

Emergic **M@ilArray**

Installation & Administration Guide



Index

Server Installation (on Linux)	3
Server Installation (on Linux).....	3
Server Installation (on Linux) Step 1; Step 2; Step 3.....	3
Configuration	5-6
(a) E-mail Encryption Password.....	5
(b) Volumes.....	5
Local Domains	7
Authentication	8-10
Basic Authentication.....	8
Active Directory Authentication.....	9
LDAP Authentication.....	10
IMAP/POP Account Connection	11-13
Sendmail Connection.....	12
Postfix Connection.....	12
Exim Connection.....	12
Other Mail Servers Configuration.....	13
Roles	14-15
Archive Rules	15
Retention Policy	16
Search Queries	16
Email Operations	17

Installation

The MailArray Server can be installed on any variety of Linux distributions. The instructions in this section show the steps required to install the server on Redhat/Fedora specific systems.

The below procedure may vary slightly on different Linux distributions. However, with sufficient knowledge of your distribution, you should be able to setup MailArray on your preferred Linux system.

Step 1. Install MailArray Server

Insert CD and give necessary inputs as per your requirement

The server executables will be installed `/opt/mailarray`.

Step 2. Check Availability of Port 2524 and Port 2525

By default, MailArray uses port 2524 and port 2525. Before starting the server, ensure that these ports are not being used by another application. You can do this by typing `"netstat -atnp | grep 252"` from the console.

If port 2524 is in use, edit the file `/opt/mailarray/conf/server.xml` and change all references from "2524" to the desired port.

Or Run the command

```
sed -i 's/2524/<desiredport>/g' /opt/mailarray/conf/server.xml
```

Step 3. Start MailArray Server

To start the MailArray Server from the commandline type:

```
/etc/rc.d/init.d/mailarray start
```

In a web browser to access the web console type.

```
http://<IP of server>:2524/mailarray
```

By default initially the user name and password are blank



If you cannot access the console, check that port 2524 is open on your firewall and examine the log files typing the command.

`tma`

On a Redhat/Fedora based system you could also stop selinux in case the frontend is unavalible

`sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/selinux/config`

and then reboot the system

To stop the server, you would type:

`/etc/rc.d/init.d/mailarray stop`

To make the service available on reboot

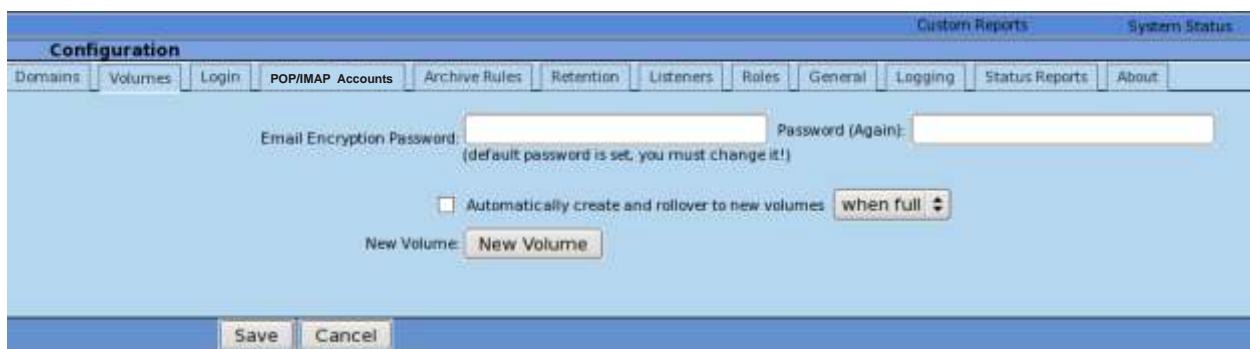
`chkconfig --level 2345 mailarray on`

Configuration

Configuration

The final step involves configuring the server.

There are three configuration tasks that need to be performed before the server is ready to start archiving e-mails:



- (a) set an encryption password
- (b) create one volume
- (c) add your local domains.

(a) E-mail Encryption Password

Triple DES password-based encryption is used to store the emails coming into the server. Before archive e-mails, a encryption password will have to be entered in the “*Email Encryption password*” in the Volumes tab of the Configuration screen.

The password once entered & saved cannot be changed, so it is very important that you remember it. Since “Triple DES password-based encryption” is used the password holds the key to your archived emails, you need to ensure that the password is kept highly confidential and secret.

