COMODO
Creating Trust Online®

Comodo KoruMail

Software Version 6.7

Quick Start Guide

Guide Version 6.7.050720

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

KoruMail Secure Email Gateway – Quick Start Guide

This quick start guide will take you through the setup, initial configuration and use of Korumail. Use the following links to go straight to the section you need help with.

Step 1 – Install the System

Korumail is deployed as a VMware image.

- Download the virtual machine image from: **https://cdn.download.comodo.com/korumail/KoruMAIL_V6_esx.rar**
- Extract the contents of the .rar file using Winrar or 7zip.
- Open the VMware Vsphere client and login to the ESXi server.
- **Click here** for a step-by-step guide on the installation process
- Contact us at **korumailsupport@comodo.com** if you require more help to install Korumail.

Step 2 – Access the System

KoruMail's default IP address is 10.0.0.123. You access the system at this address for initial configuration. The default username is 'admin'. Please contact your Comodo account manager for the password.

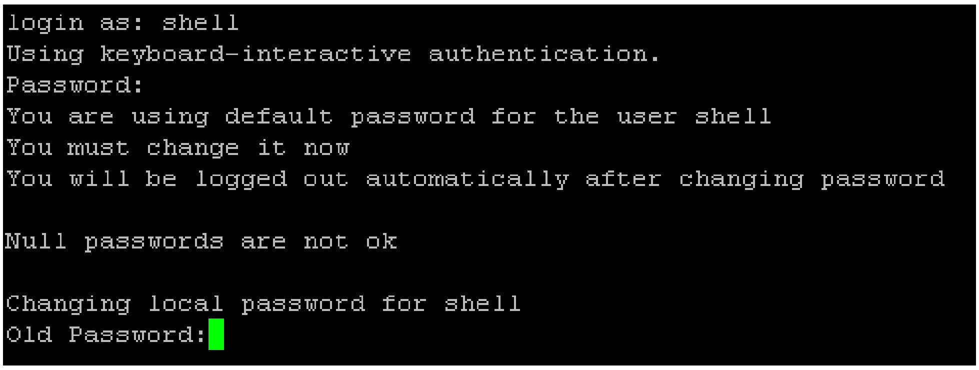
There are two ways to access the system:

1. **Command line interface (CLI) console**
2. **Graphic-based web management console**

Access via CLI Console

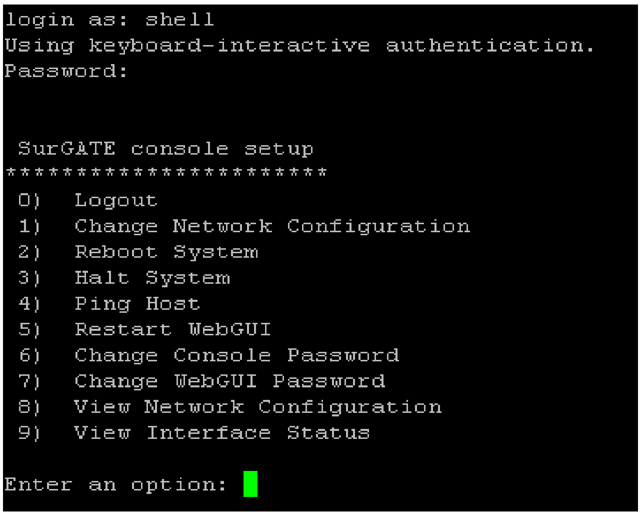
If it is not accessible from your network, then the easiest way to access the console is by using the command line interface. You can perform basic operations from this interface. The remaining **network settings** on the system can be done remotely via a web browser.

The CLI username is 'shell' and the password is 'surgateshell'. You will be asked to change the password after first login.



```
login as: shell
Using keyboard-interactive authentication.
Password:
You are using default password for the user shell
You must change it now
You will be logged out automatically after changing password

Null passwords are not ok

Changing local password for shell
Old Password:
```

You will see the following menu after logging-in in with your new password:

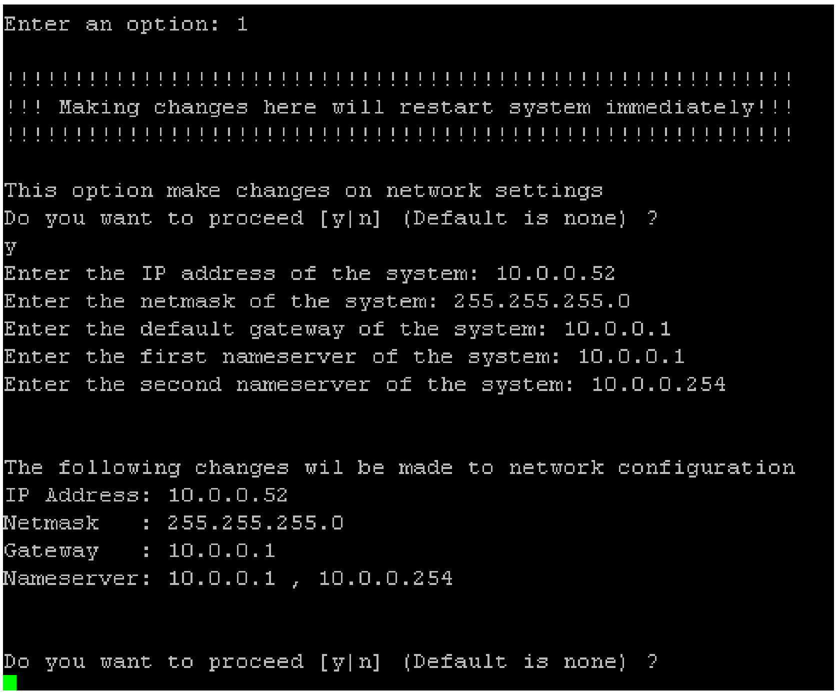


```
login as: shell
Using keyboard-interactive authentication.
Password:


 SurGATE console setup
***********************
 0)   Logout
 1)   Change Network Configuration
 2)   Reboot System
 3)   Halt System
 4)   Ping Host
 5)   Restart WebGUI
 6)   Change Console Password
 7)   Change WebGUI Password
 8)   View Network Configuration
 9)   View Interface Status

Enter an option:
```

Not all functions can be configured via the CLI. The following is a list of the tasks you can perform:

1. Network configuration
2. Reboot
3. Halt the system
4. Ping a host to check whether network access exists
5. Restart the web management console
6. Change CLI password
7. Change the password for the web management console
8. Display network configuration
9. Display network interface details

As an example, the following screenshot shows how to make network configuration.

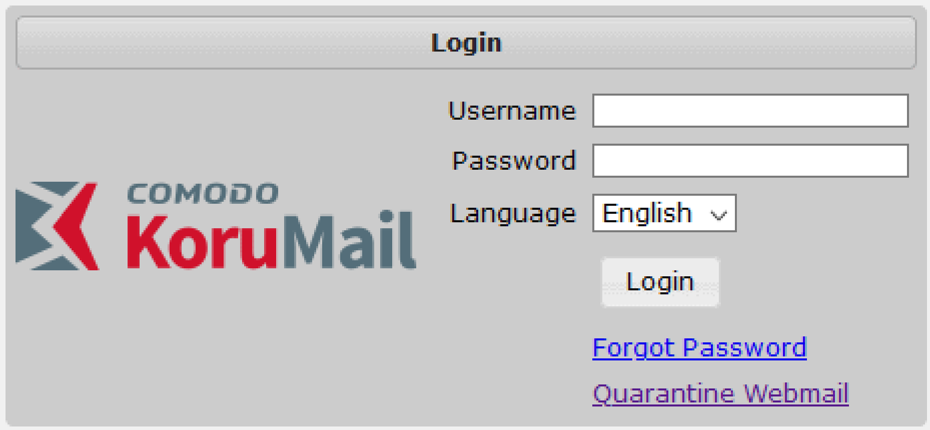


```
Enter an option: 1

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!! Making changes here will restart system immediately!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

This option make changes on network settings
Do you want to proceed [y|n] (Default is none) ?
y
Enter the IP address of the system: 10.0.0.52
Enter the netmask of the system: 255.255.255.0
Enter the default gateway of the system: 10.0.0.1
Enter the first nameserver of the system: 10.0.0.1
Enter the second nameserver of the system: 10.0.0.254


The following changes wil be made to network configuration
IP Address: 10.0.0.52
Netmask    : 255.255.255.0
Gateway    : 10.0.0.1
Nameserver: 10.0.0.1 , 10.0.0.254


Do you want to proceed [y|n] (Default is none) ?
```

See '**Step 3 – Configure Network Settings**' for help to remotely configure KoruMail network settings via the web console.

Access via Web Console

1. Enter the KoruMail Secure Email Gateway's IP or host name together with port 8080 (example: http://korumail.comodo.net:8080) in the address bar of a browser
2. Enter your username and password. Default user name is 'admin'. Please contact your Comodo account manager for your password.
3. Choose your preferred language (English/Turkish)
4. Click the login button

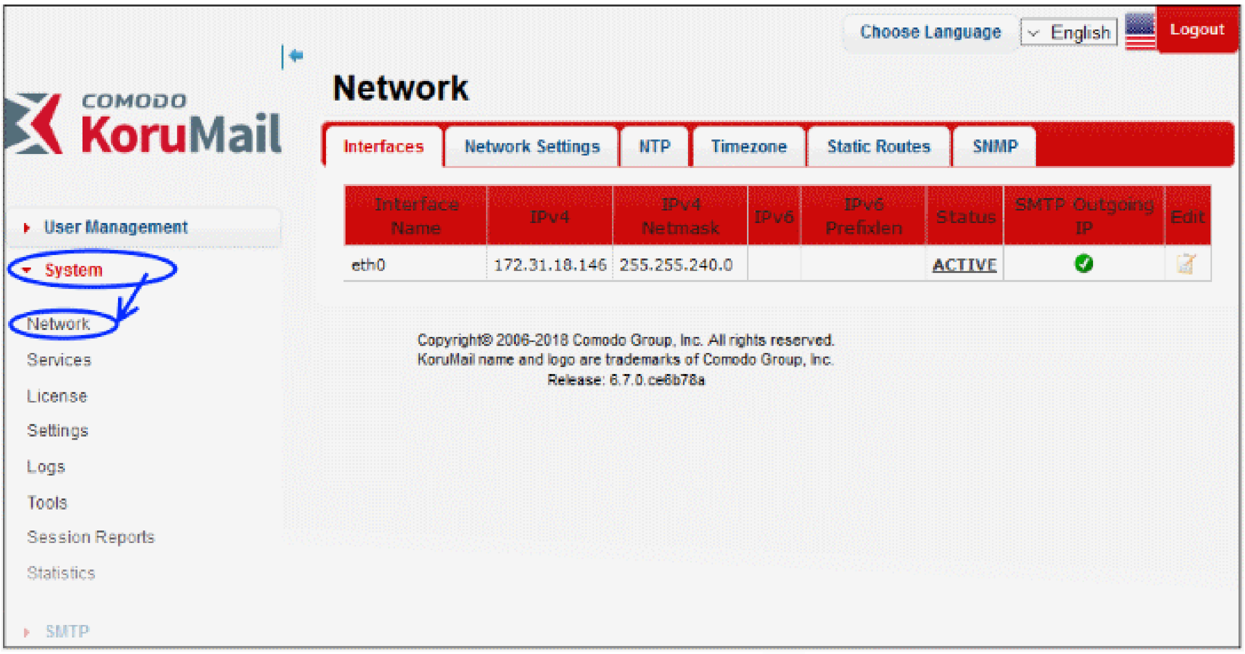


After logging-in, you can use the web console to change KoruMail network settings if you prefer. See '**Step 3 – Configure Network Settings**'.

