COMODO
Creating Trust Online®

Comodo KoruMail

Software Version 6.7

Administrator Guide

Guide Version 6.7.050720

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1 Introduction to KoruMail Secure Email Gateway

With unsolicited emails increasing with each passing day, employee mail boxes are flooded with spam messages that contain viruses, phishing links and more. Productivity can decline as individuals waste valuable time sorting genuine mails from junk. If a user opens a malicious attachment or visits a fraudulent website then organizations may find their network compromised or infected.

Comodo's KoruMail Secure Email Gateway is an antispam and threat prevention system that uses advanced filtering technologies, antivirus scanners and content analysis engines to quietly and effectively prevent unsolicited mail from entering your network.

Key Features

- LDAP control
- Realtime blocking lists
- Fast integration of MX records
- Reverse DNS
- White / grey / black list configuration
- IP scoring via Korumail reputation network
- Office 365 integration
- Active Directory Integration
- Extensive reports
- Webmail for end-users
- Containerization of untrusted attachments

Guide Structure

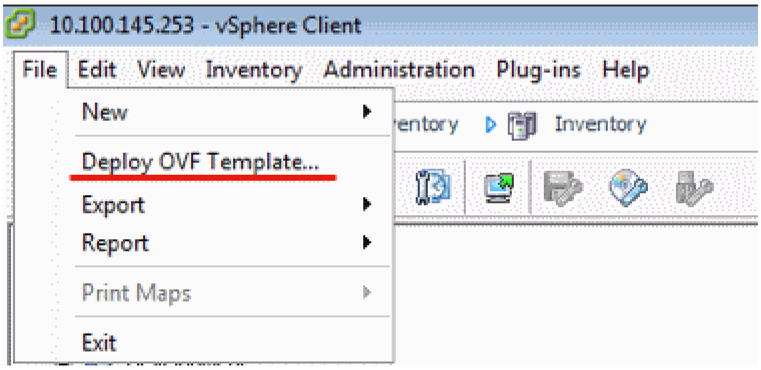
This guide is intended to take the user through the installation, configuration and use of Comodo KoruMail.

2 Korumail Deployment Process

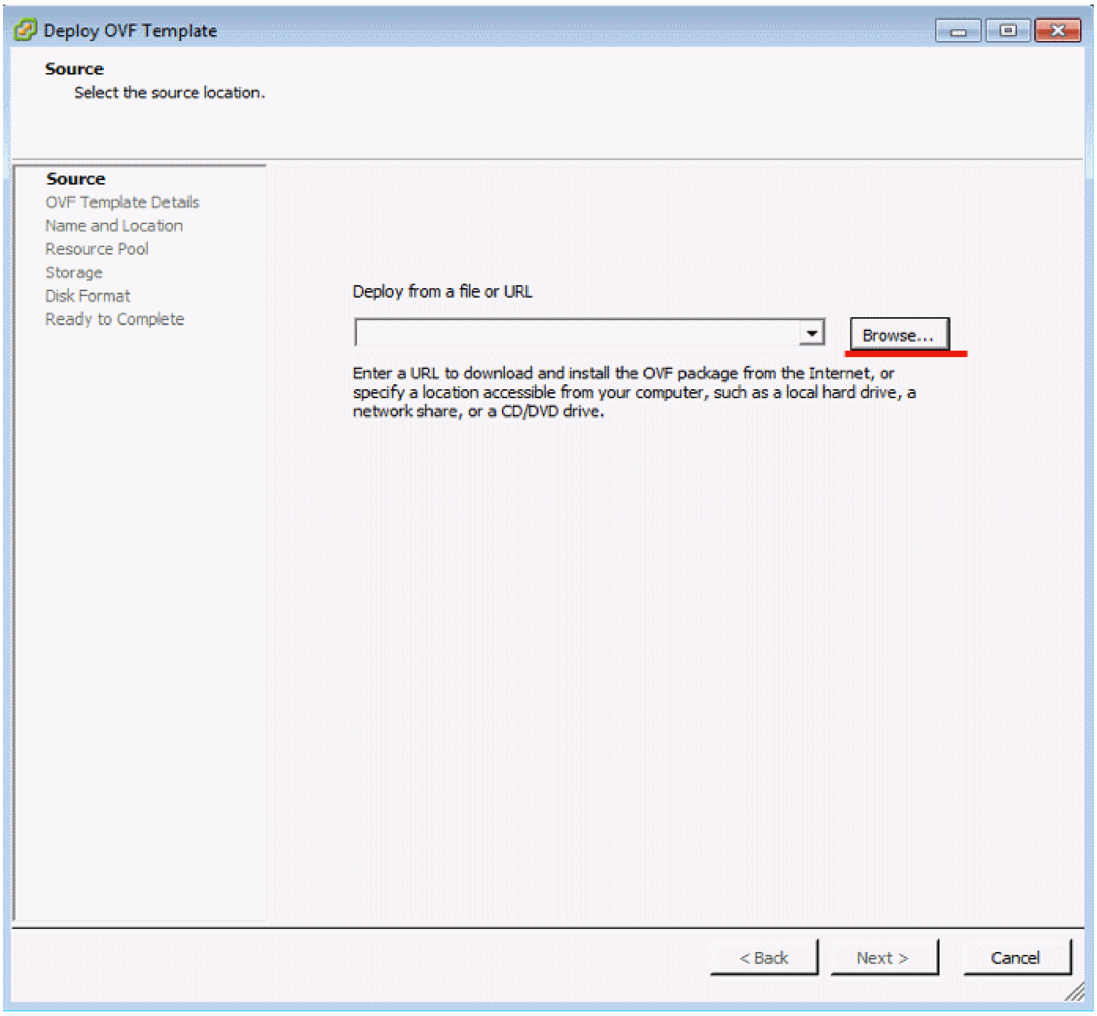
Korumail is deployed as a VMware image. Please follow the steps below to install the product.

1. Download the virtual machine image from: **https://cdn.download.comodo.com/korumail/KoruMAIL_V6_esx.rar**
2. Extract the contents of the .rar file using Winrar or 7zip.
3. Open the VMware Vsphere client and login to the ESXi server.
4. Follow the steps below to deploy Korumail to our ESX server:

- Click 'File' > 'Deploy OVF Template'

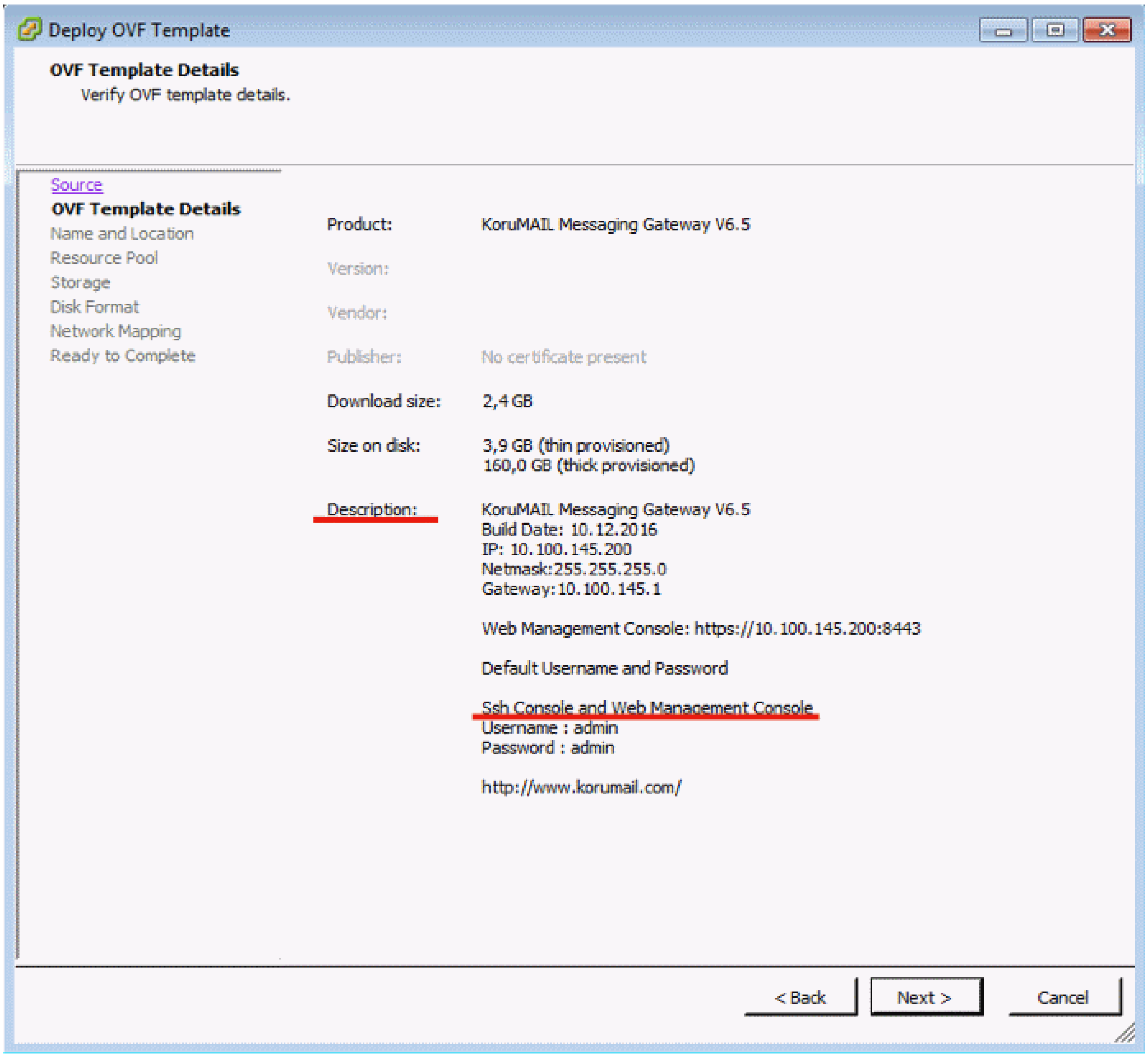


- Enter the URL of the OVF template file, or browse for the file's location on your computer:



Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

- Review the information in the details screen, especially the default username/password, then click 'Next':



OVF Template Details

Verify OVF template details.

Product: KoruMAIL Messaging Gateway V6.5

Version:

Vendor:

Publisher: No certificate present

Download size: 2,4 GB

Size on disk: 3,9 GB (thin provisioned)
160,0 GB (thick provisioned)

Description: KoruMAIL Messaging Gateway V6.5
Build Date: 10.12.2016
IP: 10.100.145.200
Netmask:255.255.255.0
Gateway:10.100.145.1

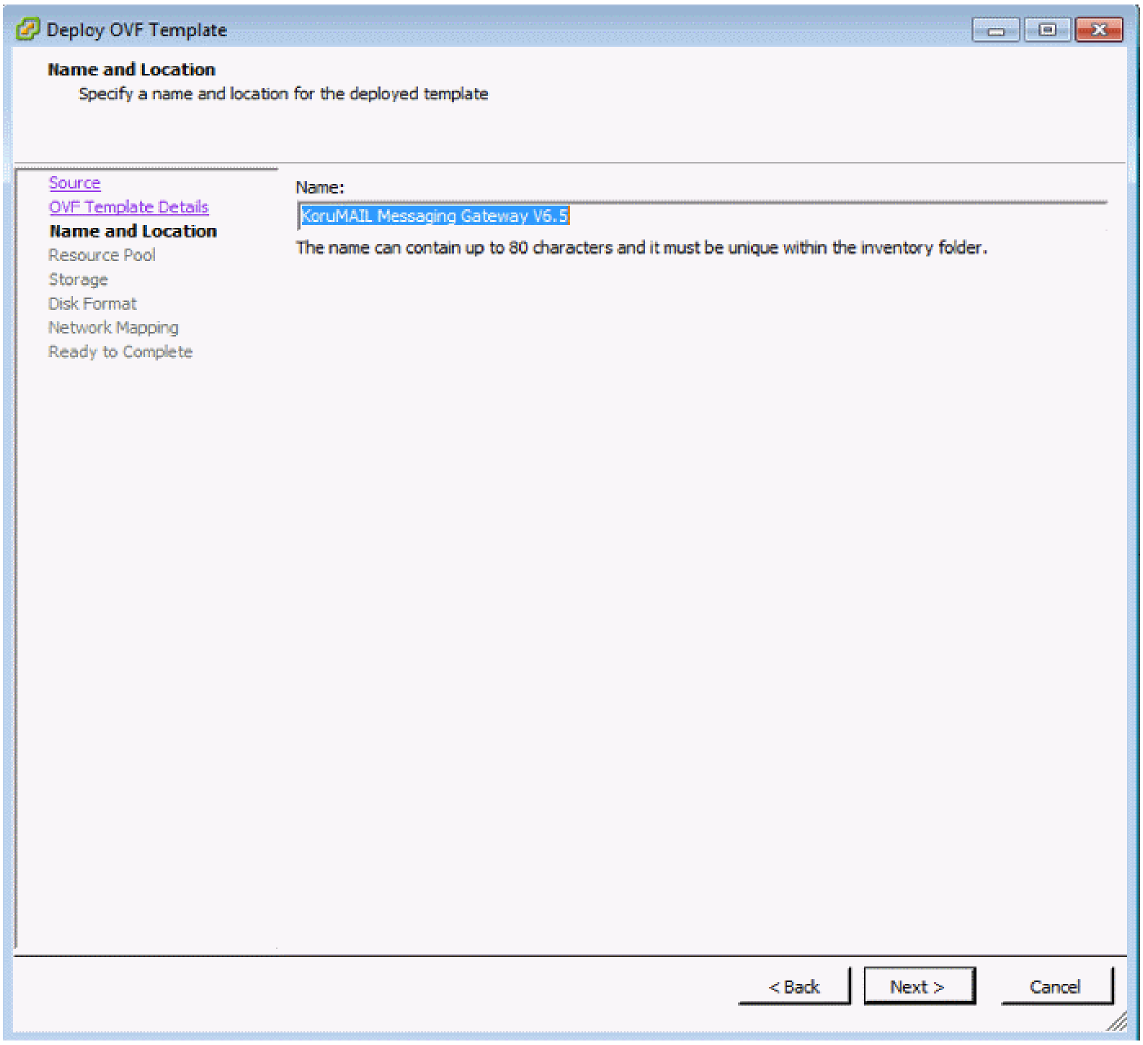
Web Management Console: https://10.100.145.200:8443

Default Username and Password

Ssh Console and Web Management Console
Username : admin
Password : admin

http://www.korumail.com/

- Specify a name for the server, or leave it at the default:



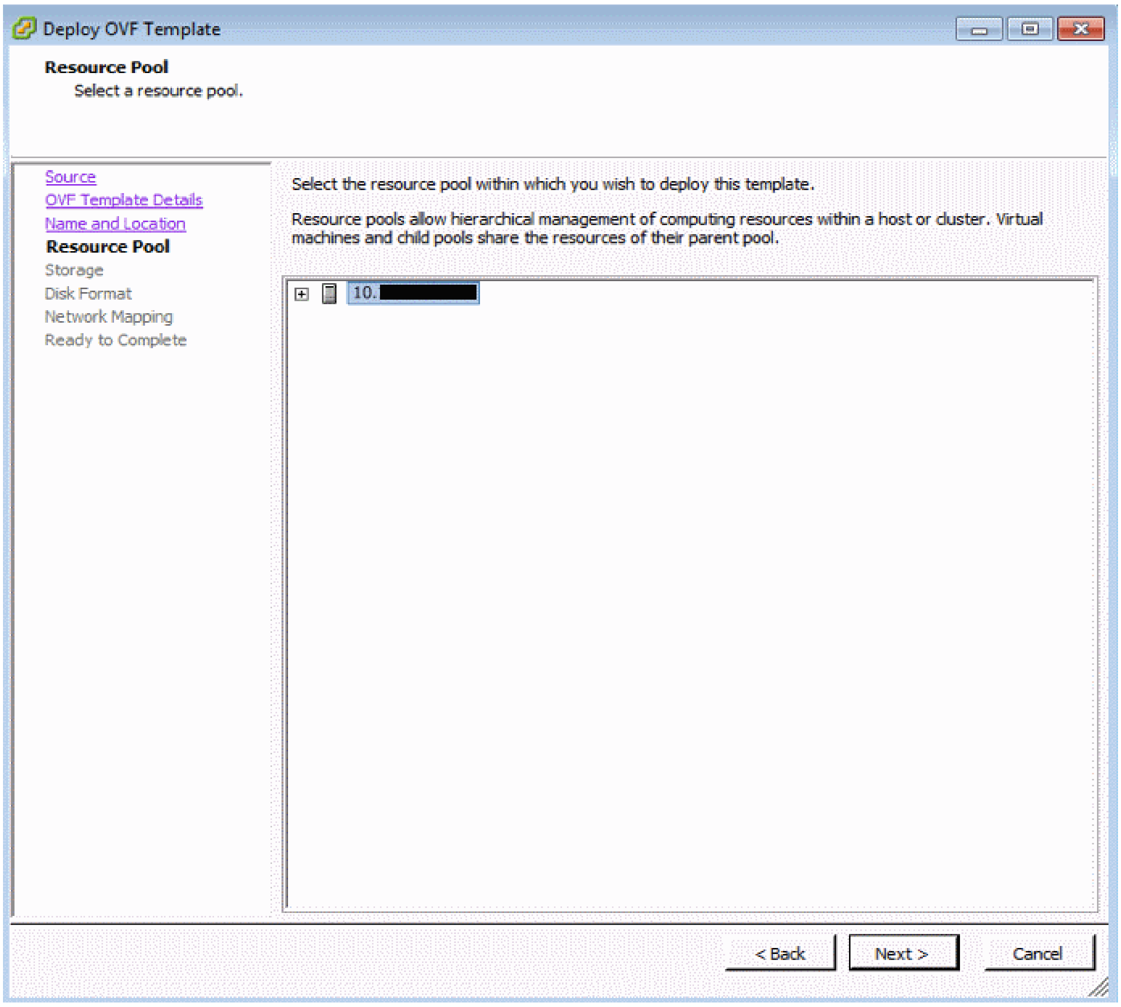
Name and Location

Specify a name and location for the deployed template

Name: KoruMAIL Messaging Gateway V6.5

The name can contain up to 80 characters and it must be unique within the inventory folder.

- Click 'Next.'
- Select a server on the ESX server with sufficient resources and click 'Next':



Resource Pool

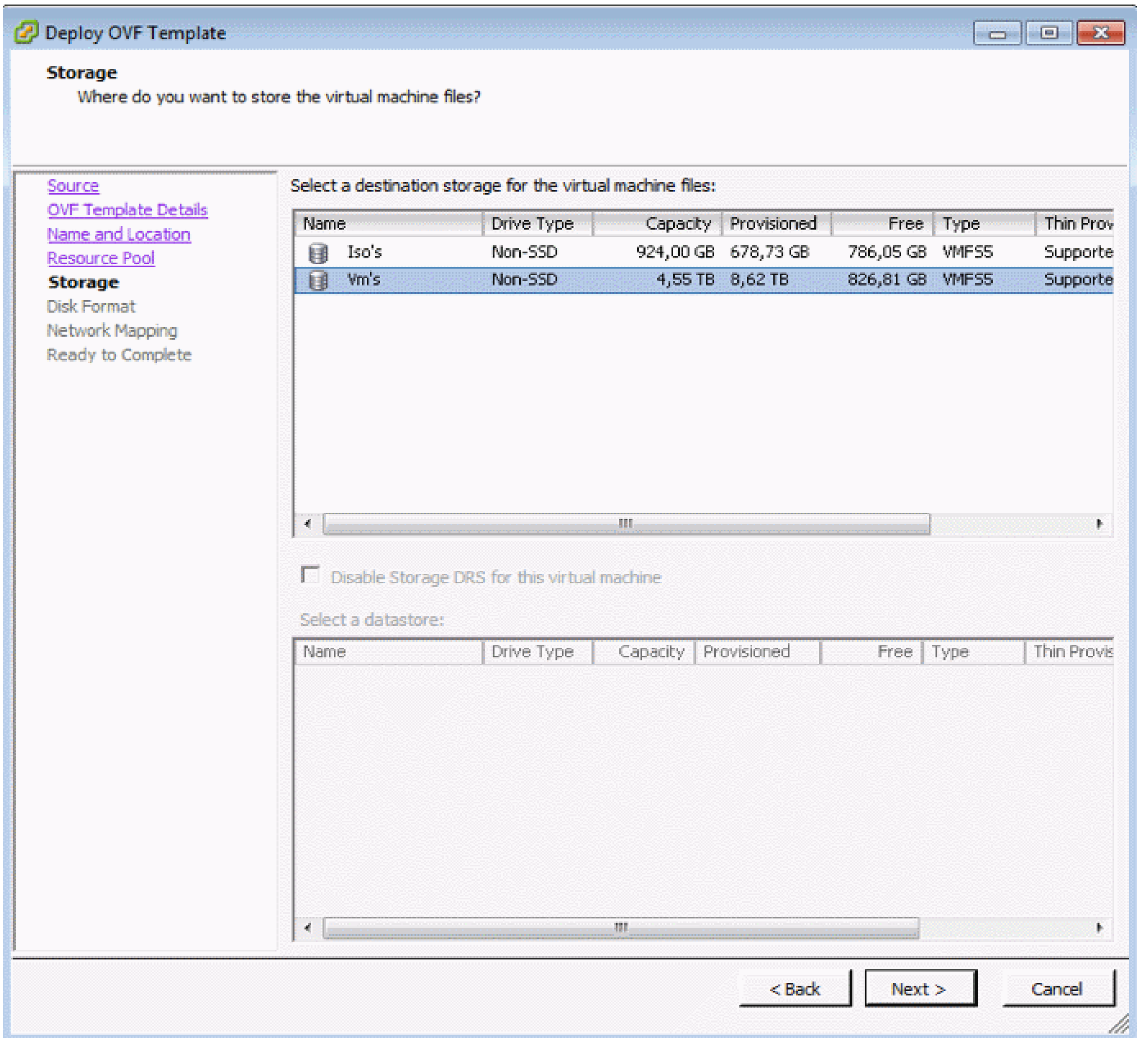
Select a resource pool.

Select the resource pool within which you wish to deploy this template.

Resource pools allow hierarchical management of computing resources within a host or cluster. Virtual machines and child pools share the resources of their parent pool.

10.[redacted]

- Choose which storage area your virtual machine image should be copied to. Korumail requires 160 Gb of disk space. Click 'Next' when done.



Deploy OVF Template

Storage

Where do you want to store the virtual machine files?

