

Willkommen
Bienvenidos
Welkom
Bienvenue
Welcome



MailArchiva
Open Source Edition
v1.7

**INSTALLATION
AND ADMINISTRATION
GUIDE**
For Windows / Linux

1 INDEX

Table of Contents

1	INDEX.....	2
2	IMPORTANT NOTE.....	4
3	CONTACT INFORMATION.....	4
4	CONTRIBUTORS.....	5
5	HARDWARE REQUIREMENTS.....	5
6	OVERVIEW.....	6
7	HIGH-LEVEL FEATURES.....	7
8	ARCHITECTURE.....	9
9	INSTALLATION.....	10
9.1	EXCHANGE SERVER CONFIGURATION.....	11
9.2	SERVER INSTALLATION (ON WINDOWS).....	14
9.3	SERVER INSTALLATION (ON LINUX).....	15
9.4	MICROSOFT EXCHANGE.....	16
9.5	SENDMAIL.....	17
9.6	POSTFIX.....	17
9.7	QMAIL / EXIM.....	17
9.8	OTHER MAIL SERVERS.....	18
10	CONFIGURATION.....	18
10.1	SERVER CONFIGURATION	18
10.1.1	Local Domains.....	18
10.1.2	E-mail Encryption Password.....	18
10.1.3	Volumes.....	19
10.1.4	Console Access.....	20
10.1.4.1	Basic Authentication.....	20
10.1.4.2	Active Directory Authentication.....	21
10.1.5	Roles.....	23
10.1.6	Archive Rules.....	23
10.1.7	Advanced Configuration Options.....	24
10.2	SERVER TROUBLESHOOTING.....	25
10.2.1	Audit & Debug Logging.....	25
10.2.2	Common Problems.....	26
11	SEARCH QUERIES.....	27
12	EMAIL OPERATIONS.....	27
13	EMAIL MIGRATION.....	28
14	DISTRIBUTED SEARCH.....	28
15	INTERNATIONALIZATION.....	28
16	DECRYPTION SOURCE CODE.....	29
17	LICENSE.....	29

18 APPENDIX	29
18.1 REGULAR EXPRESSION SYNTAX.....	29

2 IMPORTANT NOTE

This Administration Guide covers installation and configuration of MailArchiva Enterprise Edition on both Linux and Windows platforms.

 **It is essential to read this Administration Guide prior to install.**

3 CONTACT INFORMATION

Contact Method	Contact Information
Sales/Support Line	(USA) +1-(713)-366-8072 (EU) +44-20-80991035
FAX	(USA) +1-(713)-366-8072 (EU) +44-20-80991035
Web Site	http://www.mailarchiva.com
E-mail Queries	info@mailarchiva.com
Enterprise Support	support@mailarchiva.com
Knowledge Base	http://Knowledge.stimulussoft.com
Sourceforge Project Page	http://sourceforge.net/projects/openmailarchiva/
Community Support Forum	http://sourceforge.net/projects/openmailarchiva/

4 CONTRIBUTORS

We thank the below contributors for their generous support in improving MailArchiva.

Name	Contribution
Kay Zenner	Reengineering of the MailArchiva Agent, German language translation and various internationalization fixes.
Jurgen Bravenboer	Dutch translation
Jonathan Tellier Siméon Commergnat	French translation
Hailer Wang	Chinese translation
Moises Marin	Spanish translation
Valentin Popov	Russian Translation

If you would like to contribute to MailArchiva, please send us a note.

5 HARDWARE REQUIREMENTS

Operating Systems	Windows XP Professional, Advanced Server 2003 Ubuntu or Redhat Linux
Disk Storage	Compatible with most Storage Area Networks (SANs) and Network Attached Storage (NAS) devices
Hardware	Dual Core XEON 2.0 GHZ 2 GB RAM SATA (500 mailboxes)
Mail Servers	Microsoft Exchange 5.5 / 2003 Microsoft Exchange 2007 ♦ IPSwitch IMail Postfix, Sendmail, Qmail, Exim Qmail, Lotus Domino, etc.

 **If you are using an older Windows NT Domain Controller, you will need to use MailArchiva's in built authentication mechanism (i.e. Basic Authentication).**

6 OVERVIEW

MailArchiva is an easy-to-use, yet feature-rich, e-mail 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 e-mail retention, monitoring and compliance policies throughout your organisation.

In many jurisdictions around the world, the law requires that company emails are kept for up to seven years. MailArchiva 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).

MailArchiva 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.

The main business benefits are:

- ◆ Preserve and access vital company knowledge
- ◆ Monitor and audit employee e-mail communications
- ◆ Ensure strict compliance with US and EU legislation (e.g. Sarbanes Oxley Act)
- ◆ Protect against law suits and legal actions
- ◆ Enhance the performance of Exchange by storing e-mails off the server
- ◆ Lower the cost of storing e-mails (compression)
- ◆ Avoid vendor lock in with proprietary formats
- ◆ End PST Hell (and not replace it with SQL Hell)
- ◆ Give users long-term access to their emails

In contrast to many other e-mail archiving systems, MailArchiva stores e-mails 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.