Contact us at **korumailsupport@comodo.com** if you require help.

Step 3 – Configure Network Settings

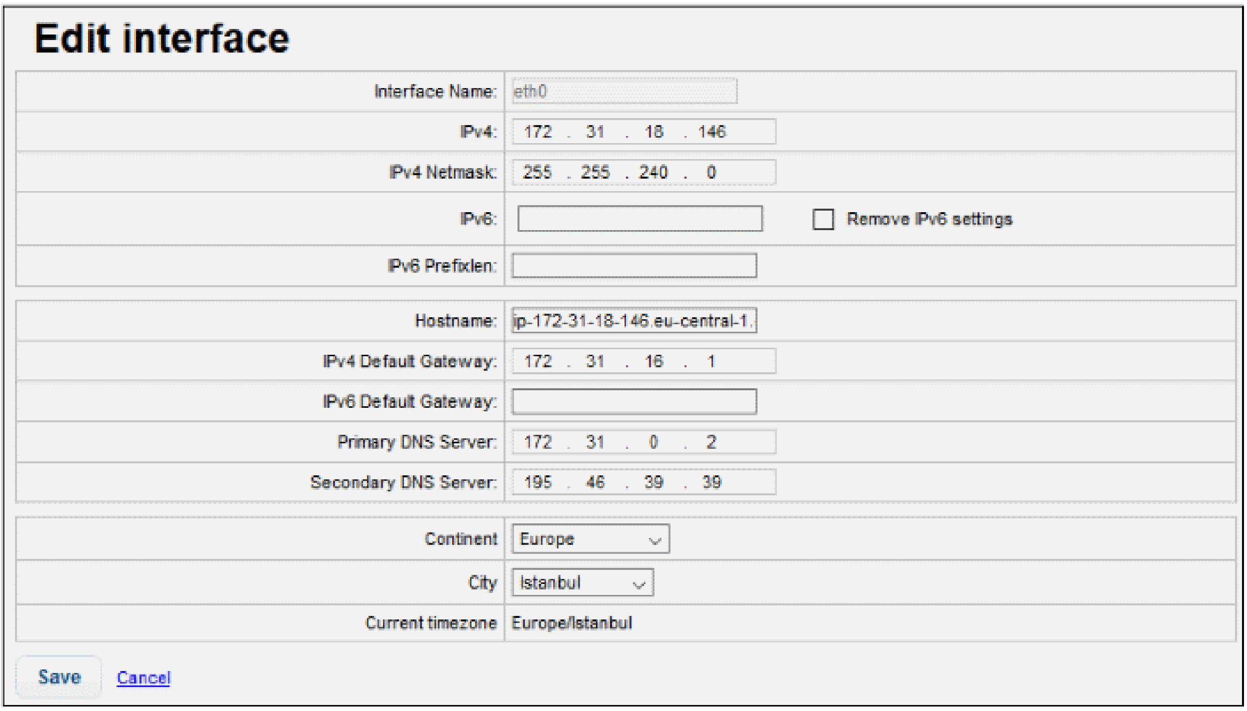
- KoruMail is initially configured at installation using the command line interface (**explained** in the previous step). You can also use the web console to edit or update KoruMail.
- The details of the network card can be edited/updated from the 'Interfaces' screen.
- To open the 'Interfaces' screen:
  - Click 'System' > 'Network' on the left
  - Click the 'Interfaces' tab



Interface Name	IPv4	IPv4 Netmask	IPv6	IPv6 Prefixlen	Status	SMTP Outgoing IP	Edit
eth0	172.31.18.146	255.255.240.0			ACTIVE	✓	📝

Copyright© 2006-2018 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 6.7.0.ce6b78a

  - The initial configuration details will be displayed. Click the 📝 icon beside the interface that you want to edit



Edit interface

Interface Name:	eth0
IPv4:	172 . 31 . 18 . 146
IPv4 Netmask:	255 . 255 . 240 . 0
IPv6:	☐ Remove IPv6 settings
IPv6 Prefixlen:	
Hostname:	ip-172-31-18-146.eu-central-1.
IPv4 Default Gateway:	172 . 31 . 16 . 1
IPv6 Default Gateway:	
Primary DNS Server:	172 . 31 . 0 . 2
Secondary DNS Server:	195 . 46 . 39 . 39
Continent	Europe
City	Istanbul
Current timezone	Europe/Istanbul

- **Interface Name:** The name of the network interface card. This name is not editable.
- **IPv4:** The IPv4 address of the port. Edit as required.
- **IPv4 Netmask:** The IPv4 netmask address of the port. Edit as required.
- **IPv6:** The IPv6 address of the port. To disable the IPv6 settings, select the 'Remove IPv6 settings' check box.
- **IPv6 Prefixlen:** Enter the prefix length for the IPv6 address
- **Hostname:** The hostname of the system. The changes will be reflected in the next tab 'Network Settings' screen also.
- **IPv4 Default Gateway:** The IPv4 default gateway that KoruMail will be using to connect to other networks or the internet. Edit as required. The changes will be reflected in the next tab 'Network Settings' screen also.
- **IPv6 Default Gateway:** The IPv6 default gateway that KoruMail will use to connect to other networks or the internet. Edit as required. Any changes will be also be shown in the next tab, 'Network Settings'.
- **Primary DNS Server:** The IP of the primary DNS server used by KoruMail. Edit as required. Any changes will be also be shown in the next tab, 'Network Settings'
- **Secondary DNS Server:** The IP of the secondary DNS server used by KoruMail. Edit as required. Any changes will be also be shown in the next tab, 'Network Settings'
- **Continent:** The continent where the system is located.
- **City:** The name of the city where the system is located.
- **Current timezone:** The timezone of the city.
- Click 'Save'.

A reboot confirmation screen will be shown. A reboot is not required for DNS setting changes. See '**Interfaces**' in the main guide for more information.

Network Settings tab

- Change the hostname of KoruMail, IPv4 and IPv6 default gateways, and primary/secondary DNS server settings. Any changes you make here will also be shown in the 'Edit Interface' of the NIC as explained above. See '**Network Settings**' for more information.

Network Time Protocol (NTP) tab

- Network Time Protocol (NTP) is an internet protocol which synchronizes computer clocks over a network. The 'NTP Servers' screen allows you to add time sync servers for KoruMail. See '**Network Time Protocol**

(NTP)' for more details.

Timezone

- Specify the time zone you want to use for system time. See '**Timezone**' for more information.

Static Routes

- In addition to the default gateway, you can use static routes to redirect traffic to different email servers. See '**Static Routes**' for more details.

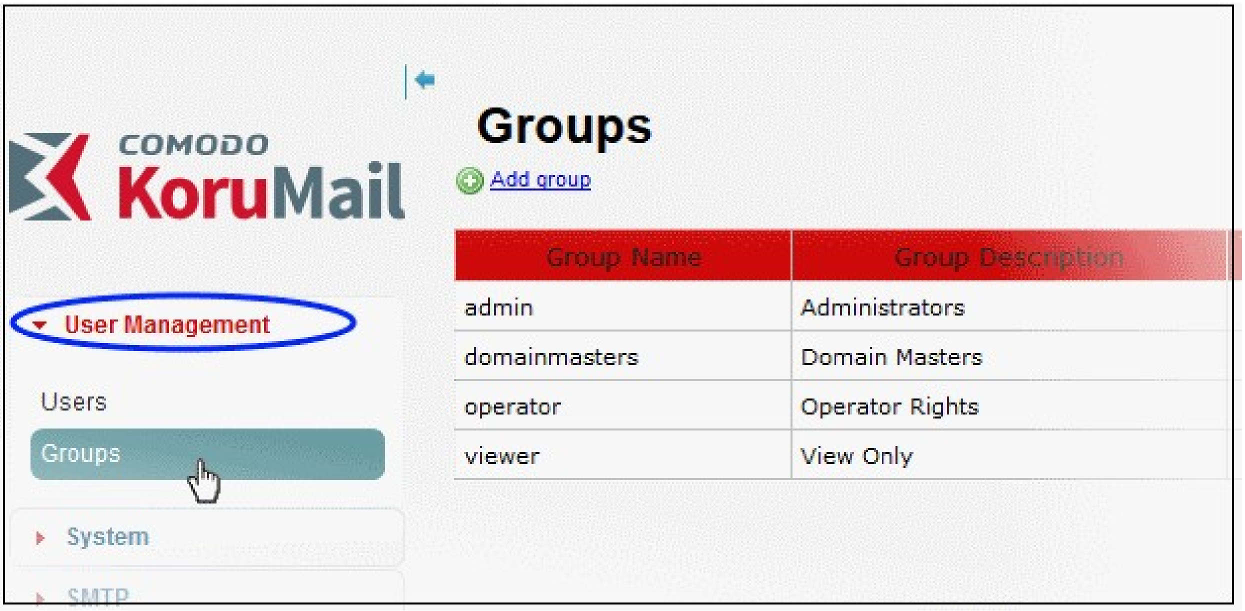
See '**Network Configuration**' in our main guide for more information.

Step 4 – Add Administrative Users

- Korumail lets you add admin users with different privilege levels.
- First create a user group and assign privileges to the group. Next, add admin users and assign them to the group.
- Admins added to a group will be assigned the privileges of that group.