Select a destination storage for the virtual machine files:

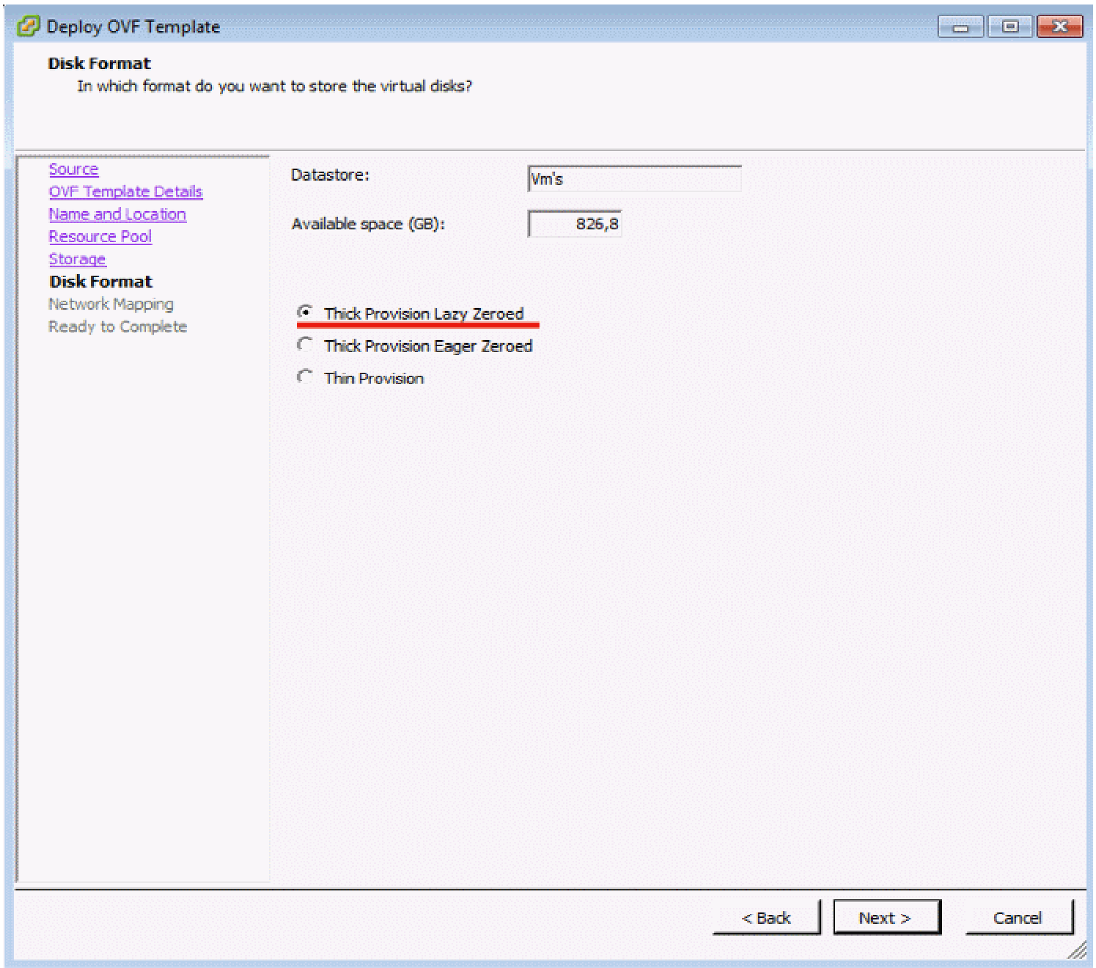
Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Prov
Iso's	Non-SSD	924,00 GB	678,73 GB	786,05 GB	VMFS5	Supporte
Vm's	Non-SSD	4,55 TB	8,62 TB	826,81 GB	VMFS5	Supporte

□ Disable Storage DRS for this virtual machine

Select a datastore:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provis

- Select 'Thick Provision' as 'Disk Format' and click 'Next':



Deploy OVF Template

Disk Format

In which format do you want to store the virtual disks?

Datastore: Vm's

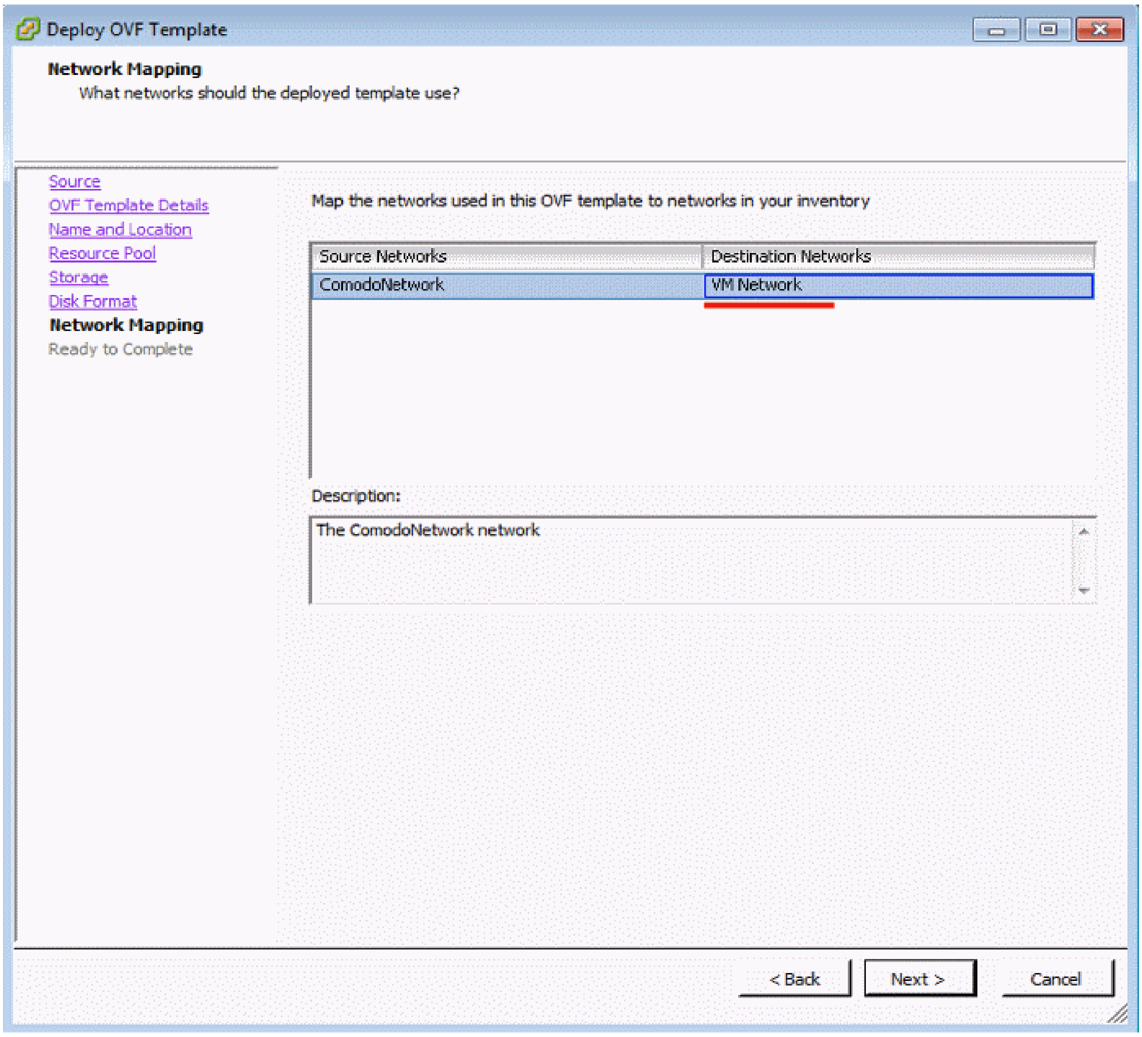
Available space (GB): 826,8

● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

- Select a network with an active internet connection:



Deploy OVF Template

Network Mapping

What networks should the deployed template use?

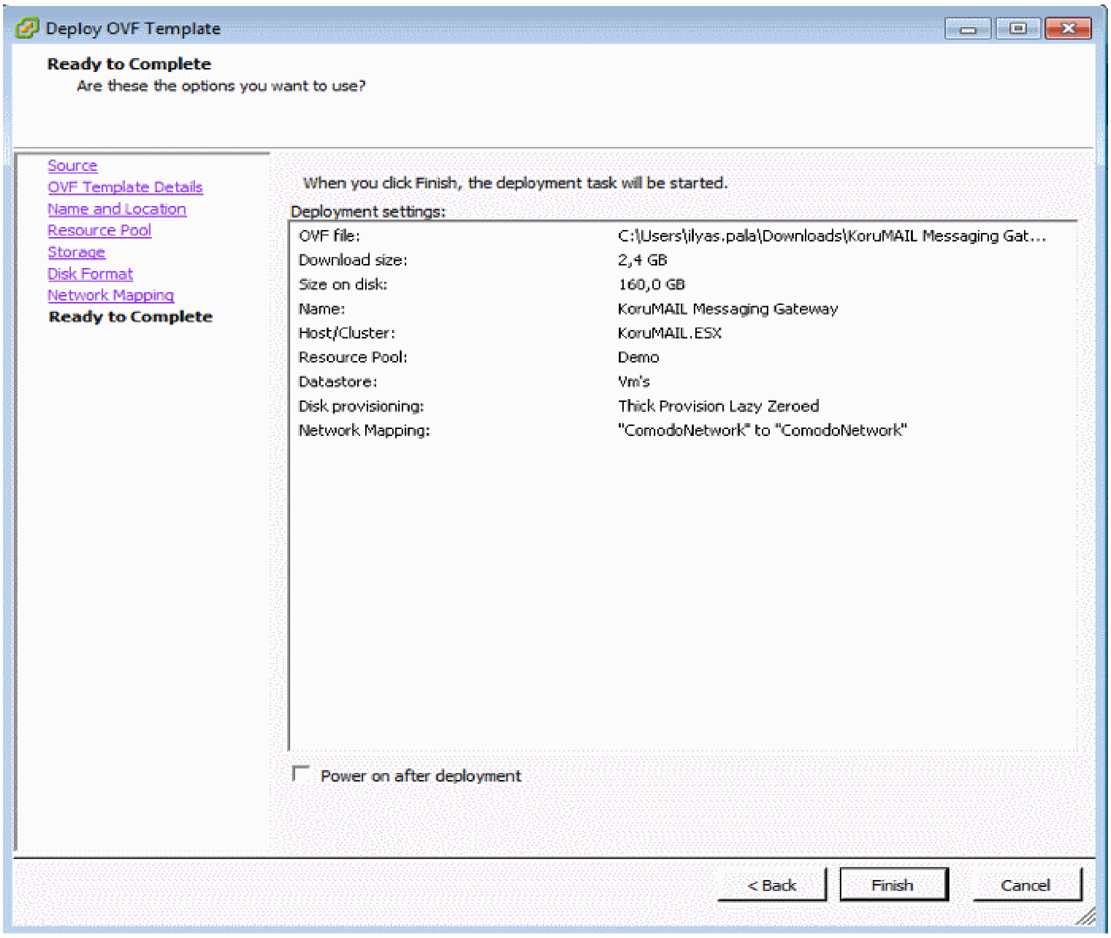
Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
ComodoNetwork	VM Network

Description:

The ComodoNetwork network

- Review the setup details then click 'Finish' to begin installation:



Deploy OVF Template

Ready to Complete

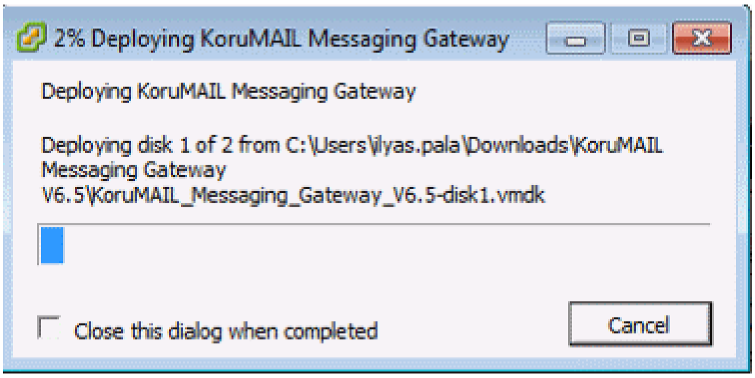
Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\Users\ilyas.pala\Downloads\KoruMAIL Messaging Gat...
Download size:	2,4 GB
Size on disk:	160,0 GB
Name:	KoruMAIL Messaging Gateway
Host/Cluster:	KoruMAIL.ESX
Resource Pool:	Demo
Datastore:	Vm's
Disk provisioning:	Thick Provision Lazy Zeroed
Network Mapping:	"ComodoNetwork" to "ComodoNetwork"

□ Power on after deployment



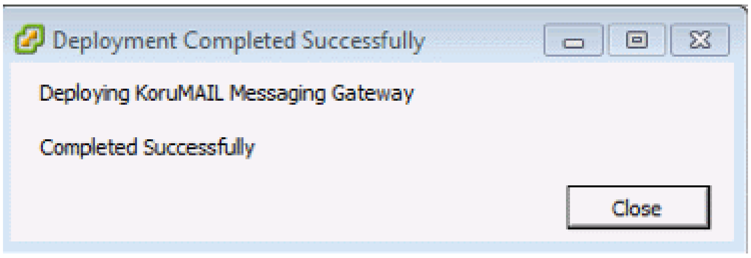
2% Deploying KoruMAIL Messaging Gateway

Deploying KoruMAIL Messaging Gateway

Deploying disk 1 of 2 from C:\Users\ilyas.pala\Downloads\KoruMAIL Messaging Gateway V6.5\KoruMAIL_Messaging_Gateway_V6.5-disk1.vmdk

□ Close this dialog when completed

- The deployment process takes a few minutes to complete.

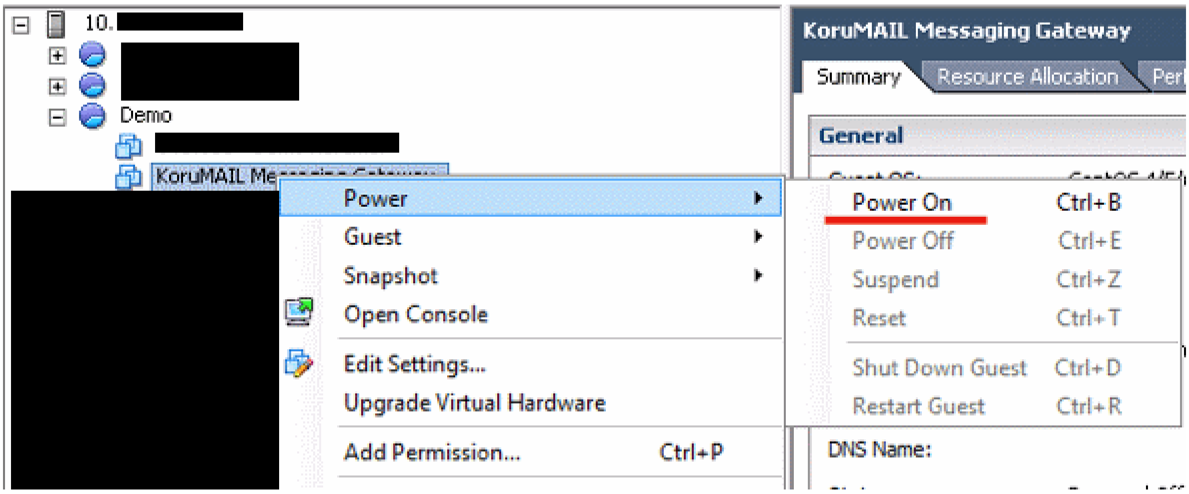


Deployment Completed Successfully

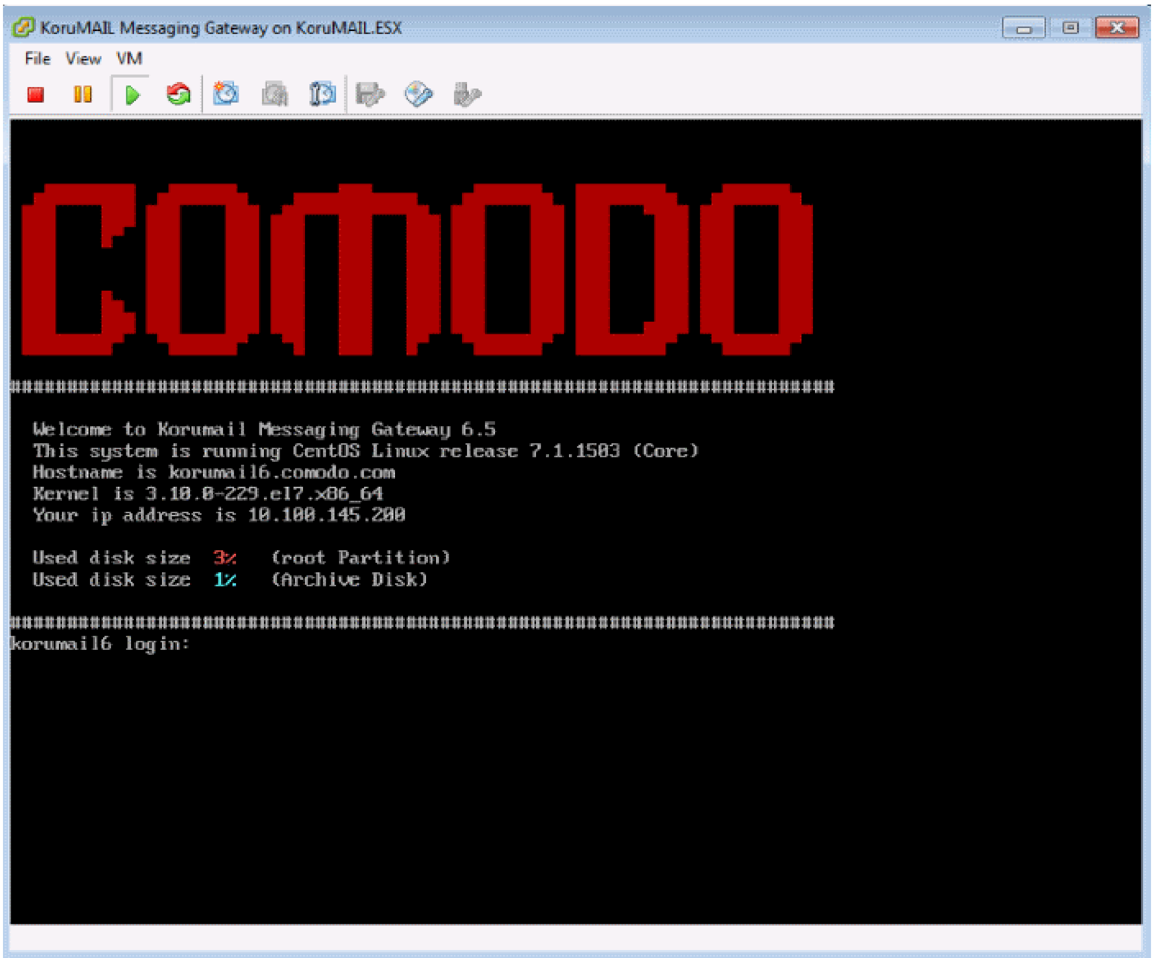
Deploying KoruMAIL Messaging Gateway

Completed Successfully

- Select the Korumail server, right-click then select 'Power On':



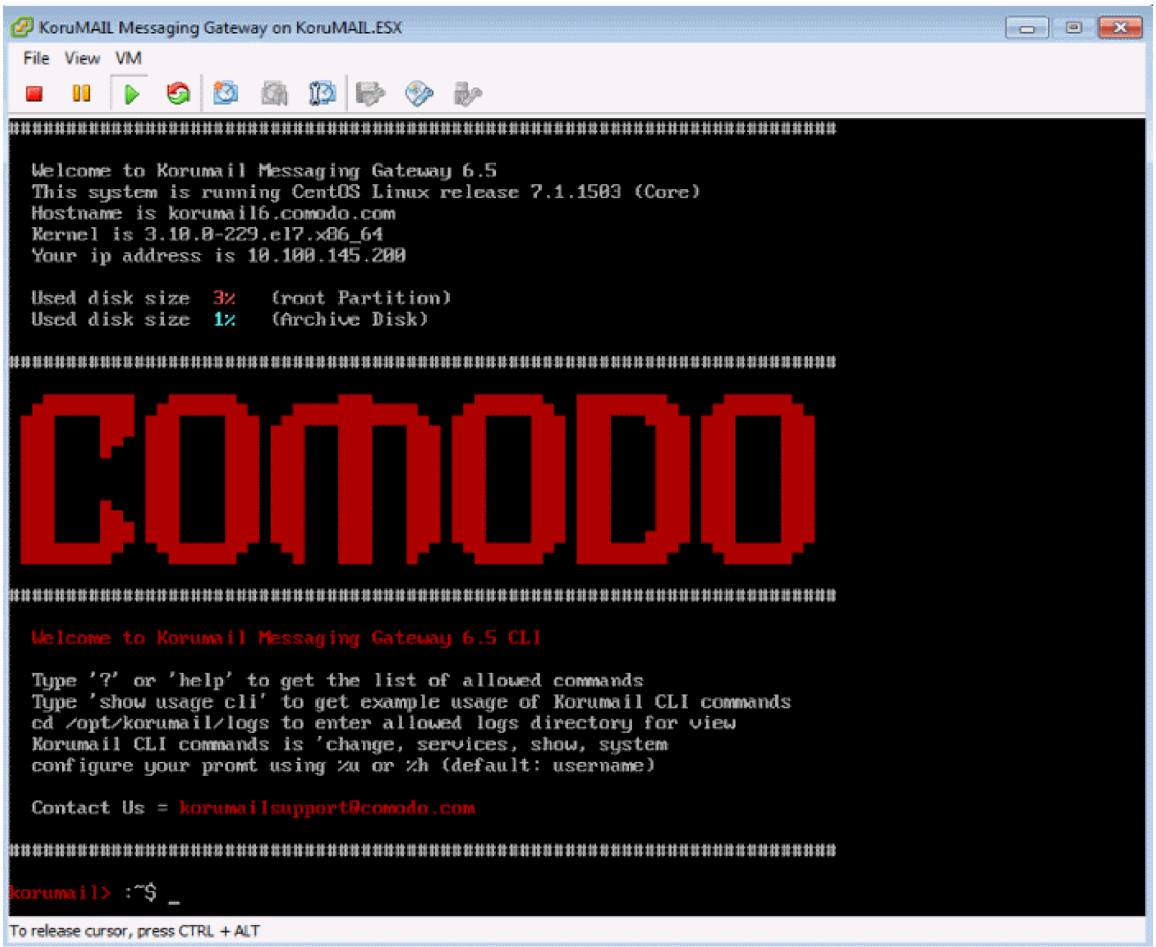
- Wait for the server to boot-up.



```
#########################################################################

  Welcome to Korumail Messaging Gateway 6.5
  This system is running CentOS Linux release 7.1.1503 (Core)
  Hostname is korumail6.comodo.com
  Kernel is 3.10.0-229.el7.x86_64
  Your ip address is 10.100.145.200

  Used disk size  3%   (root Partition)
  Used disk size  1%   (Archive Disk)

#########################################################################
korumail6 login:
```

