

Jovian Technology 2570 Matheson Blvd E., unit 114 Mississauga Ont L4W 4Z3

Tel: +1. 888. 584. 2584 Fax: +1. 905. 602. 6265 www.joviantechology.com



Europa

Installation Guide

Version 2.0



Copyright © 2006-2007 Jovian Technology Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the written permission of Jovian Technology Inc.

Disclaimer

Information in this document is subject to change without notice. The material contained here is supplied without representation or warranty of any kind. Jovian Technology Inc. therefore assumes no responsibility and shall have no liability of any kind arising from the supply or use of this document or the material contained herein.

Under no circumstances shall Jovian Technology Inc. be responsible for any loss of data or income or any special, incidental, consequential or indirect damages howsoever caused.

The contents of this document are provided 'as is'. Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy, reliability or contents of this document. Jovian Technology Inc. reserves the right to revise or withdraw this document at any time without prior notice.

Table of Contents

Table of Contents.....	3
1.1 Checklist.....	4
1.2 Installation Prerequisites.....	4
1.3 System Environment.....	5
1.4 Network Settings Requirement.....	6
1.5 Technical Support.....	7
1.6 Warranty Policy.....	7
2.0 Hardware Reference.....	8
2.1.1 Front Panel Controls and Indicators.....	8
2.1.2 Rear Panel.....	8
2.2 Physical Installation.....	9
2.2.1 Two methods for obtaining Europa's IP.....	9
3.0 Graphical User Interface (GUI) Setup.....	10
3.1 System Setup.....	11
3.2 Domain Settings.....	13
3.2.1 Service Info.....	13
3.2.1.1 Service Activation Status.....	13
3.2.1.2 System/Domain Service Setup.....	14
3.2.2 Domain Setup.....	15
3.2.2.1 Fail-over configuration.....	16
3.3 Connection Level Protection (CLP) Setup.....	17
3.4 Further Settings.....	19
3.4.1 System Admin.....	19
3.4.1.1 Change admin password.....	19
3.4.1.2 Change Read Only User Password.....	19
3.4.1.3 Define Additional Admin Email Address.....	20
3.5 Set Timezone.....	20
3.5.1 Domain Admin.....	21
3.5.2 LDAP/Active Directory Setup.....	22
3.5.2.1 LDAP configurations.....	22
3.5.2.2 Import LDAP groups.....	23
3.5.2.3 Import LDAP users.....	23

3.5.3 Personal Spam Manager (PSM) Setup.....	25
3.5.4 Anti-Spam Setup.....	26
3.5.5 Anti-Virus Setup.....	27
3.5.6 LAN Access Setup.....	28
3.5.7 Group Admin.....	29
3.5.8 User Admin.....	31
3.5.8.1 Add Single User.....	31
3.5.8.2 Import Multiple Users.....	32
3.5.9 SSL Certificate.....	33
3.6 Diagnostics and Testing.....	34
3.6.1 Reachability Test.....	34
3.6.2 SMTP Test.....	35
3.6.3 System Status.....	35
4.0 Additional Setup outside Europa.....	36
4.1.1 Firewall/Router Setup.....	36
4.1.2 DNS Setup.....	36

1.1 Checklist

You should receive the following in your shipment.

- Europa Appliance machine
- Mounting rails
- Power cord

You may need additional equipments:

- Ethernet Cables – straight and cross
- Desktop/Laptop with internet browser (Internet Explorer or Firefox recommended)

1.2 Installation Prerequisites

Before you commence the installation, please have your Service Provider to review your environment by providing the following info:

- Europa questionnaire
- LDAP (Active Directory) info, if applicable

You may obtain the Europa questionnaire from our website or your Service Provider. LDAP info can be obtained by running the following command in your Active Directory Server:

```
ldifde -f output.ldf
```

This command will create a file called 'output.ldf' containing all your LDAP info.

1.3 System Environment

Please record or select the following network and system environment information in the following section. You may want to change the defaults so that the appliance can co-exist within your network environment. You will require this information during the installation process.

Appliance IP Address: _____ default: 192.168.0.1

Network IP address of the appliance.

Appliance Name: _____ default: europa

Hostname of the appliance.

Network Domain Name: _____ default:

Your company's domain name.

Network Gateway IP address: _____ default:

IP address of your router/firewall connecting to outside internet

Subnet Mask: _____ default: 255.255.255.0

Network mask of your internal network.

DNS IP address: _____ default:

Domain Name Server in your network.

Email Server IP address: _____ default:

Email Server in your network (if applicable).

Mail Gateway IP address: _____ default:

Mail Gateway in your network (if applicable).

HTTPS Port: _____ default: 443

HTTPS port for secure web access to the Europa appliance. You may specify any port number between 1025 and 65535. For external access, you need to set up your firewall with this HTTPS port opened and forwarded to the appliance.

1.4 Network Settings Requirement

For the installation, you only require a computer with an Internet browser. The computer's network connection is required to have DHCP enabled.

1.5 Technical Support

If you have any questions or comments, please contact Jovian Technical Support:

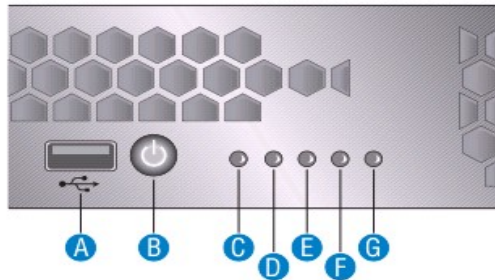
- Phone: 1-888-584-2584
- Email: support@jovianttechnology.com
- Or visit our website for FAQ <http://www.jovianttechnology.com>

1.6 Warranty Policy

Europa is covered under a 90-day warranty against manufacturing defects.