Once you have set the encryption password, please backup the file server.conf located in [/opt/mailarray/webapps/mailarray/WEB-INF/conf](#)



This file contains your encrypted password used for email encryption purposes.

Thus it is of great importance that a backup of the server.conf configuration file is made and that is stored in a secure location.

(b) Volumes

Archived emails are stored into one or more volumes.
 Each volume is made up of two parts index and store.
 The index part is used to perform efficient search queries on the archived data.
 The store is made up of multiple sub-directories where the archived information is kept.

When a creating a volume, the index path and store path can refer to any location on one or more hard disks. 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.

To create a volume, click the <New Volume button> in the Configuration screen. Enter a path for the store and index (e.g. /store1 and /index1). If you've created more than one volume, click the <Up>

and <Down> buttons to arrange them according to your order of preference.

Once you've created a volume, it is assigned the "NEW" status.

Once the archiving process begins, the server will automatically switch over to the first "Unused" volume on the list. This volume will become "Active" volume until such time as its maximum size is exceeded, the disk is full, or the volume is physically close.

Once a volume is closed, no further data can be written to it and it cannot be reopened but search will be performed on close volumes.

<i>NEW</i>	The volume has just been created and has not been saved.
<i>UNUSED</i>	The volume has been saved but it does not contain any information.
<i>ACTIVE</i>	The volume is currently being used for archiving purposes.
<i>CLOSED</i>	The volume is search able, however, no further information can be written to it.
<i>UNMOUNTED</i>	The volume is not search able, nor can it be made active.
<i>EJECTED</i>	Volume was removed without physically unmounting it.
<i>REMOTE</i>	The volumes 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 e-mails, 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. To re-index a volume, you need to close it first, and click on the <Re-Index> Button.

Local Domains

Local Domains

The screenshot shows the 'Configuration' screen for 'Local Domains'. At the top, there are tabs for 'Custom Reports' and 'System Status'. Below that is a navigation bar with tabs: 'Domains', 'Volumes', 'Login', 'POP/IMAP Accounts', 'Archive Rules', 'Retention', 'Listeners', 'Roles', 'General', 'Logging', 'Status Reports', and 'About'. The 'Domains' tab is selected. The main area contains a 'New Windows Domain/s:' label with a 'New Domain' button. Below this are two domain entries: 'Domain 0:' and 'Domain 1:'. Each entry has a 'Domain Name:' label followed by a text input field and an 'Actions:' label with a 'Delete' button. At the bottom of the form are 'Save' and 'Cancel' buttons.

When configuring MailArray for the first time, you need to add one or more of your organization's domains. To do this, click <Add Domain> in the domain section of the configuration screen and click save.

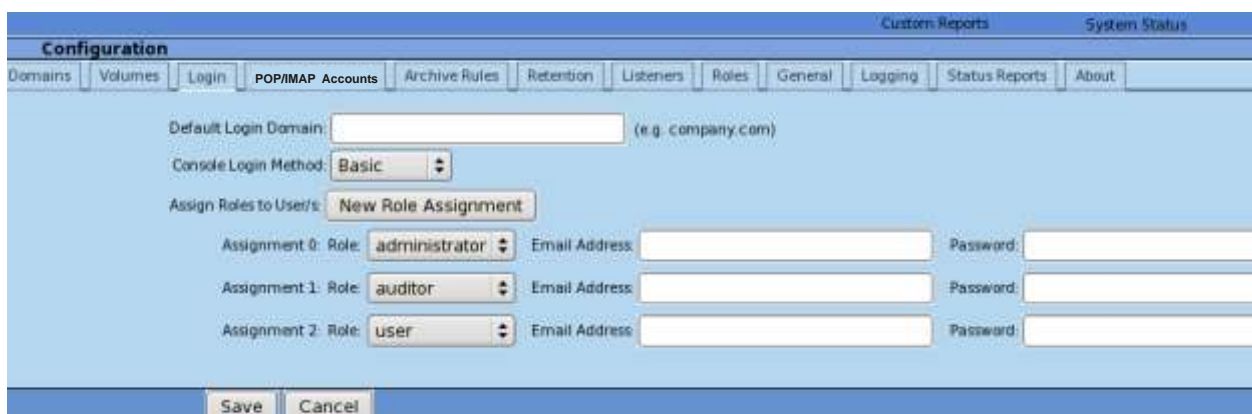
An example domain is example.com. The entered domains are used by the server to assess whether the origin and destination of emails are internal or external to your organization. If your organization has an internal domain called example.local and an external one called example.com, you need to include both these domains.