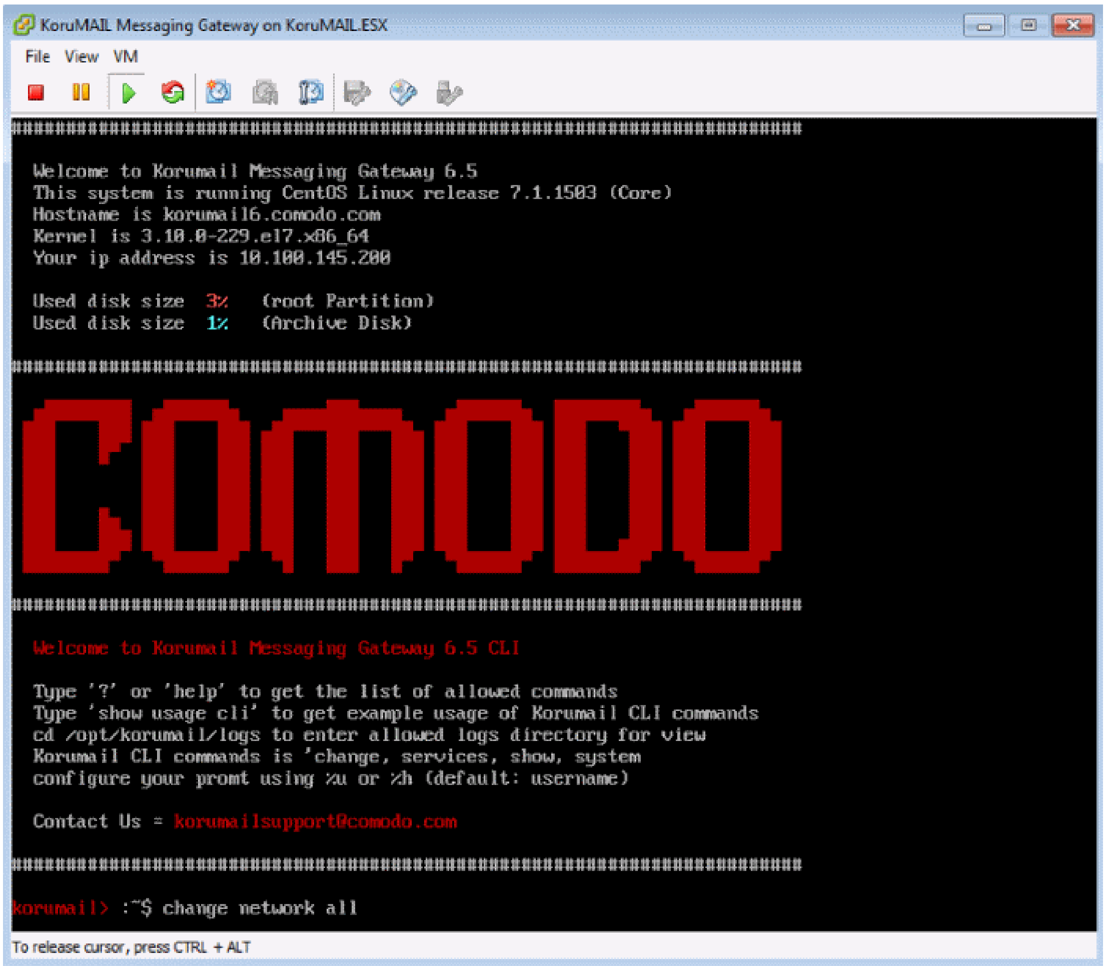
We next need to enter a new hostname, ip, netmask, gateway and DNS information. The following steps explain this process:

1. Login with the default username and password (admin/admin).


KoruMAIL Messaging Gateway on KoruMAIL.ESX
File View VM
To release cursor, press CTRL + ALT

```
################################################################################

  Welcome to Korumail Messaging Gateway 6.5
  This system is running CentOS Linux release 7.1.1503 (Core)
  Hostname is korumail6.comodo.com
  Kernel is 3.10.0-229.el7.x86_64
  Your ip address is 10.100.145.200

  Used disk size  3%   (root Partition)
  Used disk size  1%   (Archive Disk)

################################################################################

 COMODO

################################################################################

  Welcome to Korumail Messaging Gateway 6.5 CLI

  Type '?' or 'help' to get the list of allowed commands
  Type 'show usage cli' to get example usage of Korumail CLI commands
  cd /opt/korumail/logs to enter allowed logs directory for view
  Korumail CLI commands is 'change, services, show, system
  configure your promt using %u or %h (default: username)

  Contact Us = korumailsupport@comodo.com

################################################################################

korumail> :~$ _
```

2. Enter the command '**change network all**' and press 'Enter'.


KoruMAIL Messaging Gateway on KoruMAIL.ESX
File
View
VM
To release cursor, press CTRL + ALT

```
##########################################################################

  Welcome to Korumail Messaging Gateway 6.5
  This system is running CentOS Linux release 7.1.1503 (Core)
  Hostname is korumail6.comodo.com
  Kernel is 3.10.0-229.el7.x86_64
  Your ip address is 10.100.145.200

  Used disk size  3%   (root Partition)
  Used disk size  1%   (Archive Disk)

##########################################################################

COMODO

##########################################################################

  Welcome to Korumail Messaging Gateway 6.5 CLI

  Type '?' or 'help' to get the list of allowed commands
  Type 'show usage cli' to get example usage of Korumail CLI commands
  cd /opt/korumail/logs to enter allowed logs directory for view
  Korumail CLI commands is 'change, services, show, system
  configure your promt using %u or %h (default: username)

  Contact Us = korumailsupport@comodo.com

##########################################################################

korumail> :~$ change network all
```

3. After entering the command, the system will ask for a new hostname, ip, netmask, gateway and DNS.

korumail> :~$ change network all

!!

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

!!

This option will change network settings

Do you want to proceed [y|n] (Default is NO) ? > Y

- Enter the hostname of the machine: korumail.your-domain.com
- Enter the IP address: 192.168.1.10
- Enter the netmask: 255.255.255.0
- Enter the default gateway: 192.168.1.1
- Enter the first nameserver: 8.8.8.8
- Enter the second nameserver: 8.8.4.4

The following changes will be made to network configuration.

- IP Address: 19.168.1.10
- Netmask   : 255.255.255.0
- Hostname : korumail.yourdomain.com
- Gateway   : 192.168.1.1
- Nameserver: 8.8.8.8 , 8.8.4.4

4. After confirming the above, type 'y' then press enter. Wait for the device to restart.

5. The device will restart. You can then configure the device with the help of the setup wizard. Login at the IP address via a web-browser -

   https: // ip-address: 8443 (user: admin pass: admin).

3 Access the System

KoruMail's default IP address is 10.0.0.123 and you can use this to access the system for initial configuration. Default username is 'admin'. For password please contact Comodo sales representative.

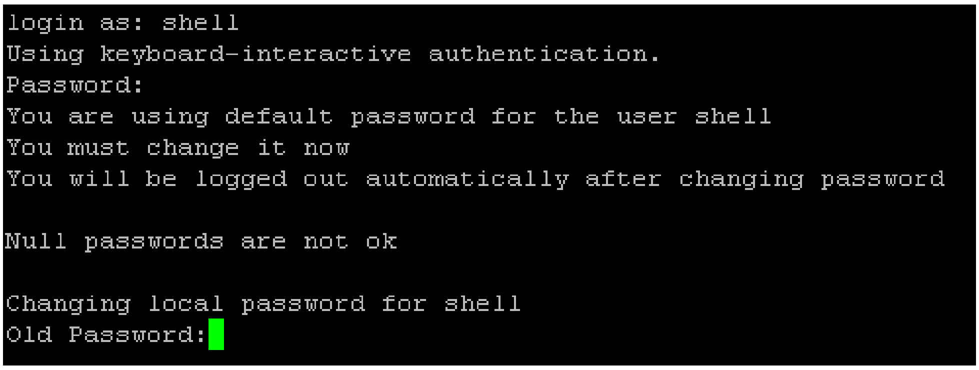
There are two ways to access the system:

1. Text menu-based CLI (Command Line Interface) console
2. Graphic-based web management console

3.1 Access via CLI Console

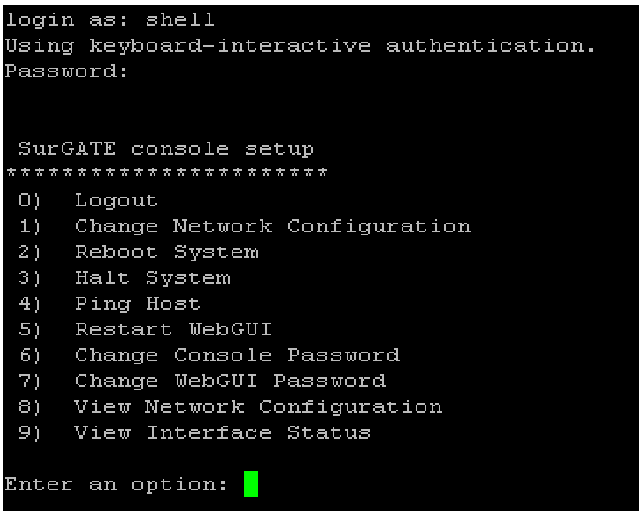
If it is not accessible from your network, then the easiest way to access the console is by using the command line interface. You can perform basic operations from this interface. The remaining network settings on the system can be done remotely via a web browser.

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:
```

After logging-in in with your new password, the following menu will be displayed.

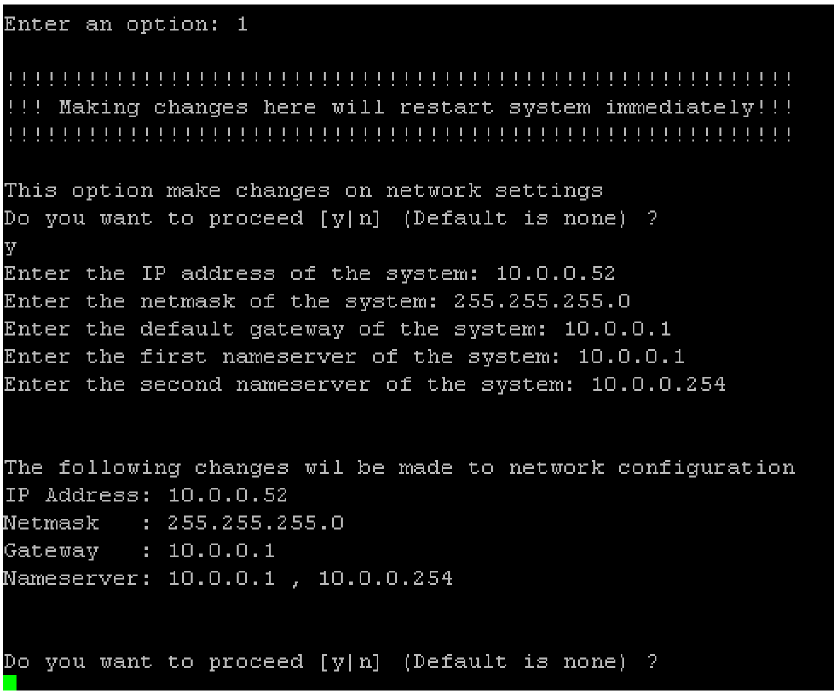


```
login as: shell
Using keyboard-interactive authentication.
Password:


 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:
```

All the functions of the system cannot be configured via the CLI and only limited important tasks can be performed in the following order:

1. Network configuration
2. Reboot
3. Halt
4. Pinging a host to check whether the network access is exist
5. Restarting the web management console
6. Changing CLI password
7. Changing the password for web management console
8. Displaying the network configuration
9. Displaying the network interface

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

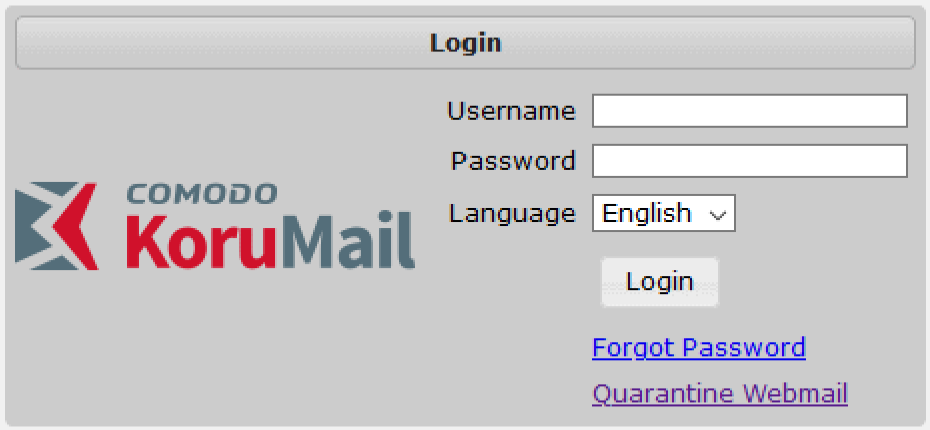