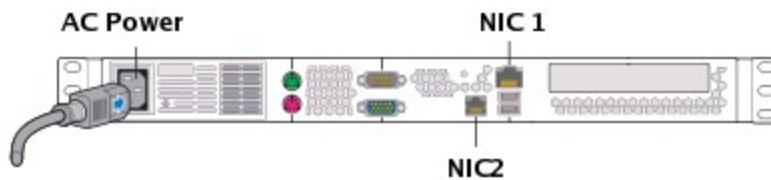
2.0 Hardware Reference

2.1.1 Front Panel Controls and Indicators



A. USB Port (Not used)	E. Hard Disk Drive Activity LED
B. Power Button	F. NIC1 LED
C. Not used	G. NIC2 LED (Not used)
D. System Power LED	

2.1.2 Rear Panel



2.2 Physical Installation

- Attach Mounting Rails to Europa Appliance and server rack if necessary
- Fasten the Europa Appliance to server rack
- Use a **straight Ethernet cable**; connect one end to your network switch and the other end to the appliance's **NIC 1** network interface.
- Connect the power cord of the appliance to an electrical outlet.
- Push the power button at the front of the appliance to power it up.
- Wait 2 – 3 minutes for the appliance to initialize.
- You are ready for Login, please go to next section for details.

2.2.1 Two methods for obtaining Europa's IP

1. DHCP

- ◆ Europa will automatically obtain an IP from your DHCP server. Use the provided MAC address of Europa, you will be able to locate which IP from your firewall/router. Please refer to your firewall/router manual for details on locating DHCP IPs.

2 Default IP: 192.168.0.1

- ◆ If Europa fails to obtain an IP from a DHCP server, it will default itself to 192.168.0.1
- ◆ You will need a **cross Ethernet cable** to connect Europa's **NIC 1** network interface directly to your desktop/laptop network interface
- ◆ Setup your desktop/laptop within the same network, eg 192.168.0.2


3.0 Graphical User Interface (GUI) Setup

From your desktop/laptops Internet browser, go to the following URL:

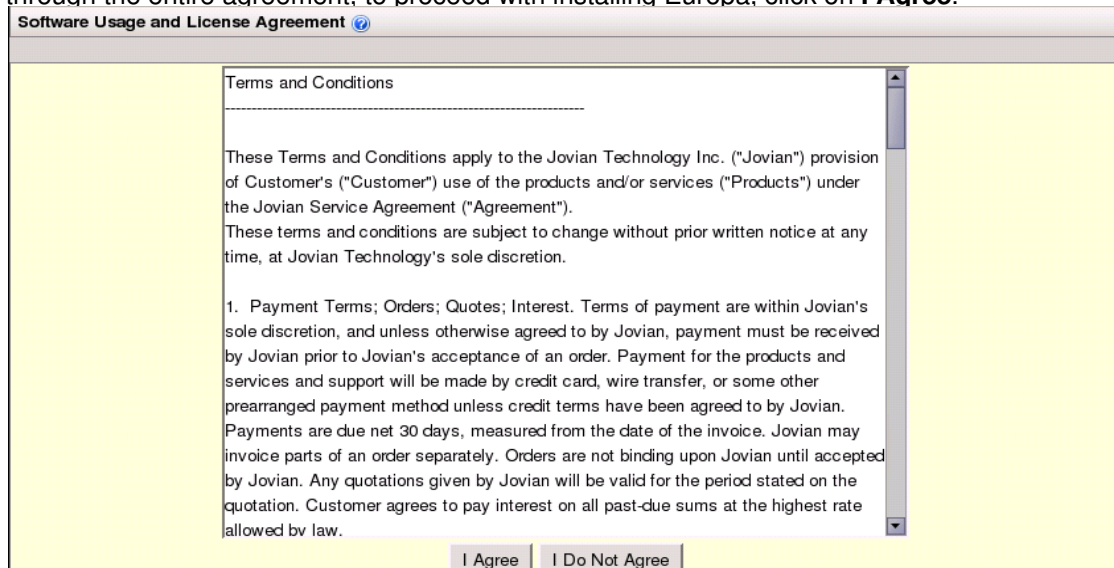
http://<europa_ip>/ - please refer to previous section on how to obtain Europa IP from DHCP server

or **http://192.168.0.1/** - default

Login as admin with Default login: **admin**, password: **admin**



After login successfully, it will lead you to the **Software Usage and License Agreement** page. Please read through the entire agreement, to proceed with installing Europa, click on **I Agree**.



Software Usage and License Agreement

Terms and Conditions

These Terms and Conditions apply to the Jovian Technology Inc. ("Jovian") provision of Customer's ("Customer") use of the products and/or services ("Products") under the Jovian Service Agreement ("Agreement").

These terms and conditions are subject to change without prior written notice at any time, at Jovian Technology's sole discretion.

1. Payment Terms; Orders; Quotes; Interest. Terms of payment are within Jovian's sole discretion, and unless otherwise agreed to by Jovian, payment must be received by Jovian prior to Jovian's acceptance of an order. Payment for the products and services and support will be made by credit card, wire transfer, or some other prearranged payment method unless credit terms have been agreed to by Jovian. Payments are due net 30 days, measured from the date of the invoice. Jovian may invoice parts of an order separately. Orders are not binding upon Jovian until accepted by Jovian. Any quotations given by Jovian will be valid for the period stated on the quotation. Customer agrees to pay interest on all past-due sums at the highest rate allowed by law.

3.1 System Setup

>> System > System Setup

System Setup ?

System Setup

Host Name:	<input type="text"/>	Company Name:	<input type="text"/>
Static IP:	<input type="text"/>	Netmask:	<input type="text"/>
Gateway IP:	<input type="text"/>	HTTPs Port:	<input type="text" value="443"/> (Default: 443)
Primary DNS Server IP:	<input type="text"/>	Secondary DNS Server IP:	<input type="text"/>
Admin Email Address:	<input type="text"/>	Alternate Admin Email/Pager Address:	<input type="text"/>
Primary Domain Name:	<input type="text"/>		
Email Domain Names:	<input type="text"/> <input type="button" value="Add"/> <input type="button" value="Delete"/>		
Behind Mail Gateway:	<input checked="" type="radio"/> Yes <input type="radio"/> No (Default: No)		
Mail Gateway IP:	<input type="text"/>	Mail Gateway Admin Email Address:	<input type="text"/>
Mail Connection Time Limit:	<input type="text" value="120"/> s (Default: 120 s)		
Mail Size Limit:	<input type="text" value="5"/> MB (Default: 10 MB)		
Access Violation Notification:	<input checked="" type="radio"/> Yes <input type="radio"/> No (Default: Yes)		
<input type="button" value="Update"/> <input type="button" value="Reset"/>			

- Enter the **Host Name** field.
- Enter the **Company Name** field.
- Enter the **Static IP** field.
- Enter the **Netmask** field.
- Enter the **Gateway IP** field.
- You may change this **HTTPs Port** from its default port of 443 to some other port number within the range of: 1024-65535. This HTTPs Port is for connection to the Europa.
- You **MUST** enter the **Admin Email Address**, so that all the emails that need be sent to the administrator can be sent to this **Admin Email Address** account.
- You may enter your external email address in the **Alternate Admin Email/Pager Address**, so that emails are reachable in case internal server is down.
- Enter the **Primary DNS Server IP** field.
- Enter the **Secondary DNS Server IP** field.