To add a new group

- Click the 'User Management' tab in the left-menu and click 'Groups'

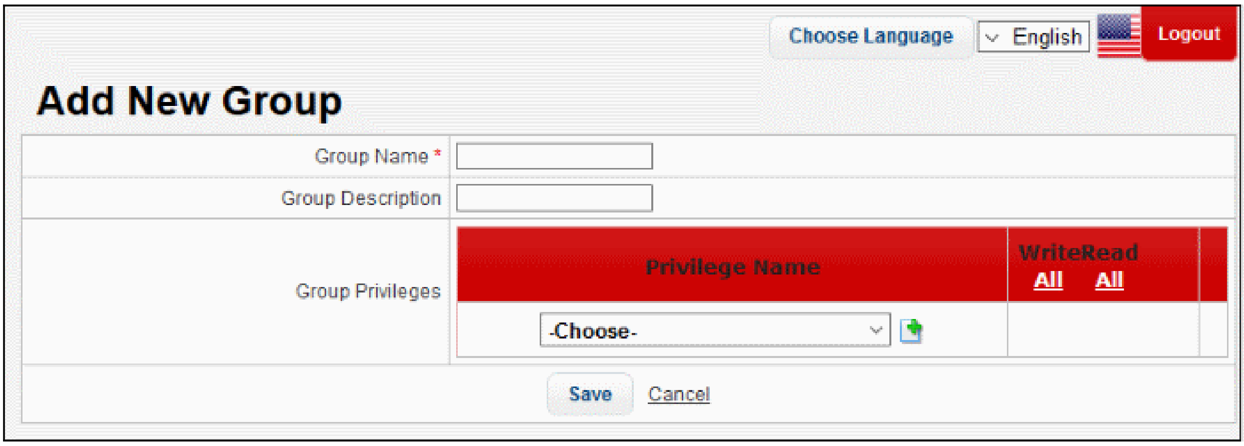


Groups

Group Name	Group Description
admin	Administrators
domainmasters	Domain Masters
operator	Operator Rights
viewer	View Only

- Click the 'Add group' link

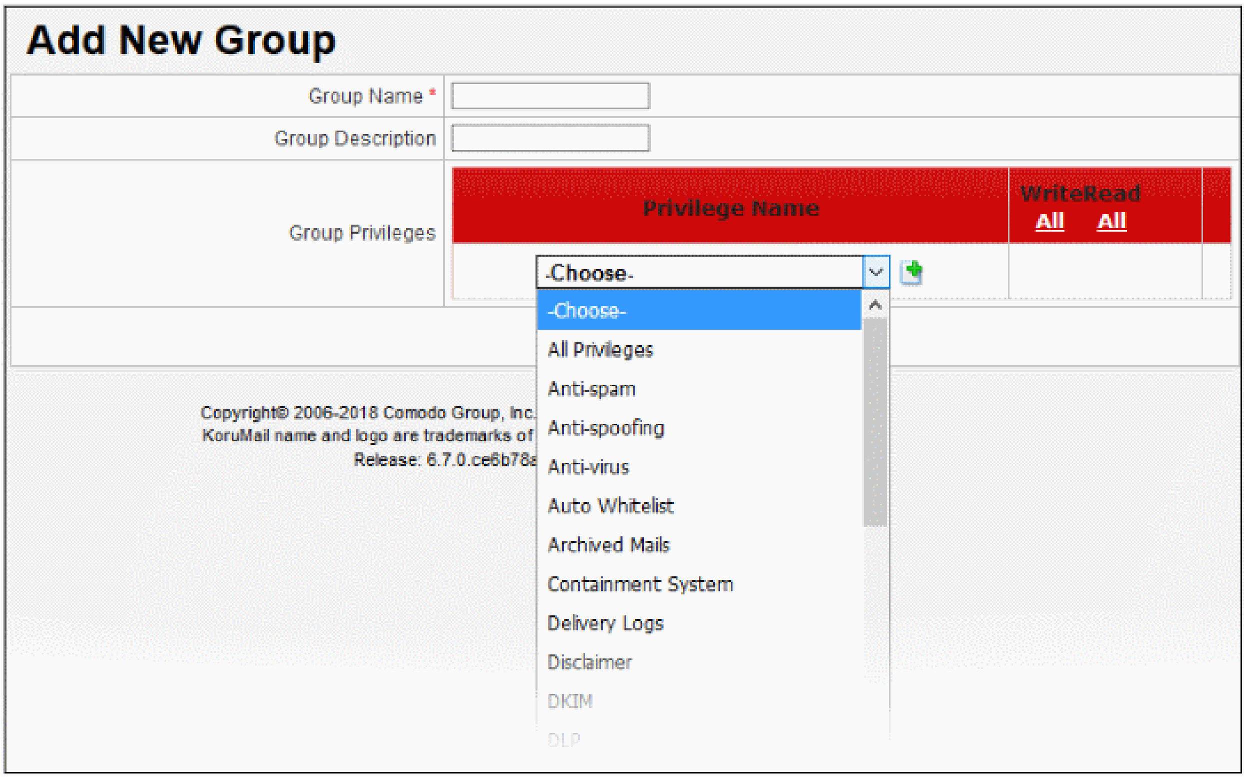
The group configuration screen will open.



Add New Group

Group Name *	
Group Description	
Group Privileges	Privilege Name: -Choose- WriteRead: All All

- **Group Name:** Create a name for the group
- **Group Description:** Enter an appropriate description for the group
- **Group Privileges:** Select the permissions you want to assign to the group. All users you draft into this group will inherit the group's permissions.



Add New Group

Group Name *	
Group Description	
Group Privileges	

Privilege Name	Write All	Read All
-Choose-		

Copyright© 2006-2018 Comodo Group, Inc.
KoruMail name and logo are trademarks of
Release: 6.7.0.ce6b78a

- Select a privilege then click the 'Add' button ➕. You can add as many or few privileges as required.

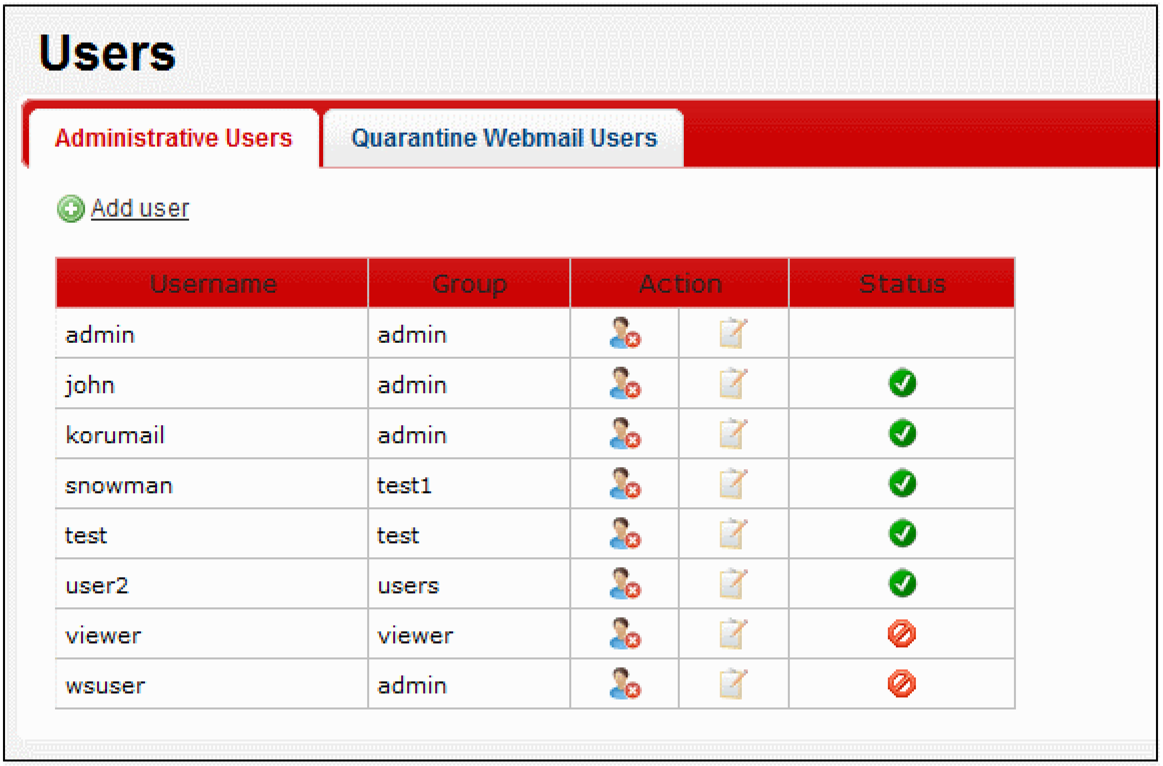
By default, each privilege has 'Read' rights only, so the feature can be viewed but not configured by group members.

- Select the 'Write' option to make a privilege configurable for group members.
- Click the 'All' links underneath 'Write' or 'Read' to apply the setting to every privilege.
- To delete a privilege, click the delete icon ✗ beside it.
- Click 'Save' to add the new group.

You can now assign admin users to the group.

To add an administrative user

- Click 'User Management' > 'Users' on the left-menu
- Click the 'Administrative Users' tab:



Users

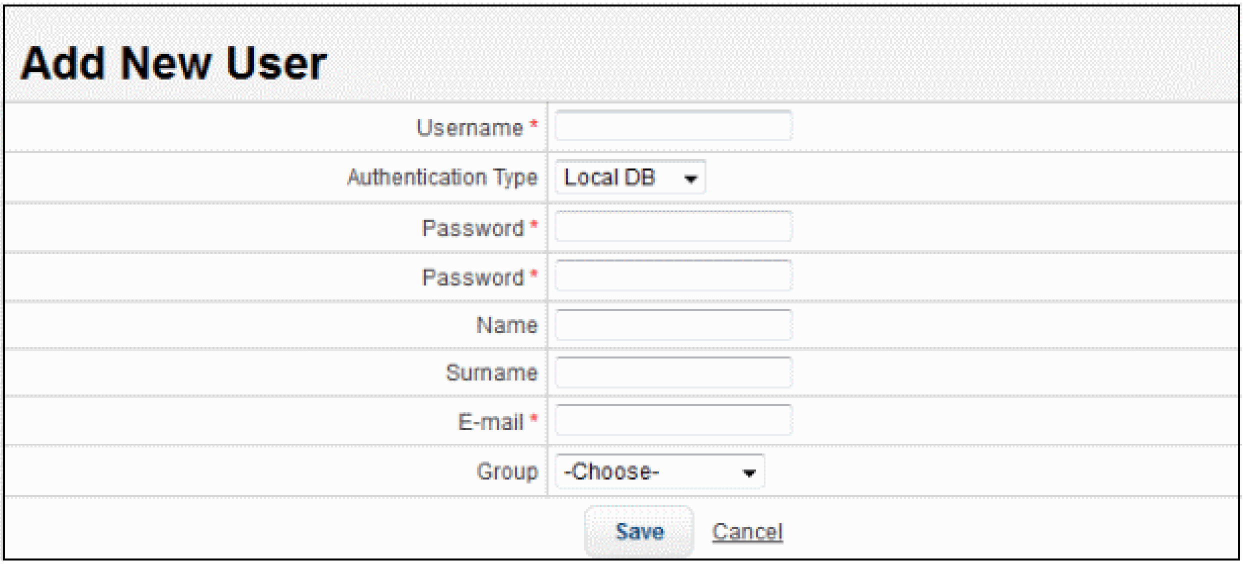
Administrative Users | Quarantine Webmail Users

Add user

Username	Group	Action		Status
admin	admin	✖	✎	
john	admin	✖	✎	✓
korumail	admin	✖	✎	✓
snowman	test1	✖	✎	✓
test	test	✖	✎	✓
user2	users	✖	✎	✓
viewer	viewer	✖	✎	⊘
wsuser	admin	✖	✎	⊘

- Click the 'Add User' link

The new user configuration screen will open:



Add New User

Username *	
Authentication Type	Local DB
Password *	
Password *	
Name	
Surname	
E-mail *	
Group	-Choose-

- **Username:** The name the admin will use to login to the console.
- **Authentication Type:** Two options are available - Local DB and LDAP AD
  - **Local DB** - Authentication of the user will be done using the local database
  - **LDAP AD** - Authentication of the user will be done using LDAP
- **Password:** The password the admin will use to access the console. Confirm it in the next field.
- **Name:** The real first name of the admin
- **Surname:** The surname of the admin
- **E-mail:** Address which KoruMail will use to send notifications to the admin
- **Group:** Select the group to which the admin user should be added. The admin will inherit the access permissions of the group.