```
Enter an option: 1

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!! 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) ?
```

.

3.2 Access via Web Console

1. Enter KoruMail Gateway’s IP or hostname + port 8080 into your browser. For example: https://korumail.comodo.net:8080
2. Enter your username and password. The default user name is ‘admin’. Please contact your Comodo representative if you have not received your password.
3. Choose a language option
4. Click 'login':



Login

Username

Password

Language: English

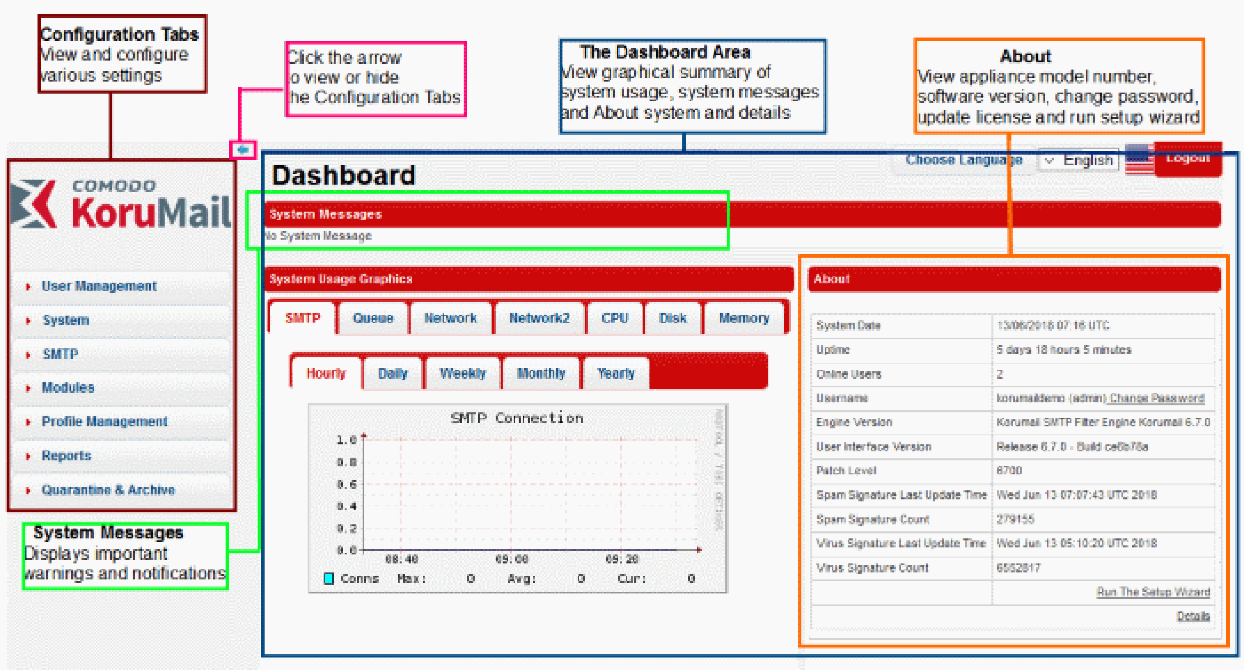
- Click the 'Forgot Password' link if you can't remember your password. Enter your email address and click the 'Send' button to receive a new password.
- The 'Quarantine Webmail' lets end-users via mails of theirs which have been quarantined. See '**Managing End Users**' for more details.

Notes:

- Username and passwords are case-sensitive.

3.2.1 The Main Interface

The admin console provides easy access to all modules, statistics and configuration screens in KoruMail Secure Email Gateway.



Configuration Tabs View and configure various settings

Click the arrow to view or hide the Configuration Tabs

The Dashboard Area View graphical summary of system usage, system messages and About system and details

About View appliance model number, software version, change password, update license and run setup wizard

System Messages Displays important warnings and notifications

Dashboard

System Messages

No System Message

About

System Date	13/06/2018 07:16 UTC
Uptime	5 days 18 hours 5 minutes
Online Users	2
Username	korumaildemo (admin) Change Password
Engine Version	Korumail SMTP Filter Engine Korumail 6.7.0
User Interface Version	Release 6.7.0 - Build ce6b78a
Patch Level	6700
Spam Signature Last Update Time	Wed Jun 13 07:07:43 UTC 2018
Spam Signature Count	279155
Virus Signature Last Update Time	Wed Jun 13 05:10:20 UTC 2018
Virus Signature Count	6552817
	Run The Setup Wizard
	Details

Configuration Tabs

The tabs on the left pane allows administrators to add new users, groups, configure various settings such as domains, SMTP, view and generate reports and more.

- **User Management:** Allows to add/edit groups and admin users with different privileges. See '**User**

Management' for more details.

- **System:** Allows administrators to configure network settings, add NTP servers, enable or disable services such as anti-spam engine, Snmpd, KoruMail delivery agent, view and update license and more. See '**System Configuration**' for more details.
- **SMTP:** Allows administrators to configure SMTP settings, add domains, add new LDAP profile, create greylist of domians, IP or network address, set outgoing limits and more. See '**SMTP Configuration**' for more details.
- **Modules:** Enable or disable anti-spam, anti-virus, anti-spoofing, anti-phishing and configure settings for anti-spam training and content filter. See **Modules** for more details.
- **Profile Management:** Configure various settings such as anti-virus, anti-spam, blacklist and more for default incoming and outgoing profile. See '**Profile Management**' for more details.
- **Reports:** View and generate log reports for incoming and outgoing mails and a summary of mails categorized as spam, RBL, phishing and more. See '**Reports**' for more details.
- **Quarantine & Archive:** Configure quarantine and mail storage settings. View quarantine logs and archived mails. See '**Quarantine & Archive**' for more details.

Dashboard

After logging-in to the console, the first screen displayed is the '**Dashboard**'. It provides an at-a-glance view of system usage such as SMTP, Queue mails, network utilization rate, CPU and memory utilization.

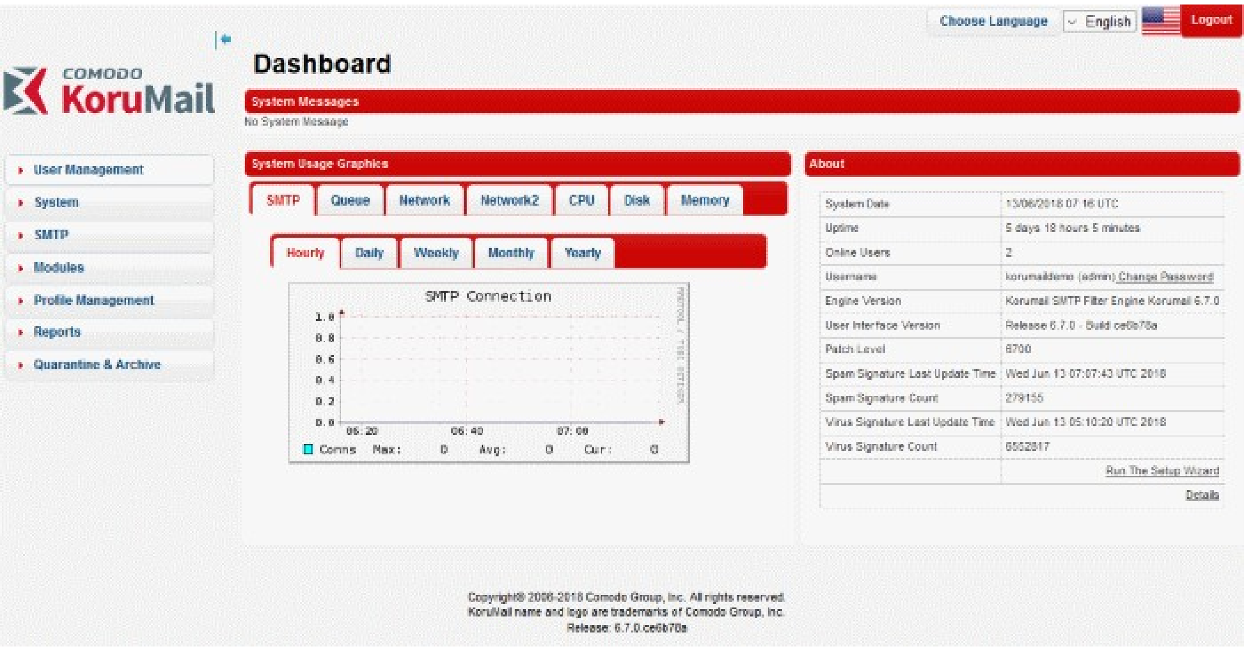
- **System Messages:** Displays error messages or important notifications that might affect the performance of the secure email gateway.
- **System Usage Graphics:** Charts showing resources used by Korumail. For example, SMTP connection rates, and utilization of CPU, disk and memory. See '**System Usage Graphics**' for more details.
- **About:** Change the current password, view filter engine and software details, and manage your license. See '**About Software**' and '**Changing your Password**' for more details.
- **Run the Setup Wizard:** Enables administrators to quickly configure the Korumail appliance.

You can change the theme from the settings interface. **Click here** to know how.

4 The Dashboard

The dashboard is an at-a-glance summary of your Korumail environment and provides access to all major functional areas of the application.

The dashboard is shown by default whenever you login to the admin interface. You can return to the dashboard at any time by clicking the 'KoruMail Secure Email Gateway' logo at the top left.



Dashboard

System Messages

No System Message

System Usage Graphics

About

System Date	13/06/2018 07 16 UTC
Uptime	5 days 18 hours 5 minutes
Online Users	2
Username	korumaildemo (admin) Change Password
Engine Version	Korumail SMTP Filter Engine Korumail 6.7.0
User Interface Version	Release 6.7.0 - Build ce6b78a
Patch Level	6700
Spam Signature Last Update Time	Wed Jun 13 07:07:43 UTC 2018
Spam Signature Count	279155
Virus Signature Last Update Time	Wed Jun 13 05:10:20 UTC 2018
Virus Signature Count	6552817
	Run The Setup Wizard
	Details

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 'System Messages' displays error messages or important notifications that might affect the performance of the secure email gateway.

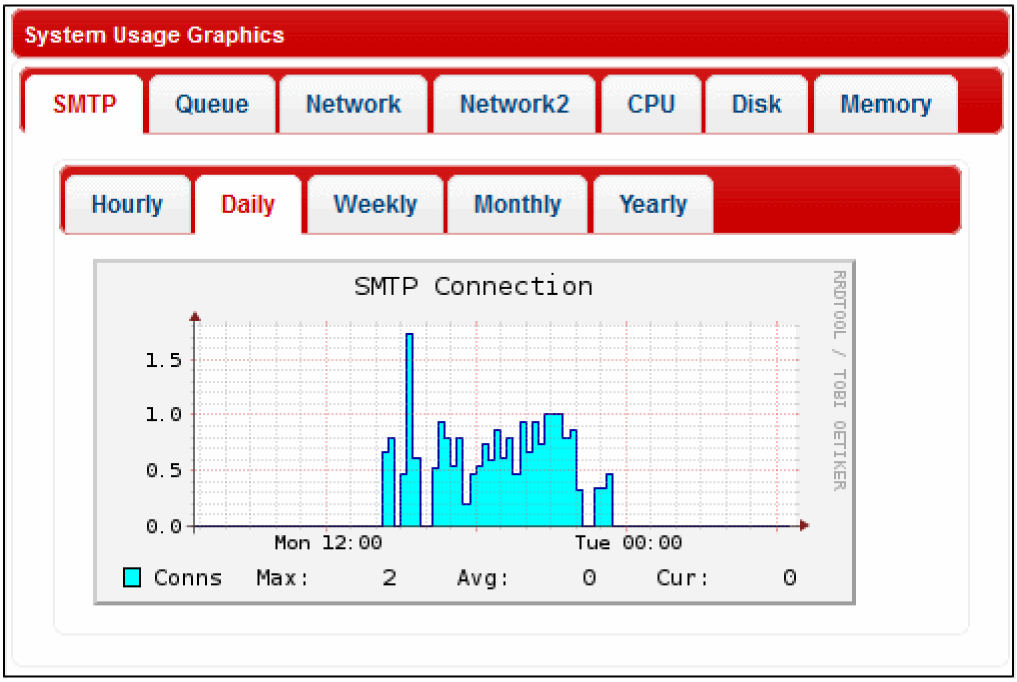
You can change the theme from the settings interface. **Click here** to know how.

Click the following links for more details about other areas in the dashboard:

- **System Usage Graphics**
- **About Software**
- **Change your Password**

4.1 System Usage Graphics

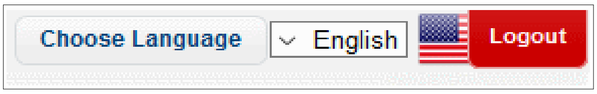
The 'System Usage Graphics' area shows SMTP connections, the number of queued mails, and the network/CPU/disk/memory utilization rate.



- **SMTP:** The maximum, average and current SMTP connections to KoruMail for the selected period.
- **Queue:** The maximum, average and current emails in queue for the selected period.
- **Network:** The network utilization rate of the system for the selected period.
- **CPU:** The maximum, average and current CPU utilization rate for the selected period.
- **Disk:** The system's disk usage ratio for the selected period.
- **Memory:** The system's memory utilization rate for thes selected period.

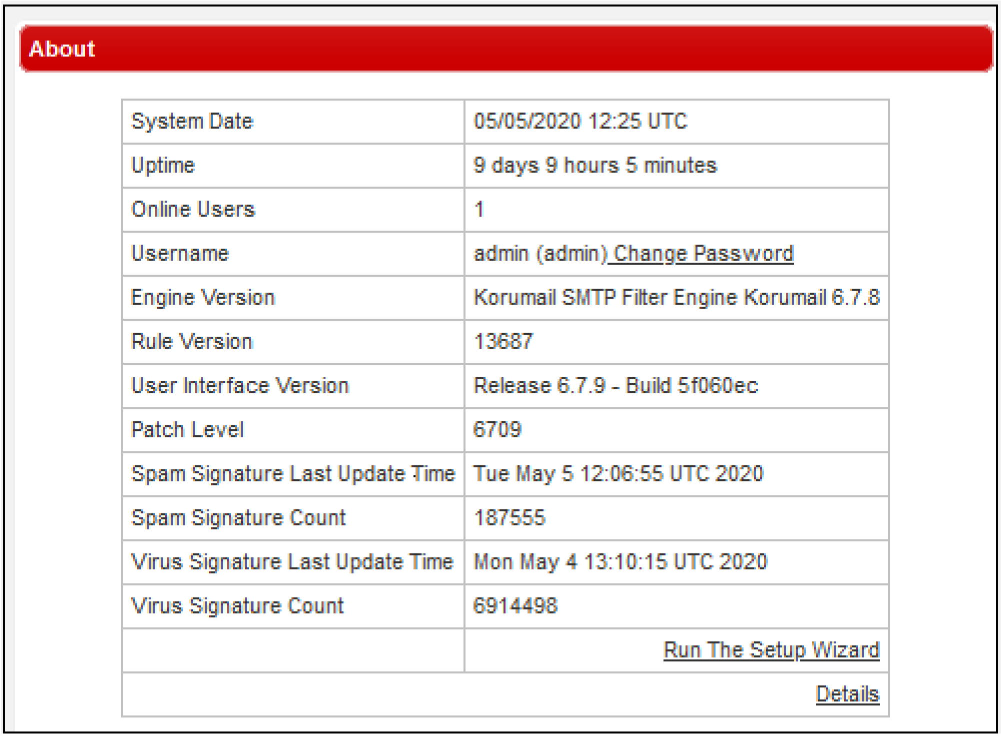
See **System Usage Statistics** for more details about each item.

You can choose your choice of language to view the 'Korumail' interface:



4.2 About Software

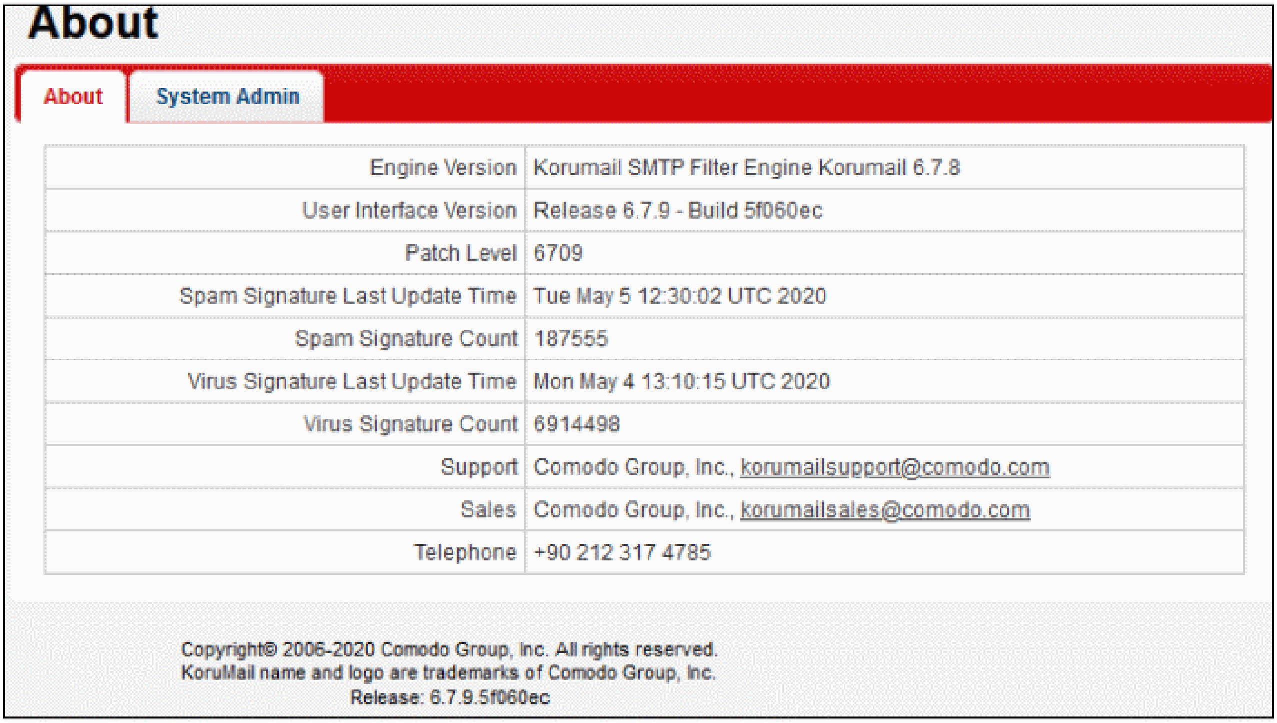
The 'About' area lists general details about hardware, software and virus update status. It also allows you to change the web console access password and run the setup wizard.



About

System Date	05/05/2020 12:25 UTC
Uptime	9 days 9 hours 5 minutes
Online Users	1
Username	admin (admin) Change Password
Engine Version	Korumail SMTP Filter Engine Korumail 6.7.8
Rule Version	13687
User Interface Version	Release 6.7.9 - Build 5f060ec
Patch Level	6709
Spam Signature Last Update Time	Tue May 5 12:06:55 UTC 2020
Spam Signature Count	187555
Virus Signature Last Update Time	Mon May 4 13:10:15 UTC 2020
Virus Signature Count	6914498
	Run The Setup Wizard
	Details

- Click 'Change Password' in the 'Username' row to update the password
- Click the 'Details' link at the bottom-right to open the advanced 'About' screen

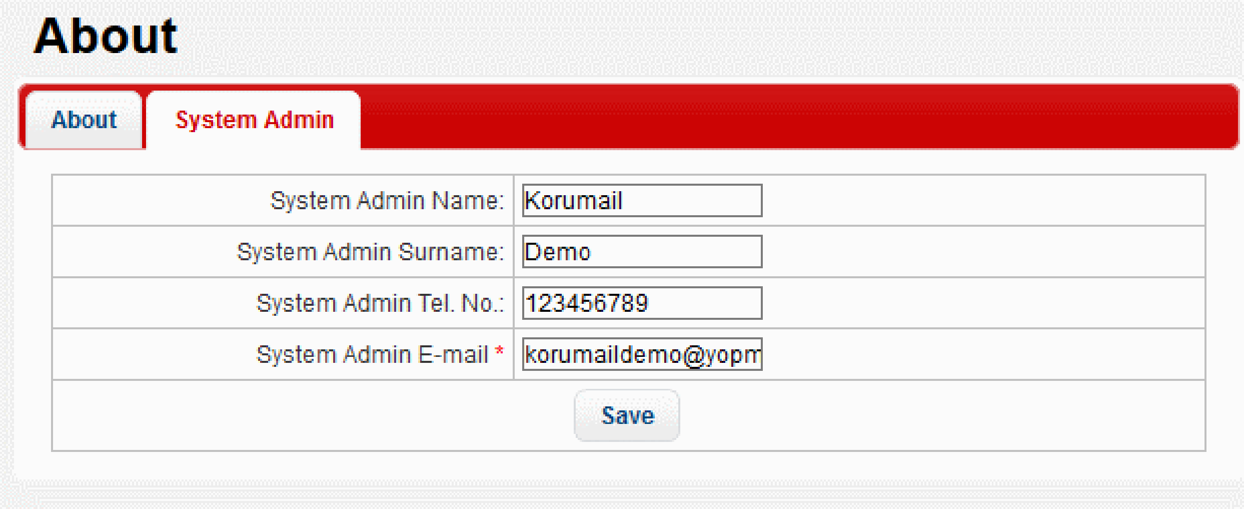


About

Engine Version	Korumail SMTP Filter Engine Korumail 6.7.8
User Interface Version	Release 6.7.9 - Build 5f060ec
Patch Level	6709
Spam Signature Last Update Time	Tue May 5 12:30:02 UTC 2020
Spam Signature Count	187555
Virus Signature Last Update Time	Mon May 4 13:10:15 UTC 2020
Virus Signature Count	6914498
Support	Comodo Group, Inc., korumailsupport@comodo.com
Sales	Comodo Group, Inc., korumailsales@comodo.com
Telephone	+90 212 317 4785

Copyright© 2006-2020 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 6.7.9.5f060ec

- Click the 'System Admin' tab to view or update administrator details:



About

About | System Admin

System Admin Name:	Korumail
System Admin Surname:	Demo
System Admin Tel. No.:	123456789
System Admin E-mail *	korumaildemo@yopm

- Click 'Save' to apply your changes.