- Enter the **Primary Domain Name** field.
- Enter additional domains in **Email Domain Names** field:
 - o **Add**: Enter addition domains
 - o **Delete**: Remove domains
- Select **Yes** next to **Behind Mail Gateway** if this Europa box is behind some mail firewall or gateway. (ie. this machine gets emails from another intermediate machine within the network)
- You **MUST** enter the **Mail Gateway IP** if you have selected **Yes** to **Behind Mail Gateway**.
- You **MUST** enter the **Mail Gateway Admin Email Address** if you have selected **Yes** to **Behind Mail Gateway**.
- Select the time for **Mail Connection Time Limit** of which the maximal connection time between this machine and the client email server
- Select the size for **Mail Size Limit** of which the size limit for each individual email.
- Select **Yes** for **Access Violation Notification** allows admin to receive daily report on access violation activities
- Click **Update**, and wait about 30 seconds for system to refresh
- An extra **Reboot** button should show up, click to reboot the machine

Mail Connection Time Limit: s (Default: 120 s)

Mail Size Limit: MB (Default: 10 MB)

Access Violation Notification: Yes No (Default: Yes)

Please reboot system.....

3.2 Domain Settings

If you are connected with a cross cable, you may remove cross cable and connect Europa machine to the main network. Also connect your desktop/laptop to the main network, and setup it's network configuration accordingly.

3.2.1 Service Info

>> System > Service Info

3.2.1.1 Service Activation Status

Service Activation Status	
Serial Number:	000000-000000-000000
Expiry Date:	Dec 31, 2010
Maximum number of Users:	100
Features:	
	Personal Filter Activated
	Anti-Spam/Anti-Virus Activated
	Email Service Activated
	MPOP Activated
Activation code:	<input type="text"/>
<input type="button" value="Activate"/>	

3.2.1.2 System/Domain Service Setup

Note: Depending on your subscriptions, some features on the Service Setup page may be disabled according to the features activated:

The screenshot shows two configuration panels. The top panel, titled 'System Service Setup', has a yellow background and contains two radio button options: 'Enable Anti-Virus:' with 'Yes' selected and 'No' unselected, and 'Enable Anti-Spam:' with 'Yes' selected and 'No' unselected. Below these is an 'Update' button. The bottom panel, titled 'Domain Service Setup', also has a yellow background. It features a 'Domain:' dropdown menu set to 'domain.com'. Below this are four radio button options: 'Enable Personal Filter:' (Yes selected), 'Enable Email Service:' (No selected), 'Enable MPOP:' (No selected), and 'Enable Forwarding Service:' (No selected). To the right of the 'Enable Email Service:' option is an 'Email Server:' text input field. An 'Update' button is located at the bottom left of this panel.

- ◆ Setting up Anti-Virus
 - ◆ Select **Yes** to turn on the anti-virus capability. Further configurations will be set in the **Anti-Virus Setup** page later.
- ◆ Setting up Anti-Spam
 - ◆ Select **Yes** to enable Europa as a mail filter. Further configurations will be set in the **Anti-Spam Setup** page later.
- ◆ Setting up Personal Spam Manager (PSM)

Select **Yes** to enable the personal spam filter. Further configurations will be set in the **Personal Filter Setup** page later.

Note: **PSM** and **Personal Filter** are used interchangeably

- ◆ Setting up Email Service

Select **Yes** to enable Europa as a mail server.

Select **No** to configure Europa as a mail filter, you must enter the email server's IP into **Email Server**.

- ◆ Setting up MPOP

Select **Yes** to turn on the MPOP capability on Europa.

Select the time interval from the **Pop Time Interval** list.

- **Mail Forwarding Service**

- o Select **Yes** if you want to enable the email forwarding service, so that users can forward their emails to their other email account.
- Select **No** if you want to disable the email forwarding service for all users. Users will no longer be able to receive emails on their other email account.

3.2.2 Domain Setup

>> System > Domain Setup

Domain Setup ⓘ

Domain:

Enable Domain: Yes No

Domain Admin Email Address:

Days of Quarantine: (Default: 1) User Session Time Limit: (Default: 8 Hrs)

Quarantine Emails: User Monitor Both Email Address for quarantine monitor:

Unknown Emails: Drop Quarantine Forward Pass Through (Default: Drop) Email Address for Unknown users:

Fail-over Configuration

Automatic Mail Service Switch: Yes No Mail Server Check Interval: (Default: 15 min)

Send Notification to Alternate Admin Address when Email Server is down

Alternate Admin Email/Pager Address:

Note: External address is preferred in case internal domain is not reachable

- Select **Yes to Enable Domain** to enable this domain
- You **MUST** enter the **Domain Admin Email Address**, all domain related emails will be sent to this **Domain Admin Email Address** account.
- You may change **Days of Quarantine** to the number of days that you want the quarantined emails to be kept on this machine.
- You may change **User Session Time Limit** to the number of hours that you want the user's session

timer to be expired.