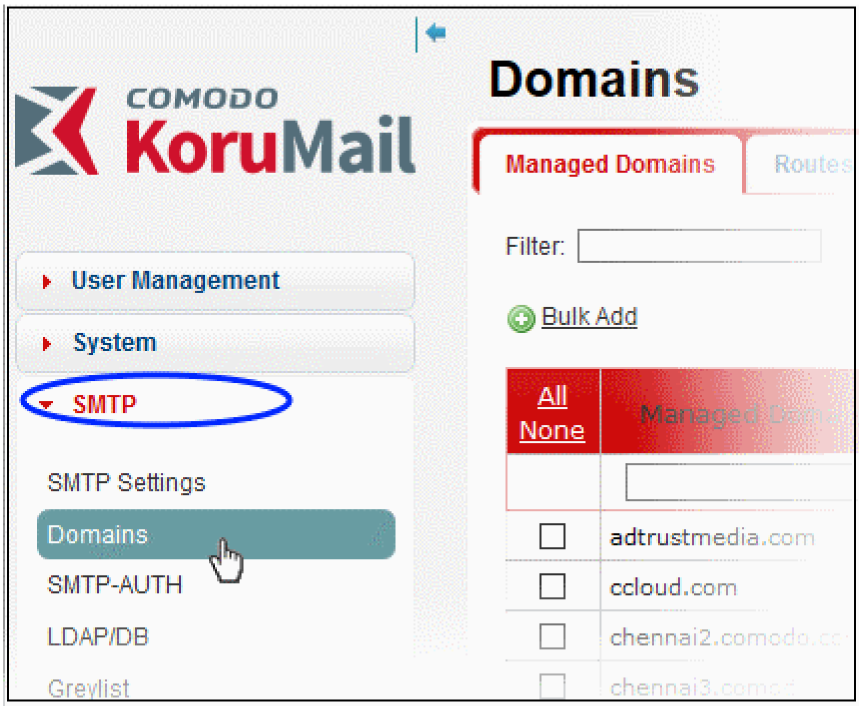
- Click 'Save' to add the new admin user.

Step 5 – Add Domains

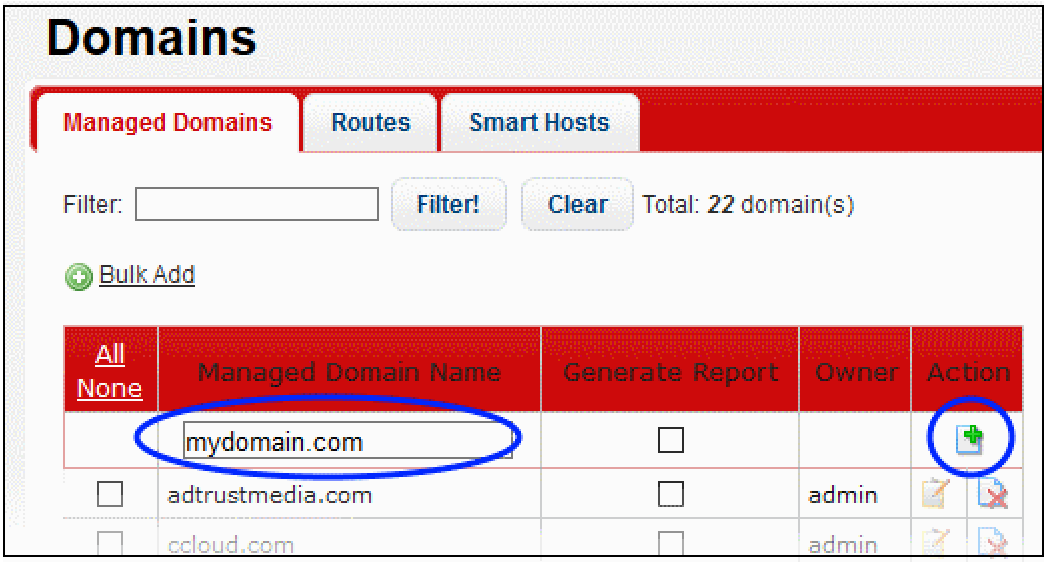
The next step is to add domains which you want to protect with KoruMail.

To add domains:

- Click 'SMTP' > 'Domains'



- Enter the domain name in the field under 'Managed Domain Name' column

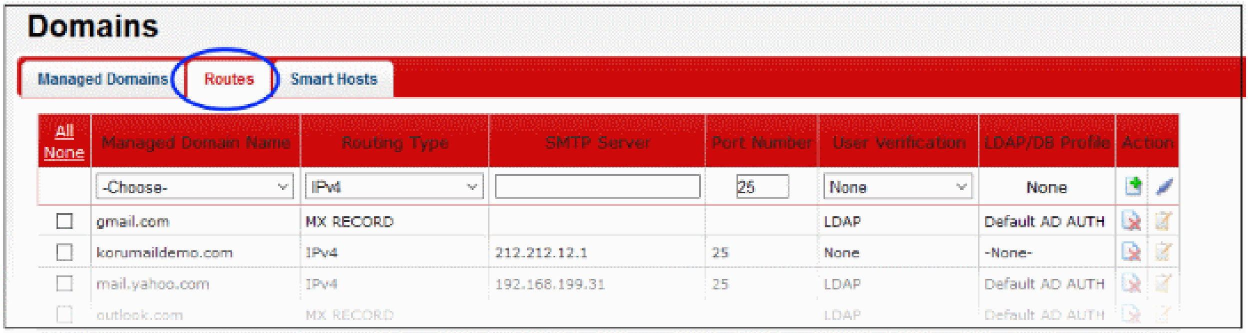


All None	Managed Domain Name	Generate Report	Owner	Action
	mydomain.com	□		+
□	adtrustmedia.com	□	admin	
□	ccloud.com	□	admin	

- Click the + button in the 'Action' column.
  - Alternatively, you can add multiple domains using the 'Bulk Add' link.

The next step is to define the route from KoruMail to your SMTP server. KoruMail will filter incoming mail then use this route to forward the mail to your server. If left undefined then the 'default route' will apply.

- Click 'SMTP' > 'Domains'
- Click the 'Routes' tab
- Use the drop-down menus in the top row to specify a route for the domain:



Domains

All None	Managed Domain Name	Routing Type	SMTP Server	Port Number	User Verification	LDAP/DB Profile	Action
	-Choose-	IPv4		25	None	None	
□	gmail.com	MX RECORD			LDAP	Default AD AUTH	
□	korumaildemo.com	IPv4	212.212.12.1	25	None	-None-	
□	mail.yahoo.com	IPv4	192.168.199.31	25	LDAP	Default AD AUTH	
□	outlook.com	MX RECORD			LDAP	Default AD AUTH	

- **Managed Domain Name** - Select the domain for which you want to configure the incoming route.
- **Routing Type** – Choose the method you want to use to send mail to the SMTP server. The options available are IP4, IP6 or Hostname, MX Record and LDAP.
- **SMTP Server** – Host name or IP address of the incoming mail server. KoruMail will forward mail to this server after filtering.
- **Port Number** – The port number of the SMTP server through which KoruMail should forward mail.
- **User Verification** and **LDAP / DB Profile** - Depending on the 'User Verification' type chosen, the 'LDAP/DB Profile' column will be populated. If 'LDAP' is chosen as 'User Verification' then the LDAP profiles added in LDAP/DB section will be shown in the drop-down. Select the LDAP profile from the options.
- Click to check the connection between KoruMail and the remote server. The result is shown at the top.
- Click the button to save the route.

The domain route will be added to the list.

Alternatively, you can define a the default route in the 'Smart Hosts' interface:

- Click SMTP > Domains > Smart Hosts tab.
- Select 'Enable Default Domain Routing' check box and provide the SMTP server details.

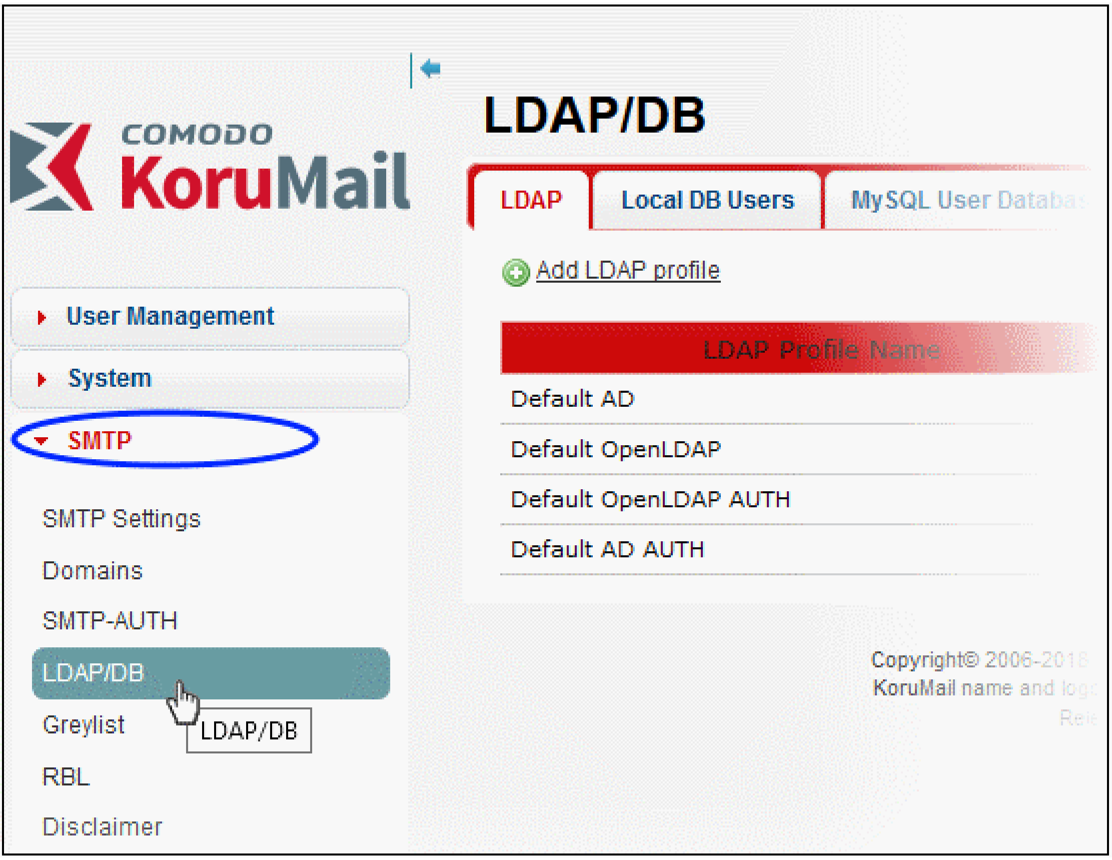
The default route will apply if you do not set a custom route for a domain. See **Default Domain Routing** for more information.