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

7 HIGH-LEVEL FEATURES

Feature	OSE	EE
Admin console available in English, French, Dutch, Chinese, German and Spanish	✓	✓
Archive all incoming, outgoing and internal e-mails	✓	✓
Search, view, sort archived e-mails	✓	✓
Find e-mails using complex search criteria	✓	✓
Search inside Word, Powerpoint, Excel, PDF, RTF, ZIP, tar, gz attachments	✓	✓
Define granular archiving rules according to policy	✓	✓
Save on storage costs by storing e-mail in compressed format	✓	✓
Easy-to-use web-based user interface	✓	✓
Login to web console using Windows authentication	✓	✓
Login to web console using in built authentication	✓	✓
Permit/restrict employee access to their own e-mails	✓	✓
Restrict access to web console based on Windows user groups and attributes	✓	✓
Comprehensive audit trail and system logging	✓	✓
No database required - messages are stored directly on the file system	✓	✓
Supports multiple volumes (disk drives)	✓	✓
Messages stored in standard RFC822 format	✓	✓
Tight security - all e-mails encrypted	✓	✓
Interfaces with multiple mail systems via MAPI, IMAP, POP	✓	✓
Sendmail support	✓	✓
Postfix support	✓	✓
QMail support	✓	✓
Exim support	✓	✓
Fully internationalized - multiple language support	✓	✓
Do-it-yourself, easy setup		✓
Export e-mails en bulk		✓
Print e-mails en bulk		✓
Delete e-mails en bulk		✓
Microsoft Exchange 2007 Support		✓
Microsoft Exchange Envelope Journaling - stores all e-mail header / addressing information (including BCC fields and Exchange groups)		✓
Multiple Microsoft Exchange Stores - archive e-mails in multiple exchange stores		✓
Multiple Exchange Servers - archive e-mails from multiple Exchange Servers		✓
Smart attachment storage - save space by storing only one copy of an attachment across several e-mails		✓
Restoration of e-mails en bulk to multiple mail systems		✓
Email retention policy		✓
Distributed search - search across multiple machines simultaneously		✓

Authenticate to the console using LDAP authentication		✓
Single instance message storage		✓
Message failover and recovery	✓	✓
Convert messages in PST files to MailArchiva	✓	✓
Convert messages from Exchange to MailArchiva	✓	✓
Flexible Role management system		✓
Builtin IMAP and POP client	✓	✓

Table 1 MailArchiva EE Features

8 ARCHITECTURE

The MailArchiva server archives emails from external mail systems such as Microsoft Exchange, Postfix, Sendmail and others. It can either accept SMTP or sendmail milter traffic from these external mail systems or it can fetch mail from them using IMAP or POP.

The MailArchiva Server can run on any server on your network provided it has TCP/IP connectivity to your mail server. Also, if you intend to authenticate users logging into the server console using Active Directory, then there must be TCP/IP connectivity between the MailArchiva server and the server hosting Active Directory. For optimal performance, and to minimize changes to the server hosting your mail system, it is recommended that the MailArchiva server run on a dedicated server platform.

In addition to archiving e-mails, the server provides a web interface that is used to administer the product. This interface, referred to as the "server console", also provides the capability for users to search and retrieve e-mails. Access to the server console is restricted to authenticated users only. An authenticated user may assume an administrator, auditor or a user role. Each of these roles implies a different set of entitlements, which are discussed later in this guide.

For simplicity sake, the server may be configured to authenticate users using credentials contained in a simple XML configuration file (Basic Authentication). Alternatively, the server may be setup to authenticate users using Microsoft Active Directory (Active Directory Authentication) or using basic LDAP authentication. The benefit of authenticating with Active Directory or an LDAP server is that you can manage all your user accounts centrally, using standard administration tools.

If there is a firewall running between any of the components in the architecture, you will need to the communications ports as described in Table 2.

Source	Destination	Protocol	Ports
MailArchiva Server	Active Directory	Kereberos, LDAP	88, 389
MailArchiva Server	Microsoft Exchange	IMAP	143, 993
Sendmail/Postfix	MailArchiva Server	Sendmail milter	8092*
Mail Server	MailArchiva Server	SMTP	8091

* by default, you can change this port

Table 2 Communication Ports

9 INSTALLATION

The MailArchiva e-mail archiving system can be configured to interoperate with a wide array of mail servers. As such, the configuration steps vary depending on your particular choice of mail systems.

Mail Server	Description	Sections
Exchange	You are using Microsoft Exchange	9.1, 9.2, 9.3, 9.4
Sendmail	You are using the Sendmail mail server	9.2, 9.3, 9.5
Postfix	You are using the Postfix mail server	9.2, 9.3, 9.6
Qmail/Exim	You are using the Qmail mail server	9.2, 9.3, 9.7
Alternate	All other mail servers	9.2, 9.3, 9.8

Table 3 Installation Sections to Complete

Before you begin the installation procedure, ensure that you have met the technical requirements of the product stated earlier. Please take note of all IP addresses, usernames and passwords entered during the installation process.