- **Quarantine Emails** refers to high potential spams which available for review
 - o Select **User** if you want the users to take care or review their own spam.
 - o Select **Monitor** if you want a centralized address (ie **Email Address for quarantine monitor**) for admin to take care or review all spams within the domain.
 - o Select **Both** if you want spam being deliver to both user and monitor
- **Email Address for quarantine monitor** defines where you want quarantined emails being deliver to. If this is empty, quarantined emails will send to **admin**'s email address by default.
- **Unknown Emails** refers to unknown recipients/domains
 - o Select **Drop** if you do not want see the mails at all.
 - o Select **Quarantine** if you want the unknown mails to be quarantined at **Unknown user's Email Address** inside Europa.
 - o Select **Forward** if you want the unknown mails to be forwarded at **Unknown user's Email Address** to mail server.
 - o Select **Pass Through** if you are not sure if its invalid, it will let the backend email server to handle. *Note: this option is only available when Europa does not act as a mail host.*
- **Unknown user's Email Address** defines where you want unknown emails being deliver to. If this is empty, unknown emails will send to **admin**'s email address by default.

3.2.2.1 Fail-over configuration

- Select **Yes** to **Automatic Mail Service Switch** to enable auto fail-over. When Europa cannot deliver email to your mail server, it will automatically switch itself into Mail service mode.
- **Mail Server Check Interval** refers to how frequent Europa checks if mails are deliverable to your mail server.
- **Check** checkbox **Send Notification to Alternate Admin Address when Email Server is down** if you want to receive notification through email.
- You may specify your external email address or pager address for notification purpose in **Alternate Admin email/pager address**.

3.3 Connection Level Protection (CLP) Setup

>> Service Admin > CLP Setup

Connection Level Protection 

Heuristic Connection Protection: Yes No (Default: Yes)

RBL Check: Yes No (Default: Yes)

SPF Check: Yes No (Default: No)
Note: Both 'SPF Check' and 'DNS Reverse Lookup' are enabled

DNS Reverse Lookup: Yes No (Default: No)

IP Whitelist

- **Heuristic Connection Protection (HCP)**
 - o Select **Yes** if you want to block mail server address that had been historically detected as harmful.
 - o Select **No** if you do not want to block mail server address that had been historically detected as harmful.
- **RBL** (Real-time Blackhole List) Check
 - o Select **Yes** if you want to have the reversed client mail server address checked against the RBL domains.
 - o Select **No** if you do not want checking on reversed client mail server address against the RBL domains.
- **SPF** (Sender Policy Framework) Check
 - o Select **Yes** if you want to have the reversed client mail server address checked against the SPF.
 - o Select **No** if you do not want checking on reversed client mail server address against the SPF.

- **DNS Reverse Lookup (rDNS)**

- o Select **Yes** if you want to have the Reverse DNS lookup check against the client mail server at the connection level.
- o Select **No** if you do not want any DNS checking at all.

***Note:** If both SPF and DNS Reverse lookup are enabled, system will first check SPF. If it fails, then check DNS Reverse Lookup.*

- **IP Whitelist**

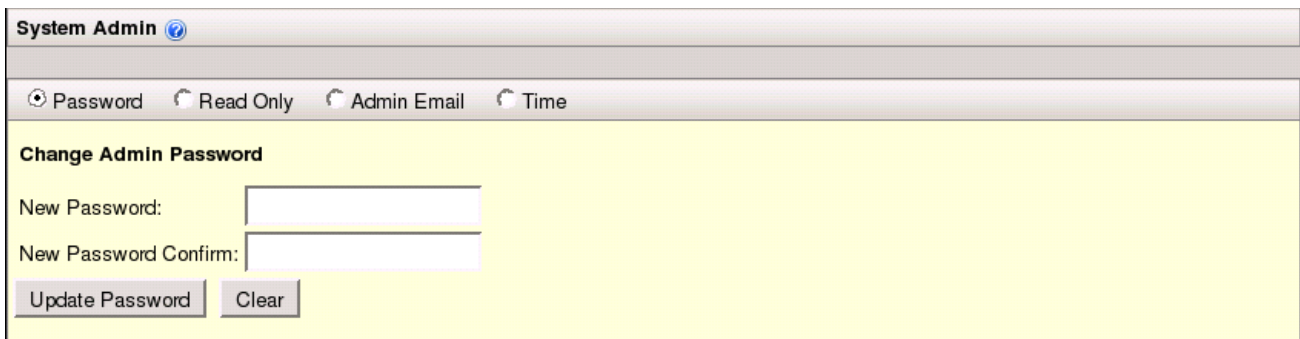
- o input known IPs which bypass CLP checks (ie, HCP, RBL, SPF, rDNS)

3.4 Further Settings

3.4.1 System Admin

3.4.1.1 Change admin password

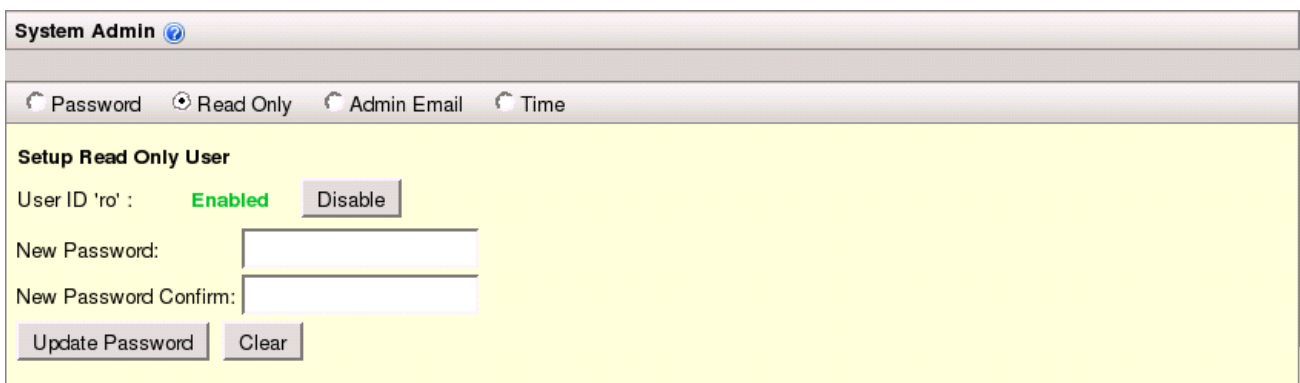
>> Appliance Admin > System Admin > Password tab



The screenshot shows the 'System Admin' interface with the 'Password' tab selected. The page title is 'System Admin' with a help icon. Below the title, there are four radio buttons: 'Password' (selected), 'Read Only', 'Admin Email', and 'Time'. The main content area is titled 'Change Admin Password' and contains two text input fields: 'New Password:' and 'New Password Confirm:'. Below these fields are two buttons: 'Update Password' and 'Clear'.