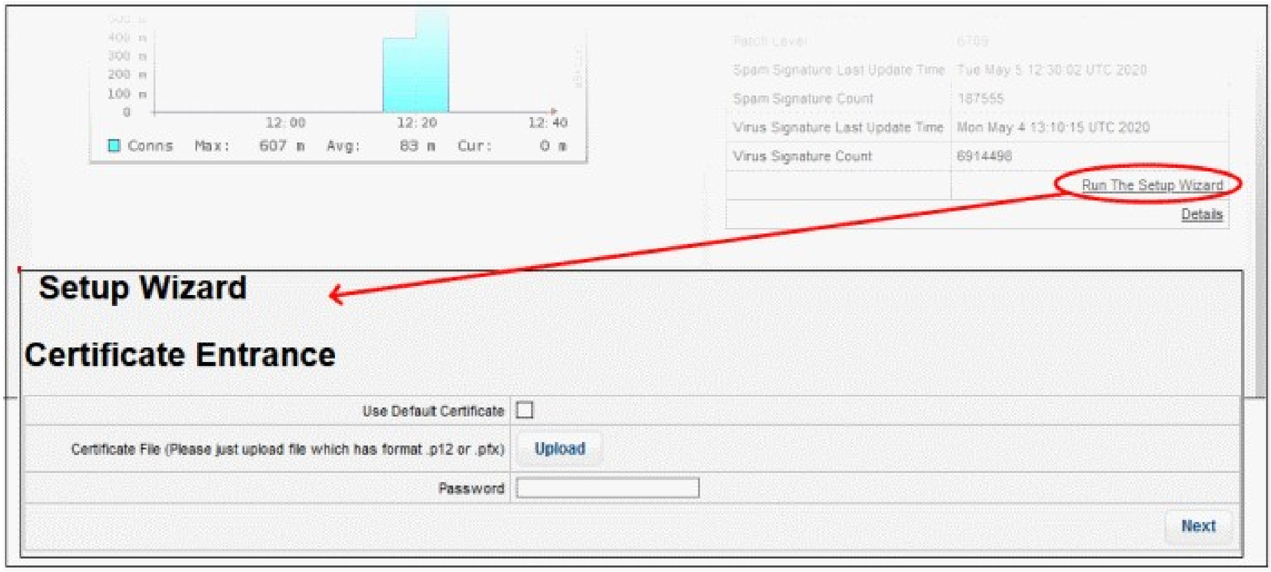
Note. When the SMTP IPS module blocks IP addresses, the details of the blocked IPs are sent to the e-mail address shown in this interface.

If 'System Admin E-mail' is left blank then an error message is shown in 'System Messages' in the 'Dashboard'.

Run the Setup Wizard

Allows you to quickly configure protection on a mail server.

- Click the 'Run the setup wizard' link at bottom-right of the 'About' screen
- Admins can configure 'Certificate Entrance', 'System Admin' details, 'Network Settings', 'Timezone', 'LDAP' profiles, 'Managed Domains', 'Routes' and 'Relay' details.



Patch Level	6709
Spam Signature Last Update Time	Tue May 5 12:30:02 UTC 2020
Spam Signature Count	187555
Virus Signature Last Update Time	Mon May 4 13:10:15 UTC 2020
Virus Signature Count	6914498

Setup Wizard

Certificate Entrance

Use Default Certificate	□
Certificate File (Please just upload file which has format .p12 or .pfx)	Upload
Password	

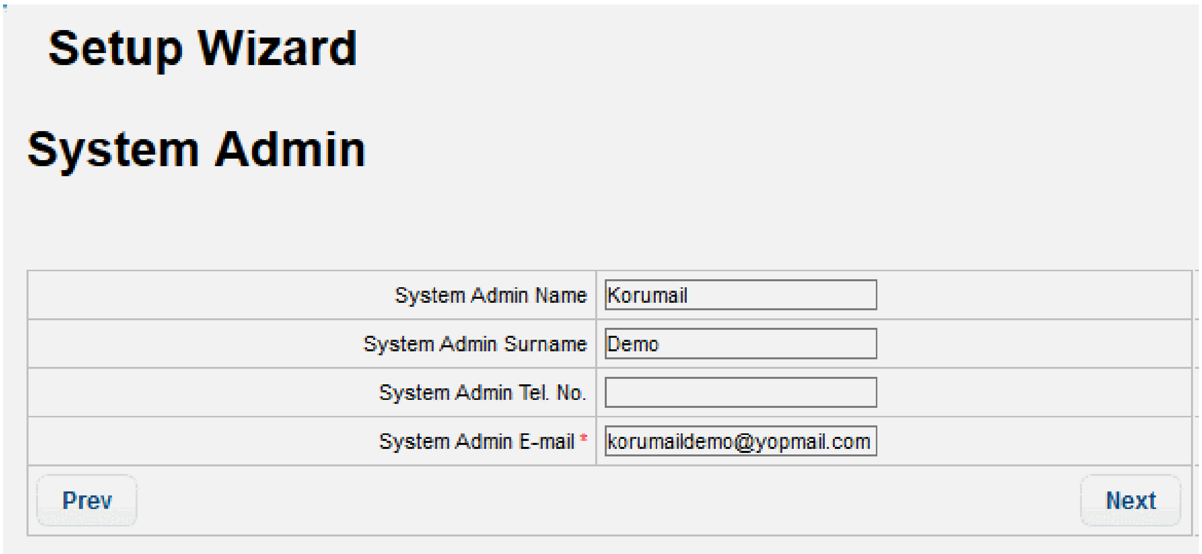
An SSL certificate is required to provide secure, HTTPS access to your Korumail admin console. The 'Certificate Entrance' screen lets you choose which type of SSL certificate you wish to use. You have two options:

- Upload a certificate you have on file. Ideally, this will be a certificate which you have obtained from a trusted certificate authority. Using such a certificate means you will not see browser error messages when you access the admin console.
- Use the default, self-signed certificate. Korumail will automatically install a self-signed certificate on your console. Your connection to the console will be just as secure as above, but your browser will show error messages as the certificate is not signed by a trusted certificate authority. You can bypass these errors

and create an exception in your browser to avoid these messages in future.

See '**System General Settings**' for more details on user preferences.

- Click 'Next' to complete 'System Admin Name', 'System Admin Surname', 'System Admin Tel. No' and 'System Admin E-mail'.

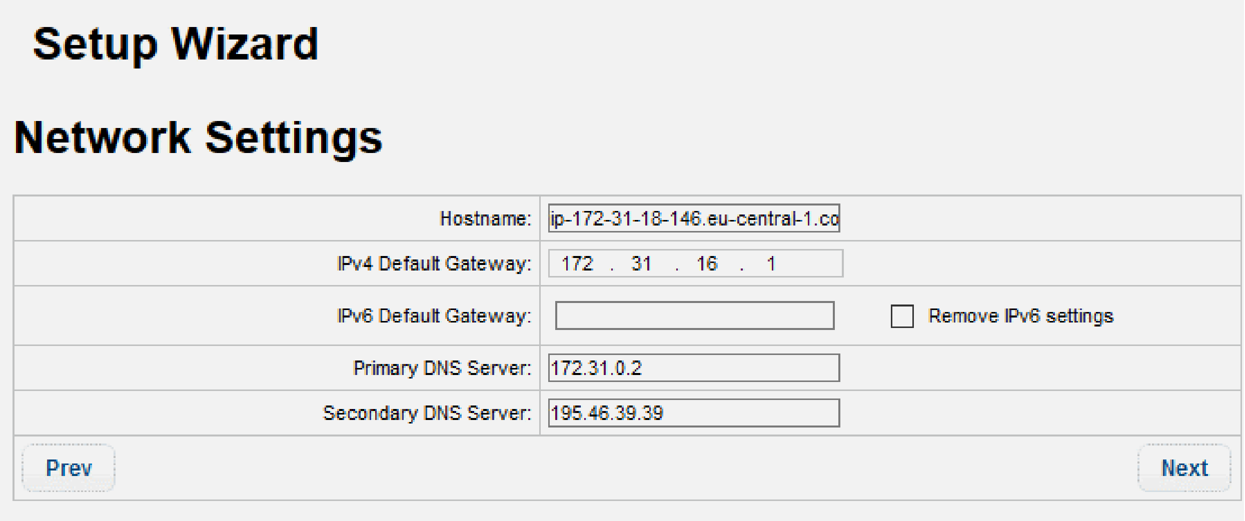


Setup Wizard

System Admin

System Admin Name	Korumail
System Admin Surname	Demo
System Admin Tel. No.	
System Admin E-mail *	korumaildemo@yopmail.com

- Click 'Next', to enter network details.



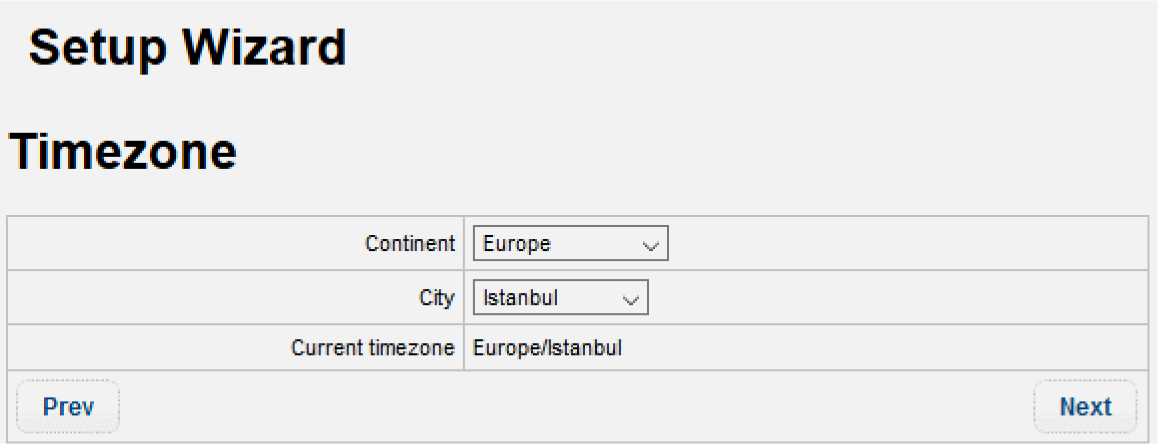
Setup Wizard

Network Settings

Hostname:	ip-172-31-18-146.eu-central-1.co	
IPv4 Default Gateway:	172 . 31 . 16 . 1	
IPv6 Default Gateway:		□ Remove IPv6 settings
Primary DNS Server:	172.31.0.2	
Secondary DNS Server:	195.46.39.39	

See '**Network Settings**' for more details on this section.

- Click 'Next', to enter details of 'Timezone'.



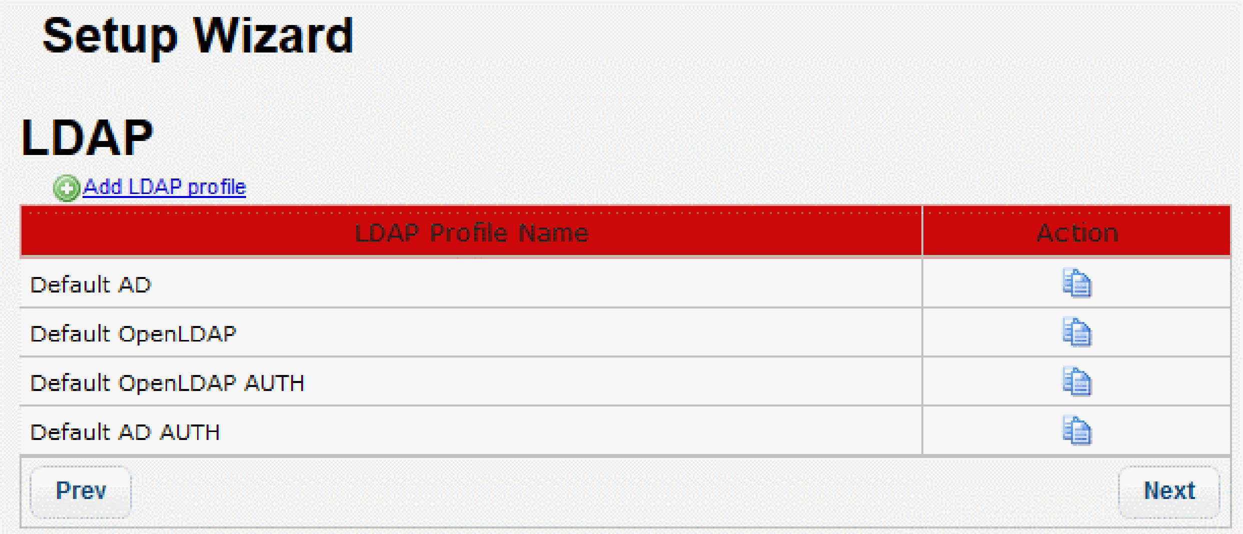
Setup Wizard

Timezone

Continent	Europe
City	Istanbul
Current timezone	Europe/Istanbul

See '**Timezone**' for more details.

- Click 'Next', to enter 'LDAP' information:

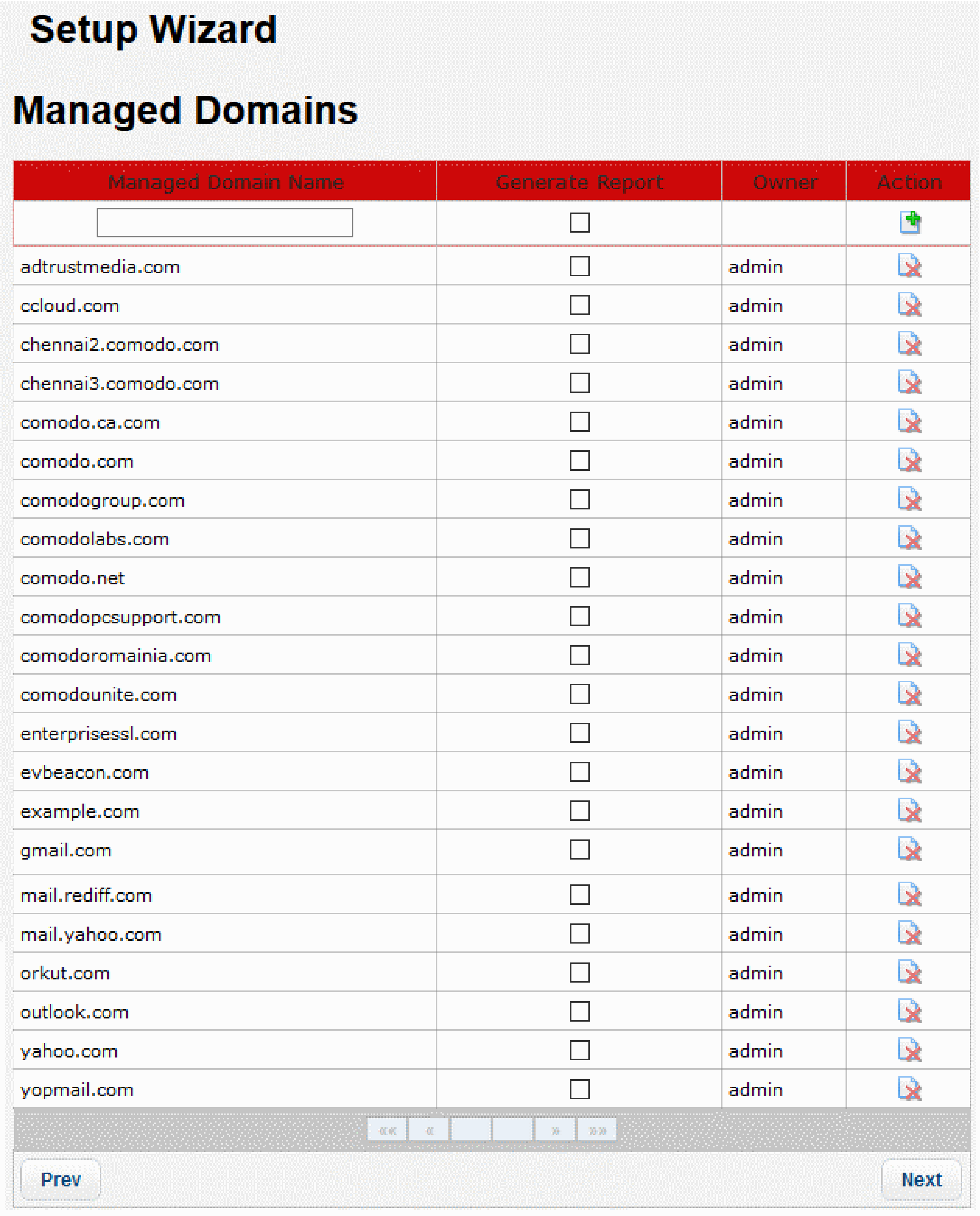


LDAP

LDAP Profile Name	Action
Default AD	
Default OpenLDAP	
Default OpenLDAP AUTH	
Default AD AUTH	

See '**LDAP**' for more details.

- Click 'Next', to enter details of 'Managed Domains'.



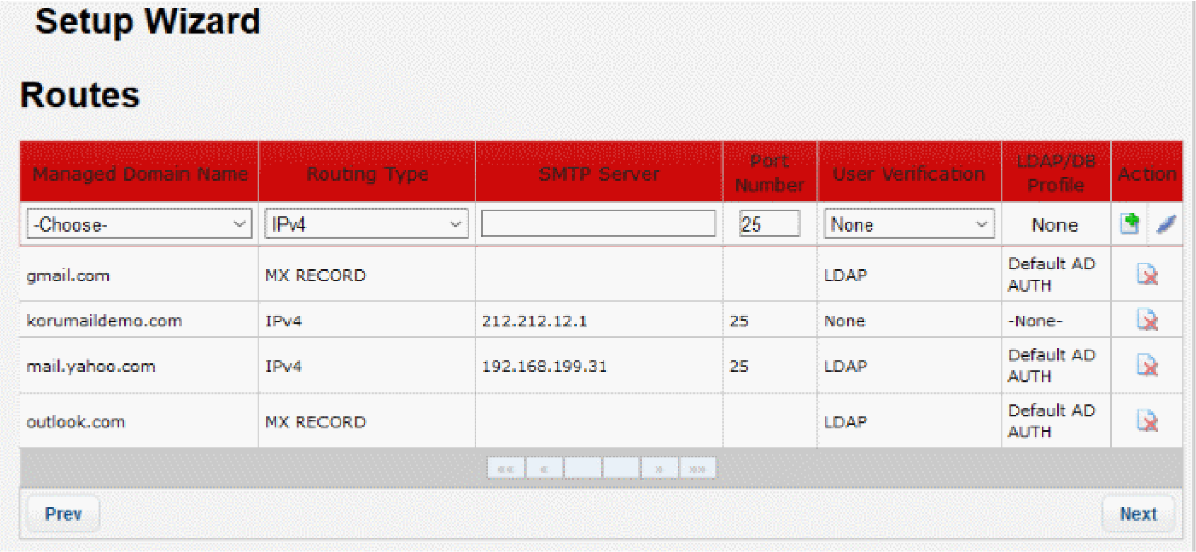
Setup Wizard

Managed Domains

Managed Domain Name	Generate Report	Owner	Action
	□		
adtrustmedia.com	□	admin	
ccloud.com	□	admin	
chennai2.comodo.com	□	admin	
chennai3.comodo.com	□	admin	
comodo.ca.com	□	admin	
comodo.com	□	admin	
comodogroup.com	□	admin	
comodolabs.com	□	admin	
comodo.net	□	admin	
comodopcsupport.com	□	admin	
comodoromainia.com	□	admin	
comodounite.com	□	admin	
enterprisessl.com	□	admin	
evbeacon.com	□	admin	
example.com	□	admin	
gmail.com	□	admin	
mail.rediff.com	□	admin	
mail.yahoo.com	□	admin	
orkut.com	□	admin	
outlook.com	□	admin	
yahoo.com	□	admin	
yopmail.com	□	admin	

See '**Manage Domains**' for more details.

- Click 'Next', to enter details of 'Routes'.



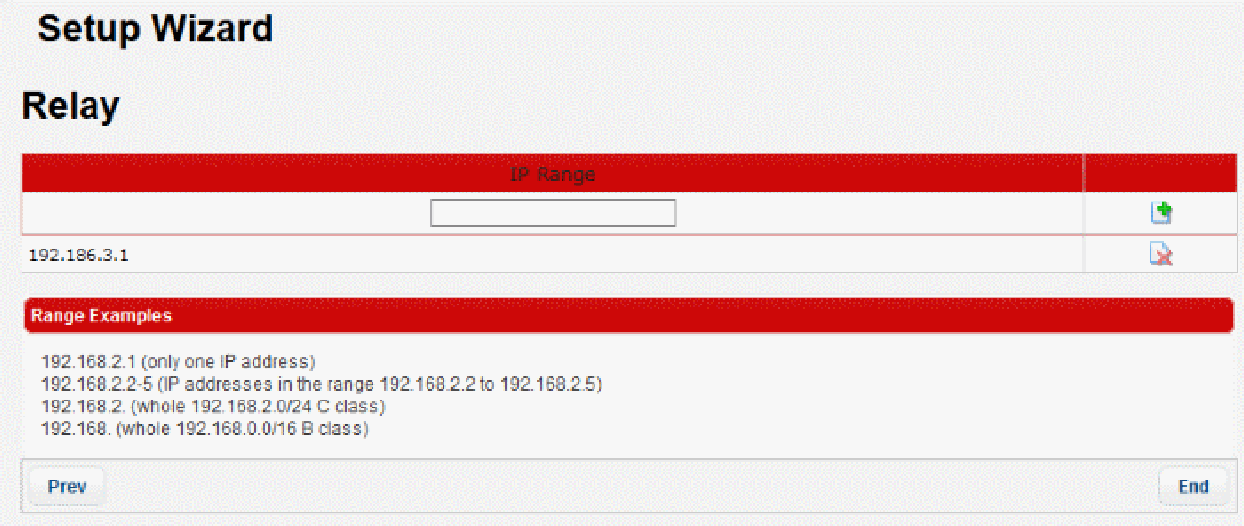
Setup Wizard

Routes

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	

See '**Routes**' for more details.

- Click 'Next', to enter details of 'Relay'.



Setup Wizard

Relay

IP Range	
192.186.3.1	

Range Examples

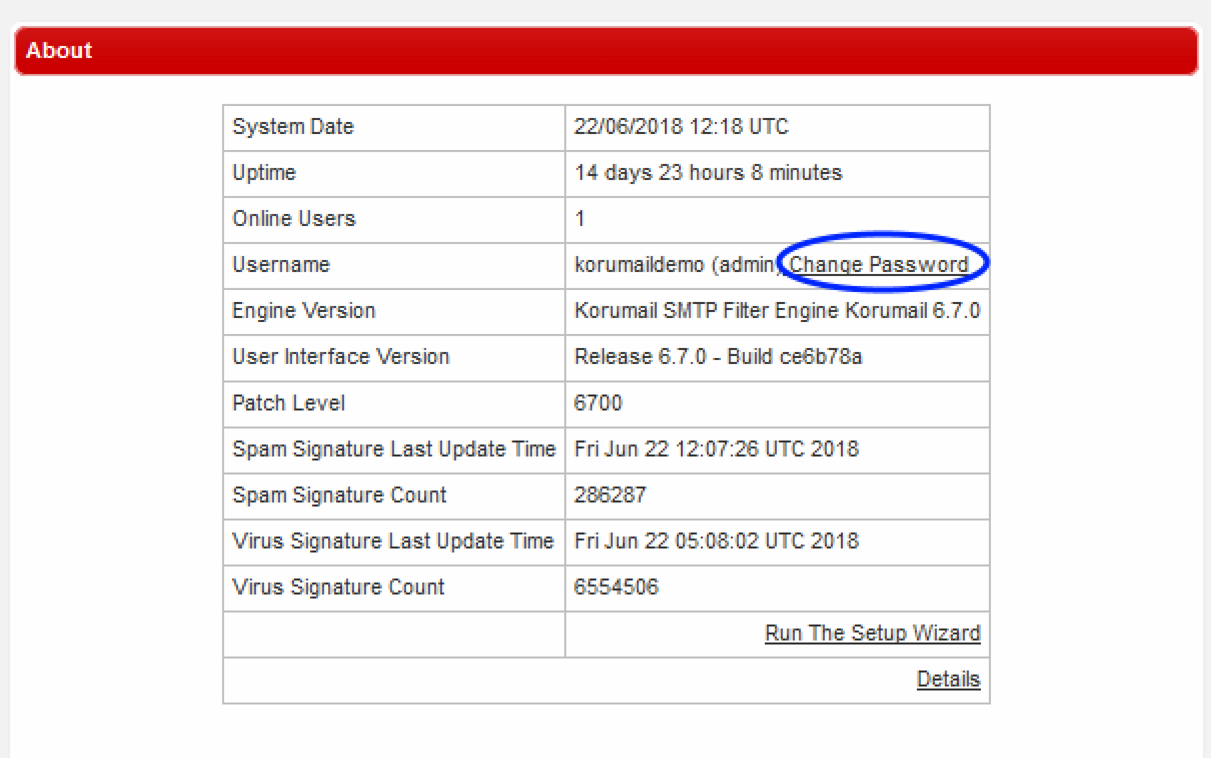
192.168.2.1 (only one IP address)
192.168.2.2-5 (IP addresses in the range 192.168.2.2 to 192.168.2.5)
192.168.2. (whole 192.168.2.0/24 C class)
192.168. (whole 192.168.0.0/16 B class)

See '**Relay**' for more details.

4.3 Change your Password

You can change your current password at anytime in the 'About' area.

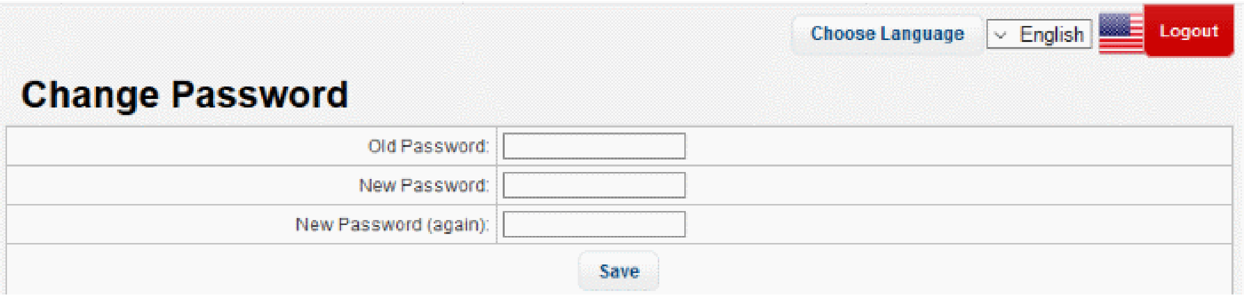
- Open the Korumail dashboard
- Go to the 'About' section > 'Username' row
- Click the 'Change Password' link



About

System Date	22/06/2018 12:18 UTC
Uptime	14 days 23 hours 8 minutes
Online Users	1
Username	korumaildemo (admin) Change Password
Engine Version	Korumail SMTP Filter Engine Korumail 6.7.0
User Interface Version	Release 6.7.0 - Build ce6b78a
Patch Level	6700
Spam Signature Last Update Time	Fri Jun 22 12:07:26 UTC 2018
Spam Signature Count	286287
Virus Signature Last Update Time	Fri Jun 22 05:08:02 UTC 2018
Virus Signature Count	6554506
	Run The Setup Wizard
Details	

Enter your current password then the new one. Confirm your new password in the last field.



Change Password

Old Password:	
New Password:	
New Password (again):	

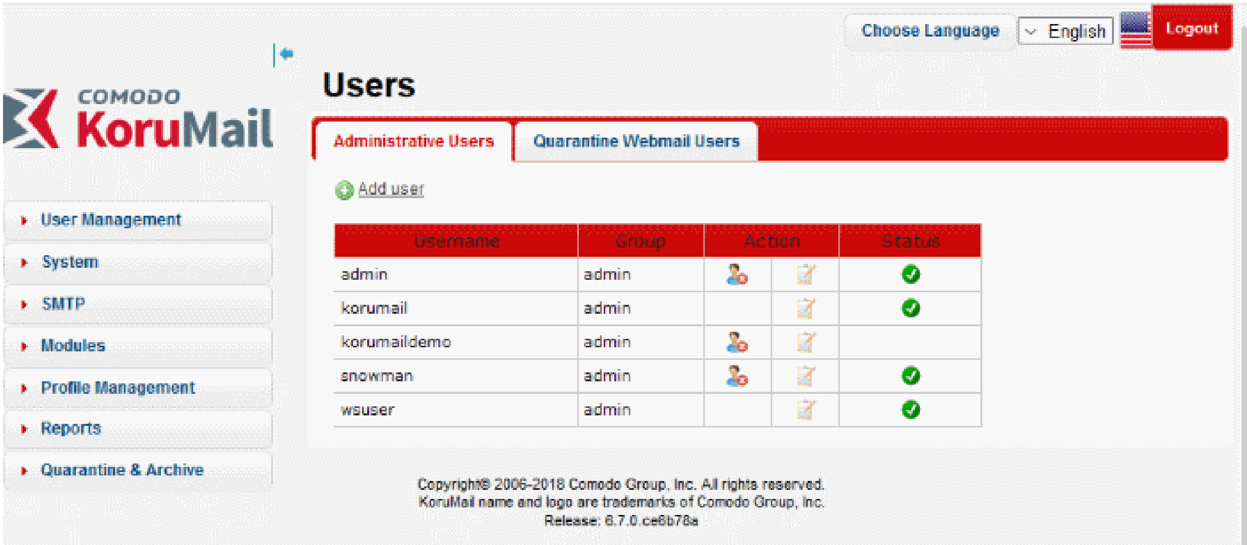
- Click 'Save'

You can now use your new password to access KoruMail.

5 User Management

The 'User Management' area allows you to create new admins and configure their privileges.

The 'Quarantine Webmail User' tab lets you add end-users so they can login and view their quarantined mails. The interface also allows the creation of user 'Groups' with different access levels.



Username	Group	Action		Status
admin	admin			✓
korumail	admin			✓
korumaildemo	admin			
snowman	admin			✓
wsuser	admin			✓

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 following links for more details:

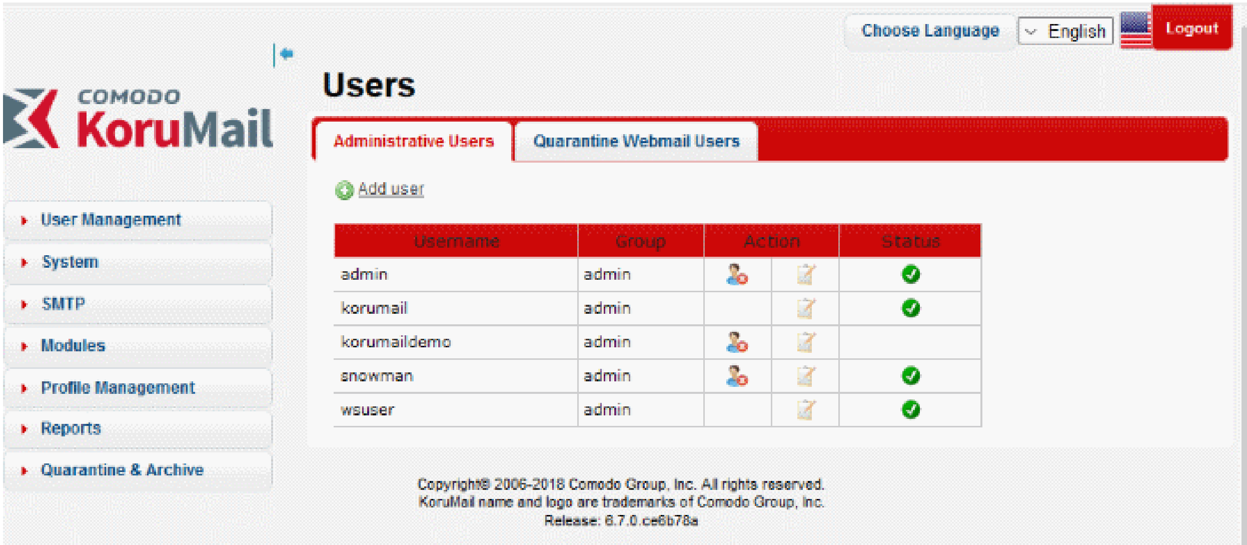
- Manage Admins and End Users
- Manage Groups

5.1 Manage Admins and End Users

- The KoruMail web console can be accessed by admins according to their designated privileges.
- The 'User Management' area lets you add end users so that they can access the console and view their quarantined emails.
- A new administrator must have a group assigned to them, so make sure an appropriate group already exists. See '**Manage Groups**' for more details.

To open the 'Users' screen,

- Click the 'User Management' tab on the left menu and click 'Users'.



Username	Group	Action		Status
admin	admin			✓
korumail	admin			✓
korumaildemo	admin			
snowman	admin			✓
wsuser	admin			✓

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

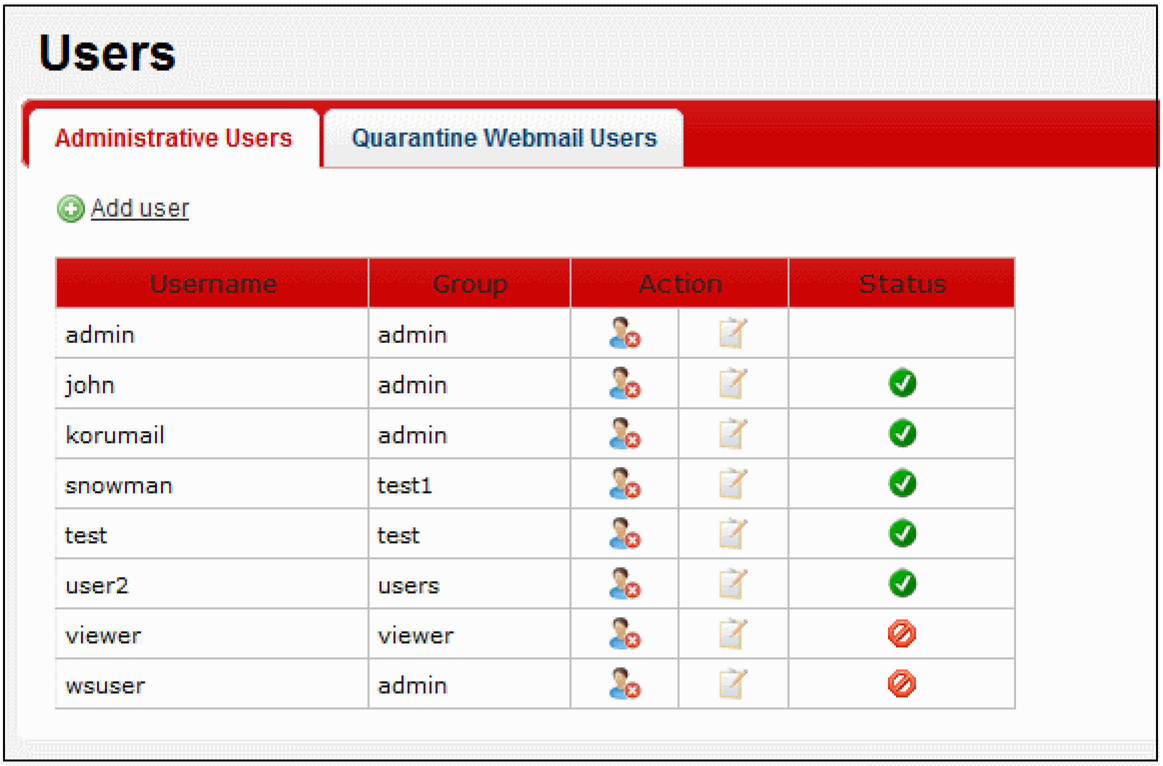
Click the following links for more details:

- Manage Admin Users
- Manage End Users

5.1.1 Manage Admins

To open this area:

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



Users

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

Administrative Users - Table of Column Descriptions

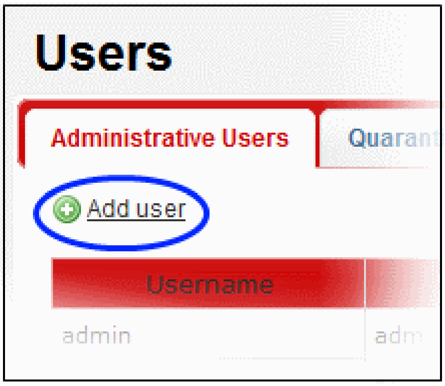
Column Header	Description	
Username	The admin name.	
Group	The name of the group to which the administrator belongs. See '**Manage Groups**' for more details.	
Action		Delete the admin. Administrators with appropriate privileges can delete other admins by clicking this icon. Please note, admins that are currently logged in cannot delete themselves.
		Administrators with appropriate privileges can edit other admins' details. See '**Edit an Administrator**' for more details.
Status	Indicates whether the admin is in enabled or disabled status. Disabled admins cannot log into the web console. See '**Enable/Disable Administrators**' for more details.	

From the this interface an appropriately privileged administrator can:

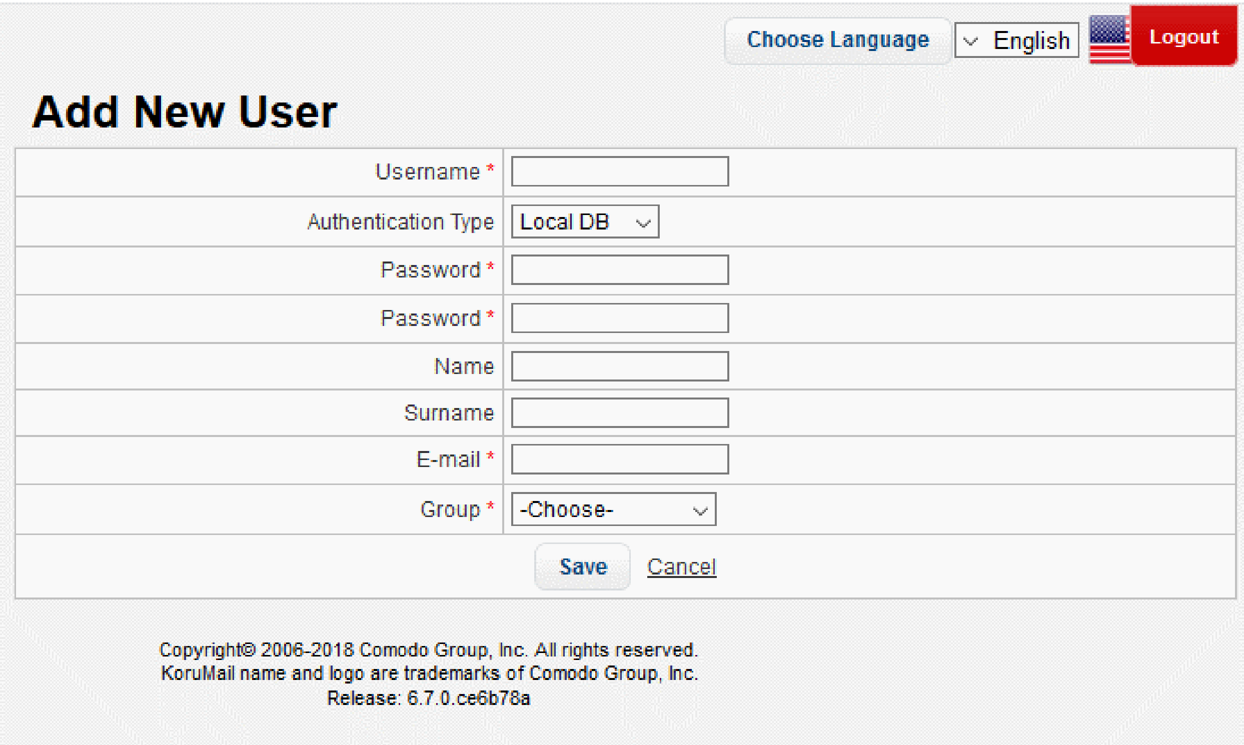
- **Add an administrative user**
- **Delete an administrative user**
- **Edit an administrative user**
- **Enable/Disable an administrative user**

To add an administrative user

- Click the 'Add User' link



The 'Add New User' screen will be displayed.



Add New User

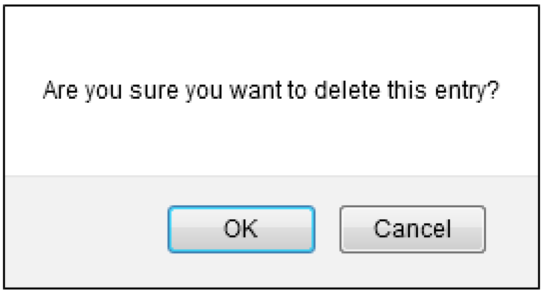
Username *	
Authentication Type	Local DB
Password *	
Password *	
Name	
Surname	
E-mail *	
Group *	-Choose-

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

- **Username:** Enter the username to access 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:** Enter the password to access the console and confirm it in the next field.