See **Manage Domains** for more details about managing domains, domain routes and smart hosts.

Step 6 – Add End Users

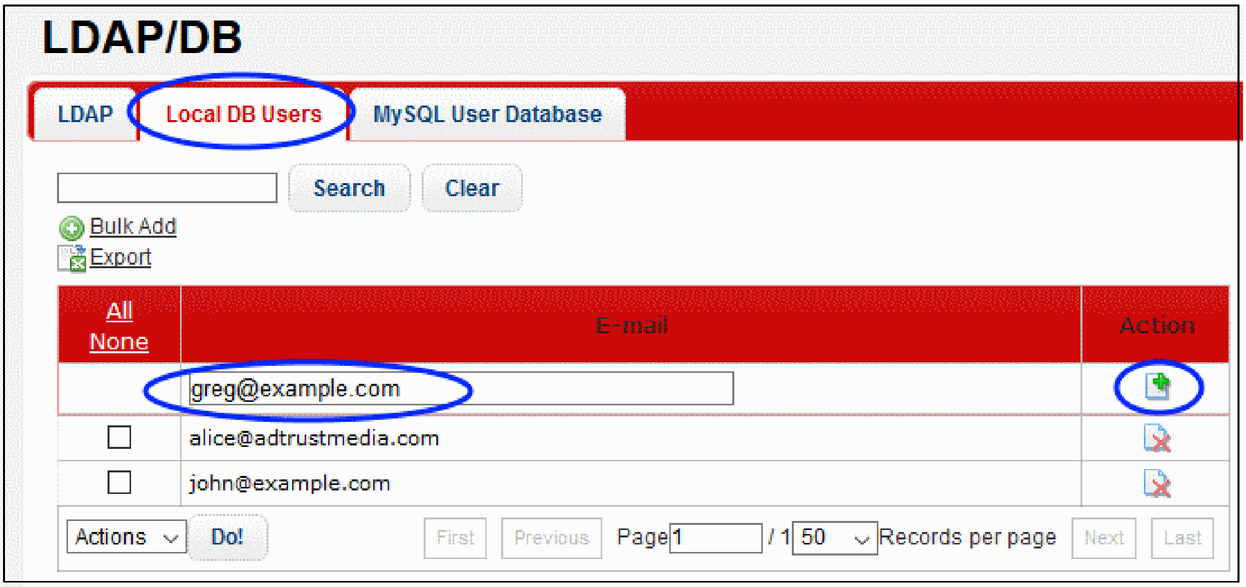
KoruMail will only filter mail for valid recipients. You can add users manually and/or import users from an LDAP server / My SQL User Database.

- Click SMTP > LDAP/DB:



To add users manually

- Click the 'Local DB Users' tab
- Enter the user's email address as shown:



LDAP/DB

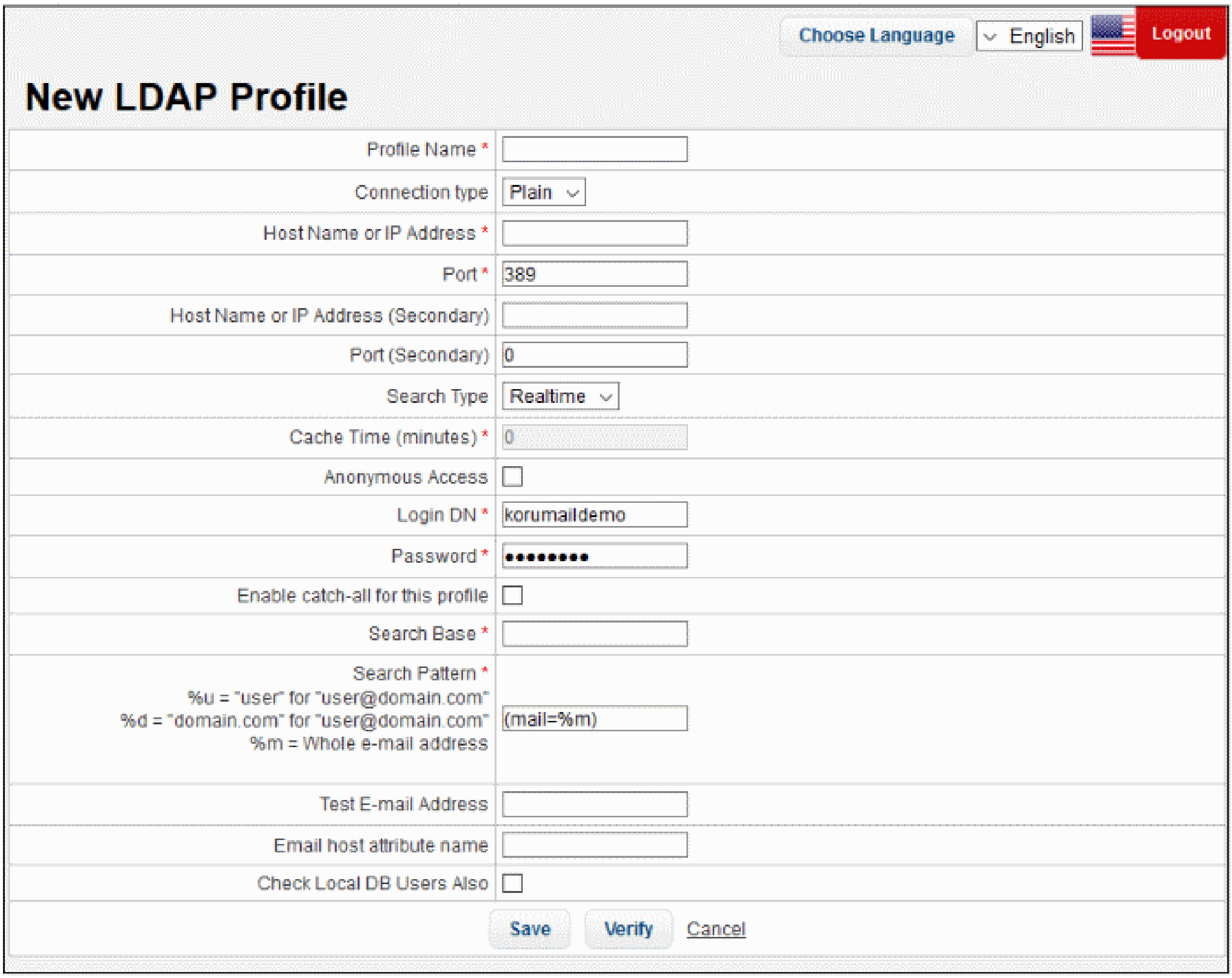
All None	E-mail	Action
	greg@example.com	
□	alice@adtrustmedia.com	
□	john@example.com	

- Click the button in the 'Action' column.
- You can add multiple users using the 'Bulk add' link.

Note – You can only add users for managed domains.

To integrate an LDAP server

- Click the LDAP tab
- Click the 'Add LDAP profile' link at the top



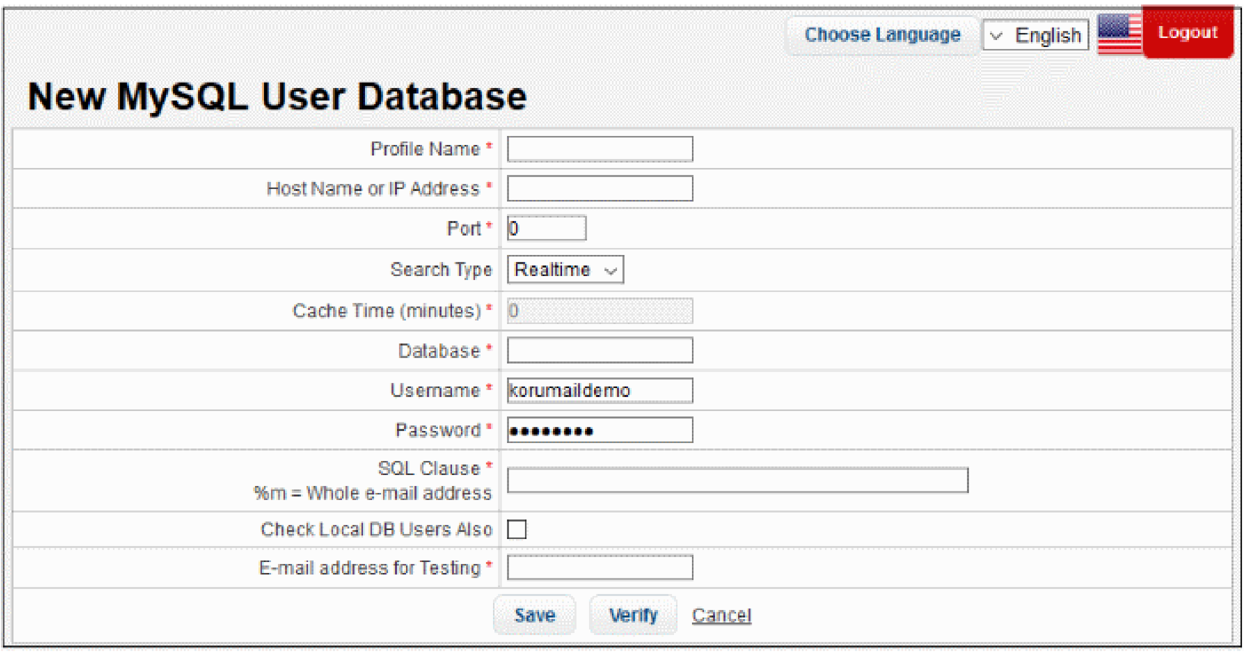
New LDAP Profile

Profile Name *	
Connection type	Plain
Host Name or IP Address *	
Port *	389
Host Name or IP Address (Secondary)	
Port (Secondary)	0
Search Type	Realtime
Cache Time (minutes) *	0
Anonymous Access	□
Login DN *	korumaildemo
Password *	●●●●●●●●●
Enable catch-all for this profile	□
Search Base *	
Search Pattern * %u = "user" for "user@domain.com" %d = "domain.com" for "user@domain.com" %m = Whole e-mail address	(mail=%m)
Test E-mail Address	
Email host attribute name	
Check Local DB Users Also	□

- Complete the profile form with the details of your LDAP server.
- Click the 'Verify' button to test the connection with the parameters you entered.
- Click the 'Save' button to apply your changes.