3.4.1.2 Change Read Only User Password

>> Appliance Admin > System Admin > Read Only tab



The screenshot shows the 'System Admin' interface with the 'Read Only' tab selected. The page title is 'System Admin' with a help icon. Below the title, there are four radio buttons: 'Password', 'Read Only' (selected), 'Admin Email', and 'Time'. The main content area is titled 'Setup Read Only User' and contains a 'User ID 'ro'' field with a toggle switch set to 'Enabled' (with a 'Disable' button next to it). Below this are two text input fields: 'New Password:' and 'New Password Confirm:'. At the bottom are two buttons: 'Update Password' and 'Clear'.

3.4.1.3 Define Additional Admin Email Address

>> Appliance Admin > System Admin > Admin Email tab

System Admin

Password Read Only Admin Email Time

Additional Admin Email Addresses

Admin Email Address #2:

Admin Email Address #3:

Admin Email Address #4:

Admin Email Address #5:

3.5 Set Timezone

>> Appliance Admin > System Admin > Time tab

System Admin

Password Read Only Admin Email Time

Changing System Time

New Date: Current Date: 05-17-2007

New Time: Current Time: 14:09:25

New Timezone: Current Timezone: EDT

3.5.1 Domain Admin

>> Appliance Admin > Domain Admin > Admin Email tab

The screenshot shows the 'Domain Admin' configuration page with the 'Admin Email' tab selected. The 'Domain' is set to 'domain.com'. Under the 'Virus Notification' section, the checkbox 'Send Notification when email contain virus and sender is in the whitelist' is checked. Below this, there are five input fields for 'Additional Admin Email Addresses', labeled 'Admin Email Address #2' through '#5'. At the bottom, there are 'Update' and 'Clear' buttons.

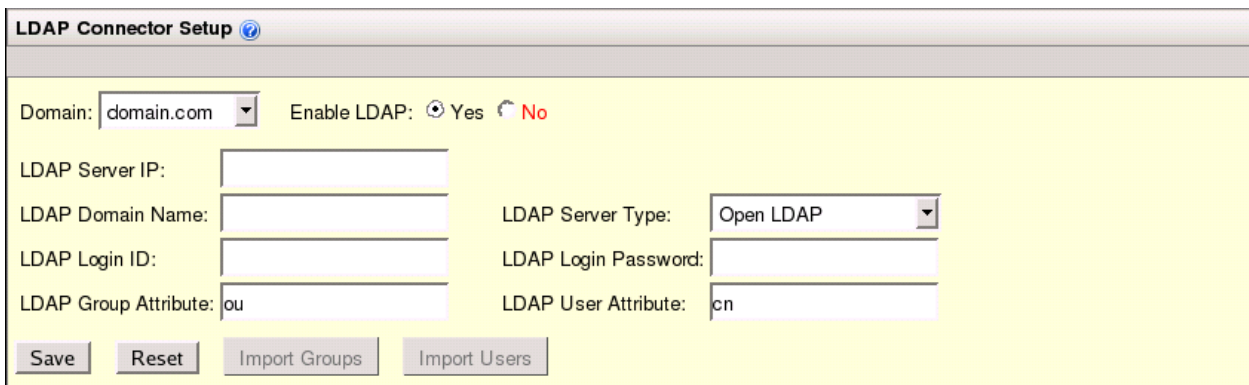
- Check box **Send Notification when email contain virus and sender is in the whitelist** if you want to receive notification.

3.5.2 LDAP/Active Directory Setup

>> Email Policy > LDAP Connector

3.5.2.1 LDAP configurations

Select **Yes** to **Enable LDAP** if you want to import the groups and users information from the LDAP or Active Directory server. Fill in all the LDAP server information to the fields accordingly. If you are using Active directory, please use **ou** as LDAP Group Attribute and **cn** as LDAP User Attribute. Click **Save** to save configuration.



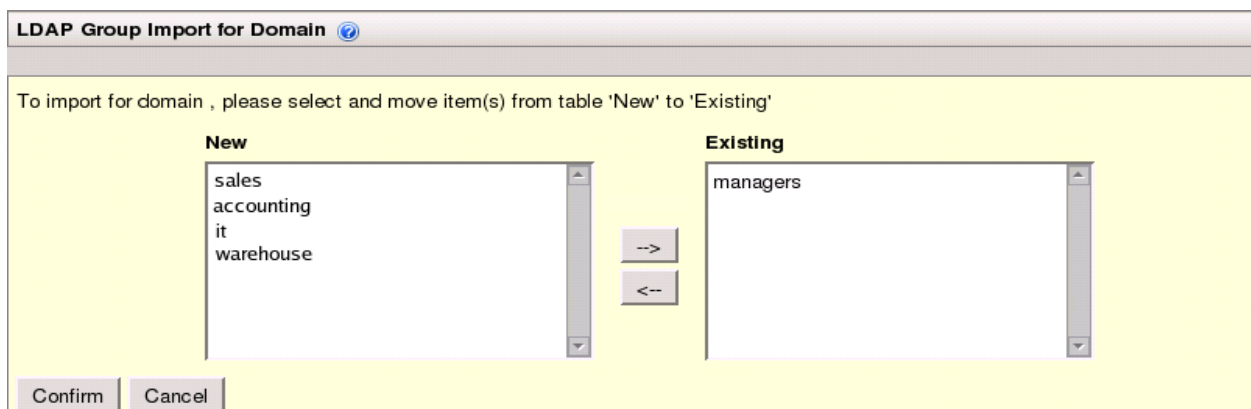
The screenshot shows the 'LDAP Connector Setup' configuration page. It includes a domain dropdown set to 'domain.com', an 'Enable LDAP' section with 'Yes' selected, and several input fields for LDAP server details. The 'LDAP Group Attribute' is set to 'ou' and the 'LDAP User Attribute' is set to 'cn'. There are buttons for 'Save', 'Reset', 'Import Groups', and 'Import Users'.