- **Name:** The first name of the administrative user
- **Surname:** The surname of the user
- **E-mail:** Enter the email address of the administrative user
- **Group:** Select the group to which the admin user should be added. See '**Manage Groups**' for more details.
- Click 'Save' to add the new admin user.

To delete an administrative user

- Click the icon beside the user that you want to delete



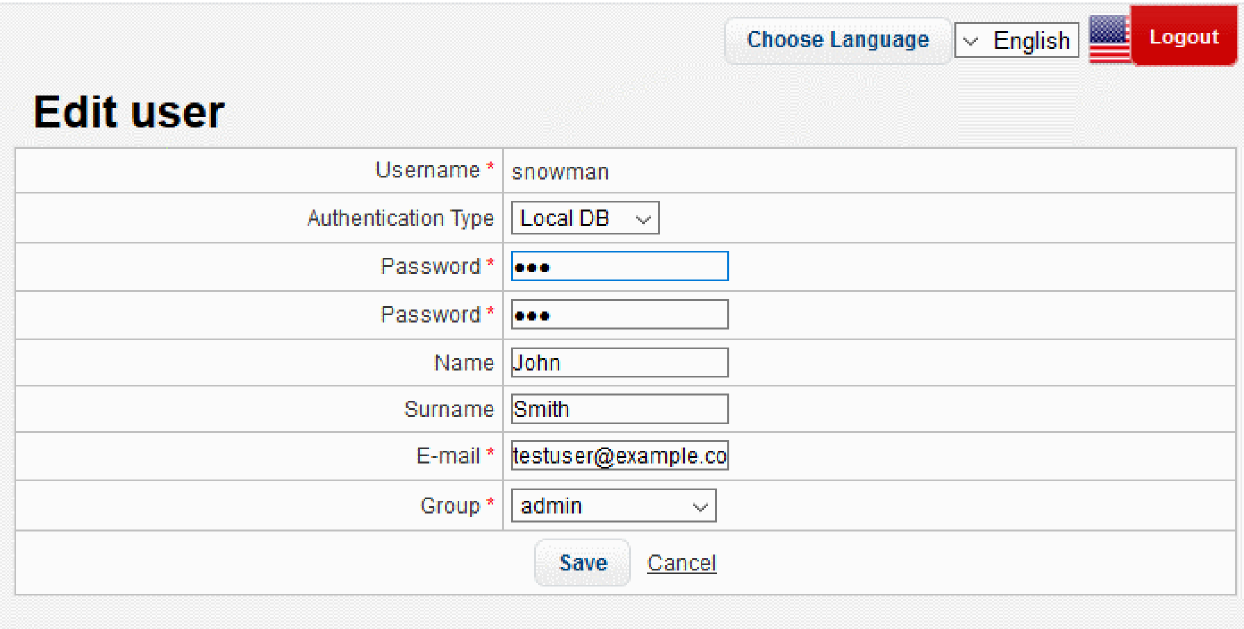
Are you sure you want to delete this entry?

- Click 'OK' to confirm the deletion.

To edit an administrative user

- Click the 📝 icon beside the user that you want to edit

The 'Edit User' screen will be displayed:



Edit user

Username *	snowman
Authentication Type	Local DB
Password *	●●●
Password *	●●●
Name	John
Surname	Smith
E-mail *	testuser@example.co
Group *	admin

- Edit the details as required. The screen is similar to the 'Add New User' section. See '**Add an administrative user**' for more details.
- Click 'Save'.

The changes will be saved and a confirmation note will be displayed.

To enable/disable an administrative user

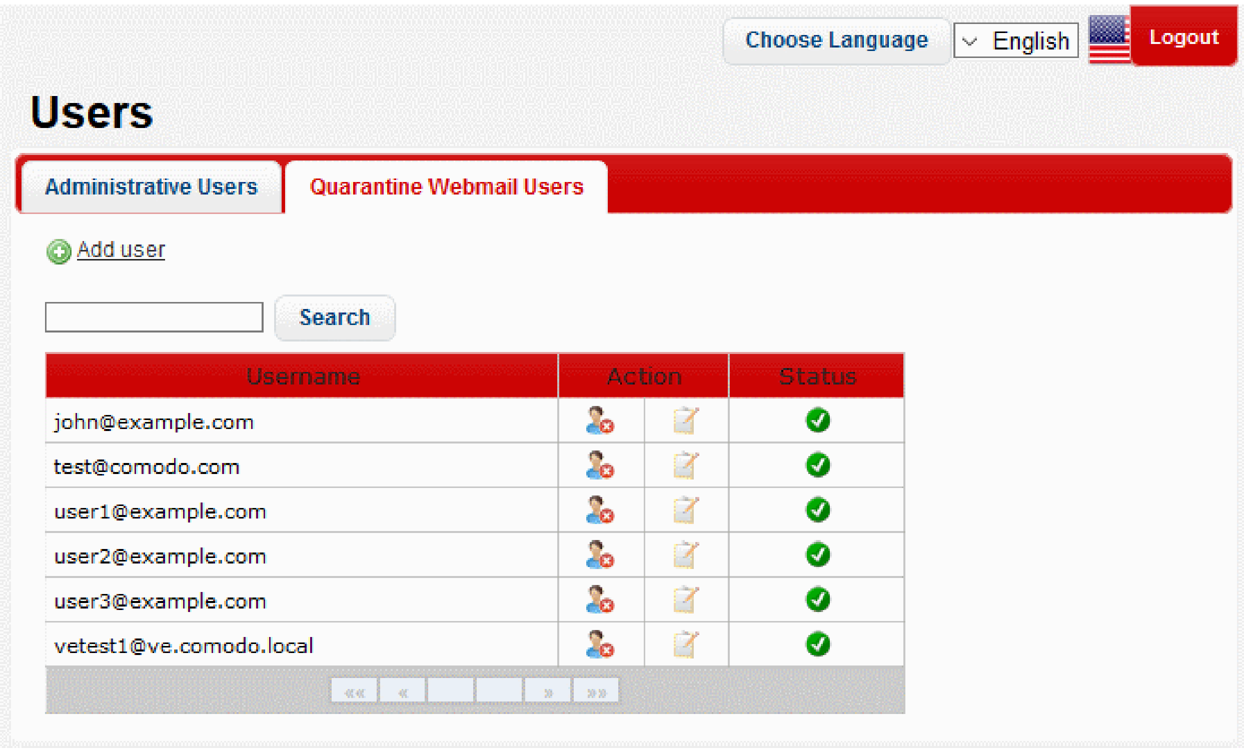
The icon under the 'Status' column indicates whether the 'Administrator User' is enabled or disabled.

⊘	Indicates the user is disabled and cannot login to the web console
✓	Indicates the user is enabled and can access the web console

- Click the icon to toggle between enabled and disabled statuses.
- Click 'OK' in the confirmation dialog.

5.1.2 Manage End Users

- 'Users' are email recipients protected by Korumail who are allowed login to the console to view their quarantined messages.
- The 'Quarantine Webmail Users' tab allows admins to manage these end users.
- To open this screen:
  - Click 'User Management' > 'Users' on the left-menu
  - Click the 'Quarantine Webmail Users' tab:



Username	Action		Status
john@example.com	✖	✎	✓
test@comodo.com	✖	✎	✓
user1@example.com	✖	✎	✓
user2@example.com	✖	✎	✓
user3@example.com	✖	✎	✓
vetest1@ve.comodo.local	✖	✎	✓

Quarantine Webmail Users - Table of Column Descriptions

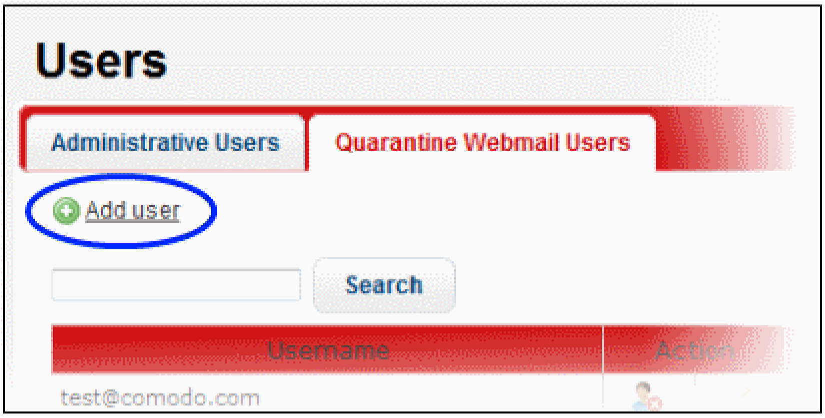
Column Header	Description	
Username	The name provided for the user when they were given webmail access.	
Action	✖	Delete the end-user
	✎	Edit end-user details. See 'Editing an End User' for more details.
Status	Whether or not the user is allowed to login and view quarantined mail. See 'Enabling/Disabling End Users' for more details.	

Admins can use this interface to:

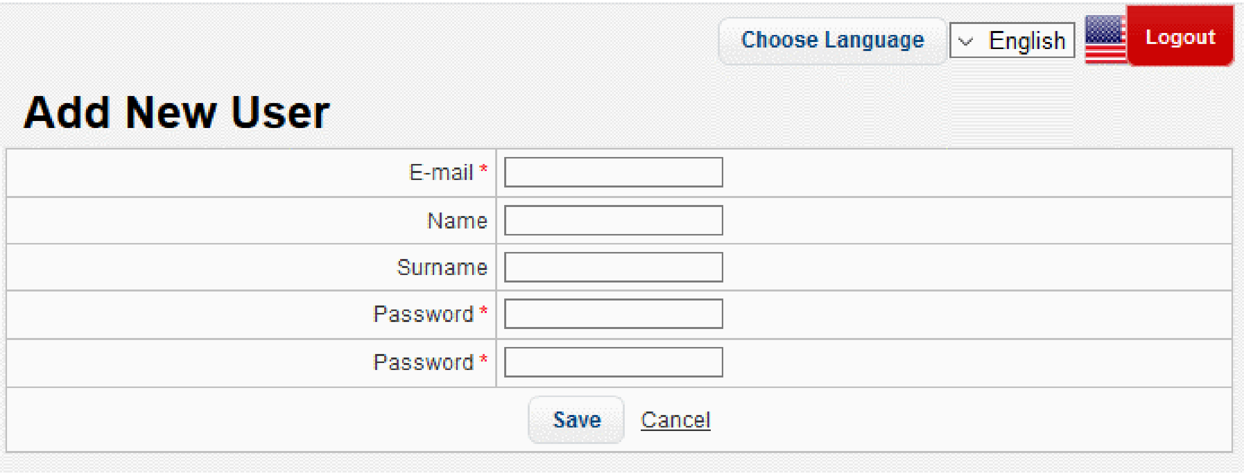
- **Add an end user**
- **Delete an end user**
- **Edit an end user**
- **Enable/Disable an end user**

To add an end user

- Click the 'Add User' link



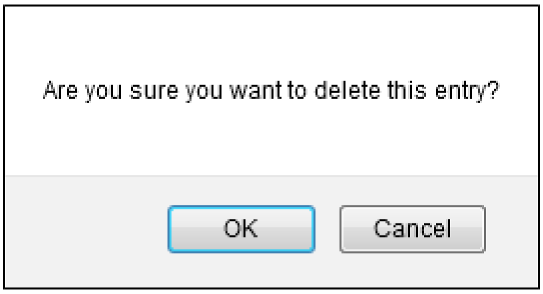
The 'Add New User' screen will be displayed.



    - E - mail: The email address of the end user
    - Name: The first name of the end user
    - Surname: The surname of the end user
    - Password: Enter the password to access the web console and confirm it in the next field.
- Click 'Save' to add the new end user.

To delete an end user

- Click the icon beside the user that you want to delete



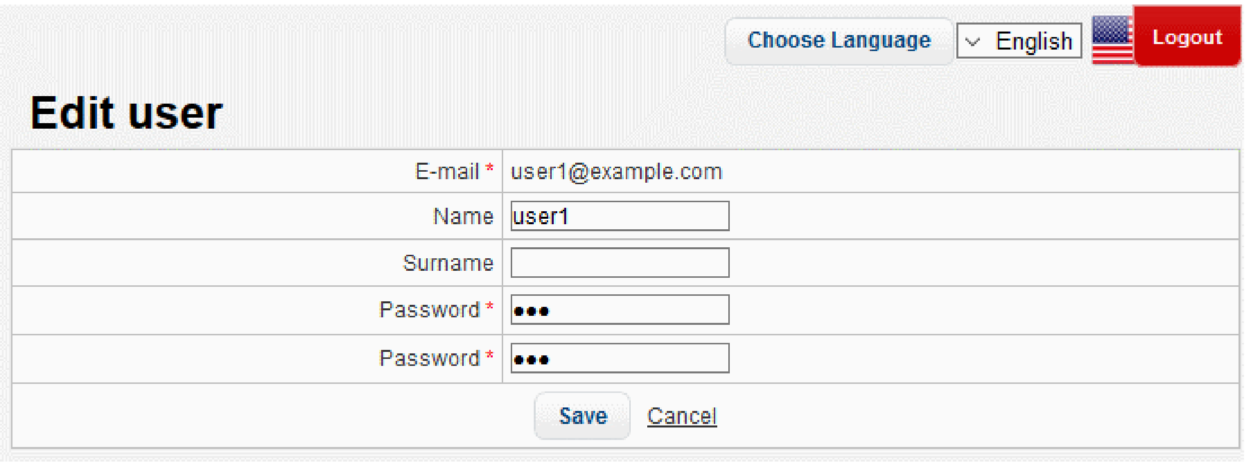
Are you sure you want to delete this entry?

- Click 'OK' to confirm the deletion.

To edit an end user

- Click the icon beside the user that you want to edit

The 'Edit User' screen will be displayed:



Edit user

E-mail *	user1@example.com
Name	user1
Surname	
Password *	●●●
Password *	●●●

- Edit the details as required. The screen is similar to the 'Add New User' section. See '**Add an end user**' for more details.
- Click 'Save'.

The changes will be saved and a confirmation note will be displayed.

To enable/disable an end user

The icon under the 'Status' column indicates whether the 'Administrator User' is enabled or disabled.

⊘	Indicates that the user is disabled and cannot access the web console
✓	Indicates that the user is enabled and can access the web console

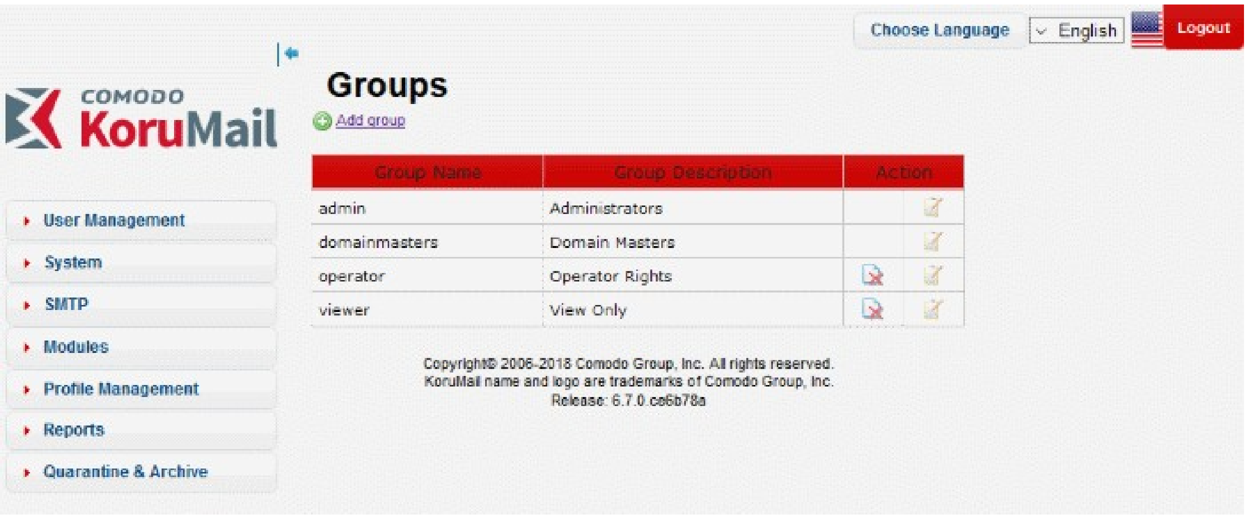
- Click the icon to toggle between enabled and disabled statuses.
- Click 'OK' in the confirmation dialog.

5.2 Manage Groups

- User groups simplify the process of configuring permission levels for admins and users. New (or existing) users added to a group will inherit the policy assigned to the group.
- Each group can be configured with different permission levels.
- The admin interface will vary according to a user's permission level. See 'Managing Admin Users' for more details.

To open the 'Groups' screen

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



Groups

Add group

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

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

Groups - Table of Column Descriptions		
Column Header	**Description**	
Group Name	The name of the group	
Group Description	Enter an appropriate description for the group	
Action	✗	Administrators with appropriate privileges can delete the group by clicking this icon.
	✎	Administrators with appropriate privileges can edit group details and its privileges. See '**Edit a Group**' for more details.

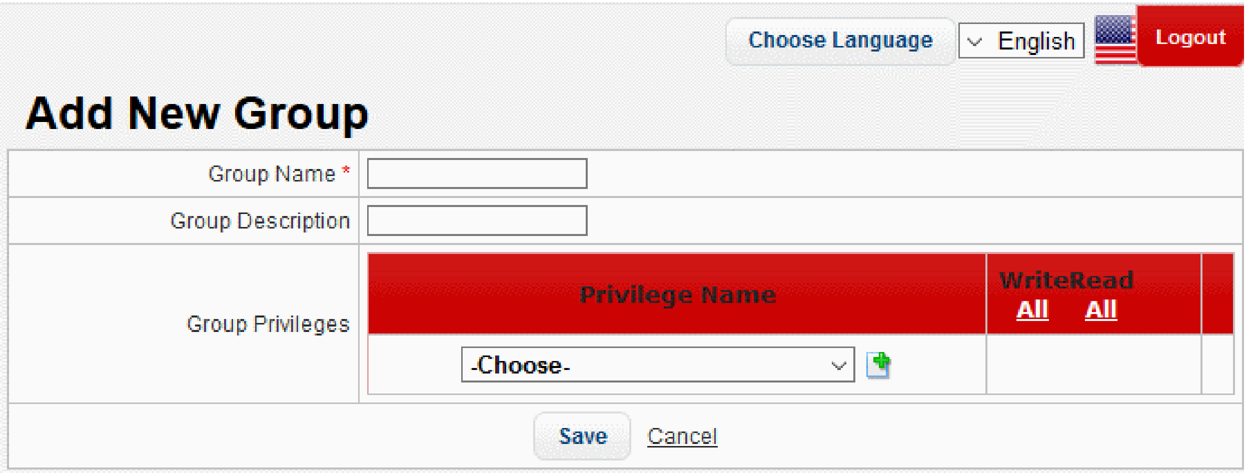
From the this interface an appropriately privileged administrator can:

- **Add a new group**
- **Delete a group**
- **Edit a group**

To add a new group

- Click the 'Add group' link

The 'Add New Group' screen will be displayed.

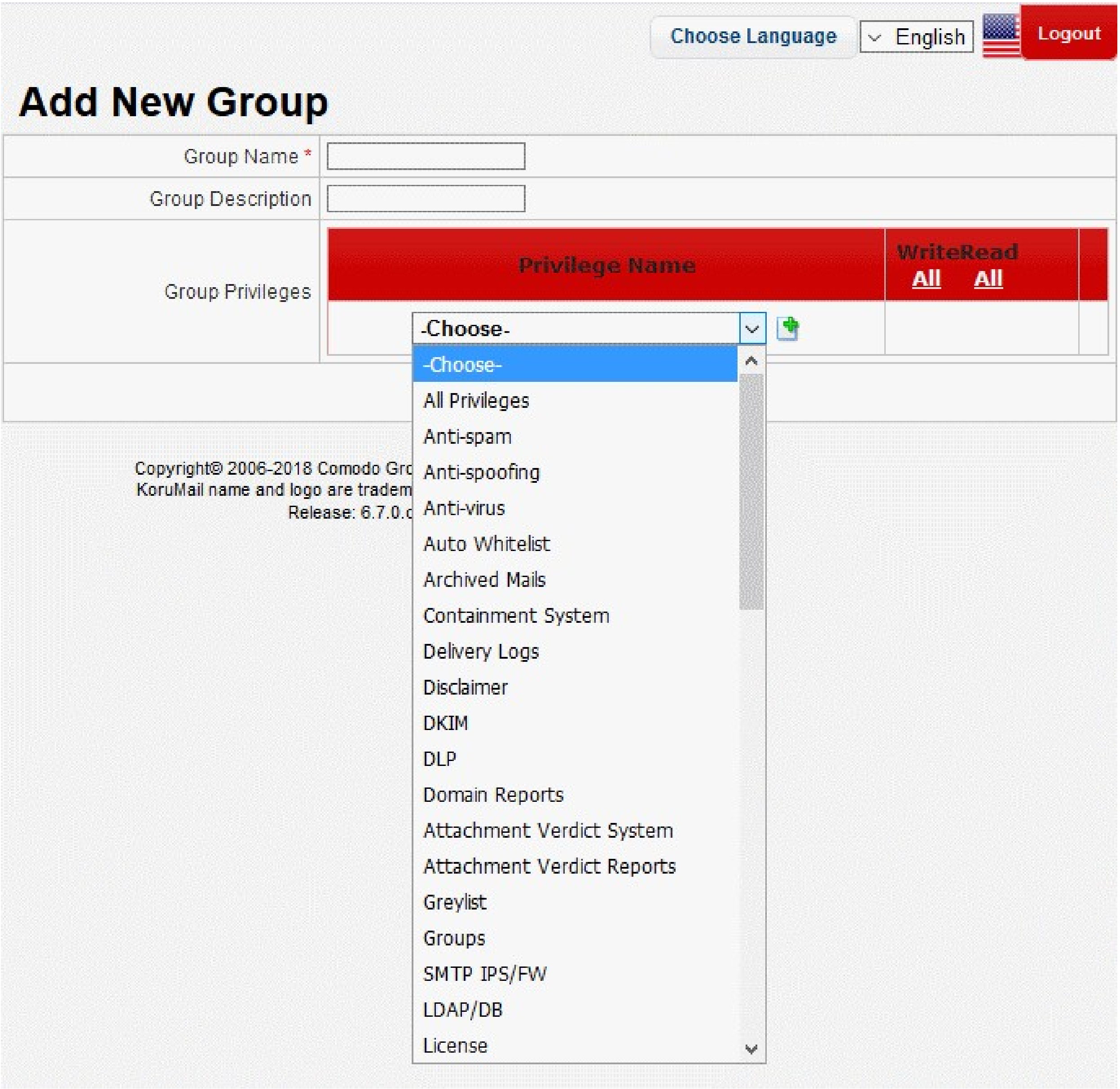


Add New Group

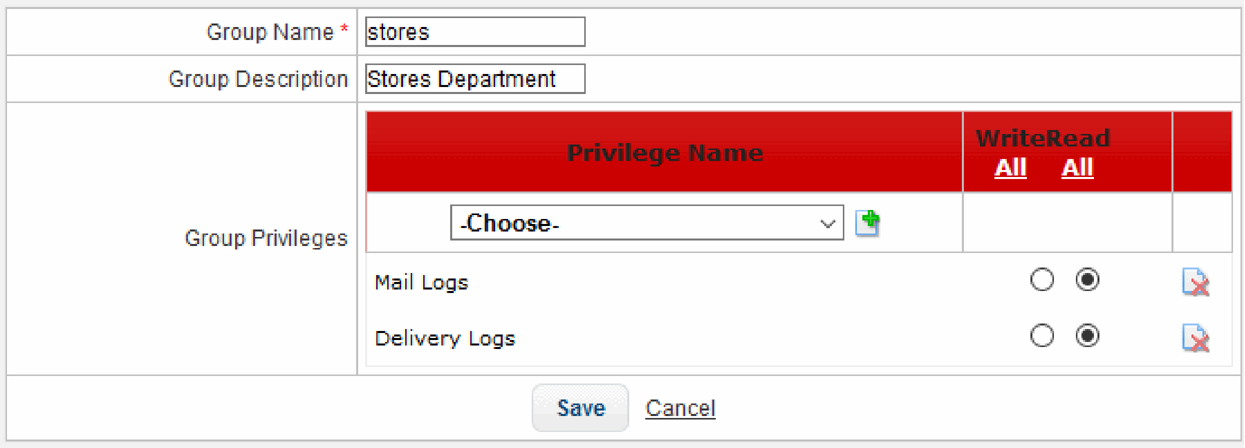
Group Name *	
Group Description	
Group Privileges	Privilege Name: -Choose- / Write All / Read All

Save   Cancel

- **Group Name:** Enter the name of the group
- **Group Description:** Enter an appropriate description for the group
- **Group Privileges:** Select the privileges that should be assigned to the group from the 'Privilege Name' drop-down.



- After the selecting the privilege for the group, click the 'Add' button ➕ to include it. The added privileges will be displayed.



Group Name *	stores
Group Description	Stores Department
Group Privileges	

Privilege Name	Write All	Read All	
-Choose-			
Mail Logs	○	●	
Delivery Logs	○	●	

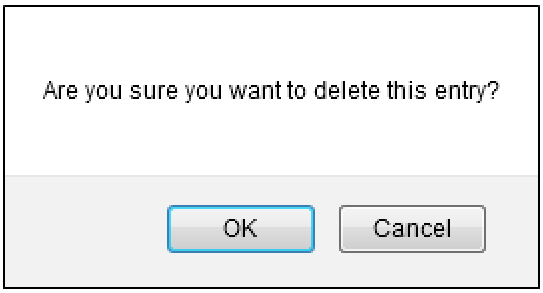
By default, the added privileges will have 'Read' rights only, meaning the features can be viewed and cannot be configured by the admin user.

  - Select the 'Write' option to make the privileges configurable for the admin user.
  - To select the 'Write' or 'Read' option for all the privileges, click the 'All' link below it.
  - To delete a privilege, click the delete icon beside it.
- Click 'Save' to add the new group.

Now this new group can be assigned to admin users. See '**Manage Admin Users**' for more details on how to assign a group to admin users.

To delete a group

- Click the icon beside the group that you want to delete



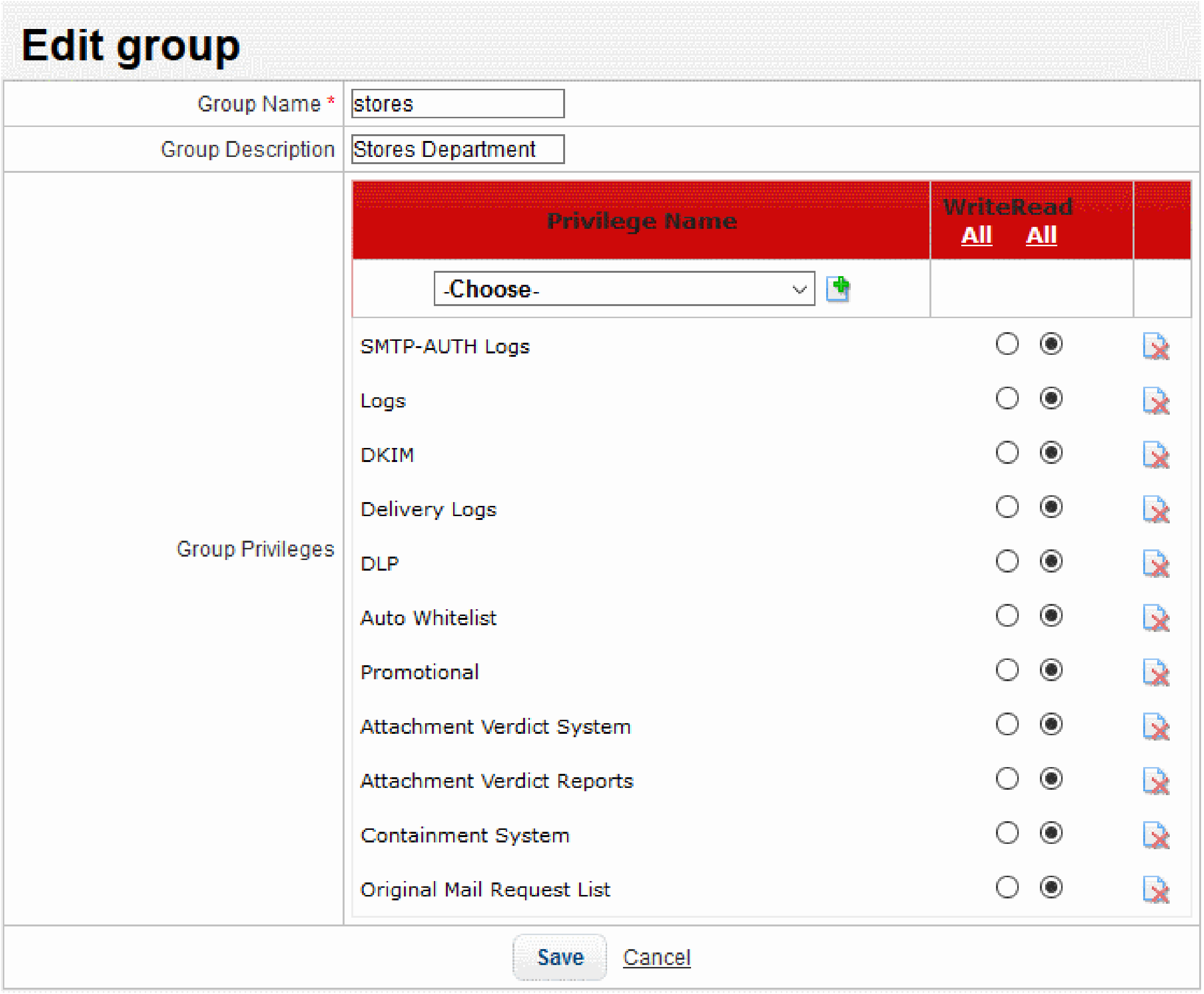
Are you sure you want to delete this entry?

- Click 'OK' to confirm the deletion.

To edit a group

- Click the icon beside the group that you want to edit

The 'Edit group' screen will be displayed.



Edit group

Group Name *	stores
Group Description	Stores Department

Group Privileges

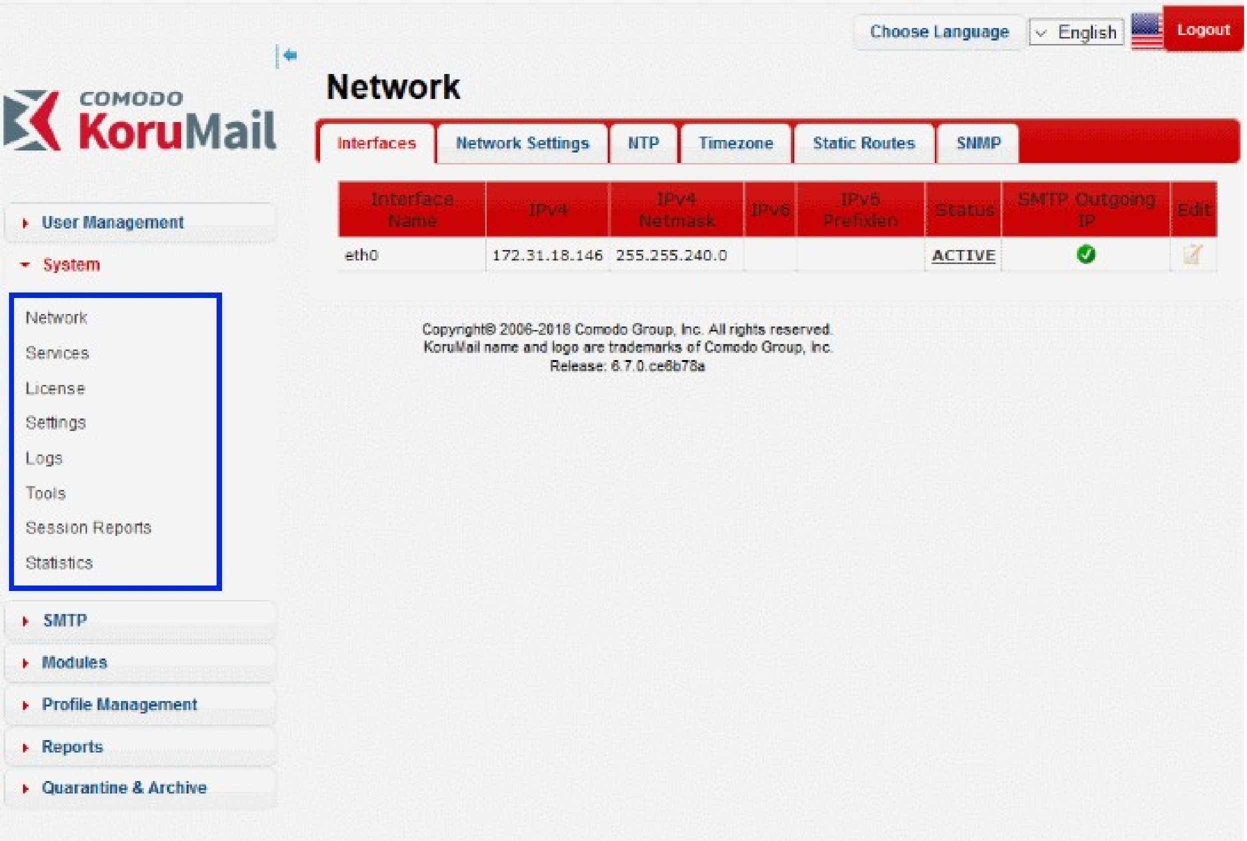
Privilege Name	Write All	Read All	
-Choose-			
SMTP-AUTH Logs	○	●	
Logs	○	●	
DKIM	○	●	
Delivery Logs	○	●	
DLP	○	●	
Auto Whitelist	○	●	
Promotional	○	●	
Attachment Verdict System	○	●	
Attachment Verdict Reports	○	●	
Containment System	○	●	
Original Mail Request List	○	●	

- Edit the details as required. The screen is similar to the 'Add New Group' section. See '**Add a new group**' for more details.
- Click 'Save'.

The changes will be saved.

6 System Configurations

- The 'System' menu allows admins to configure important parameters after **initial configuration**.
- Click 'System' on the left to open the menu:



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

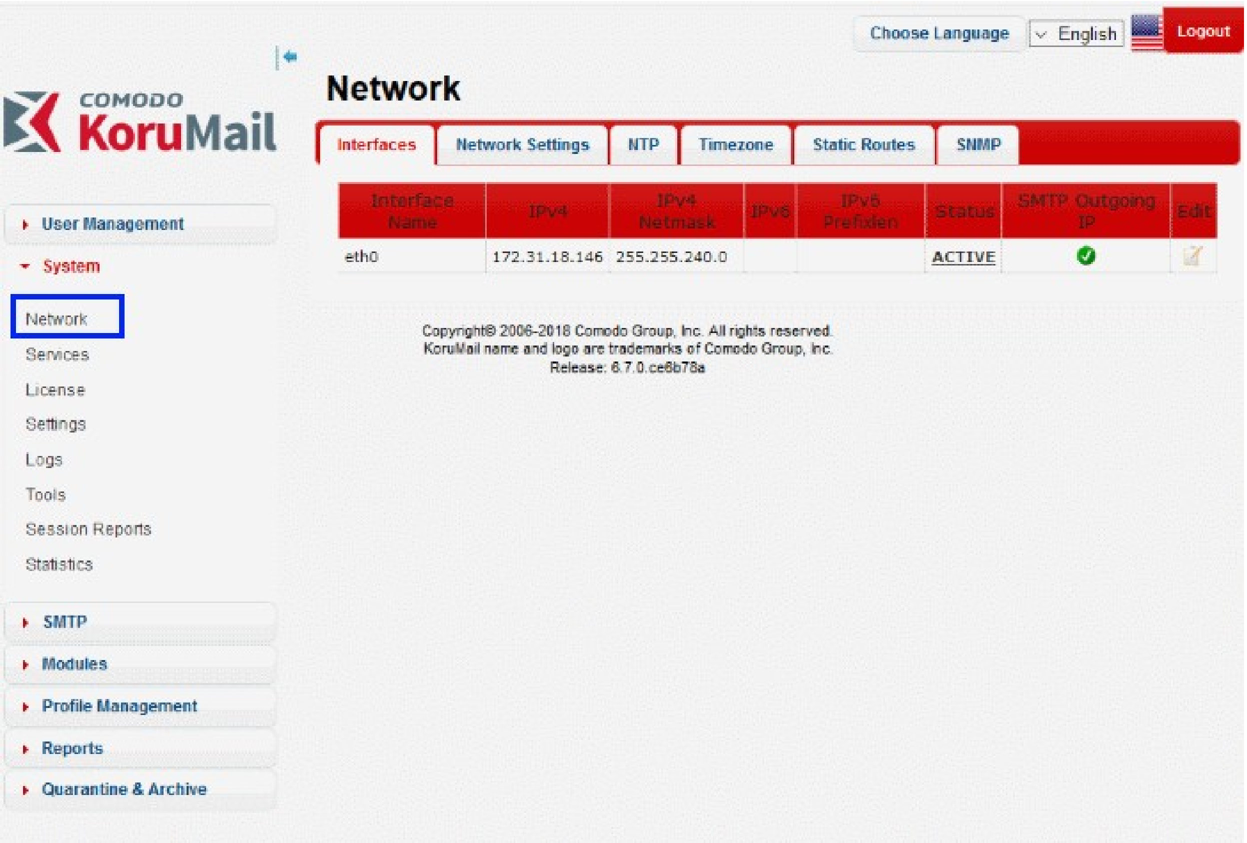
Copyright© 2006-2018 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 6.7.0.ce6b78a

- **Network:** Configure various network settings of KoruMail such as default gateways, DNS servers, NTP servers and more. See '**Network Configuration**' for more details.
- **Services:** Allows admins to start or stop various services such as Delivery Agent, SMTP, Snmpd, Scheduler and more. See '**Services**' for more details.
- **License:** View and update KoruMail licenses from this interface. See '**License**' for more details.