To add My SQL User Database

- Click the 'My SQL User Database' tab
- Click 'Add MySQL User Database' link at the top



New MySQL User Database

Profile Name *	
Host Name or IP Address *	
Port *	0
Search Type	Realtime
Cache Time (minutes) *	0
Database *	
Username *	korumaildemo
Password *	●●●●●●●●●
SQL Clause * %m = Whole e-mail address	
Check Local DB Users Also	□
E-mail address for Testing *	

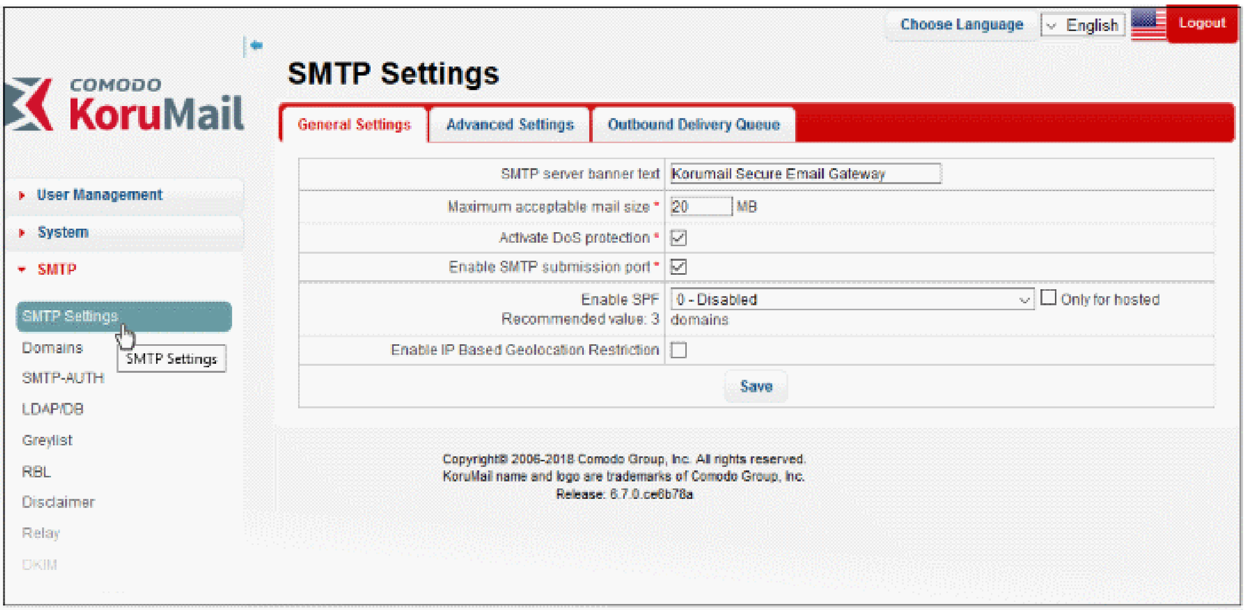
- Complete the profile form with the details of your MySQL database.
- Click the 'Verify' button to check the connection with the parameters you have specified.
- Click 'Save' to apply your changes.

See '**LDAP/Local DB/My SQL User Database**' if you need more help with this.

Step 7 – Configure SMTP Settings

Next, configure the SMTP settings for incoming and outgoing mails.

- Click 'SMTP' > 'SMTP Settings'



SMTP Settings

SMTP server banner text	Korumail Secure Email Gateway
Maximum acceptable mail size *	20 MB
Activate DoS protection *	☑
Enable SMTP submission port *	☑
Enable SPF Recommended value: 3	0 - Disabled □ Only for hosted domains
Enable IP Based Geolocation Restriction	□

Copyright© 2006-2018 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 6.7.0.ce6b78a

General Settings

SMTP Settings - General Settings Table of Parameters	
Parameter	**Description**
SMTP server banner text	The welcome message shown on the server after successfully connecting to KoruMail port 25.
Maximum acceptable mail size (MB)	The maximum permitted size of a single email + attachments. The default value is 20 MB.
Activate DoS protection	A DoS (Denial of Service) attack occurs when a malicious actor tries to overload your mail server by bombarding it with unsolicited mail. DoS protection implements limits to help ensure your servers are not brought to a standstill by such attacks.
Enable SMTP submission port	If enabled, KoruMail will not accept outgoing messages from unauthenticated sources, thus helping to protect your network and users from spam emails.
Enable SPF	SPF (Sender Policy Framework) is a standard designed to block the forgery of sender addresses. SPF values 1. Just add received-SPF header 2. Return temporary failure in DNS query error 3. If SPF result fails (ban) then reject it (recommended) 4. If SPF result is softfail then reject it 5. If SPF result is neutral then reject it 6. If SPF result is not passed then reject it You can disable SPF by selecting '0' from the list. If the check box 'Only for hosted domains' is selected, then the SPF check will be performed for outgoing mails for domains that are hosted in the network.
Enable IP Based Geolocation Restriction	Sender IP based location detection. This should be enabled here in order to activate the geo location restriction settings in the incoming profiles. Mails from restricted countries list will be rejected.

- Click the 'Save' button to apply your changes.

Advanced Settings

- Click the 'Advanced Settings' tab

SMTP Settings - Advanced Settings Table of Parameters	
Parameter	**Description**
Minimum number of filter processors	The least filter processes that the filtering engine should use. Filter processors are threads used to scan and handle mail. • Fewer processors = Lower resource overhead / slower performance
Maximum number of filter processors	The most filter processes that the filtering engine should use. Filter processors are threads used to scan and handle mail. • More processors = Higher resource overhead / better performance

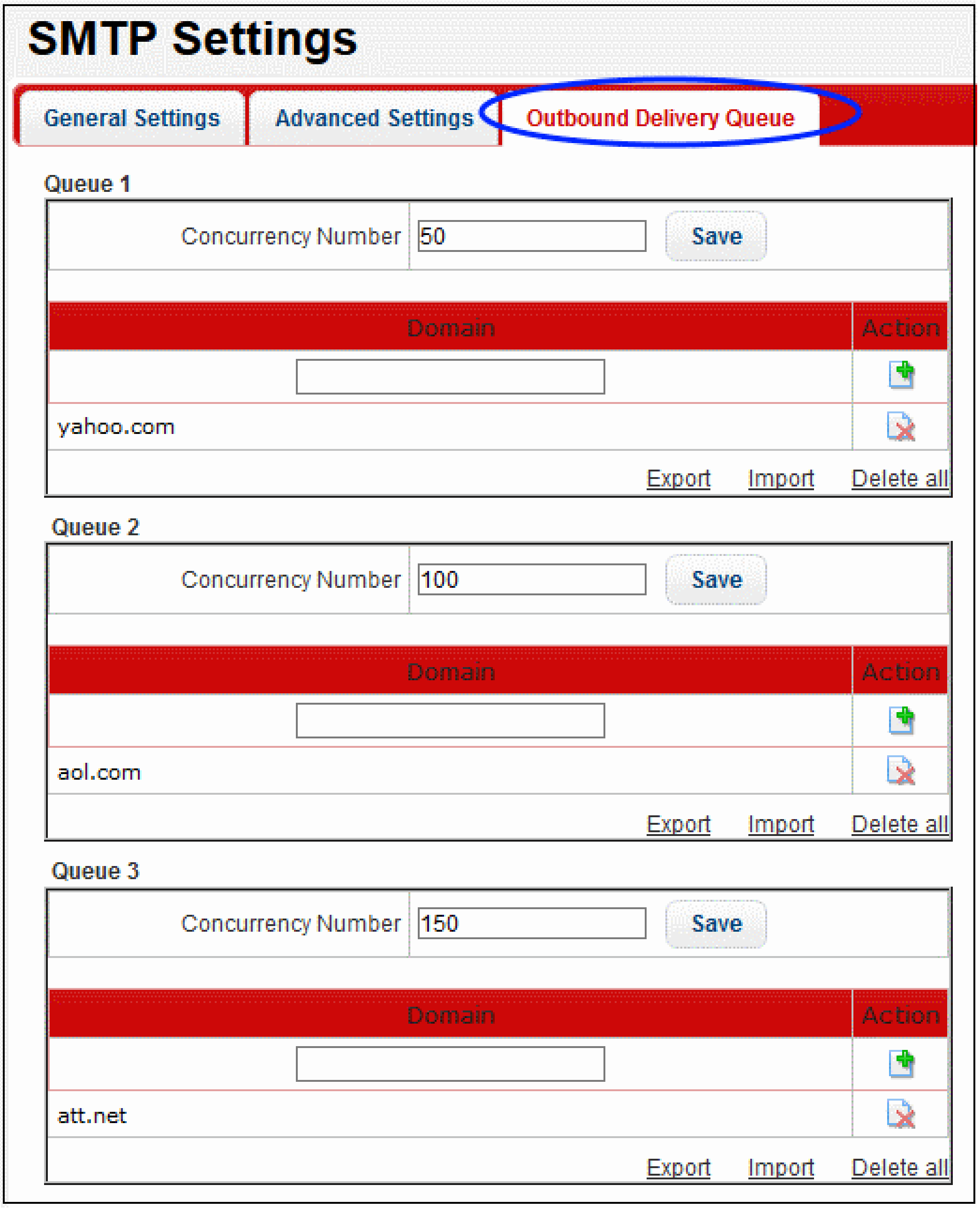
Maximum number of recipients per SMTP transaction	The highest number of mailboxes to which KoruMail will forward mail per transaction.
Incoming SMTP session timeout (seconds)	Timeout duration of each SMTP session.
RBL Timeout (seconds)	If this time is exceeded, the RBL query is canceled and next filter is applied to the e-mail.
Early talker drop time (seconds)	After a client makes a TCP connection, SMTP servers will wait a for short time before sending a greeting message. The client replies with a HELO or a EHLO response. If the server receives the response before sending the greeting, then the client could be serving spam. The waiting time before sending the greeting is called 'Early talker drop time'. We recommend you leave the setting at the default.
Reject invalid addresses	If enabled, incoming mails with invalid address will be rejected
Queue life time (hour)	Enter the number of hours that a mail can be queued for delivery before it is bounced.
Enable tarpitting	Tarpitting helps thwart spammers by slowing the transmission of bulk emails. Tarpits slow communication times with spam servers when they send mail to several of your recipients during one session. Spammers may stop sending emails to your server if the response to their requests is very slow.
Tarpit count	Tarpitting will become active if the number of recipients exceeds the Tarpit count.
Tarpit delay (second)	The number of seconds that Tarpitting will delay the transmission response
Maximum number of SMTP sessions	Maximum number of simultaneous SMTP sessions.
Maximum number of concurrent mail delivery	Maximum number of simultaneous outgoing messages that can be sent.
Main Filter engine log level	Select the level of main filtering engine event that should be logged. Selecting 'Debug' will log all the levels.