When applying archive rules, the server will match the domain of a given email address with all of the domains entered here.

Authentication

Authentication

Basic Authentication



In the Basic Authentication mode, the server authenticates users from credentials stored in an XML configuration file.

The users.conf configuration file is located in </opt/mailarray/webapps/mailarray/WEB-INF/conf>

```
<Users version="1.0">
<User e-mail="admin@example.com" role="administrator" password="123"/>
<User e-mail="user@example.com" role="user" password="abc"/>
<User e-mail="auditor@example.com" role="auditor" password="xyz"/>
</Users>
```

You can either add users directly using the eMailArray server console configuration screen.

If basic authentication is enabled and no users are defined in the users.conf file, the system will assume that any user can login using any credentials. If you update users.conf using a text editor, the server will pick the changes up automatically without having to restart.

Active Directory Authentication

To configure the AD, enter the fields as described in Table below.

LDAP Server Enter the fully IP of your AD controller

Base DN Base DN where eMailArray must start looking for user accounts. e.g.
For a domain nstest10.nstest1.com the following will be specified for user1

Console Login Method: LDAP/AD

LDAP Server Address: (IP:port)

Base DN: *dc=nstest10,dc=nstest1,dc=com*

Service DN: *cn=administrator,cn=Users,dc=nstest10,dc=nstest1,dc=com*

Service Account *****

Password:

Bind Attribute: Cn

Email Attribute: Email

Assign Roles to User/s: <new role>

Assignment 0: Role: administrator /auditor /user

LDAP Attribute:cn

Match Criterion: user1

Note: The match criterion field also accepts regular expressions for complex pattern matching requirements.

LDAP Authentication

Console Login Method: LDAP/AD

LDAP Server Address: (IP:port)

Base DN: *dc=nstest10,dc=nstest1,dc=com*

Service DN: *cn=administrator,cn=Users,dc=nstest10,dc=nstest1,dc=com*

Service Account *****

Password:

Bind Attribute: Cn

Email Attribute: Email

Assign Roles to User/s: <new role>

Assignment 0:

Role: administrator/auditor/user

LDAP Attribute: cn

Match Criterion: user1

When LDAP authentication is enabled, eMailArray authenticates to a directory service such as Open LDAP using pure password-based credentials. It is configured in the same way as Active Directory authentication.

NOTE in both LDAP/AD In specifying the match criterion field, it is useful to lookup the LDAP attribute name and values associated with a user. You do this by clicking the Lookup button and entering a user's username (e.g. admin@nstet1.com) and a password. A simple way to assign a role to an individual user is to copy one of the values of any of the attributes and paste them into the match criterion field. There is likely to be an error in your configuration if the Lookup dialog does not return any LDAP attribute values.

Note: If you get locked out from the web console during the below configuration procedure, Do the following:

1. Edit the file server.conf located in /opt/maillarray/webapps/maillarray/WEB-INF/conf
2. Set .security.loginmethod=basic and edit the file users.conf
3. Restart the server

IMAP/POP Account Connection

IMAP/POP Account Connection

In the Journal Accounts tab of the emailarray server console configuration screen, click Add Journal Account and do the following:

- Select IMAP as the preferred protocol
- Enter the server address of your Exchange server
- Enter the IMAP account username and password
- For the Connection Mode, select .TLS when available.

Configuration form for IMAP/POP Account Connection:

- Polling Wait Interval (Secs): 0
- Maximum Messages To Process: 50 (when polling)
- New POP/IMAP Account: New POP/IMAP Account
- Connection 0:
 - Enabled:
 - Polling Schedule: Any Time
 - Protocol: IMAP
 - Server: [Empty]
 - Port: 143 SSL Port: 993
 - Username: [Empty]
 - Password: [Empty]
 - Connection Mode: TLS, when available
 - During IMAP retrieval, process unread messages only (enable recommended)
 - Listen for message arrival notifications from server (IMAP Idle)
 - Authenticate server x.509 certificate
- Actions: Delete Test POP/IMAP Account Connection

Ensure Auth Certs is unchecked

Test Account Connection

Click the Test Connection button to determine if the connection is established. If the test is successful, save your configuration settings and emails should start appearing in the search results in a matter of a few seconds. If eMailArray cannot establish a connection to IMAP server, verify that you entered the correct information in case of Exchange verify that SMTP connector is listening. For POP the configuration is similar except that Protocol is POP and the port is 110.