- **Settings:** Configure various system settings such as Cache, Session, Backup and more. See '**Configure System Settings**' for more details.
- **Logs:** View and download mail log files and configure how long the system should retain mail log records, archived mails and quarantined mails. See '**Logs**' for more details.
- **Tools:** Allows admin users to check connectivity such as SMTP, Ping, Nslookup, Telnet as well as clear SMTP queue. See '**Tools**' for more details.
- **Session Reports**: Enables you to view the details of last login and last activity performed on the user interface. See '**Session Reports**' for more details
- **Statistics:** View the graphical summary of system usage. See '**System Usage Statistics**' for more details.

6.1 Network Configuration

The 'Network' tab allows you to configure settings such as network card IP address, hostnames, default gateway addresses, DNS server details, time-zones, static routes and SNMP servers.

- To open the interface, click the 'System' tab then the 'Network' sub-tab.



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

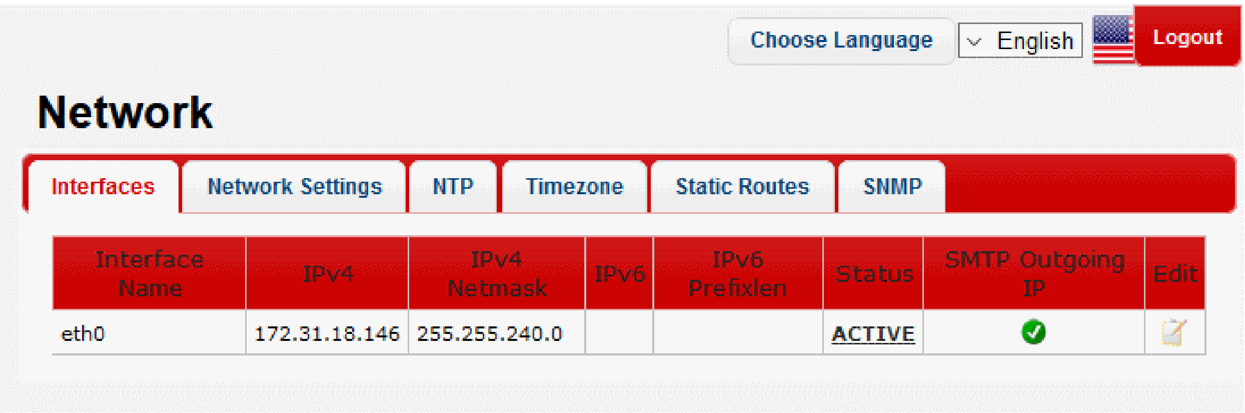
Copyright© 2006-2018 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 6.7.0.ce6b78a

Click the following links for more details of each of the settings:

- **Interfaces**
- **Network Settings**
- **Network Time Protocol (NTP)**
- **Timezone**
- **Static Routes**
- **System Usage Statistics**

6.1.1 Interfaces

- KoruMail is initially configured at installation using the command line interface. It can also be edited and updated using the web console. See '**Install the System**' for more details.
- The details of the network card can be edited/updated from the 'Interfaces' screen.
- To open the 'Interfaces' screen:
  - Click the '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	✓	📝

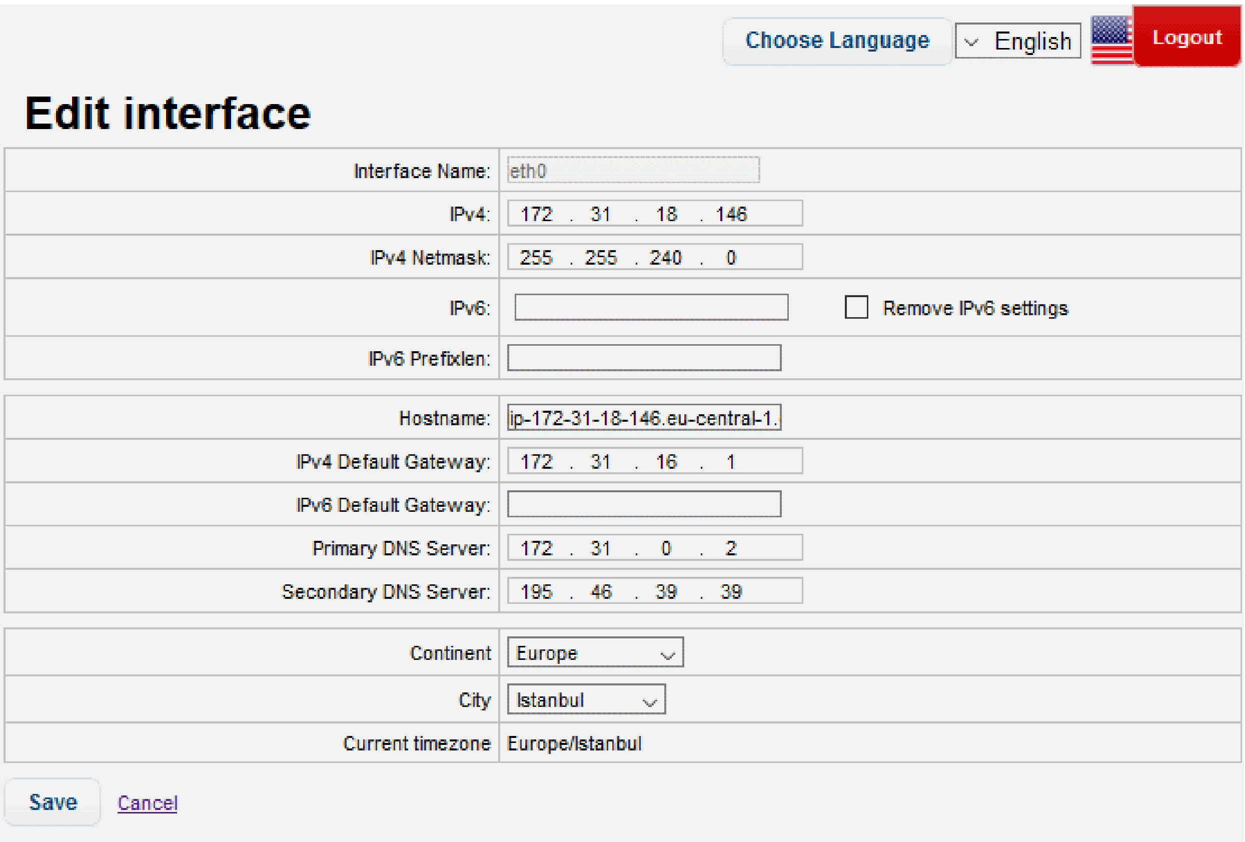
Interfaces - Table of Column Descriptions	
Column Header	**Description**
Interface Name	• The name of the network interface card (NIC) with physical ethernet ports. • The number of ports available depends on the system model. • If two ports are available, then the system can be configured to route inbound and outbound emails on separate ports. • This configuration is preferable because it provides the best network bandwidth. • If a single ethernet port is available then both incoming and outgoing emails are routed via the same port. • This may result in network bottlenecks, but can be used for organizations with relatively low mail traffic.
IPv4	The IPv4 address assigned to the port.
IPv4 Netmask	The IPv4 netmask address assigned to the port.
IPv6	The IPv6 address assigned to the port.
IPv6 Prefixlen	The prefix of the IPv6 address.
Status	Indicates whether the interface is enable or disabled. The link toggles between 'Active' and 'Inactive' statuses. Click on the link to make the interface 'Active' or 'Inactive'.
SMTP Outgoing IP	Sets the corresponding interface IP address as SMTP outgoing IP address. Clicking 'Select' applies the setting after a confirmation dialogue.
Edit	📝 Allows to edit the settings of the NIC. See '**To edit the interface**' for more details.

From this screen, administrators can edit the interface settings.

To edit the interface

- Click the 📝 icon beside the interface that you want to edit

The 'Edit interface' screen will be displayed.

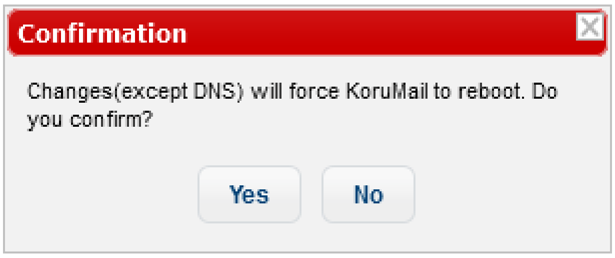


Edit interface

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 '**Network Settings**' interface 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 '**Network Settings**' interface also.
- **IPv6 Default Gateway:** The IPv6 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 '**Network Settings**' interface also.
- **Primary DNS Server:** The IP of the primary DNS server that KoruMail is configured. Edit as required. The changes will be reflected in the '**Network Settings**' interface also.
- **Secondary DNS Server:** The IP of the secondary DNS server that the system is configured. Edit as required. The changes will be reflected in the '**Network Settings**' interface also.
- **Continent:** The name of 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 displayed. Reboot will not be required for DNS setting changes.



Confirmation

Changes(except DNS) will force KoruMail to reboot. Do you confirm?

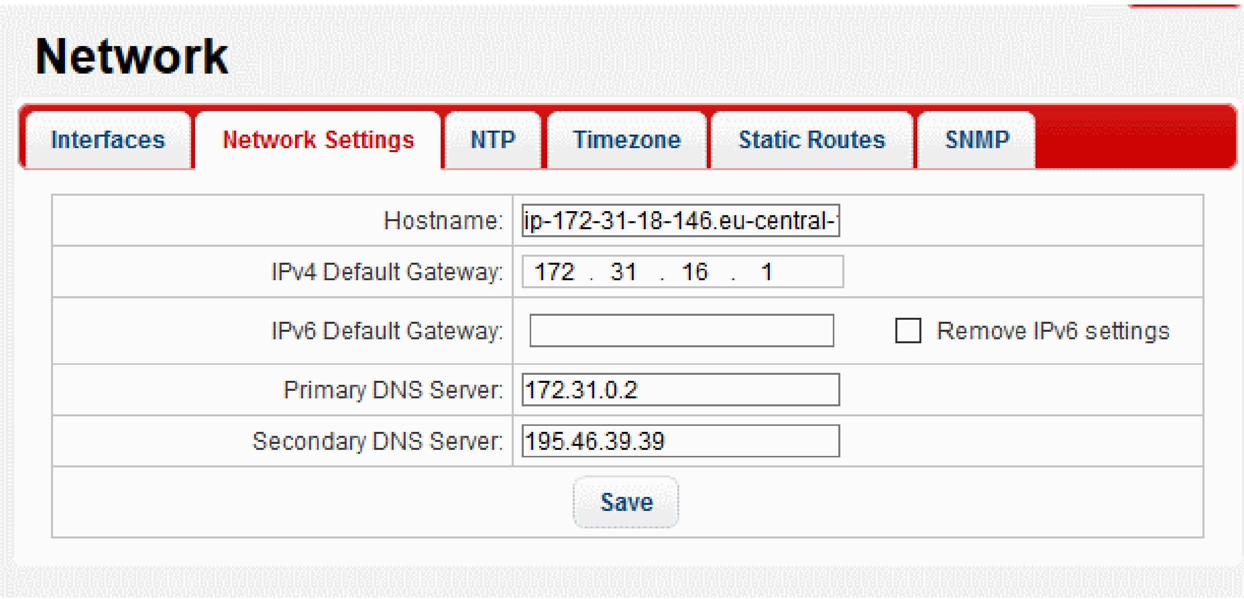
- Click 'Yes' to confirm the changes and reboot the system.

6.1.2 Network Settings

The 'Network Settings' interface allow administrators to change the hostname of KoruMail, IPv4 and IPv6 default gateways, primary and secondary DNS server settings. The changes done here will also be reflected in the '**Edit Interface**' of the NIC as explained in the previous section '**Interfaces**'.

To open the 'Network Settings' screen,

- Click the 'System' tab on the left menu, then 'Network' > 'Network Settings'

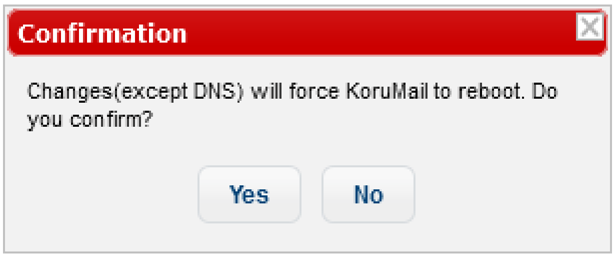


Network

Hostname:	ip-172-31-18-146.eu-central-1
IPv4 Default Gateway:	172 . 31 . 16 . 1
IPv6 Default Gateway:	□ Remove IPv6 settings
Primary DNS Server:	172.31.0.2
Secondary DNS Server:	195.46.39.39

- **Hostname:** The hostname of KoruMail. The changes will be reflected in the '**Edit interface**' of the NIC 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 '**Edit interface**' of the NIC also.
- **IPv6 Default Gateway:** The IPv6 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 '**Edit interface**' of the NIC also. To disable the IPv6 settings, select the 'Remove IPv6 settings' check box.
- **Primary DNS Server:** The IP of the primary DNS server that the system is configured. Edit as required. The changes will be reflected in the '**Edit interface**' of the NIC also.
- **Secondary DNS Server:** The IP of the secondary DNS server that the system is configured. Edit as required. The changes will be reflected in the '**Edit interface**' of the NIC also.
- Click 'Save'.

A reboot confirmation screen will be displayed. Reboot will not be required for DNS setting changes.



Changes(except DNS) will force KoruMail to reboot. Do you confirm?

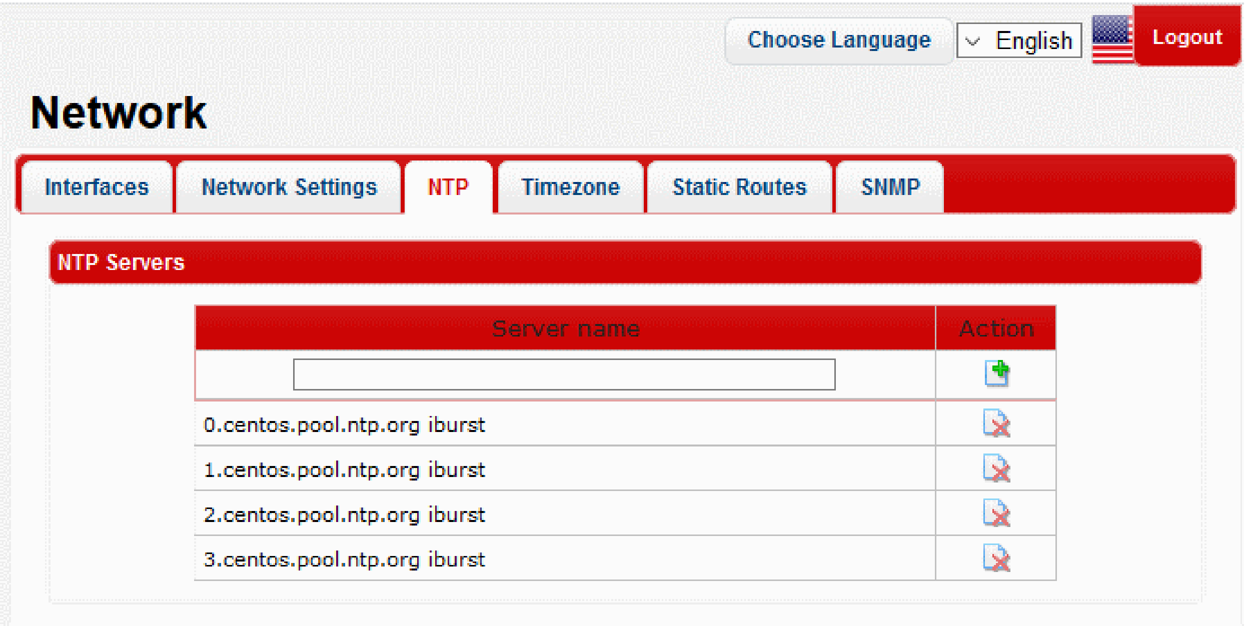
- Click 'Yes' to confirm the changes and reboot the system.

6.1.3 Network Time Protocol (NTP)

Network Time Protocol (NTP) is an Internet protocol that is used to synchronize computer clocks over a network. The 'NTP Servers' screen allow administrators to add time synch servers for KoruMail.

To open the 'NTP Servers' screen,

- Click the 'System' tab on the left menu,then 'Network' > 'NTP'



Server name	Action
	➕
0.centos.pool.ntp.org iburst	✗
1.centos.pool.ntp.org iburst	✗
2.centos.pool.ntp.org iburst	✗
3.centos.pool.ntp.org iburst	✗

To add a new NTP server

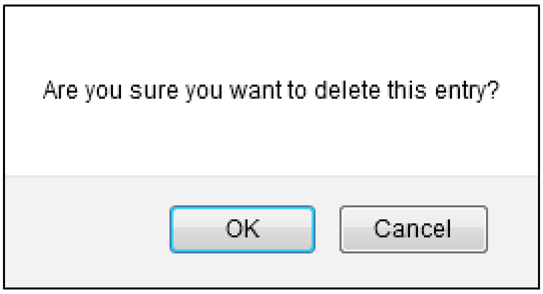
- Enter the name or IP address of the server in the 'Server name' field and click the 'Add' button ➕.

The message 'Settings saved successfully' will be displayed.

To remove a NTP server

- Click the 'Delete' button ✗ beside the server name in the list.

In the confirmation dialog, click 'OK' to remove the NTP server from the list.

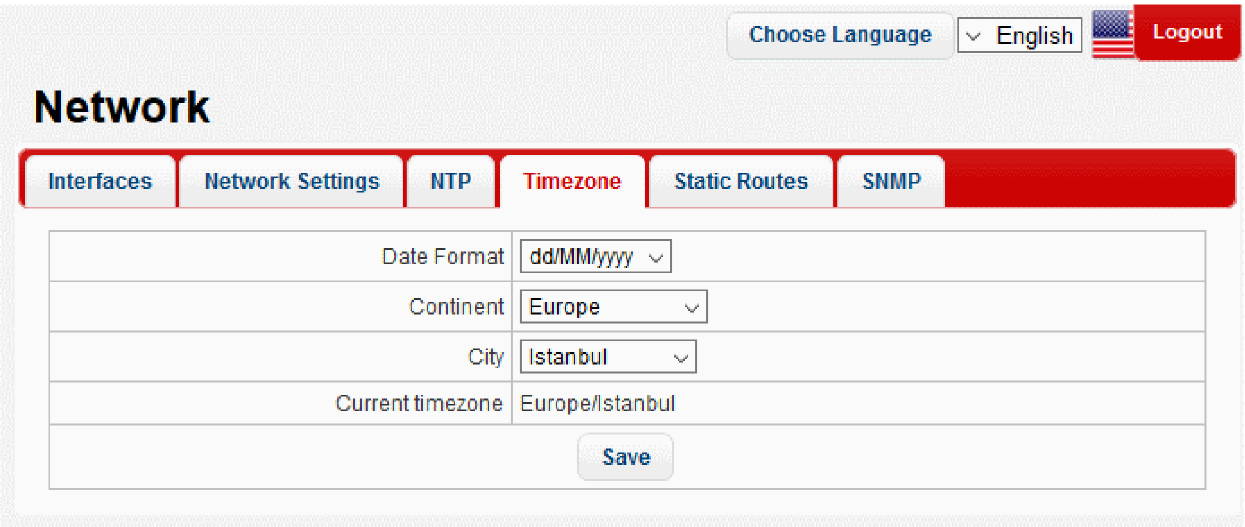


Are you sure you want to delete this entry?

6.1.4 Timezone

The 'Timezone' tab in the web console allow administrators to configure the time zone of the system to which you want to synchronize the time.

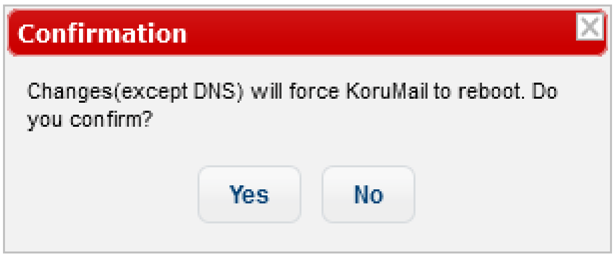
- To open the 'Timezone' screen, click the 'System' tab on the left menu, then 'Network' and 'Timezone' from the 'Network' screen.



Date Format	dd/MM/yyyy
Continent	Europe
City	Istanbul
Current timezone	Europe/Istanbul

- **Date Format**: Select the format to display date from drop down
- **Continent:** Select the continent from the drop-down
- **City:** Select the city from the drop-down

Click the 'Save' button. A reboot confirmation screen will be displayed.



Changes(except DNS) will force KoruMail to reboot. Do you confirm?

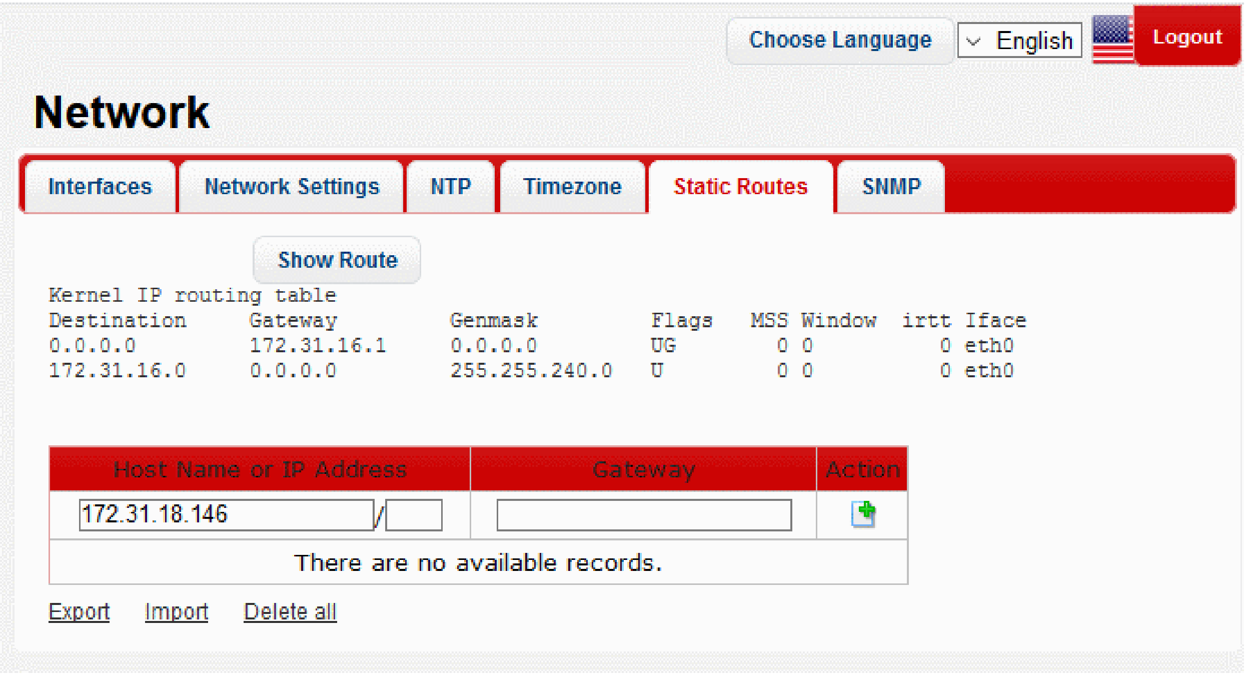
Click 'Yes' to confirm the changes and reboot the system. The changes done here will also be reflected in the '**Edit Interface**' of the NIC as explained in the previous section '**Interfaces**'.

6.1.5 Static Routes

KoruMail can be configured to redirect traffic to different email servers using the static route in addition to the default gateway configured in '**Network Settings**' section.

To open the 'Static Routers' screen,

- Click the 'System' tab on the left menu, then 'Network' > 'Static Routes' from the 'Network' screen.



