, Iplanet etc.).

**IMail** – Choose this option for synchronizing and importing all of the organization's users automatically (including automatic default role assignment), in case you use IMail™ mail server.

## Volumes Tab

Archived emails are organised into one or more volumes. Each volume consists of an index and a store. The index is used to enable auditors to perform efficient search queries on the archived data. The store consists of multiple sub-directories where the Archived information is kept.



**Email Encryption Password** - all emails are encrypted using triple DES password-based encryption. Before using the server to archive emails, you need to choose and enter an Email Encryption Password in the Volumes tab of the Configuration screen.

Bear in mind, the password you enter is irrecoverable, so it is very important that you remember it. Furthermore, since the password holds the key to your archived emails, you need to ensure that the password is kept highly confidential and secret. It is also important to bear in mind that you cannot change the password once the server has begun to archive emails.

**Automatically create and rollover to new volumes** – upon checking this option (marked in a blue square in the picture above), Archive-SeCure will automatically create new volumes once the certain picked condition is fulfilled.

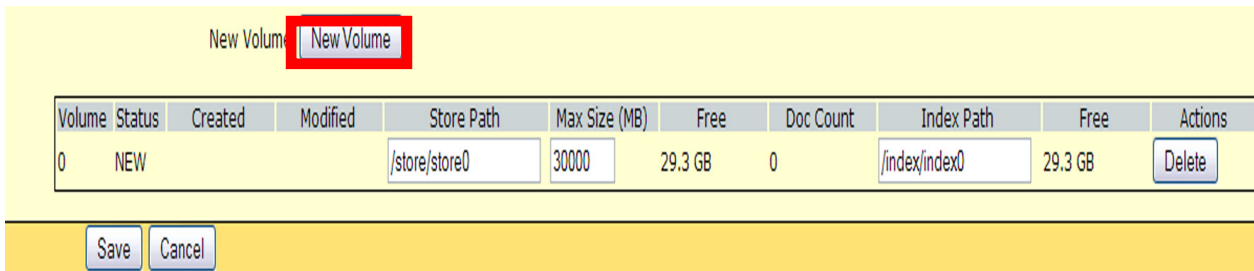
Condition dropdown menu – the dropdown menu on the right of the feature contains the following conditions:

**When full** – whenever one volume reaches its full capacity, a new volume will be created.

**Monthly/Quarterly/Annually** – Close all volumes exactly one month/quarter/year from their creation.

When creating a volume, the index path and store path can refer to any location on one or more hard disks. Furthermore, volumes are defined in terms of their order of preference. When a volume has reached its size limit, the server will automatically switch over to the next available volume on the list. This mechanism allows one to archive information on multiple hard disks, without necessitating manual intervention.

## Adding a new volume -



- Click on the **"New Volume"** button (marked in a red square in the picture above) in the Configuration screen.
- Enter a path for the store and index (e.g. "c:\store" and "c:\index"). If you've created more than one volume, click the **"Up"** and **"Down"** buttons to organise them according to your order of preference.

Once you've created a volume, you'll notice that it is assigned the **"NEW"** status, as described in Table 5 below. Volumes have a lifecycle of their own. Once the archiving process begins, the server will automatically switch over to the first unused volume on the list. This volume will become the active volume until such time as its maximum size is exceeded, the disk is full, or the administrator independently decides to close it. Once a volume is closed, no further data can be written to it and it cannot be reopened.

If at any stage during the archiving process, the server finds that an active volume is not available, it will always activate the next unused volume on its list. Assuming there are no remaining unused volumes available, the server will stop the archiving process until a new volume is added.

### Volume Status Table

Volume Status	Description
NEW	The volume has just been created and has not been saved.
UNUSED	The volume has been saved but it does not contain any information.
ACTIVE	The volume is currently being used for archiving purposes.
CLOSED	The volume is searchable, however, no further information can be written to it.
UNMOUNTED	The volume is not searchable, nor can it be made active.
EJECTED	Volume was removed without explicitly unmounting it.
REMOTE	The volume's index resides on a remote machine. The volumes store must still be held locally.

When using removable disks, it is not recommended to remove the disk containing the active volume data without closing the volume first. You may remove any physical disk containing a closed volume. When doing so, is it usually a good idea to explicitly unmount the volume, although this is not absolutely necessary.

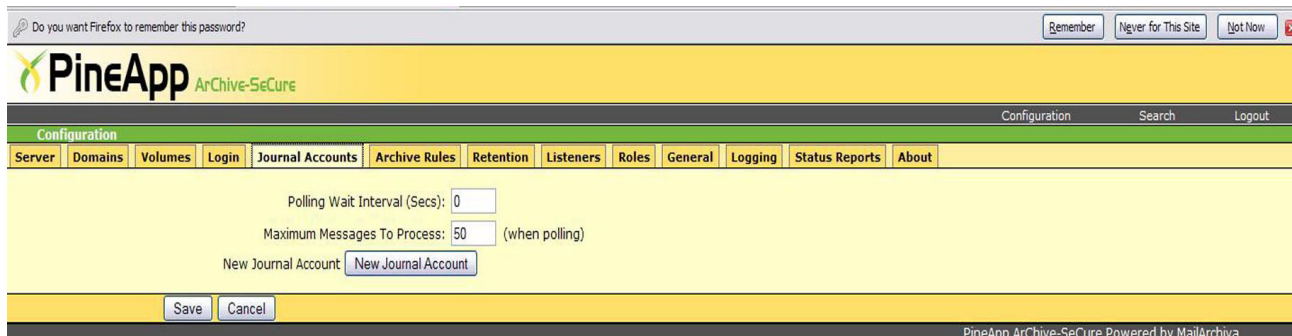
When users search for emails, the search is conducted across all active and closed volumes. In the unlikely event that a volume's search index is corrupted, it can be regenerated. Re-indexing is a time consuming process and is only recommended in the event of data loss.

### Re-indexing a volume

- Close the volume first, by switching its status to **"Closed"**.
- Click on the **"Re-Index"** button.

## Journal Accounts tab

Archive-SeCure can interface with Microsoft Exchange in a variety of ways. The easiest way is to configure Archive-SeCure to fetch emails from the journal account using Exchange's IMAP connector. On a fresh install of the Exchange product, the IMAP connector is switched on and ready for action.



The screenshot shows the PineApp Archive-SeCure web interface. At the top, there's a header with the PineApp logo and 'ArChive-SeCure'. Below the header is a navigation bar with tabs: Configuration, Search, and Logout. Under the Configuration tab, there's a sub-menu with various options: Server, Domains, Volumes, Login, Journal Accounts (selected), Archive Rules, Retention, Listeners, Roles, General, Logging, Status Reports, and About. The main content area is for the Journal Accounts configuration. It includes fields for 'Polling Wait Interval (Secs): 0' and 'Maximum Messages To Process: 50 (when polling)'. There's a 'New Journal Account' button. At the bottom, there are 'Save' and 'Cancel' buttons. The footer of the interface says 'PineApp ArChive-SeCure Powered by MailArchiva'.

## Pre Installation Exchange Server Configuration

The Microsoft Exchange product includes a message journaling feature that saves a copy of every email message that is sent from or received on a specific mail store. To archive all messages processed by Exchange, the Archive-SeCure server requires that this message journaling feature is enabled.

Microsoft Exchange supports three different types of message journaling: standard journaling, BCC journaling and envelope journaling. In standard journaling, when an email message is copied to the journaling mailbox, that message does not include BCC or alternative recipient information. Furthermore, if the message is addressed to a distribution group, the addressing information does not contain the individual recipients comprised of the distribution group.

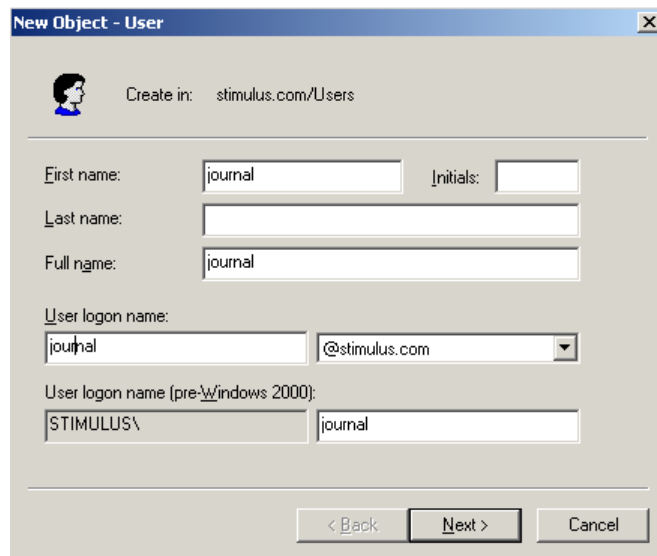
BCC journaling is similar to standard journaling except that the BCC field is included with all archived messages. In envelope journaling, all available RFC2821 and RFC2822 recipients are captured. Thus, an archived message includes all available header information, including BCC fields and the full expansion of distribution groups.