9.1 Exchange Server Configuration

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

Microsoft Exchange supports three different types of message journaling:

- Standard Journaling
- BCC Journaling
- Envelope Journaling


In Standard Journaling, when an e-mail 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. With 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 Table 4 for an overview of Microsoft Exchange related features supported by MailArchiva OSE and EE.

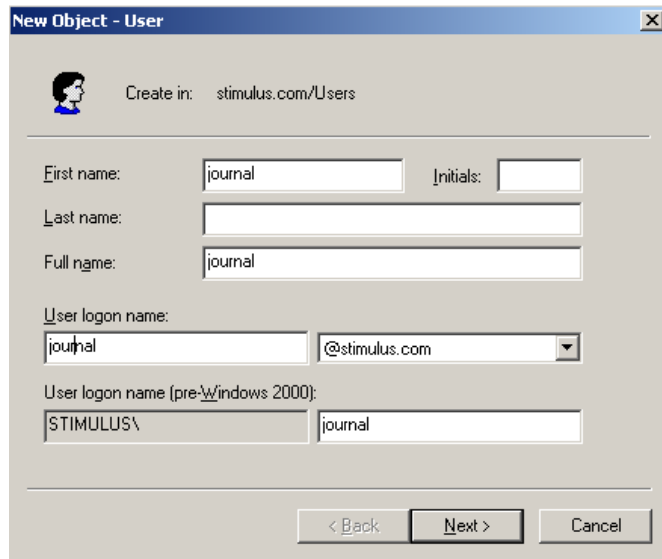
Microsoft Exchange	MailArchiva OSE	MailArchiva EE
Standard journaling	✓	✓
BCC journaling	✓	✓
Envelope journaling		✓
Multiple mail stores		✓
Multiple exchange servers		✓

Table 4 MailArchiva Exchange Features

 **The Enterprise Edition has the capability to display and index Envelope journalled messages correctly. If you intend to enable Envelope Journalling, it recommended to use the Enterprise Edition.**

Step 1. Create 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

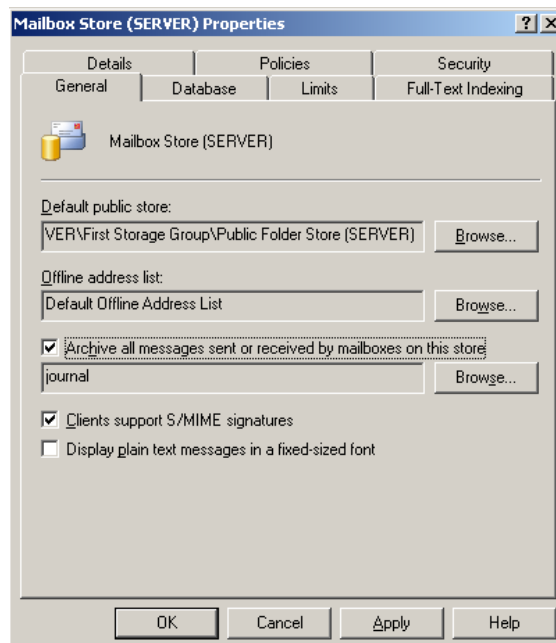
User logon name (pre-Windows 2000): STIMULUS\ journal

< Back Next > Cancel

Figure 1 Journaling Account Creation

Step 3. 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 will appear as in Figure 2. 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

Figure 2 Enable Journaling


Step 3. Enable BCC Journaling

 **IGNORE this step if you running Microsoft Exchange 2007.**

(envelope journaling is enabled by default in Microsoft Exchange 2007)

Follow the below steps to enable BCC journalling on your Microsoft Exchange 2003 server:

- 1) Start the registry editor (regedit.exe).
- 2) Navigate to
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeTransport\Parameters.
- 3) From the Edit menu, select New - DWORD value.
- 4) Enter a name of JournalBCC and press Enter.
- 5) Double-click the new value and set it to 1. Click OK.
- 6) Restart the SMTP service (open a command line and enter net stop smtpsvc, then net start smtpsvc).

 **The Open Source Edition does not currently support Envelope Journalling. If you wish to use Envelope Journalling, we recommend the use of the MailArchiva Enterprise Edition product. MailArchiva EE indexes MS Exchange envelope data and displays original message content in the search interface.**

9.2 Server Installation (on Windows)

Step 1. Install MailArchiva

Run the MailArchiva Server Setup and follow the instructions on screen. It is strongly recommended that you install both the MailArchiva Server and Application Server components. In the event that you wish to install the server application on an existing instance of Apache Tomcat, you may install the .WAR file on its own.