****Note

In case of MS Exchange if you do not want to have IMAP or POP connector you can configure it to SMTP all mails through a journal.

The configuration is explained in the exchange connection document.

Sendmail Connection

The emailarray server incorporates a sendmail milter server and thus is able to integrate with sendmail and postfix directly.

(1) Add the following to Sendmail.s sendmail.mc file:

```
INPUT_MAIL_FILTER(`eMailArray', `S=inet:8092@127.0.0.1')dnl
```

(2) Compile the sendmail.mc file

```
sudo m4 /etc/mail/sendmail.mc >/etc/mail/sendmail.cf
```

(3) Restart send mail

```
sudo /etc/init.d/sendmail restart
```

Postfix Connection

(1a) Add the following to Postfix.s main.cf file:

```
milter_default_action = tempfail
```

```
smtpd_milters = inet:127.0.0.1:8092
```

(1b) For larger volumes use in main.cf

```
always_bcc = archive@archive.domain.com
```

```
fast_flush_domains = archive.domain.com
```

```
in postfix transport
```

```
archive.domain.com smtp:[192.168.X.X]:2525
```

```
postmap transport
```

(2) Restart send mail

```
sudo /etc/init.d/postfix restart
```

Exim Connection

Add a new router to the exim.conf file before the existing router(s) that accepts all mail and is defined as unseen. For example, add the following block right after the line "begin routers":

```
netcore_archive:
```

```
driver = accept
```

```
transport = netcore_delivery
```

```
unseen
```

Define the SMTP transport for the router. For example, add the following block right after the line "begin transports":

```
netcore_delivery:
```

```
driver=smtp
```

```
hosts=<ip>
```

```
port=2525
```

```
Allow_localhost=true
```

Other Mail Servers Configuration

There are 3 main ways to connect your mail server to eMailArray, namely:

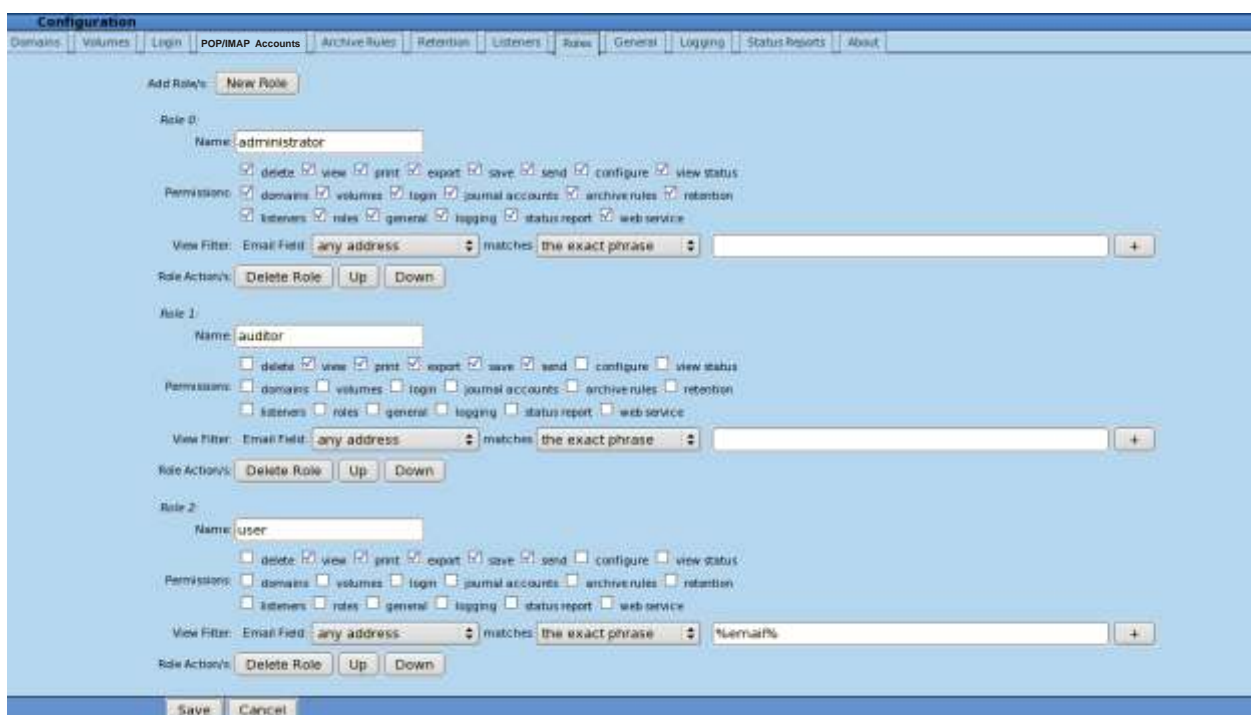
By forwarding SMTP traffic to eMailArray