- Click the 'Save' button to apply your changes.

Outbound Delivery Queue

You can queue outbound mails per domain so only a certain number of mails will be delivered at once.

- Click the 'Outbound Delivery Queue' tab



Queue 1

Concurrency Number: 50 — Save

Domain	Action
	+
yahoo.com	✗

Export Import Delete all

Queue 2

Concurrency Number: 100 — Save

Domain	Action
	+
aol.com	✗

Export Import Delete all

Queue 3

Concurrency Number: 150 — Save

Domain	Action
	+
att.net	✗

Export Import Delete all

The interface has three preset delivery queues that can be configured according to your needs. You can assign as many domains as required to a particular concurrency number. You can also change the concurrency number itself if required.

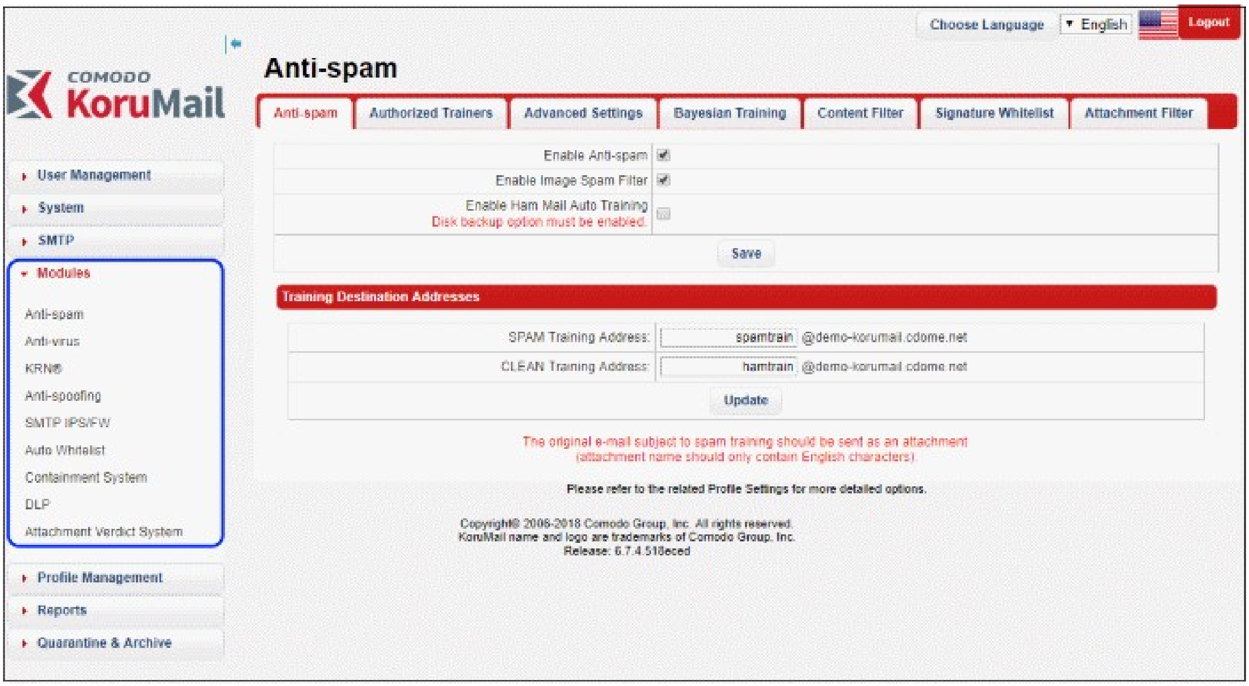
- Concurrency Number – The maximum number of emails that can be sent at once from the domain.
- To remove a domain from the list, click the ✗ button beside it.
- To remove all domains from the list, click the 'Delete all' link and confirm the removal in the 'Confirmation Dialog'.

The 'SMTP' section also allows you to configure other settings such as outgoing limits, incoming limits and more. See '**SMTP Configuration**' for more details.

Step 8 – Configure KoruMail Security Components

The 'Modules' section lets you configure KoruMail security components.

- Click 'Modules' on the left
- Help for each module is listed under the following screenshot:



Enable Anti-spam ☑

Enable Image Spam Filter ☑

Enable Ham Mail Auto Training ☐
Disk backup option must be enabled.

SPAM Training Address: spamtrain @demo-korumail.cdome.net

CLEAN Training Address: hamtrain @demo-korumail.cdome.net

The original e-mail subject to spam training should be sent as an attachment (attachment name should only contain English characters).

Please refer to the related Profile Settings for more detailed options.

Copyright© 2006-2018 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 6.7.4.518eced

Click the links below:

- **Anti-spam**
- **Antivirus**
- **KRN**
- **Anti-spoofing**
- **SMTP IPS / FW**
- **Auto Whitelist**
- **Containment System**
- **DLP**
- **Attachment Verdict System**

Anti-spam

- **Anti-spam General Settings** - Enable/disable anti-spam and image filters. Ham mail = legitimate mail. Upload ham training materials help teach the antispam system to identify legitimate mail – useful if you are getting too many false-positives. The anti-spam module must be enabled in order to activate the anti-spam parameters specified in profile settings.
- **Authorized Trainers** - Define the sources from which spam training emails can be sent. Submitting sample spam emails allows the system to learn, adapt and protect against new spam types.
- **Advanced Settings** - The languages you select here will be analyzed for spam using the Bayesian spam classifier.
- **Bayesian Training** - The Bayesian engine analyzes emails for patterns which may indicate that the mail is

spam. You can upload sample spam and HAM (legitimate) emails in order to 'train' the engine to provide more accurate verdicts.

- **Content Filter** – Add words that when detected in message body will be marked as spam
- **Signature Whitelist** – A list of digital signatures that came attached to white-listed emails. You can manually whitelist mails from the 'Mail Logs' interface.
- **Attachment Filter** – Define how many archive levels should be checked by KoruMail. For example, a zip file may contain another zip file inside it. A depth of '2' means KoruMail will check inside both files.

See '**AntiSpam**' in the main user guide for more information.

Antivirus

Configure antivirus settings and select the program that should be used for AV scans.

- **General Settings** – Enable / disable anti-virus and select the virus scanner.
- **Advanced Settings** – Define scanner settings such as size of mails that should be scanned, file types that should be scanned and so on.

See '**AntiVirus**' for more information.

KRN

Korumail Reputation Network is a system which assigns a trust rating to IP addresses. It not only includes traditional features such as real-time IP blacklists but also has ‘whitelist’ and ‘greylisting ignore’ features.

- **Servers** - A newly added KRN server will be in enabled status by default. Click the 'Yes' or 'No' link under the 'Enabled' column to switch between enabled and disabled statuses.
- **Settings** – Enable / disable Reputation Network blacklist, whitelist and whitelist triplet scan.

See '**Reputation Network (KRN)**' if you need more help with this.

Anti-spoofing

Email spoofing is a technique used to forge email headers so that the message appears to originate from a source other than the true sender. You can configure the settings to check whether an email is being sent from an authorized server.

- Select 'Enable Anti-spoofing' check box
- Select the managed domain from the 'Choose Domain' drop-down and enter the IP addresses.

See '**Anti-Spoofing**' if you need more help with this.

SMTP IPS / FW

Configure the intrusion prevention system (IPS) and firewall (FW) to protect against denial of service (DoS) and SYN attacks.

- **General** – Enable / disable SMTP IPS/FW module and configure the security profile.
- **Whitelist** – Add trusted networks so they will not be filtered by the SMTP IPS module.
- **Blocked** – Add IP addresses so that mails from these sources never reach the SMTP level for processing.
- **Rate Control** - The 'Rate Control' feature protects your company from spammers that send huge amount of emails to the server in a small amount of time. Configure the rate control settings in order to automatically add IP addresses to blacklist if the set threshold is exceeded.

See '**SMTP IPS / FW**' if you need more help with this.

Auto Whitelist

Configure this setting to automatically trust emails sent between specific senders and recipients.

- The threshold means how many emails must be exchanged before the remote sender is added to the whitelist. The threshold must be achieved within the 'Maximum Day Count' underneath this setting.

See '**Auto Whitelist**' if you need more help with this.

Containment System

- Protects users from zero-day malware by opening any untrusted attachments in a secure, virtual environment known as the container.
- Items in the container are not allowed to access other processes or user data and will write to a virtual hard-drive and registry.
- KoruMail checks the trust rating of all attachments. PDF and .exe attachments with a trust rating of 'Unknown' are removed and replaced with a link.
- The link allows recipients to download a special version of the file wrapped in Comodo's containment technology. The file will be open in a virtual container on the endpoint

DLP (Data Leak Prevention)

- Data loss prevention helps stops sensitive information from leaving your organization via email. You configure it by specifying keywords that should be monitored.
- If triggered, you can configure actions such as quarantine or block the mail.
- You specify the keywords themselves in the antispam profile.
- **DLP** – Enable / disable DLP, Incoming Profiles and Outgoing Profiles.

See '**Data Leak Prevention**' if you need more help with this.

Attachment Verdict System

Configure to submit email attachments (executable and pdf files) that are rated as 'Unknown' to Valkyrie, a file analysis and verdicting system.

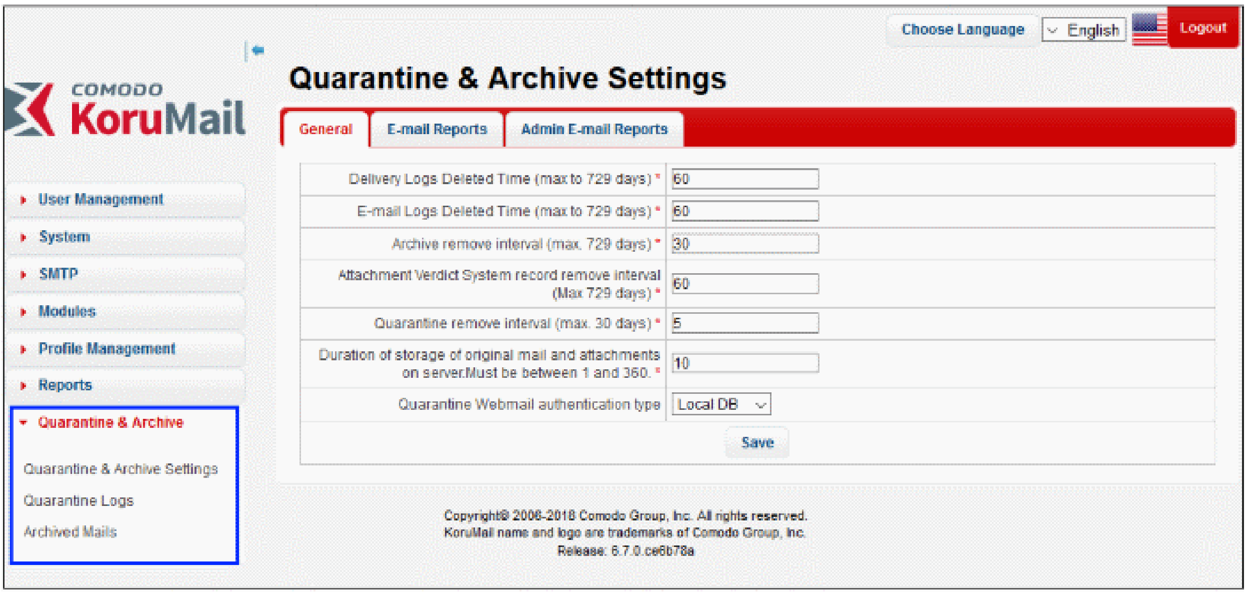
- **General Settings** – Enable / disable attachment verdict system. Provide your KoruMail license key. The host name is by default set to Valkyrie.