Step 2. Check Availability of Port 8090

By default, MailArchiva uses port 8090. Before starting the server, ensure that port 8090 is not being used by another application. You can do this by typing "netstat -abn" from the console. If port 8090 is in use, edit the file C:\Program Files\MailArchiva\Server\conf\server.xml and change all references from "8090" to the desired port.

Step 3. Start MailArchiva Server

The MailArchiva application appears in the Windows task tray. Double click the MailArchiva task tray and click Start. Verify that the server is started correctly by clicking Start->Program Files->MailArchiva Console Login. If you see a login box in the browser window, the MailArchiva server is installed correctly. You can control the MailArchiva service directly from the Windows Services applet in the Control Panel.

Step 4. Configure Server Settings

This final step involves configuring the server. There are at minimum four 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. To complete these tasks, follow the instructions Chapter 10.

9.3 Server Installation (on Linux)

The MailArchiva Server can be installed on a variety of Linux distributions and operating systems. The instructions in this section illustrate the steps required to install the server on Fedora specifically.

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

Step 1. Install/Upgrade MailArchiva Server

To install the server, type the following:

```
tar -xvzf mailarchiva_open_source_edition_server_v1_7_7_linux.tar.gz
cd mailarchiva_dist
sudo install.sh
```

Following the above, the server executables will be installed `/usr/local/mailarchiva/server`.

```
cd /usr/local/mailarchiva/server
```

Step 2. Check Availability of Port 8090 and Port 8091.

By default, MailArchiva uses port 8090 and port 8091. Before starting the server, ensure that these ports are not being used by another application. You can do this by typing "netstat -vatn" from the console. If port 8090 is in use, edit the file `/usr/local/mailarchiva/server/conf/server.xml` and change all references from "8090" to the desired port.

Step 3. Start MailArchiva Server

To start the MailArchiva Server from the commandline type:

```
sudo sh /etc/init.d/mailarchiva start
```

Type: "<http://localhost:8090/mailarchiva>" in a web browser to access the web console. If you cannot access the console, check that port 8090 is open on your firewall and examine the log files in `/usr/local/mailarchiva/server/logs`

To stop the server, you would type:

```
sudo sh /etc/init.d/mailarchiva stop
```

Step 4. Configure Server Settings

This final step involves configuring the server. There are at minimum 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. To complete these tasks, follow the instructions Chapter 10.

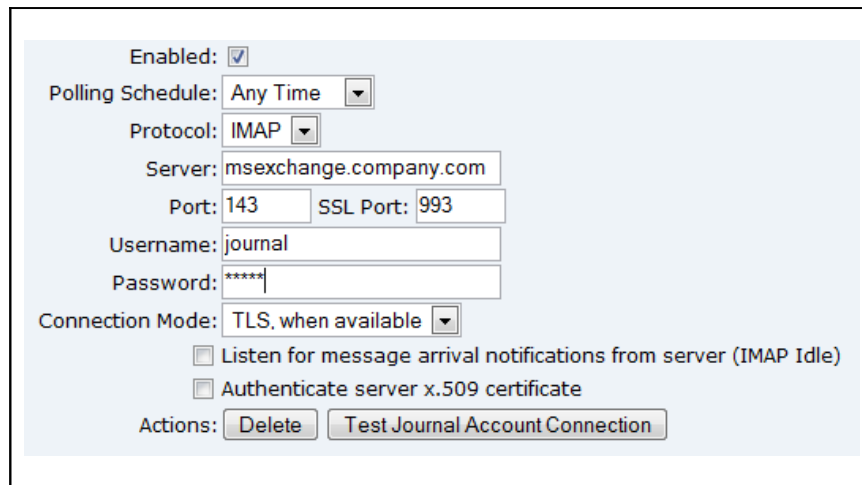
9.4 Microsoft Exchange

MailArchiva can interface with Microsoft Exchange in a variety of ways. The easiest way is to configure MailArchiva 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.

Step 1. Add a Journal Account Connection

In the Journal Accounts tab of the MailArchiva 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 Microsoft Exchange journal account username and password
- For the Connection Mode, select "TLS when available"
- Ensure Auth Certs is unchecked



The screenshot shows the configuration interface for adding a journal account. The 'Enabled' checkbox is checked. The 'Polling Schedule' is set to 'Any Time'. The 'Protocol' is set to 'IMAP'. The 'Server' field contains 'msexchange.company.com'. The 'Port' is '143' and the 'SSL Port' is '993'. The 'Username' is 'journal' and the 'Password' is masked with asterisks. The 'Connection Mode' is set to 'TLS, when available'. There are two unchecked checkboxes: 'Listen for message arrival notifications from server (IMAP Idle)' and 'Authenticate server x.509 certificate'. At the bottom, there are 'Delete' and 'Test Journal Account Connection' buttons.

Figure 3 Mailbox Connection To Microsoft Exchange

Step 2. Test Journal 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 MailArchiva 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) and the short name (e.g. journal).