By configuring eMailArray to fetch mail from your mail server using POP

By configuring eMailArray to fetch mail from your mail server using IMAP

Roles

ROLES



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:

Permissions . what the user can do (e.g. delete email)

View filters . which emails the user can see (e.g. only emails within a 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 X and X, respectively.

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

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. To define a custom role:

Click on the Add Role button in the Custom Role tab of the server console configuration screen

Enter an appropriate name for the role

Select the permissions associated with the role

Archive Rules

Archive Rules

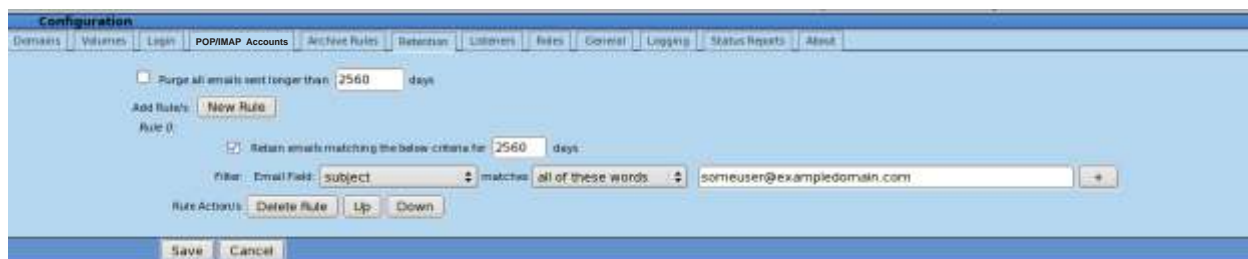
In some circumstances, it may not be desirable to archive all e-mails. Archive rules are used to determine whether or not an e-mail should be archived. As an administrator, you can choose to archive incoming, outgoing and/or internal e-mails. If these basic rules are not granular enough, advanced rules may be defined that will determine whether or not to archive an e-mail based on specific criteria.

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 e-mail 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. By selecting any of the following or all of the following, any or all of the clauses in the rule must match for it to apply. Each clause consists of an email field, an operator and a value. When processing a clause, the value of the selected email field is retrieved from the e-mail and compared against the value specified in the clause. If they match, the action, either .ignore., .archive. or .do not archive., is applied. For example, to ensure all e-mails addressed to john@company.com are archived, you would simply select the field .to., select the "contains" operator and enter .john@company.com..

Retention Policy

Retention Policy



Your company retention policies are defined in the Retention tab of the Configuration screen. By selecting .purge all emails sent longer than X days., eMailArray will automatically delete all emails that are older than X days. If so desired, the option is available to define granular retention rules for emails that match certain criteria. When a rule matches, the eMailArray may delete the email if it is older than the specified period.

Search Queries

SEARCH QUERIES

The search function in the server console is sufficiently intuitive that it does not warrant detailed discussion. However, it's worth mentioning that eMailArray 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.

Email Operations

EMAIL OPERATIONS



To perform an operation such as export a set of emails:

- (1) perform a search using the search field and matches
- (2) select the concerned emails
- (3) click the icon appropriate icon in the toolbar

Icon Description

Select across all search pages	
Deselect every email	
View the selected emails	
Print selected emails	
Export the selected emails to a compressed ZIP file	
Save the search results to a CSV file	
Restore the selected to emails to a given email address	
Delete selected emails	