Please refer to the table below for an overview of Microsoft Exchange related features supported by Archive-SeCure.

## Archive-SeCure's Exchange Features

Microsoft Exchange	Archive-SeCure
Standard journaling	✓
BCC journaling	✓
Envelope journaling	✓
Multiple mail stores	✓
Multiple exchange servers	✓

**Creating a Journal Account** - On the server running Microsoft Exchange, using the Active Directory Users and Computers browser, create a Windows user account where all incoming and outgoing mail will be temporarily archived. This account must reside on your company's domain (i.e. not a local machine account).



**New Object - User**

Create in: stimulus.com/Users

First name: journal Initials:

Last name:

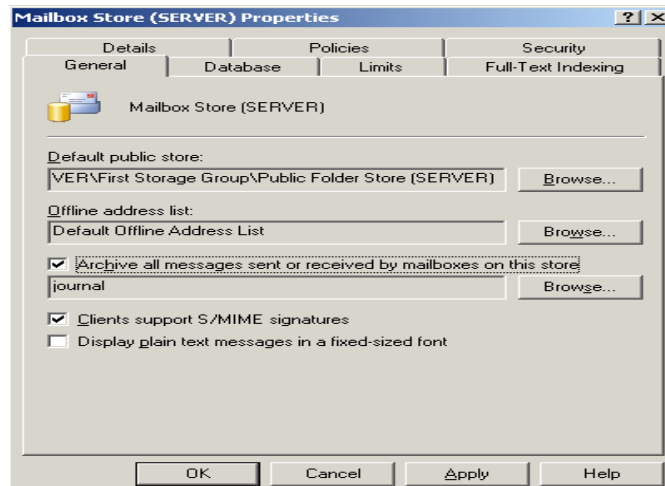
Full name: journal

User logon name: journal @stimulus.com

User logon name (pre-Windows 2000): STIMULUS\ journal

< Back Next > Cancel

**Enable Journaling on Microsoft Exchange** - On the same server, run the System Manager Application included with Microsoft Exchange. Locate the Mailbox Store node in the tree view on the left. It is in Servers->First Storage Group->Mailbox Store. Right click the Mailbox Store object and click Properties. A dialog box will appear as in the above figure. Click Browse and enter "journal" for the object name. Click **OK**. Journaling is now enabled for the Mailbox Store.



**Mailbox Store (SERVER) Properties**

Details Policies Security

General Database Limits Full-Text Indexing

Mailbox Store (SERVER)

Default public store: VER\First Storage Group\Public Folder Store (SERVER) Browse...

Offline address list: Default Offline Address List Browse...

☒ Archive all messages sent or received by mailboxes on this store journal Browse...

☒ Clients support S/MIME signatures

☐ Display plain text messages in a fixed-sized font

OK Cancel Apply Help



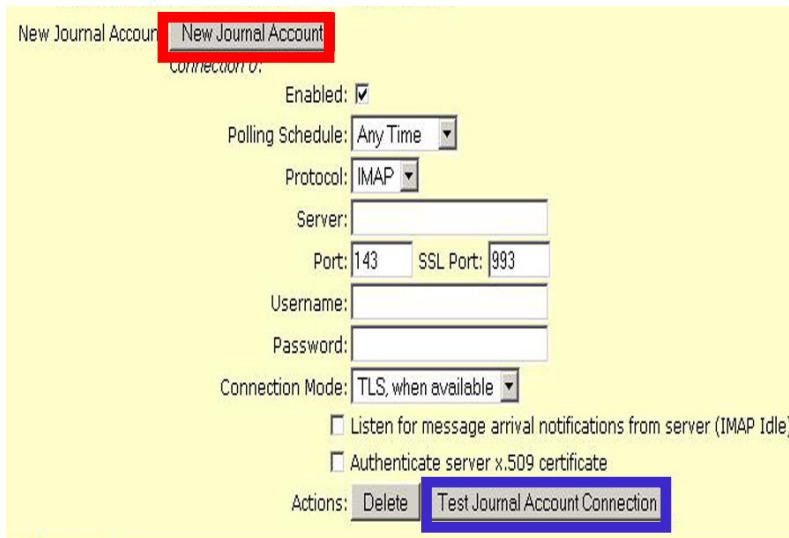
## Enable Envelope Journaling\* - If you are running Exchange 2003:

- a. Install the latest Service Pack.
- b. Download the Exejcfg.exe utility from Microsoft's Download Center.

To enable envelope journaling, from command prompt, type: **Exejcfg -e**

\* IGNORE this step if you are running Microsoft Exchange 2007 (Envelope journaling is enabled by default in Microsoft Exchange 2007).

**Adding a Journal Account Connection** - In the Journal Accounts tab of the Archive-SeCure server console configuration screen, click on the **New Journal Account** button (marked in a red square in the picture below) and do the following:



Set polling schedule to the desired interval (anytime by default).

- a. Select **IMAP** as the preferred protocol.
- b. Enter the server address of your Exchange server, and change the Port/SSL Port numbers, in case they do not match the default values (443 & 993 accordingly).
- c. Enter the Microsoft Exchange journal account username and password in the relevant fields.
- d. For the **Connection Mode**, select "**TLS when available**".
- e. Ensure **Authenticate Server x.509 Certificate** is unchecked.
- f. Click the **Test Journal Account Connection** button (marked in a blue square in the picture above) to determine if the connection is established.

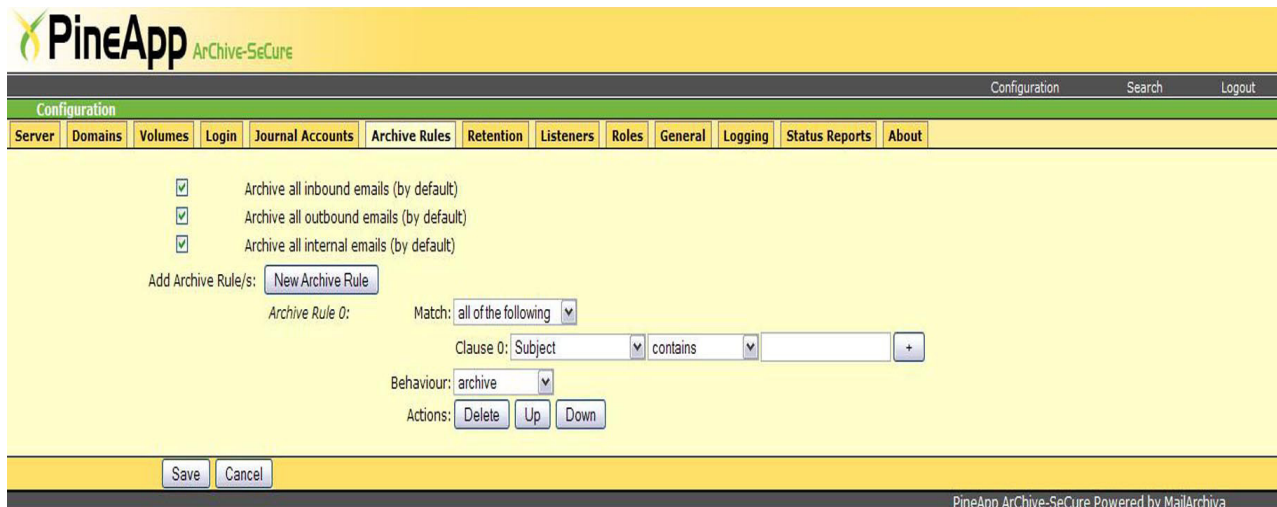
If the test is successful - save your configuration settings. Emails should start appearing in the search results in a matter of a few seconds.

If Archive-SeCure cannot establish a connection to Microsoft Exchange's IMAP server, verify that you entered the correct information and that Microsoft Exchange's SMTP connector is listening. You could also try using both the full journal account name (e.g. [journal@company.com](mailto:journal@company.com)) and the short name (e.g. journal).



## Archive Rules Tab

In some circumstances, it may not be desirable to archive all emails. Archive rules are used to determine whether or not an email should be archived.