 **If you do not wish to have Exchange's IMAP service enabled, you can also interface with MailArchiva by configuring Exchange to forward SMTP traffic to MailArchiva. Alternatively, you can also use the MailArchiva Exchange agent. Refer to <http://knowledge.mailarchiva.com> for more information on these approaches.**

9.5 Sendmail

The MailArchiva 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(`mailarchiva', `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
```

9.6 Postfix

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

```
milter_default_action = tempfail  
smtpd_milters = inet:127.0.0.1:8092
```

(2) Restart send mail

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

9.7 Qmail / Exim

Consult the MailArchiva Knowledge Base (<http://knowledge.mailarchiva.com>) as it contains a patch that provides interoperability with Qmail.

9.8 Other Mail Servers

There are four main ways to connect your mail server to MailArchiva, namely:

- By forwarding SMTP traffic to MailArchiva
- By forwarding Sendmail milter traffic to MailArchiva
- By configuring MailArchiva to fetch mail from your mail server using POP
- By configuring MailArchiva to fetch mail from your mail server using IMAP

The MailArchiva knowledge base (<http://knowledge.mailarchiva.com>) includes further instructions on how to interface MailArchiva with a variety of mail systems.

10 CONFIGURATION

10.1 Server Configuration

The server configuration settings are accessible from the Configuration screen in the web console. Only users with administrator rights can view or modify configuration settings.

To access the web console from Windows, click Start->Program Files->MailArchiva->MailArchiva Console Login. On Linux, type: "<http://localhost:8090/mailarchiva>" in a web browser.

If the server is installed correctly, you should see the MailArchiva login screen. If this is the first time you are configuring the product, you may simply hit enter to login. By default, authentication to the web console is disabled.

10.1.1 Local Domains

When configuring MailArchiva 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. An example domain is "company.com" or "company.local". The entered domains are used by the server to assess whether the origin and destination of e-mails are internal or external to your organization. When applying archive rules, the server will match the domain of a given e-mail address with all of the domains entered here. If your organization has an internal domain called "company.local" and an external one called "company.com", you need to include both these domains.


10.1.2 E-mail Encryption Password


All e-mails are stored encrypted using triple DES password-based encryption. Before using the server to archive e-mails, you need to choose and enter an E-mail 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 e-mails, you need to ensure that the password is kept highly confidential and secret. It is also

important to bear mind that you cannot change the password once the server has begun to archive e-mails.

Once you have set the encryption password, it is essential to backup the file server.conf located in mailarchiva\server\webapps\MailArchiva\WEB-INF\conf from the root of your MailArchiva installation directory. This file contains your password and a specific salt value used for e-mail encryption purposes. If you lose either of these, you will be unable to access the e-mails archived by the server in perpetuity!

 **It is of paramount importance that a backup of the server.conf configuration file is made and that is stored in a secure location.**

 **Java source code to decrypt archived messages to RFC822 is available on sourceforge.net.**

10.1.3 Volumes

Archived e-mails 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.

When a 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.

To create a volume, click the "New Volume" button 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 you explicitly close the volume. 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 such time as a new volume is added.

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.

Table 5 Volume Status

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.

10.1.4 Console Access

The MailArchiva server can be configured such that only authorised users are able to access the web console and its features. There are two types of authentication mechanisms currently supported: Basic, Active Directory and LDAP authentication. When the server is set to use Basic Authentication, users are authenticated using credentials stored in a configuration file. When Active Directory Authentication is enabled, users login to the web console using their normal Windows login credentials. In addition, MailArchiva can be configured to authenticate against users in standard directory such as OpenLDAP.

In all modes, if authentication is successful, a role is assigned to the authenticated user. The user's role determines what the user can and cannot do within the application. Refer to Section X to learn more about MailArchiva's role mechanism.

10.1.4.1 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 mailarchiva\server\webapps\MailArchiva\WEB-INF\conf from the root of your MailArchiva installation directory.

You can either add users directly using the MailArchiva server console configuration screen or by editing the server.conf directly. The server.conf file, as illustrated in Figure 4, contains a list of users, each of which has an e-mail address, role and a password. The users listed in users.conf will login using an e-mail address and password that corresponds with an entry in the file. Once a user is authenticated, the user will be assigned the specified role.

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

Figure 4 Users.conf

! 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.