Domain:	domain.com	Enable LDAP:	<input checked="" type="radio"/> Yes <input type="radio"/> No
LDAP Server IP:	<input type="text"/>	LDAP Server Type:	Open LDAP
LDAP Domain Name:	<input type="text"/>	LDAP Login Password:	<input type="text"/>
LDAP Login ID:	<input type="text"/>	LDAP User Attribute:	cn
LDAP Group Attribute:	ou		

Buttons: Save, Reset, Import Groups, Import Users

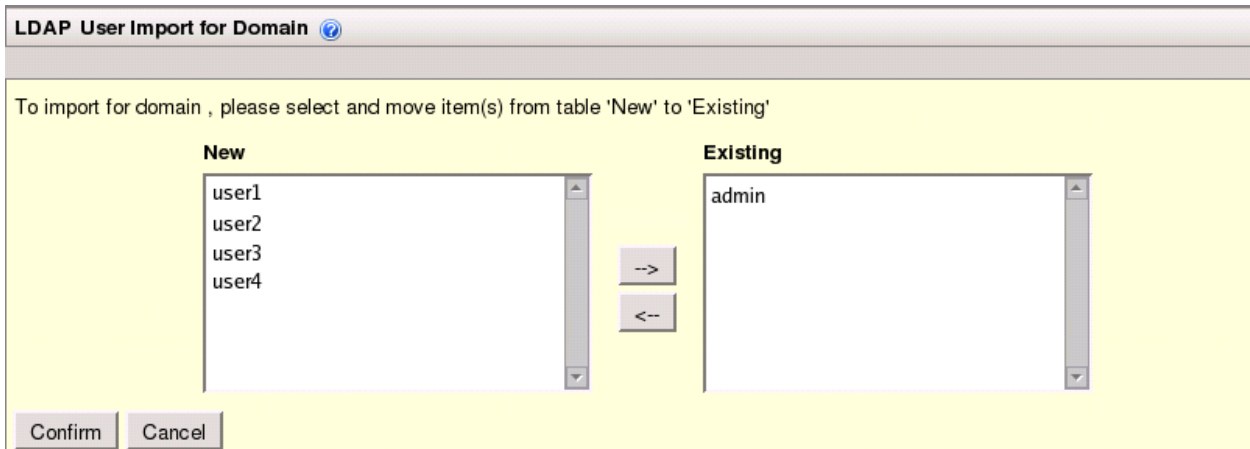
3.5.2.2 Import LDAP groups

Click on **Import Groups**, this will show the groups exist in the LDAP Server ('New' Table), and groups already added in Europa ('Existing' Table). To import the new groups, select and move groups from table 'New' to 'Existing' by using the arrow buttons between the two tables. Click **Confirm** to start importing groups.



3.5.2.3 Import LDAP users

Click on **Import Users**, it may take a while to refresh depending on number of users. You will see a similar screen as the group import. It shows you the users exist in your LDAP Server ('New' Table), and users already added in your Europa ('Existing' Table). To import the new users, select and move users from table 'New' to 'Existing' by using the arrow buttons between the two tables. Click **Confirm** to start importing users.



3.5.3 Personal Spam Manager (PSM) Setup

>> **Email Policy > PSM**

Select **Yes** to **Enable Envelope Mode** if you want to have the envelope icons or text links in all the incoming emails. Note: This is defaulted to **No** and this may take about 10 seconds for system to refresh

Personal Spam Management (PSM) Setup

Domain Personal Spam Management: **Enabled**

Domain:

Enable Envelope Mode for: All Users Selective Users None

Envelope Mode: Large Icons Small Icons
 Long Text Short Text

Envelope Position: Top Bottom

Display Domain Icon: Yes No

Additional text after Icons:

Tag Prefix for Whitelist Subject Header:


Send Original Mail if Whitelisted: Yes No

Rename Known Attachment Extensions: Yes No

Match Subdomains: Yes No

Sample Email Preview:

From: Sender <sender@sender.com>
To: Sample <sample@sample.com>
Subject: Sample Mail
Attachment: potentialvirus.exe

 Powered by Europa SPAM controller

Dear Sample,
...sample email content...

Regards,
Sender

3.5.4 Anti-Spam Setup

>> Email Policy > Anti-Spam

Configure anti spam features: **Keywords, OCR, Self-Learn, External Spam Database** applies to system wide.

Anti-Spam Setup

System Anti-Spam: **Enabled**

Default Keywords Download

Spam Keyword List

Enable OCR Yes No

Enable Self-Learn Function Yes No

Check External Spam Database Yes No

Save Changes

For domain wide, you may adjust the control level for your organization to the level that you want them to be in. Please note that each user could have his/her personalized Spam Scanner setup.

Domain Anti-Spam

Domain:

Control Level:

Type	Value	Control
Drop	<input type="text" value="10"/>	<input type="range"/>
Quarantine	<input type="text" value="6.4"/>	<input type="range"/>
Tag	<input type="text" value="4"/>	<input type="range"/>

Enable Per-User Configurable Control Level: Yes No


Tag Prefix for Subject Header:

Save Changes

3.5.5 Anti-Virus Setup

>> **Service Admin > Anti-Virus**

Select if you want to drop or quarantine virus infected mails.

Anti-Virus Setup 

Anti-Virus: **Enabled**

Synchronize Virus Definitions every Hr(s) (Minimum of 4 Hours is highly recommended)

Domain Anti-Virus

Domain:

Virus Infected Mails: Drop Quarantine

3.5.6 LAN Access Setup

>> **Service Admin > Anti-Relay**

Add in any IPs within the network to this **IP Access List** so as to allow these IPs to access this Europa box.