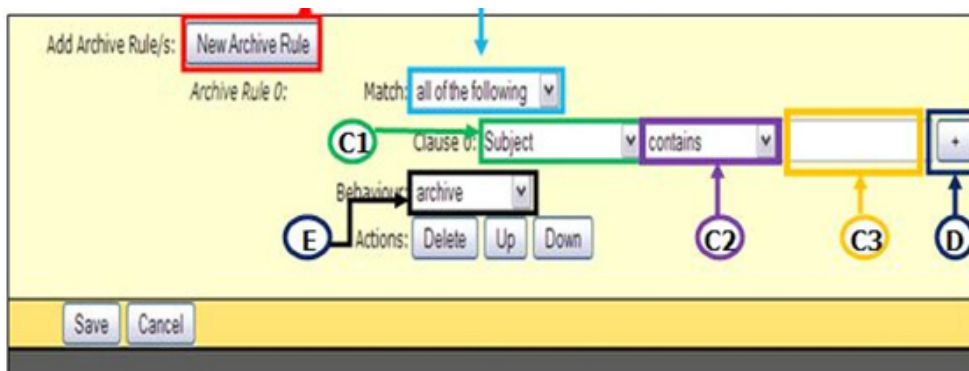
The screenshot shows the PineApp ArChive-SeCure configuration interface. At the top, there's a navigation bar with 'Configuration', 'Search', and 'Logout' links. Below this is a tabbed interface with tabs for 'Server', 'Domains', 'Volumes', 'Login', 'Journal Accounts', 'Archive Rules' (selected), 'Retention', 'Listeners', 'Roles', 'General', 'Logging', 'Status Reports', and 'About'. The 'Archive Rules' tab is active, displaying a list of default rules with checkboxes: 'Archive all inbound emails (by default)', 'Archive all outbound emails (by default)', and 'Archive all internal emails (by default)'. Below these is a 'New Archive Rule' button. The 'Add Archive Rule/s:' section shows 'Archive Rule 0:' with a 'Match:' dropdown set to 'all of the following'. A 'Clause 0:' is defined with 'Subject' in the field, 'contains' in the operator dropdown, and an empty text field. The 'Behaviour:' dropdown is set to 'archive'. At the bottom of this section are 'Delete', 'Up', and 'Down' buttons. At the very bottom of the interface are 'Save' and 'Cancel' buttons. The footer text reads 'PineApp ArChive-SeCure Powered by MailArchiva'.

As an administrator, you can choose to archive incoming, outgoing and/or internal emails, by checking/unchecking the boxes next to the relevant options. If these basic rules are not granular enough, advanced rules that determine whether or not to archive an email based on specific criteria may be defined.

The sequence in which the archiving rules are processed is significant. By design, advanced rules are always processed before basic rules. Furthermore, an advanced rule that appears before another will always be processed first. If during processing, an advanced rule determines that an email should not be archived then the action will be applied, irrespective of whether a subsequent rule contradicts the decision.

An advanced rule consists of one or more clauses.

## Adding a new Archive rule –



- a. Click on the **New Archive Rule** button (marked in a red square in the picture above)
- b. By selecting **any of the following** or **all of the following** from the dropdown menu (marked in a light blue square in the picture above), any or all of the clauses in the rule must match for it to apply.
- c. Each clause consists of 3 main sections:
  1. **Email field** - the dropdown menu containing the field or mail component that will be inspected for the trigger expression's presence, (marked in a green square in the picture above).
  2. An **operator** - the dropdown menu containing the condition according to which the rule will be activated (contain, doesn't contain, match etc.) (marked in a purple square in the picture above).
  3. A **value** - input text field, which determines the main trigger of the clause, (marked in an orange square in the picture above).

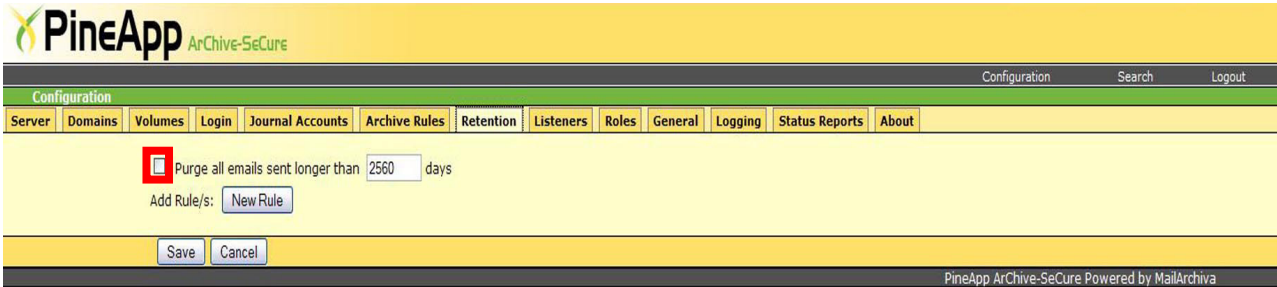
When processing a clause, the value of the selected email field is retrieved from the email and compared against the value specified in the clause.
- d. To add a clause, simply click on the **+** icon right next to the first clause, and edit it according to your preferences (marked in a dark blue square in the picture above).
- e. If they match, the behaviour, either **Ignore**, **Archive** or **do not Archive** (chosen from the dropdown menu marked in a black square in the picture above), is applied.
- f. Click on the **Save** button to save the rule you've created.

For example, to ensure all emails addressed to john@company.com are archived, you would simply select the field **to**, select the **contains** operator and enter "john@company.com".

**Deleting an Archive rule** – In order to delete a specific archive rule, simply click on the **Delete** button underneath it.

## Retention Tab

Your company retention policies are defined in the Retention tab of the Configuration screen.

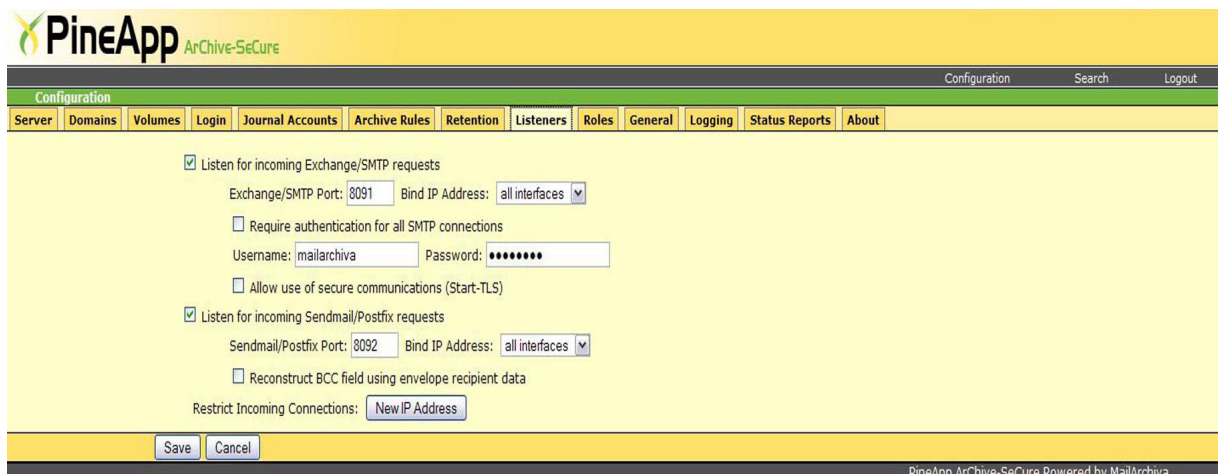


The screenshot shows the PineApp ArChive-SeCure web interface. The top navigation bar includes the PineApp logo and the text "ArChive-SeCure". Below this is a "Configuration" tab, with "Search" and "Logout" links. A secondary navigation bar lists various configuration options: Server, Domains, Volumes, Login, Journal Accounts, Archive Rules, Retention (selected), Listeners, Roles, General, Logging, Status Reports, and About. The main content area is titled "Retention" and features a checkbox labeled "Purge all emails sent longer than" followed by a text input field containing "2560" and the word "days". A red square highlights the checkbox. Below this is a link "Add Rule/s:" and a "New Rule" button. At the bottom of the main area are "Save" and "Cancel" buttons. The footer of the interface reads "PineApp ArChive-SeCure Powered by MailArchiva".

By checking “**purge all emails sent longer than X days**” checkbox (marked in a red square in the picture above), Archive-SeCure will automatically delete all emails that are older than X days. In case of need, it is possible to define granular retention rules for emails that match certain criteria. When a rule matches, Archive-SeCure may delete the email if it is older than the specified period.

## Listeners Tab

The listeners tab contains configuration which determines the ports in which the appliance listens to SMTP connections, along with the participating interface/interfaces in the listening procedure.