10.1.4.2 Active Directory Authentication

Users logging into the MailArchiva web console can be authenticated using their credentials residing in Active Directory (AD). The following process occurs during login:

- 1) User enters user name and password into the console login screen
- 2) MailArchiva authenticates with AD using a service (i.e. admin) account
- 3) MailArchiva searches all entries in the subtree from a base DN
- 4) MailArchiva finds a user account in AD whose SamAccountName field matches the username supplied in the login screen
- 5) MailArchiva retrieves the DN of the found user
- 6) MailArchiva authenticates the user
- 7) MailArchiva assigns a role to the user by matching the LDAP attribute of the role with the user's attributes in AD

To configure the AD, enter the fields as described in Table 6 below.

Volume Status	Description
Kerberos Server (KDC) FQDN	Enter the fully qualified domain name of your AD controller (do not enter the IP address)
Kerberos Server (KDC) IP Address	Enter the IP address of your AD controller
LDAP Server	Enter the fully qualified domain name of your AD controller (do not enter the IP address)
Base DN	Base DN where MailArchiva must start looking for user accounts. e.g. dc=company, dc=com.
Service Account Login	Login name of an account with sufficient privileges to search the LDAP tree as specified by the Base DN. Must be in the form SamAccountName@realm.
Service Account Password	Password of the service account.

Table 6 Active Directory Settings

When assigning roles to Active Directory users, it is necessary to select a role, select an LDAP attribute and enter a match criterion.

Field	Description
Role	Role to be assigned
LDAP Attribute	LDAP attribute to use for the role assignment
Match Criterion	A value that is compared against a corresponding LDAP attribute in Active Directory for an authenticating user.

Table 7 Role Assignment Fields

A user in Active Directory has a set of LDAP attributes associated with it. These attributes are essentially properties about the user (e.g. account name, user group, etc.). During console authentication, once the user has been identified, the value of your attribute selection is retrieved from Active Directory. This value is compared against the value you enter in the match criterion field. If there is a match, the role you select is assigned to the user.

To assign a role to a Windows user, simply select "SAMAccountName" as the LDAP attribute and enter the user's name in the match criterion field.

To assign a role to all users within a user group, select "memberOf" in the attribute field and enter the distinguished name of the user group in Active Directory (e.g. "CN=Enterprise Admins,CN=Users,DC=company,DC=com").

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

LDAP Attribute	Match Criterion Value
memberOf	Active Directory user group CN=Enterprise Admins,CN=Users,DC=company,DC=com
userPrincipalName	jdoe@company.com
SAMaccountName	Jdoe
distinguishedName	CN=John Doe,CN=Users,DC=company,DC=com

Table 8 Match Criterion Sample Values

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@company.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 described in Table 5 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.

Once you've configured your role assignments, execute a Test Login to ensure that your Kerberos settings, LDAP settings and user roles have been configured correctly. If you encounter problems, enable server debugging as described in Section 10.2.1 to determine the source of the problem.

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 `mailarchiva\server\webapps\MailArchiva\WEB-INF\conf`
2. Set `"security.loginmethod=basic"` and edit the file `users.conf`
3. Restart the server

10.1.5 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 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 9 and Table 10, 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

Table 9 Built-In Role Permissions

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

Table 10 Built-In Role Email Filters

If the built-in roles are not suitable, consider upgrading to the Enterprise Edition. The EE product offers the capability to define custom roles with any desired set of permissions. In addition, it is possible to restrict users assigned a given role to viewing only a specific set of emails.

10.1.6 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”.

10.1.7 Advanced Configuration Options

In addition to the configuration options accessible in the server console, there are a variety of hidden options that one can use to fine tune the server. All configuration outlined in Table 11 below are set in server.conf located in mailarchiva\server\webapps\MailArchiva \WEB-INF\conf.

Key	Values	Description
Volume.diskspace.wait	seconds	seconds to wait between disk space checks
Volume.diskspace.warn	megabytes	megabytes remaining on volume before disk space warning is outputted in debug log
Volume.diskspace.threshold	megabytes	megabytes remaining on volume before disk space is considered used
Volume.diskspace.check	yes/no	Whether to perform disk space checks
security.pbealgorithm	algorithm name	Java password-based encryption (PBE) algorithm used for encrypting messages. Default is “PBEWithMD5AndTripleDES”. See JCE API for more details
search.maxresults	number	Default maximum search results
search.analyzer.language	two letter language identifier	Used in conjunction with search.analyzer.class to specify custom Lucene analyzer for specific a language. e.g. “en”
search.analyzer.class	java class name	Specifies the Java class name of a custom Lucene analyzer. Binds index/search languages to bespoke analyzers.
e-mailaddress.map.attribute	LDAP attribute	The LDAP attribute containing the smtp e-mail address in Active Directory. This attribute is used to extract the user’s e-mail address for the purposes of limiting search results for those users who are assigned the