See '**Attachment Verdict System**' if you need more help with this.

Step 9 – Configure Quarantine & Archive Mail Settings

Configure the number of days that logs and archived files should be retained in KoruMail.

- Click 'Quarantine & Archive' on the left then 'Quarantine & Archive Settings'



Quarantine & Archive Settings

Delivery Logs Deleted Time (max to 729 days) *	60
E-mail Logs Deleted Time (max to 729 days) *	60
Archive remove interval (max. 729 days) *	30
Attachment Verdict System record remove interval (Max 729 days) *	60
Quarantine remove interval (max. 30 days) *	5
Duration of storage of original mail and attachments on server.Must be between 1 and 360. *	10
Quarantine Webmail authentication type	Local DB

Copyright© 2006-2018 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 6.7.0.ce6b78a

- Click the 'General' tab

Quarantine & Archive General Settings - Table of Parameters	
Parameter	**Description**
Delivery Logs Deleted Time	Delivery logs are a record of incoming and outgoing mails which were accepted by mails servers. Specify the number of days these logs should be kept.
E-mail Logs Deleted Time	Mail logs are a record of all incoming and outgoing mails handled by KoruMail, regardless of whether the mail was accepted. Enter the number of days for which the email logs should be retained.
Archive remove interval	The number of days that KoruMail should store a copy of emails.
Attachment Verdict System record remove Interval	Attachment verdicts tell KoruMail whether or not an attachment is safe, malicious or unknown. These verdicts are awarded by Valkyrie after it has analyzed the files behavior. Enter the number of days the verdicts should be retained by KoruMail. This is for the purposes of to view log history and the analysis result. KoruMail asks Valkyrie verdict for each attachment regardless of prior requests.
Quarantine remove interval	Enter the number of days after which the 'Quarantined Logs' will be removed. The maximum period that can be set is 30 days.
Duration of storage of original mail and attachments on server	This setting pertains to Containment. Specify the number of days that emails including attachments should be retained by KoruMail. The period should be between 1 and 360 days. Original emails and contained attachments are deleted after this period.
Quarantine Webmail authentication type	Select the user authentication type from the option for users that access the Webmail interface to check their quarantined mails.

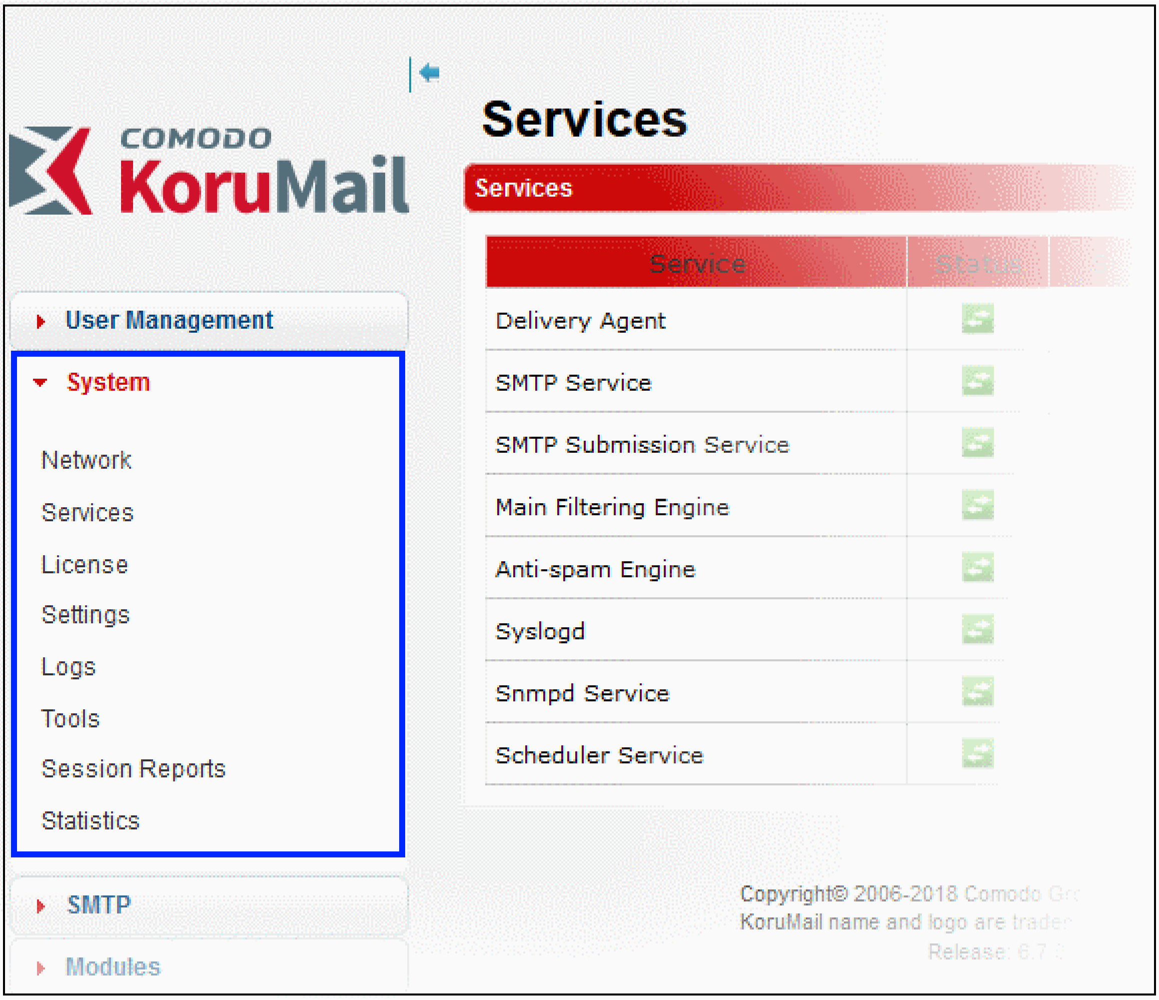
- Click the 'Save' button to apply your changes.

You can also configure the email reports settings for users to access their quarantined emails and admin email reports settings for sending reports to administrators. See '**Quarantine & Archive**' for more details.

Step 10 – System Configuration

After completing the initial steps explained above, you can check and configure other system settings such as GUI customization and more.

- Click 'System' on the left, then the sub-menu that you want to configure



Service	Status
Delivery Agent	🟩
SMTP Service	🟩
SMTP Submission Service	🟩
Main Filtering Engine	🟩
Anti-spam Engine	🟩
Syslogd	🟩
Snmpd Service	🟩
Scheduler Service	🟩

- **Network** – Initial KoruMail network settings. See **Step 3**.
- **Services** - Start or stop various services such as delivery agent, SMTP, Snmpd, scheduler and more.
- **License** – View current license, create license requests and / or install a new license.
- **Settings** – Configure important KoruMail settings:
  - **General** - Enable or disable automatic upload of selected spam messages to Comodo for analysis.
  - **Cache** – Configure cache expire time for Greylist IP addresses, SMTP Auth logs and LDAP.
  - **Session** - Configure the session timeout period and the maximum number of concurrent login count to the account.
  - **GUI Customization** - Customize the look and feel of the console. You can also change the name and the logo which is displayed in the interface.
  - **Backup** – Store copies of system configuration settings and logs. You can restore your Antispam configuration from your backup at any time.
  - **Restore** - Reverts your KoruMail configuration and logs to a previous system state.
  - **Log Upload** – Automate the process of uploading various types of KoruMail logs.
  - **Postmaster** – Forward mails directed to postmaster@ to another address.
  - **Web UI SSL Certificate** – Deploy an SSL certificate in order to provide secure, HTTPS access to your KoruMail admin console.
  - **SMTP TLS** – Configure to encrypt messages transmitted between Mail Transfer Agents (MTAs).

  - **Database Update** – Allows you to update virus and spam database manually.
  - **Syslog** – Forward logs to a remote server.
- **Logs** - Download logs and delete unwanted logs.
- **Tools** - Check the connectivity to the mail servers and clients. Clear the mails in the SMTP delivery queue.
- **Statistics** - View SMTP connection statistics, mail statistics and utilization statistics of hardware and software resources like network, CPU, hard disks and system memory as graphs.

See **System Configurations** for more details.

See the admin guide at **https://help.comodo.com/topic-290-1-632-8025-Introduction-to-KoruMail-Secure-Email-Gateway.html** for information about all the features and settings.

Dashboard – View statistics about your mail traffic and overall system details. You can also view important system messages and update the license. See **https://help.comodo.com/topic-290-1-632-8036-The-Dashboard.html** for more information.

User Management – Add administrative users with appropriate privileges for managing your KoruMail account. Also add end-users to access their quarantined emails. See **https://help.comodo.com/topic-290-1-632-8041-User-Management.html** for more details.

System – Configure antispam services, upgrade license and more. See **https://help.comodo.com/topic-290-1-632-8048-System-Configurations.html** for details.

SMTP – Configure settings for incoming and outgoing mails, manage domains and more. See **https://help.comodo.com/topic-290-1-632-8065-SMTP-Configuration.html** for more information.

Modules – In this section, you can configure the core security components of KoruMail email defense system. See **https://help.comodo.com/topic-290-1-632-8073-Modules.html** for more details.

Profile Management – Create rules and settings that can be applied to specific domains, e-mail addresses, incoming mails and outgoing mails. See **https://help.comodo.com/topic-290-1-632-8128-Profile-Management.html** for more information.

Reports – Configure report settings and generate reports for mail logs, SMTP queue and more. See **https://help.comodo.com/topic-290-1-632-8129-Reports.html** for more details.

Quarantine & Archive – In this section, you can configure the number of days that logs and archived files should be retained. Also view the details of 'Quarantine Logs' and 'Archived Mails'. See **https://help.comodo.com/topic-290-1-632-8133-Quarantine-&-Archive.html** for more information.

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**