**PineApp** ArChive-SeCure

Configuration Search Logout

Server Domains Volumes Login Journal Accounts Archive Rules Retention **Listeners** Roles General Logging Status Reports About

☒ Listen for incoming Exchange/SMTP requests

Exchange/SMTP Port: 8091 Bind IP Address: all interfaces

☐ Require authentication for all SMTP connections

Username: mailarchiva Password: \*\*\*\*\*

☐ Allow use of secure communications (Start-TLS)

☒ Listen for incoming Sendmail/Postfix requests

Sendmail/Postfix Port: 8092 Bind IP Address: all interfaces

☐ Reconstruct BCC field using envelope recipient data

Restrict Incoming Connections: New IP Address

Save Cancel

PineApp ArChive-SeCure Powered by MailArchiva

**Listen for incoming Exchange/SMTP requests** - Check this option in case you are using a Microsoft Exchange based mail server.

**Exchange/SMTP Port** - In this tab, fill in the port number that the appliance will listen to for SMTP traffic archiving.

**Bind IP address** - This option enables you to choose, using the dropdown menu, a singular configured interface (or all of them) to participate in the listening procedure.

Allow use of Secured communications (TLS) – check this option to allow the archiving of encrypted emails.

**Listen for incoming Sendmail/Postfix requests** - Check this option in case you are using a Postfix/Sendmail based mail server.

**Sendmail/Postfix Port** - In this tab, fill in port number that the appliance will listen to for SMTP traffic archiving.

**Bind IP address** - This option enables you to choose, using the dropdown menu, a singular configured interface (or all of them) to participate in the listening procedure.

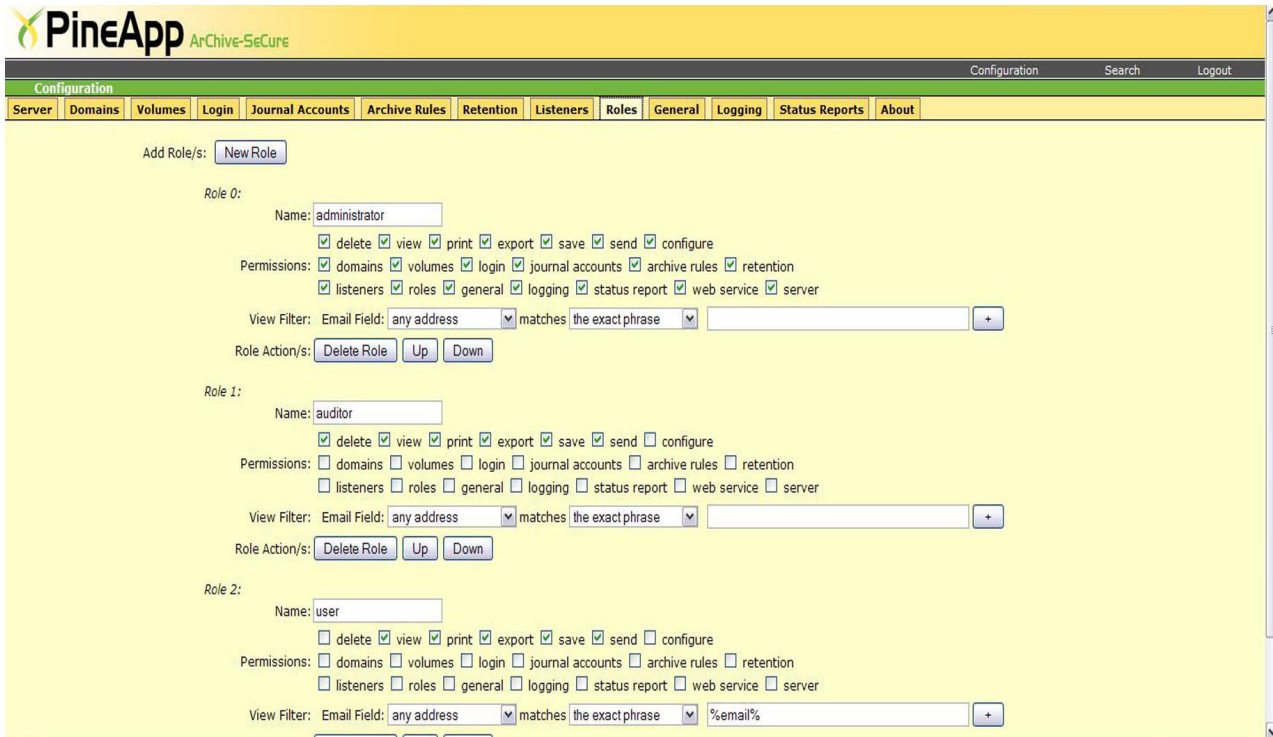
Reconstruct BCC field using envelope recipient data – a Sendmail/Postfix BCC formatting related feature.

**Restrict Incoming connections** – Click on the **New IP Address** button to type in the text field any source IP addresses that you do not wish to archive mail from.

To delete a record from the restricted list, simply click on the **Delete** button next to it.

## Roles Tab

Once a user has logged into the console, the user is assigned a security role. The security role determines what the user can do and which emails the user can see. There are two main aspects to role definition:



The screenshot shows the PineApp Roles configuration interface. It features a navigation bar with tabs for Configuration, Search, and Logout. Below this is a sub-navigation bar with tabs for Server, Domains, Volumes, Login, Journal Accounts, Archive Rules, Retention, Listeners, Roles, General, Logging, Status Reports, and About. The main content area is titled 'Add Role/s:' and includes a 'New Role' button. It displays three roles: Role 0 (Name: administrator), Role 1 (Name: auditor), and Role 2 (Name: user). Each role has a list of permissions (delete, view, print, export, save, send, configure, domains, volumes, login, journal accounts, archive rules, retention, listeners, roles, general, logging, status report, web service, server) and a view filter (Email Field: any address, matches the exact phrase). Role actions (Delete Role, Up, Down) are also shown for each role.

**Permissions** – what kind of executable actions are available for a certain user (e.g. delete email).

**View filters** – which emails the user can see (e.g. only emails within his own domain).

There are three built in roles in the system: administrator, auditor and user. The default permissions and view filters associated with these roles are described in table **Built-In Role Permissions** and **Built-In Role Email Filters**, respectively.

### Built-In Role Permissions

Role	Allow Delete	Allow View	Allow Print	Allow Export	Allow Save	Allow Send	Allow Configure
User	No	Yes	Yes	Yes	Yes	Yes	No
Audit	No	Yes	Yes	Yes	Yes	Yes	Yes
Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes

### Built-In Role Email Filters

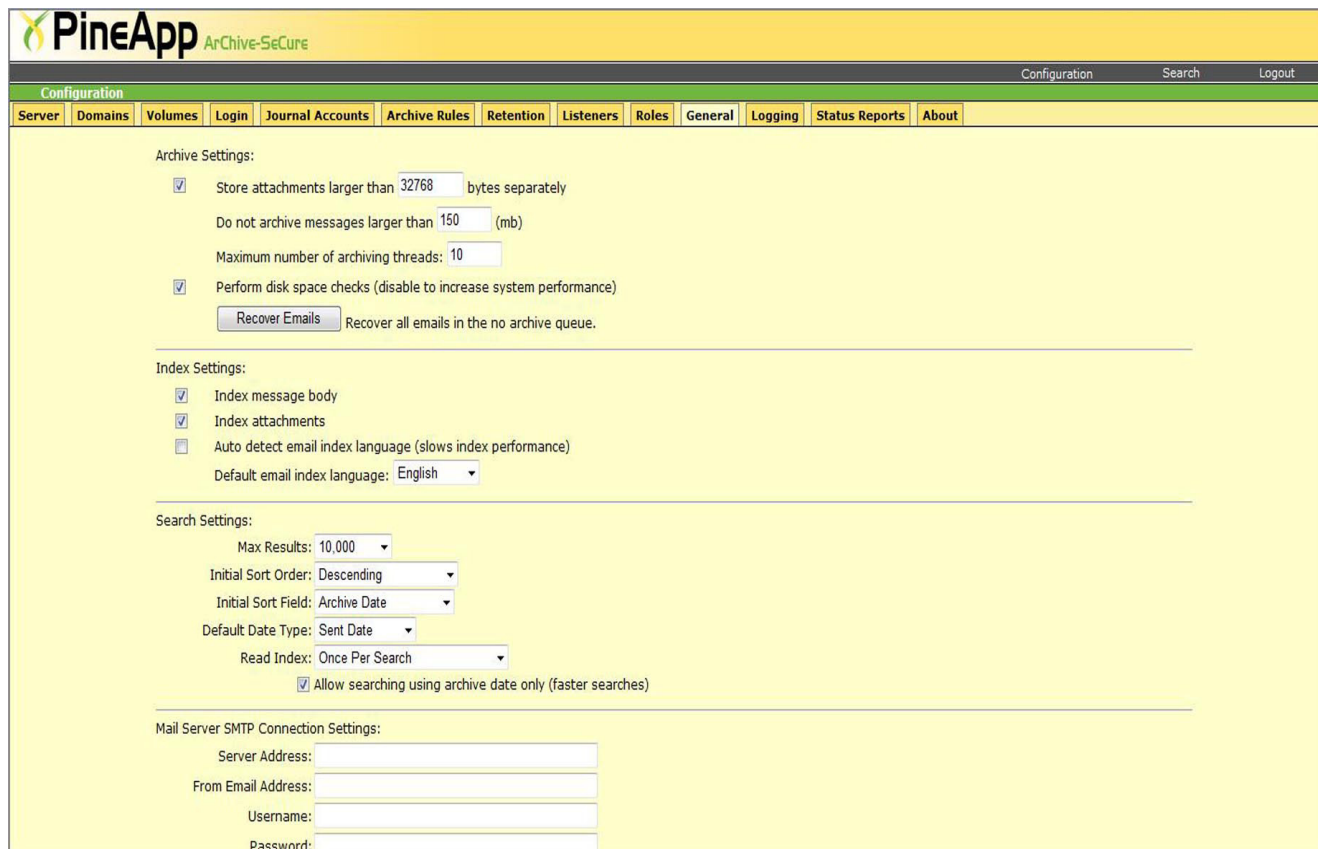
Role	View Filter
User	Can only view own emails (all addresses must match user's email address)
Audit	Can view any email
Admin	Can view any email