The screenshot displays the 'Anti-Relay Setup' web interface. At the top, there is a title bar 'Anti-Relay Setup' with a help icon. Below it, the main heading is 'Modify LAN's IP Access List'. The central area is a light yellow panel containing the text 'IP Access List:' on the left and a large, empty white rectangular box on the right, which serves as a list for IP addresses. Below this box are two buttons: 'Add' and 'Delete'. At the bottom left of the yellow panel are 'Save' and 'Cancel' buttons. Below the yellow panel, there is a section for domain settings: 'Allow Mails from Same Domain External Users for domain: domain.com' with a dropdown arrow, followed by radio buttons for 'Yes' and 'No' (where 'No' is selected). At the bottom of this section are 'Save Changes' and 'Edit External Users List' buttons.

3.5.7 Group Admin

>> Email Policy > Group

Click on the **Add Group** button to add group.

Note: The groups are automatically created if you set up as integrated with LDAP

Group Administration 	
Select All	
Current Groups for Domain	domain.com  <input type="button" value="Add Group"/> <input type="button" value="Delete Group"/>
Group Name	Administrators
domain.com	
<input type="checkbox"/> accounting	
<input type="checkbox"/> it	
<input type="checkbox"/> development	
<input type="checkbox"/> managers	
<input type="checkbox"/> sales	

The screenshot displays the 'Group Administration' window. At the top, there is a header 'Group Administration' with a help icon. Below this is a table with two columns: 'Group Name' and 'Administrators'. The first row shows a checkbox, the text 'development', and 'user1'. Below the table is the 'Group Information' section, which is highlighted in yellow. It contains the following fields: 'Group Name' with the value 'development', 'Parent' with a dropdown menu showing 'domain.com/it', and 'Group Administrators (Optional):' with two list boxes. The left list box is titled '--- Administrators ---' and contains 'user1'. The right list box is titled '--- All Users ---' and contains 'admin', 'user2', 'user3', and 'user4'. Between the list boxes are two buttons: '-->' and '<--'. At the bottom of the 'Group Information' section are 'Save' and 'Cancel' buttons.

Under the **Group Information**, enter the group name and select appropriate entries from the lists. Click on the **Save** button to save.

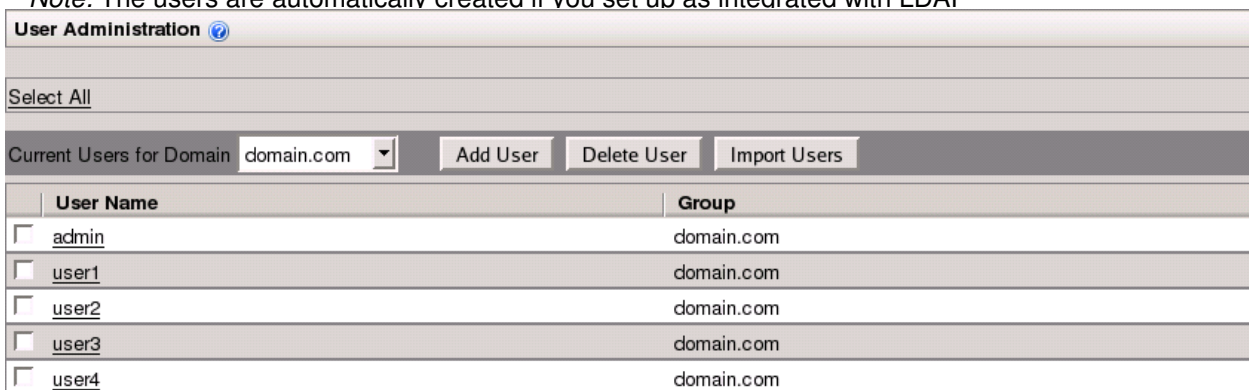
3.5.8 User Admin

>> Email Policy > User

3.5.8.1 Add Single User

Click on the **Add User** button to add user.

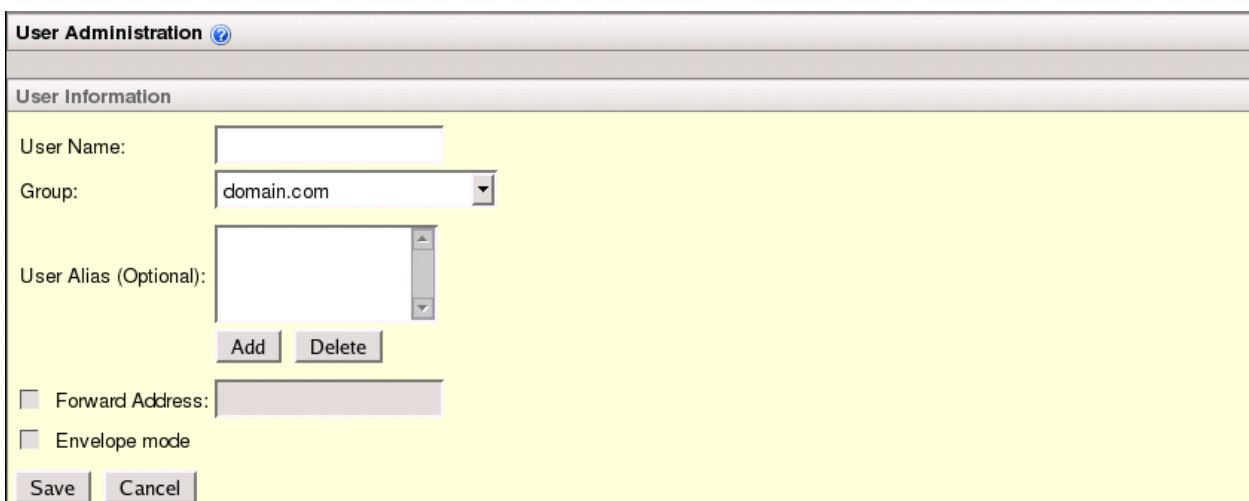
Note: The users are automatically created if you set up as integrated with LDAP



The screenshot shows the 'User Administration' interface. At the top, there is a 'Select All' link. Below it, a dropdown menu shows 'Current Users for Domain' set to 'domain.com'. To the right of this dropdown are three buttons: 'Add User', 'Delete User', and 'Import Users'. Below these buttons is a table with two columns: 'User Name' and 'Group'. The table contains five rows of user data:

User Name	Group
<input type="checkbox"/> admin	domain.com
<input type="checkbox"/> user1	domain.com
<input type="checkbox"/> user2	domain.com
<input type="checkbox"/> user3	domain.com
<input type="checkbox"/> user4	domain.com

Under the **User Information**, enter the user name and select appropriate entries from the lists. Click on the **Save** button to save.