Key	Values	Description
		"user role".
emailaddress.map.pattern	Regex Pattern	Used in conjunction with emailaddress.map.attribute to extract smtp addresses from users in Active Directory.
smart.attachment.minimum.size	Bytes	Minimum size of an attachment before it is separated from the body of an email.

Table 11 Advanced Configuration Options

To change the port that you use to connect to the Web Console edit the file server\conf\server.xml and change all references from "8080" to the desired port.

10.2 Server Troubleshooting

10.2.1 Audit & Debug Logging

The MailArchiva server has comprehensive logging facilities. There are two logs: the audit log and debug log:

- Audit Log - used for audit and forensic analysis purposes. It records all archiving and user activities in a concise manner.
- Debug Log - used for troubleshooting and debugging purposes. All errors and exceptions are reported in the debug log.

A shortened summary of each log file is accessible from the server console configuration screen. Table X outlines where the log files can be found on disk.

Log	Location
Audit Log	MailArchiva\Server\logs\audit.log (Windows) /usr/local/mailarchiva/server/logs/audit.log (Linux)
Debug Log	MailArchiva\Server\logs\debug.log (Windows) /usr/local/mailarchiva/server/logs/debug.log (Linux)

Table 12 Log File Locations

If you are experiencing problems with the server, the debug log is an invaluable tool that will assist you in getting to the root of the problem. By default, the server will output all warnings, exceptions and errors to the debug log. To enable detailed logging (i.e. to include troubleshooting messages) set the log level to troubleshoot in the Logging tab of the server console configuration. Alternatively, edit the file log4j.properties in server\webapps\WEB-INF\classes and replace all references to "info" with "debug". You will need to restart the server before the settings will take effect.

Log4j.logger.com.stimulus.MailArchiva.audit=debug, MailArchivaaudit Log4j.logger.com.stimulus.MailArchiva=debug, MailArchivadebug
--

Figure 5 log4j.properties

During normal operations, for performance reasons, it is not recommended to run the server with detailed debug logging enabled.

10.2.2 Common Problems

The most commonly encountered Server problems are described Table 13.

Problem	Resolution
The server wont start	(1) The server is not pointing to a valid JRE (2) There is not enough memory allocated to the JVM (3) There is not enough physical memory on the machine Please check all log files in mailarchiva/server/logs. Run the file MailArchivaServer .exe in mailarchiva/server /bin manually.
The server archives zero byte messages	The Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files are not installed correctly.
Archived emails are not showing up in the console.	This could be any of the following: (1) Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files are not installed correctly (2) No UNUSED volumes are available (3) You've run out of disk space (4) An encryption password is not yet (5) You have an older version of the JRE installed. You need V1.6. (6) The server is running out of memory. You need to increase the heap space allocated to the server JVM.
Server has run out of memory	The server may require large amount of memory to process extremely large emails. If you see out of memory exceptions in the server logs, you need to increase the heap space allocated to the server JVM. You do this by following the below: (1) Right click the server task tray icon at bottom right corner of the screen (2) Click Configure (3) Click Java tab (4) Increase the Maximum memory pool size (5) Restart the server (6) Test by sending a very large message (7) Examine debug.log to determine if successful

Table 13 Common Server Problems

11 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 MailArchiva 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. Refer to Section 15 for an explanation of MailArchiva's internationalization capabilities.

MailArchiva embeds the highly regarded Lucene search engine. As such it can perform a range of other search functions such as fuzzy and proximity based searches. For a comprehensive description of these capabilities, please refer to Lucene's documentation available at <http://lucene.apache.org>.

12 EMAIL OPERATIONS

The bulk email-related operations described in Table 14 are available in MailArchiva Enterprise Edition only. To perform an operation such as export a set of emails:

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

In (2), you may select emails individually, in the currently displayed page, or across the entire search results.









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

Table 14 Bulk Email Operations

13 EMAIL MIGRATION

MailArchiva archives emails as they are processed by the email server. If you'd like to access older (pre-deployment) emails, you will need to import them using a variety of utilities. available in the MailArchiva utilities package (available on ftp.stimulusoft.com site).

The utilities package contains the following migration tools:

- Ex2MailArchiva – copies emails directly from Microsoft Exchange to MailArchiva. It can also sweep up loose .eml files on hard disks.
- PST2MailArchiva – copies emails from PST files to MailArchiva.

Utilities are available for importing messages in PST, EML/MSG, MBOX and maildir formats. For current information on this topic, refer to the Migration Guide available at:

<http://knowledge.stimulusoft.com/bin/view/Main/MigrationGuide>

14 DISTRIBUTED SEARCH

The MailArchiva server includes a distributed search capability for large deployments. Using this feature, you can execute simultaneous searches on multiple indexes distributed on several machines. By doing this, you can leverage the resources of multiple server simultaneously and thereby increase search performance.