If the built-in roles are not suitable, you can define one or more custom roles.

### **Adding a Custom Role -**

- a.** Click on the **Add Role** button in the Custom Role tab of the server console configuration screen.
- b.** Enter an appropriate name for the role.
- c.** Select the permissions associated with the role, according to your preferences.
- d.** Add a **view filter** clause to limit which emails users assigned the role can view.

## General Tab



The screenshot shows the PineApp Archive-SeCure web interface. At the top is the PineApp logo and tagline. Below is a navigation bar with tabs: Configuration, Search, and Logout. Under Configuration, there are sub-tabs: Server, Domains, Volumes, Login, Journal Accounts, Archive Rules, Retention, Listeners, Roles, General (selected), Logging, Status Reports, and About. The main content area is titled 'General' and contains three sections of settings:

- Archive Settings:**
  - ☒ Store attachments larger than 32768 bytes separately
  - Do not archive messages larger than 150 (mb)
  - Maximum number of archiving threads: 10
  - ☒ Perform disk space checks (disable to increase system performance)
  - Recover Emails Recover all emails in the no archive queue.
- Index Settings:**
  - ☒ Index message body
  - ☒ Index attachments
  - ☐ Auto detect email index language (slows index performance)
  - Default email index language: English
- Search Settings:**
  - Max Results: 10,000
  - Initial Sort Order: Descending
  - Initial Sort Field: Archive Date
  - Default Date Type: Sent Date
  - Read Index: Once Per Search
  - ☒ Allow searching using archive date only (faster searches)
- Mail Server SMTP Connection Settings:**
  - Server Address:
  - From Email Address:
  - Username:
  - Password:

The General tab contains some advanced configuration settings, mainly for archiving and indexing behavior adjustments.

### **Archive Settings –**

**Store attachments larger than X bytes separately** – By checking this option, all files bigger than the number entered in this field, will be stored in a different storage volume.

**Do not Archive messages larger than X (mb)** – By checking this option, a maximum message size threshold can be determined according to the number typed in this field.

**Perform disk space checking** – By checking this option, Archive-SeCure will independently perform capacity inspections or any over capacitated volumes alerts.

**Recover Emails** – In case you wish to recover all emails that were not archived (due to oversize and/or according to other archiving settings), simply click on this button.

**Index Settings -** The index is used to enable auditors to perform efficient search queries on the archived data. The store consists of multiple sub-directories where the archived information is kept.

Archive-SeCure is an internationalized email archiving system. By default, Archive-SeCure supports the indexing, search and retrieval of emails written in English, Portuguese, Chinese, Czech, German, Greek, French, Dutch, Russian, Japanese, Korean and Thai.



As part of the email archiving process, Archive-SeCure will automatically attempt to determine the language of the email using N-GRAM analysis. The algorithm requires that there is sufficient text available to determine the language that was used. If the text is not sufficient, Archive-SeCure will assume that the email is written in the default language. Automatic language indexing is available by checking the option “**Auto detect email index language (slows index performance)**”

The Archive-SeCure administration console user interface is currently available in English, French, German, Dutch, Chinese and Spanish. Archive-SeCure will automatically determine the appropriate language to display based on the user's browser settings. Furthermore, all entered and displayed dates are formatted according to the locale of the user's computer.

In addition, the indexing of message body and any attached files is possible by checking the options **Index message body & Index attachments** under the **Index Settings** section.

**Search settings** - This section concerns fine tuning of the default search options in the appliance.

**Max Results** - maximum results for each search query.

**Initial Sort Order - the order in which the results will appear;**

**Descending** - (newest/biggest record appears first in search result; oldest/smallest record appears last in search result).

**Ascending** - (newest/biggest record appears last in search result; oldest/smallest record appears first in search results).

**Unsorted** - search results appear randomly.

**Initial sort field** - This section concerns the sort criteria, according to which the records are arranged by default. For example, in case you choose the “From” option, the records will be sorted alphabetically according to the sender's address initial letters.

**Default date type** - search results will be automatically sorted according to the default date type that is picked (from the dropdown menu) under this section.

**Read Index** - The date according to which the records will be sorted;

- a. Sent Date (Default)** - the date when the message was sent will determine the order of appearance of messages, according to the default sorting preferences.
- b. Archive Date** - the date when the message was archived will determine the order of appearance of messages, according to the default sorting preferences.
- c. Received Date** - the date when the message was received will determine the order of appearance of messages, according to the default sorting preferences.

**Mail Server SMTP Connection Settings** - This section determines the Archive-SeCure's periodical reports' delivery details.

**Server Address** - Fill in the IP address of the SMTP server that will be relaying the reports' delivery.

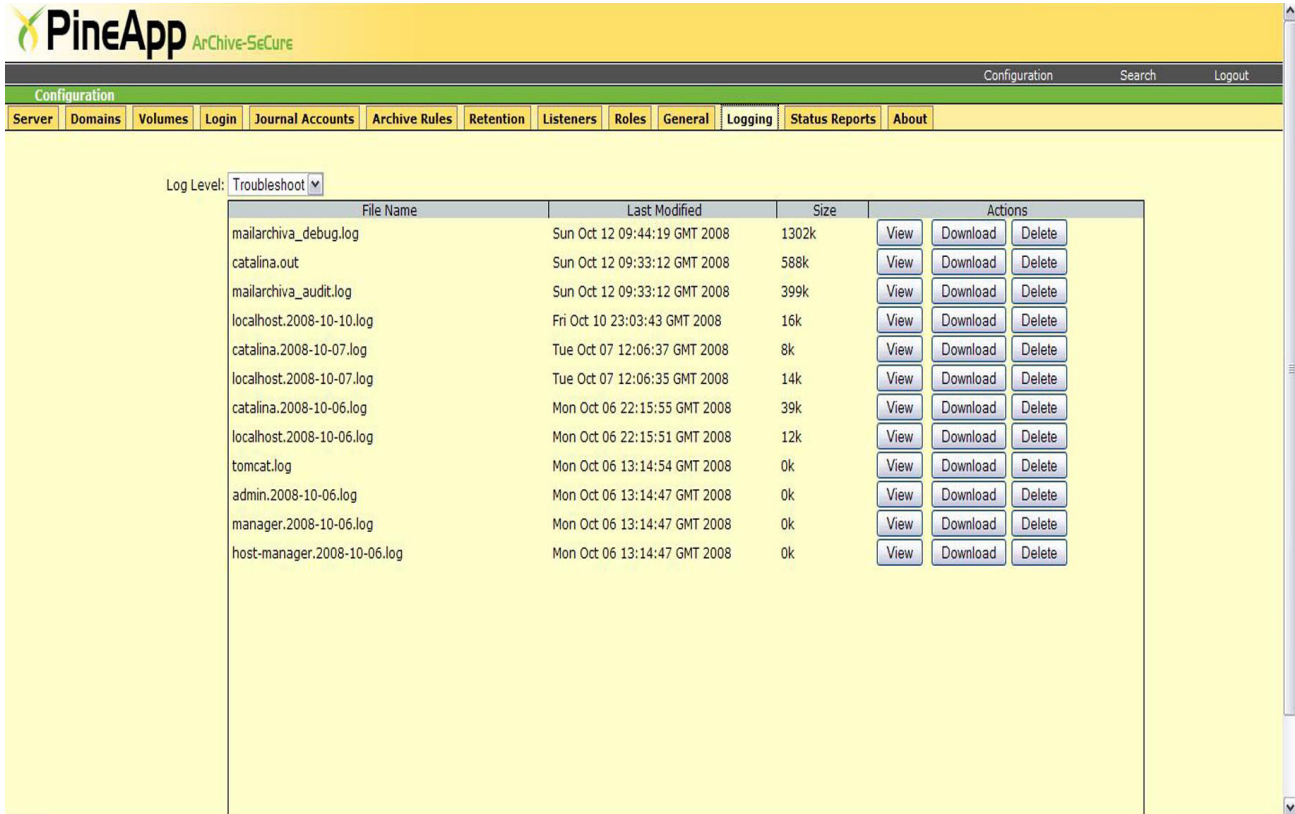
**From Email Address** - Fill in the reports sender's email address.