The screenshot shows the 'User Information' form. It has a yellow background. The form contains the following fields and controls:

- User Name:** A text input field.
- Group:** A dropdown menu with 'domain.com' selected.
- User Alias (Optional):** A text input field with 'Add' and 'Delete' buttons below it.
- Forward Address:** A checkbox followed by a text input field.
- Envelope mode:** A checkbox.
- Save** and **Cancel** buttons at the bottom.

3.5.8.2 Import Multiple Users

You may import a list of users with a CSV file

Click the **Import User** button

Import Users [?](#)

Import User Info for domain **domain.com** from CSV file: [See CSV Examples](#)

Note: CSV file has to be in the following format

CSV Examples [?](#)

CSV Definition:
System requires CSV file with 7 fields separated by comma character and records separated by newlines. Fields that contain a comma, newline, or double quote character, must be enclosed in double quotes.

User Name	User Alias 1	User Alias 2	User Alias 3	Forward Address	Password	Group
-----------	--------------	--------------	--------------	-----------------	----------	-------

Example:

```
user1,user1alias,,forward@external.com,newpassword,domain.com/department1
user2,,,forward@external.com,,domain.com
user3,alias2,,, "pass,word",domain.com/department2
```

Click **Browse** and locate your CSV file, then click **Upload**

Modify Existing Users:

User Name	User Alias 1	User Alias 2	User Alias 3	Forward Address	Password	Group
user1				forward@forward.com	Password Unchanged	domain.com/it

New Users:

User Name	User Alias 1	User Alias 2	User Alias 3	Forward Address	Password	Group
newuser1				forward@forward.com	New Password	domain.com/it
newuser2				forward@forward.com	Password Unchanged	domain.com/accounting
newuser3	newuser3alias	newuser3alias2			Password Unchanged	domain.com
newuser4	newuser4alias				New Password	domain.com/sales


Once you review the user information are correct, click **Import** to start importing

3.5.9 SSL Certificate

Europa is designed to communicate with secure HTTPS protocol for all web access sessions. By default, Europa comes with a self-generated HTTPS certificate, which most browsers would not be able to lookup as a trusted source. In case you want to eliminate the warning message, you can purchase a certificate and upload into the Europa appliance.

Please follow the SSL Certificate vendor instructions to obtain the **Certificate** and the **Private Key**.

>> **Appliance Admin > Certificate**

SSL Certificate Setup 	
Company Name:	<input type="text" value="name123"/>
Generate Certificate	Generate a self-signed certificate
Upload Certificate	Upload certificate

Click **Upload Certificate** to upload purchased certificate.

Copy and paste your **Certificate** and **Private Key** into according fields and click **Save Certificate**.

Logout Europa and restart your browser.

3.6 Diagnostics and Testing

3.6.1 Reachability Test

>> Tools > Reachability Test

Check if servers are reachable by *ping* test. Click on button **Check Reachability** to start testing

Reachability Test

Check Reachability

Reachability - Ping Test		
Name	IP	Status
DNS Server	1.2.3.4	OK
Gateway	1.2.3.4	OK
Email Server: domain.com	1.2.3.4	OK
Realtime Blackhole List - 1	sbl.spamhaus.org	Unreachable
Realtime Blackhole List - 2	bl.spamcop.net	OK
Realtime Blackhole List - 3	cbl.abuseat.org	OK
Virus Definitions - 1	db.ca.clamav.net	OK
Virus Definitions - 2	database.clamav.net	OK

Reverse Look up - NSlookup Test			
Name	Hostname	IP	Status
Europa	europa	1.2.3.4	OK

3.6.2 SMTP Test

For additional SMTP testing on your email server, you may use the SMTP test tools.

>> **Tools > SMTP Test**

SMTP Connection Test ⓘ
Test: Mail Server Connection SMTP Email Ping Traceroute DNS Lookup
Mail Server Connection Test
SMTP Server IP/Host:

3.6.3 System Status

Check current system, connections, email status.

>> **Logs and Reports > Operation Status**

Operation Status ⓘ
Refresh: Last Detail level Order: Reverse
May 17 16:12:13 user2@domain.com : Quarantine SPAM from [test@test.com] (level 6.245 > quarantine level 6 defined in system) ?
May 17 16:12:08 disconnect from tester.test.com
May 17 16:12:08 connect from tester.test.com
May 17 16:11:11 Delete unknown recipient domain [user2@unknown.com] email
May 17 16:11:06 disconnect from tester.test.com
May 17 16:11:06 connect from tester.test.com
May 17 16:10:29 user2@domain.com : Tag email from [test@test.com] (level 6.245 > tag level 4 defined in system) ?
May 17 16:10:25 disconnect from tester.test.com
May 17 16:10:25 connect from tester.test.com
May 17 16:10:20 user3@domain.com : Tag email from [test@test.com] (level 6.245 > tag level 4 defined in system) ?
May 17 16:10:12 disconnect from tester.test.com
May 17 16:10:12 connect from tester.test.com
May 17 16:09:58 user1@domain.com : Delete SPAM from [spam@spam.com] (level 17.52 > cutoff 10.00 defined in system) ?
May 17 16:09:43 disconnect from tester.test.com
May 17 16:09:43 connect from tester.test.com

4.0 Additional Setup outside Europa

4.1.1 Firewall/Router Setup

Now you had finished setup Europa. In order for Europa to filter your emails, you need to redirect the mails (SMTP port 25) from your firewall/router to Europa.

For detail instructions, please refer to your firewall/router manual.

TCP Port	Description
25	SMTP
443 (or user-configured port number)	HTTPS
22	Remote Support

If your Europa is set at mail host, you may need to open the following ports for remote mail access

TCP Port	Description
465	SMTPs
993	IMAPs
995	POP3s

4.1.2 DNS Setup

In order for your client machines lookup Europa properly, you need to add Europa's hostname into your DNS server.

For detail instructions, please refer to your DNS server setup.

[Thank you and enjoy your cleaner email.](#)