Here is how to implement distributed search:

- (1) Copy an old index to a second machine
- (2) Mount an NFS share, accessible to both machines, on the volume store directory
- (3) Install MailArchiva on the second machine
- (4) Copy the MailArchiva server.conf file from the first machine
- (5) Create a volume on the second machine
 - a) Set archive store to be the mount point that refers to the shared NFS drive
 - b) Set index to be the local index that was copied from the first machine
- (6) On the second machine, click the publish volume for distributed search in the Volumes screen
- (7) On the first machine, in the volume's index location, type "rmi//ipaddress" (where ipaddress is the IP address of the second machine)

You should see that the volume status changes to "REMOTE". This means that the volume is pointing to the index on the external machine.

When you do a search on the first machine, it will use the processing resources of the second machine. The first search operation is slow because it has to initialize the connection. Once this is established, the process works very smoothly.

15 INTERNATIONALIZATION

MailArchiva is an internationalized e-mail archiving system. By default, MailArchiva 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 e-mail archiving process, MailArchiva will automatically attempt to determine the language of the e-mail using N-GRAM analysis. The algorithm requires that there is sufficient text available to determine the language that was used. If there is not sufficient text, MailArchiva will assume that the e-mail is written in the default language. To change the default language, refer to the Section 10.1.7.

The MailArchiva administration console user interface is currently available in English, French, German, Dutch, Chinese and Spanish. MailArchiva 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.

If you would like MailArchiva to support any other language, simply edit the file application.properties in webapps\MailArchiva\WEB-INF\classes\properties. If you do this, it would be most appreciated if you could send us a copy of your translation file for inclusion in future releases.

16 DECRYPTION SOURCE CODE

To ensure that your e-mails are attainable over the long-term, a DecryptMessage utility, along with source code, is available in the mailarchiva/server/utilities directory. If you study the code, you'll notice that it is very straight forward to decrypt and decompress messages in the store. You are free to modify this source code as you see fit.

17 LICENSE

MailArchiva Enterprise Edition is licensed under a proprietary license agreement. Please refer to the license agreement that is bundled with the software.

18 APPENDIX

18.1 Regular Expression Syntax

Construct	Matches
Characters	
<code>x</code>	The character <code>x</code>
<code>\\</code>	The backslash character
<code>\0n</code>	The character with octal value <code>0n</code> ($0 \leq n \leq 7$)
<code>\0nn</code>	The character with octal value <code>0nn</code> ($0 \leq n \leq 7$)
<code>\0mnn</code>	The character with octal value <code>0mnn</code> ($0 \leq m \leq 3, 0 \leq n \leq 7$)
<code>\xhh</code>	The character with hexadecimal value <code>0xhh</code>
<code>\uhhhh</code>	The character with hexadecimal value <code>0xhhhh</code>
<code>\t</code>	The tab character (<code>'\u0009'</code>)
<code>\n</code>	The newline (line feed) character (<code>'\u000A'</code>)
<code>\r</code>	The carriage-return character (<code>'\u000D'</code>)
<code>\f</code>	The form-feed character (<code>'\u000C'</code>)
<code>\a</code>	The alert (bell) character (<code>'\u0007'</code>)
<code>\e</code>	The escape character (<code>'\u001B'</code>)
<code>\cx</code>	The control character corresponding to <code>x</code>
Character classes	
<code>[abc]</code>	<code>a</code> , <code>b</code> , or <code>c</code> (simple class)
<code>[^abc]</code>	Any character except <code>a</code> , <code>b</code> , or <code>c</code> (negation)
<code>[a-zA-Z]</code>	<code>a</code> through <code>z</code> or <code>A</code> through <code>Z</code> , inclusive (range)
<code>[a-d[m-p]]</code>	<code>a</code> through <code>d</code> , or <code>m</code> through <code>p</code> : <code>[a-dm-p]</code> (union)
<code>[a-z&&[def]]</code>	<code>d</code> , <code>e</code> , or <code>f</code> (intersection)
<code>[a-z&&[^bc]]</code>	<code>a</code> through <code>z</code> , except for <code>b</code> and <code>c</code> : <code>[ad-z]</code> (subtraction)
<code>[a-z&&[^m-p]]</code>	<code>a</code> through <code>z</code> , and not <code>m</code> through <code>p</code> : <code>[a-lq-z]</code> (subtraction)
Predefined character classes	
<code>.</code>	Any character (may or may not match line terminators)
<code>\d</code>	A digit: <code>[0-9]</code>
<code>\D</code>	A non-digit: <code>[^0-9]</code>
<code>\s</code>	A whitespace character: <code>[\t\n\x0B\f\r]</code>
<code>\S</code>	A non-whitespace character: <code>[^\s]</code>
<code>\w</code>	A word character: <code>[a-zA-Z_0-9]</code>
<code>\W</code>	A non-word character: <code>[^\w]</code>
POSIX character classes (US-ASCII only)	
<code>\p{Lower}</code>	A lower-case alphabetic character: <code>[a-z]</code>
<code>\p{Upper}</code>	An upper-case alphabetic character: <code>[A-Z]</code>
<code>\p{ASCII}</code>	All ASCII: <code>[\x00-\x7F]</code>
<code>\p{Alpha}</code>	An alphabetic character: <code>[\p{Lower}\p{Upper}]</code>
<code>\p{Digit}</code>	A decimal digit: <code>[0-9]</code>
<code>\p{Alnum}</code>	An alphanumeric character: <code>[\p{Alpha}\p{Digit}]</code>
<code>\p{Punct}</code>	Punctuation: One of <code>!"#\$%&'()*+,-./:;<=>?@[\]^_`{ }~</code>
<code>\p{Graph}</code>	A visible character: <code>[\p{Alnum}\p{Punct}]</code>