**Username & Password** - The sender's address has to be affiliated with an activated and listed account on the mail server that relays it. Type the account's username & password in the corresponding fields.



## Logging Tab

The Logging tab contains all of the appliance's system logs. It provides a major debugging and inspection tool for the system administrator.



File Name	Last Modified	Size	Actions		
mailarchiva_debug.log	Sun Oct 12 09:44:19 GMT 2008	1302k	View	Download	Delete
catalina.out	Sun Oct 12 09:33:12 GMT 2008	588k	View	Download	Delete
mailarchiva_audit.log	Sun Oct 12 09:33:12 GMT 2008	399k	View	Download	Delete
localhost.2008-10-10.log	Fri Oct 10 23:03:43 GMT 2008	16k	View	Download	Delete
catalina.2008-10-07.log	Tue Oct 07 12:06:37 GMT 2008	8k	View	Download	Delete
localhost.2008-10-07.log	Tue Oct 07 12:06:35 GMT 2008	14k	View	Download	Delete
catalina.2008-10-06.log	Mon Oct 06 22:15:55 GMT 2008	39k	View	Download	Delete
localhost.2008-10-06.log	Mon Oct 06 22:15:51 GMT 2008	12k	View	Download	Delete
tomcat.log	Mon Oct 06 13:14:54 GMT 2008	0k	View	Download	Delete
admin.2008-10-06.log	Mon Oct 06 13:14:47 GMT 2008	0k	View	Download	Delete
manager.2008-10-06.log	Mon Oct 06 13:14:47 GMT 2008	0k	View	Download	Delete
host-manager.2008-10-06.log	Mon Oct 06 13:14:47 GMT 2008	0k	View	Download	Delete

**Log level** – this feature allows you to inspect all logs for a certain aspect of the system's information, and screen out all other irrelevant information.

For example, fine tuning the Log level for Errors (by choosing **Error** from the Log level dropdown menu) will sort out all information on ALL of the appliance's logs, aside of any given system errors.

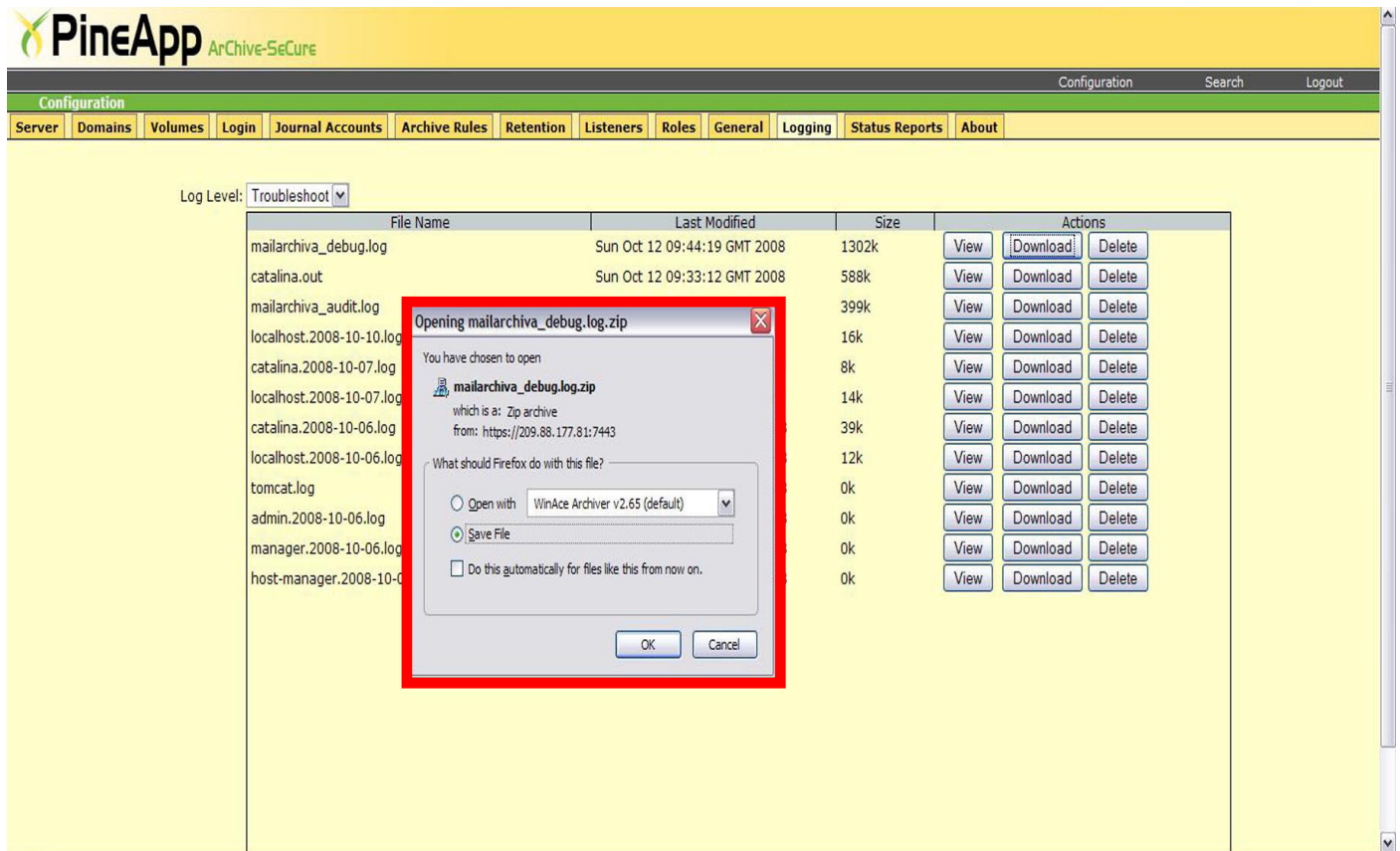
The logs can be arranged by name (alphabetical order), last modification date, and their size, simply by clicking on the desired sorting field, as shown in the picture above.

**Viewing log's contents** - Clicking on the **View** button next to each log opens up a pop up window on your browser, containing the log's current content.

#### View Log

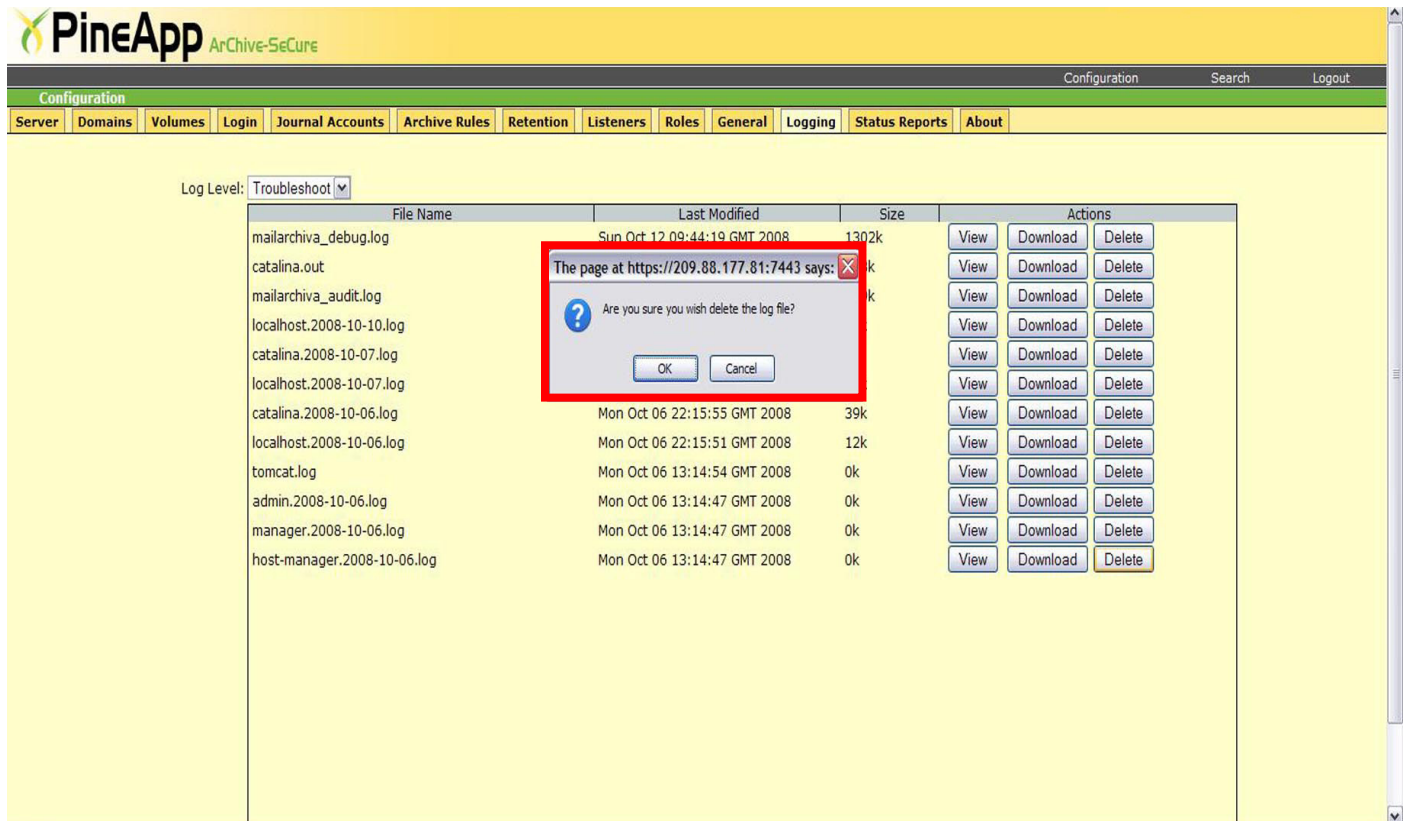
```
DEBUG Oct/12 09:08:57 - getAnalyzer() {language='en'}
DEBUG Oct/12 09:08:57 - standard search executed {query='null'}
DEBUG Oct/12 09:08:57 - search email
{name='pineapp',role='administrator',ipAddress='192.168.2.95'}
INFO Oct/12 09:08:57 - search emails
{name='pineapp',role='administrator',ipAddress='192.168.2.95',query='null'}
DEBUG Oct/12 09:08:57 - searchMessage {querystring='null'}
DEBUG Oct/12 09:08:57 - search() {searchquery='null'}
DEBUG Oct/12 09:08:57 - searchmessages() begin
DEBUG Oct/12 09:08:57 - search() {action='search', value='null'}
DEBUG Oct/12 09:08:57 - search() begin
DEBUG Oct/12 09:08:57 - setAfter() {sentafter='8/13/08 1:00 AM'}
DEBUG Oct/12 09:08:57 - setBefore() {before='10/13/08 11:59 PM'}
DEBUG Oct/12 09:08:55 - getLanguage() {language='en'}
DEBUG Oct/12 09:08:55 - getBefore() {sentbefore='10/13/08 11:59 PM'}
DEBUG Oct/12 09:08:55 - getAfter() {sentafter='8/13/08 1:00 AM'}
DEBUG Oct/12 09:08:55 - searchmessages() end
DEBUG Oct/12 09:08:55 - there are no volumes to search
DEBUG Oct/12 09:08:55 - searching for suitable searchers
DEBUG Oct/12 09:08:55 - getVolumeSearchers()
DEBUG Oct/12 09:08:55 - standard search: parsing filter query {query='' }
DEBUG Oct/12 09:08:55 - getUserRoleFilter() {filterQuery='' }
DEBUG Oct/12 09:08:55 - successfully parsed search query {query='(subject:lior) AND
archivedate:[d20080813010000 TO d20081013235900]'}
DEBUG Oct/12 09:08:55 - successfully returned search analyzer {language='en',
class='com.stimulus.archiva.search.ArchivaAnalyzer'}
DEBUG Oct/12 09:08:55 - analyzer class instance created {language='en',
class='com.stimulus.archiva.search.ArchivaAnalyzer'}
DEBUG Oct/12 09:08:55 - retrieved analyzer class {language='en',
class='com.stimulus.archiva.search.ArchivaAnalyzer'}
```

**Downloading log's contents** - Logs can also be downloaded individually to the local hard drive, by clicking on the Download button on the right side of each log.



A download Dialog window will appear (marked in a red square in the picture above). Choose your preferred option (**Open/Save file**) and click on **OK** to download the log file.

**Clearing log's contents** - To clear a certain log's contents and reset it, click on the **Delete** button on the right hand side of the specific log.



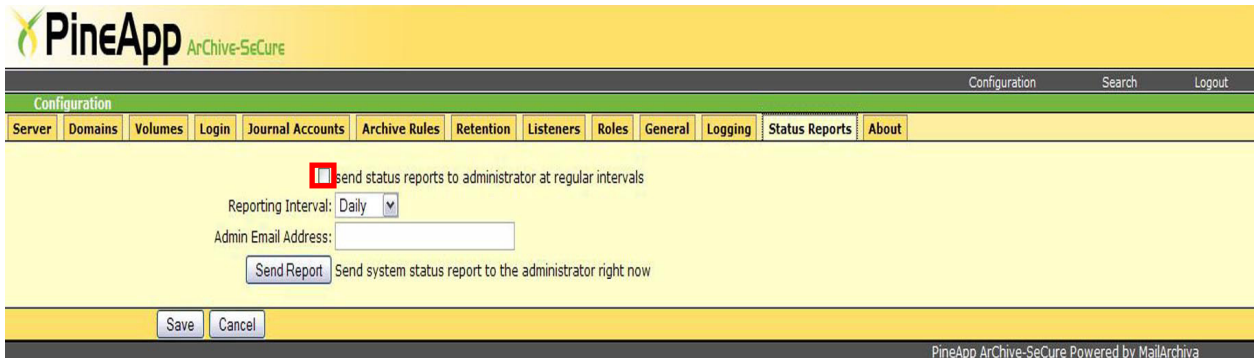
A pop up message will appear (marked red in the picture above) and will ask you **"Are you sure you wish delete the log file?"**.

To finalize your action, click on **OK**, and the log will be cleared.



## Status Reports Tab

The Status Reports tab contains the adjustment features for administrative reports email delivery. The Archive-SeCure administrative report contains system information and statistical data, regarding the appliance's activity and current storage and index status for each configured. In addition, it contains license and system logs' related information.



The Report delivery interval can be determined for one delivery per day, week or month, using the Reporting Interval dropdown menu.

**Send Status Reports to administrator at regular intervals** – Checking/unchecking this option (marked in a red square in the picture above) enables/disables Status Reports delivery from the appliance, to the listed system administrator's address.

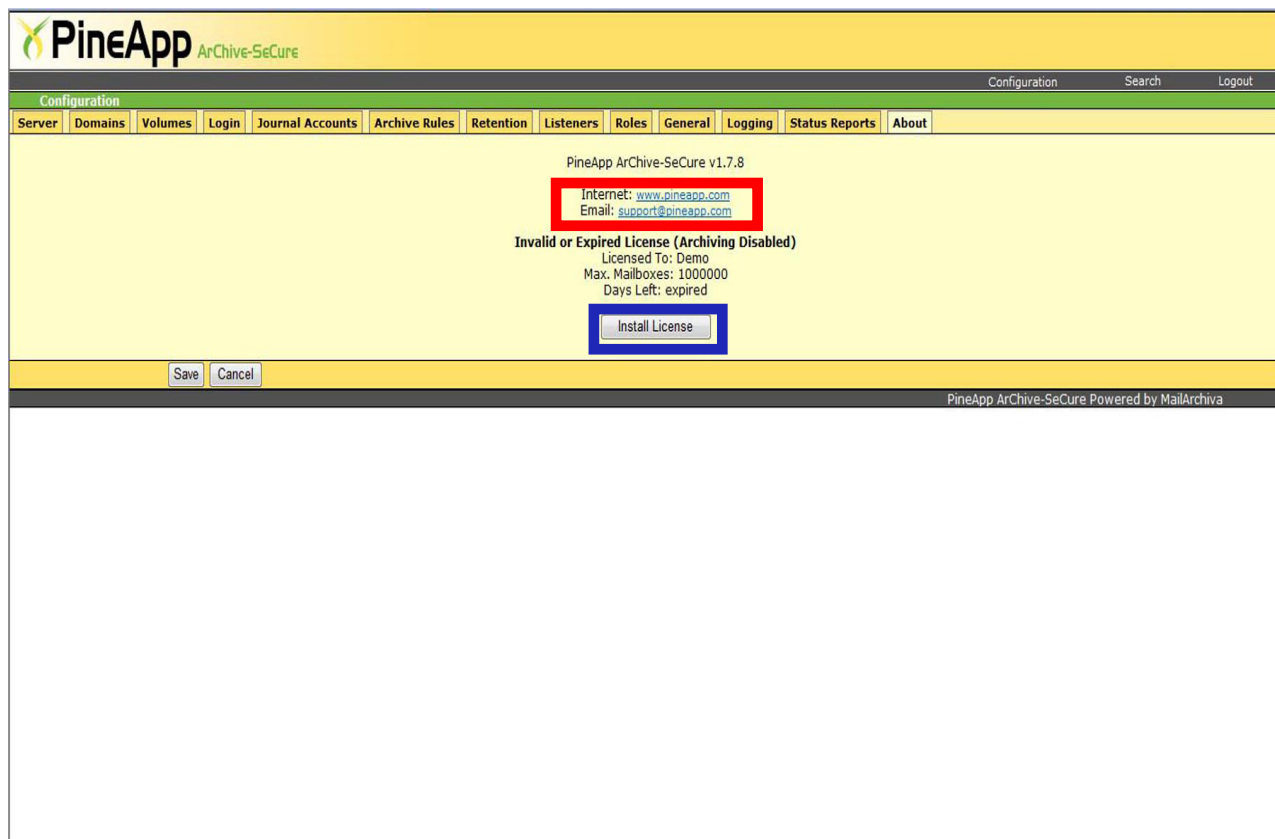
**Admin Email** - The address listed in this field (and this address only) will receive all of the administrative reports.

**Send Report** - By clicking on this button, the appliance will compile and send a report containing the appliance's current statistics, starting from the last delivery period up to current time.

Please review appendix A: Status Report delivery example for a detailed specification of the delivery report's content.

## About Tab

The About tab contains license related information, and referrals to PineApp's support website & email address (marked red in the picture below).



**Licensed to** - This line shows the legal registered owner of the appliance.

**Max Mailboxes** - This line contains the mailbox archiving limitation, according to the license type.

**Days left** - This line shows the number of remaining days before the appliance's license expiry.

### Updating the appliance's license -

- a. Click on the **Install License** button (marked in a blue square in the picture above).
- b. A new window will open up on the upper left hand side of the screen, as shown below.

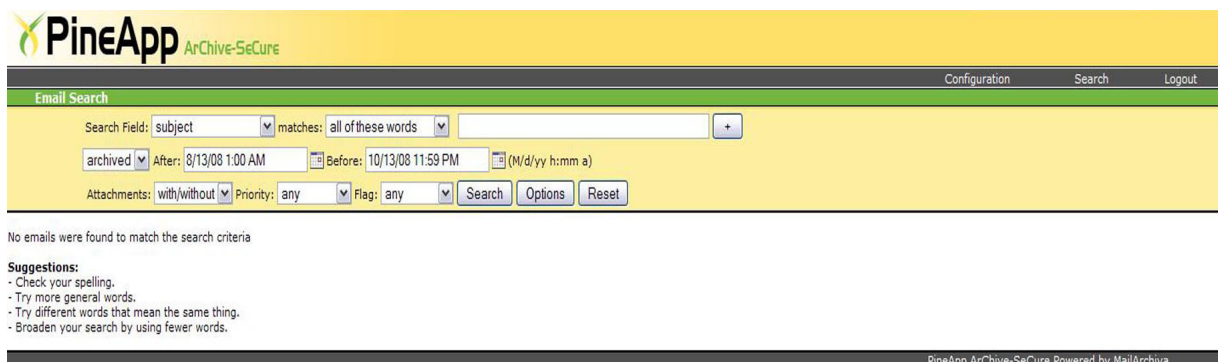


- c. Upload the license file that was sent by your local reseller/PineApp's Sales department, using the **Browse** button (do not forget to first save the file on your local computer).
- d. Click on the **Install License** button in the pop-up window.

# CHAPTER 3

## Search

### Search Queries



The screenshot shows the PineApp Archive-SeCure web interface. At the top is a yellow header with the PineApp logo and 'ArChive-SeCure' text. Below this is a navigation bar with 'Configuration', 'Search', and 'Logout' links. The main section is titled 'Email Search' and contains a search form. The form has a 'Search Field' dropdown set to 'subject', a 'matches' dropdown set to 'all of these words', and a text input field. Below these are date and time filters: 'archived' dropdown, 'After: 8/13/08 1:00 AM', 'Before: 10/13/08 11:59 PM', and a date format selector '(M/d/yy h:mm a)'. At the bottom of the form are 'Attachments: with/without' dropdown, 'Priority: any' dropdown, 'Flag: any' dropdown, and 'Search', 'Options', and 'Reset' buttons. Below the form, a message states 'No emails were found to match the search criteria'. Underneath is a 'Suggestions' section with four bullet points: 'Check your spelling.', 'Try more general words.', 'Try different words that mean the same thing.', and 'Broaden your search by using fewer words.' At the very bottom, a footer bar reads 'PineApp ArChive-SeCure Powered by MailArchiva'.

The search function in the server console is sufficiently intuitive that it does not warrant detailed discussion. However, it's worth mentioning that Archive-SeCure supports multiple and single character wildcard searches. The "?" symbol is used to indicate a single character wildcard, while the "\*" symbol indicates a multiple character wildcard. For example, to search for "text" or "test" you can use the search term "te?t". To search for "test", "tests" or "tester", the search term "test\*" can be used. Wildcards may be used anywhere in a search term, except at the beginning of the term. Thus, "?est" and "\*est" are both invalid.

By default, when performing a search, up to 50,000 result items will be retrieved at a time. You can change this setting if you so desire, by clicking "Options" and changing the Max Results setting. It is also possible to sort the search results according to size, sent date, from, to and subject. Simply click on their respective column labels in the search results page to search in ascending and descending order. As an added benefit, you can also search for emails multiple languages.

## **Appendix A: Status Report delivery example**

Below is an example for an appliance status report mail message, followed by a detailed explanation as for every section in it.

```
Server Version: 1.7.6
Server Start Time: 8/25/08 8:27 AM
Server Up-Time: 0 days 15 hours 32 mins
Last Archival Time: 8/26/08 12:00 AM
Duration Since Last Archival: 0 days 0 hours 0 mins
No. Archived Messages Since Start: 44751
No. Messages In No-Archive Queue: 0

Volumes

Vol: 20080820104815
Status: ACTIVE
Store: /var/data/archiva/store0 ( 69.48 GB free 48.7 MB used )
Index: /var/data/archiva/index0 ( 69.5 GB free 18.38 MB used )
Document Count: 44251

Events

8/25/08 8:27 AM server demo license is about to expire (6days remaining)
8/25/08 8:27 AM server demo license is about to expire (6days remaining)
8/25/08 8:27 AM server demo license is about to expire (6days remaining)
8/25/08 8:27 AM server demo license is about to expire (6days remaining)
8/25/08 8:27 AM server demo license is about to expire (6days remaining)
8/26/08 12:00 AM server demo license is about to expire (5days remaining)

Warning: Your license is valid for 5 days only.
To upgrade your license, email info@pineapp.com.
```

**Server Version** - The appliance's current software version.

**Server Start Time** - The accurate time when the appliance was first turned on.

**Server Up-Time** - Elapsed time from the last appliance's boot.

**Last Archival Time** - The accurate time when last archival process was performed.

**Duration since Last Archival** - Elapsed time from the last archival process.

**No. Archived Messages Since Start** - Total number of Archived messages throughout the appliance's activity.

**No. Messages In No-Archive Queue** - Total number of non-Archived messages, due to oversize and/or other.

**Volumes** – This section concerns the appliance's current volumes status.

**Vol** - The volume's name\*.

**Status** - Current volume's activity status (ACTIVE/INACTIVE).

**Store** - The volume store's detailed path, and information regarding its current capacity status.

**Index** - The volume index's detailed path, and information regarding its current capacity status.

**Document Count** - Total number of archived documents in the specific volume.



\*If there is more than one volume configured, it will be listed, along with its corresponding information, under the first volume's information details listed above.

**Events** – This section details any special events in different topics, taken from the appliance's system logs. In the example above, alerts regarding the appliance's upcoming license expiry are shown, though it is possible to also review various system/hardware alerts via the Events section on the status report.