```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         172.31.16.1     0.0.0.0         UG        0 0          0 eth0
172.31.16.0     0.0.0.0         255.255.240.0   U         0 0          0 eth0
```

Host Name or IP Address	Gateway	Action
172.31.18.146 /		⊞
There are no available records.		

Export Import Delete all

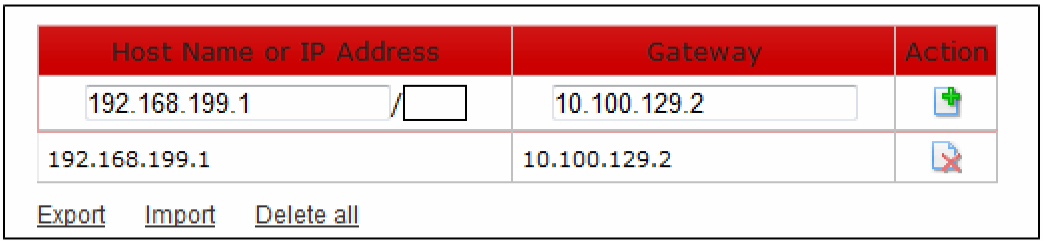
From this screen an administrator can:

- Add host names or IP address
- Delete host names or IP address
- View the network route

To add host names or IP address

- Enter the host name or IP address of the machine that you want to specify a static route in the 'Host Name or IP Address' field.
- Enter the IP address of the gateway that the machine should connect to.
- Click the ⊞ button under the 'Action' column.

The system will be added and displayed below the field.



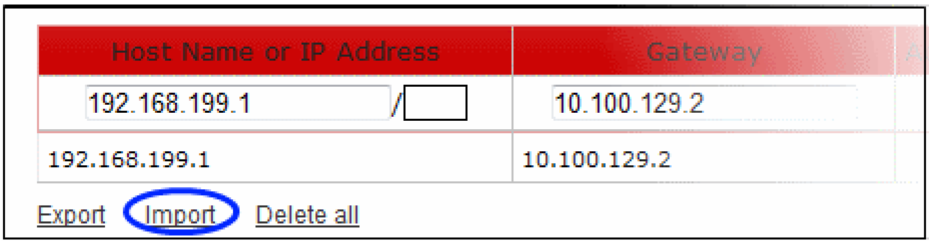
Host Name or IP Address	Gateway	Action
192.168.199.1 /	10.100.129.2	⊞
192.168.199.1	10.100.129.2	☒

Export Import Delete all

- Repeat the process to add more machines.

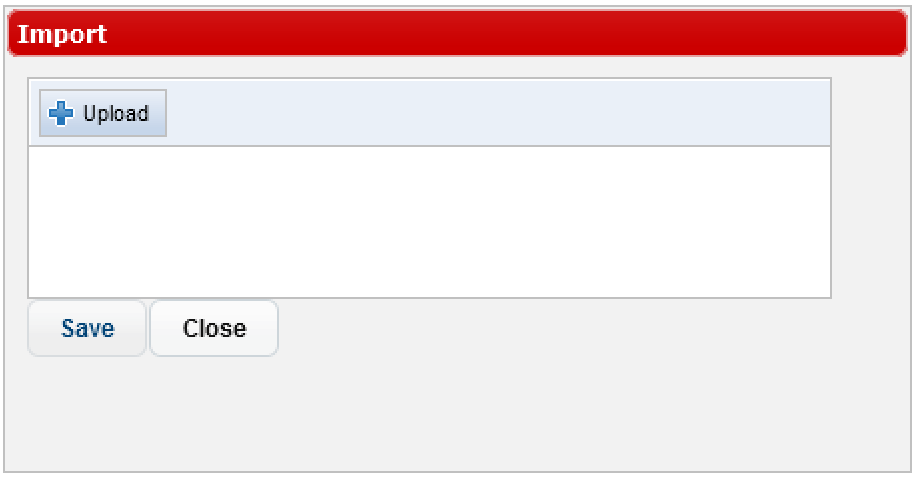
Alternatively, you can also import the machines from a file.

- To import the machines, click the 'Import' link



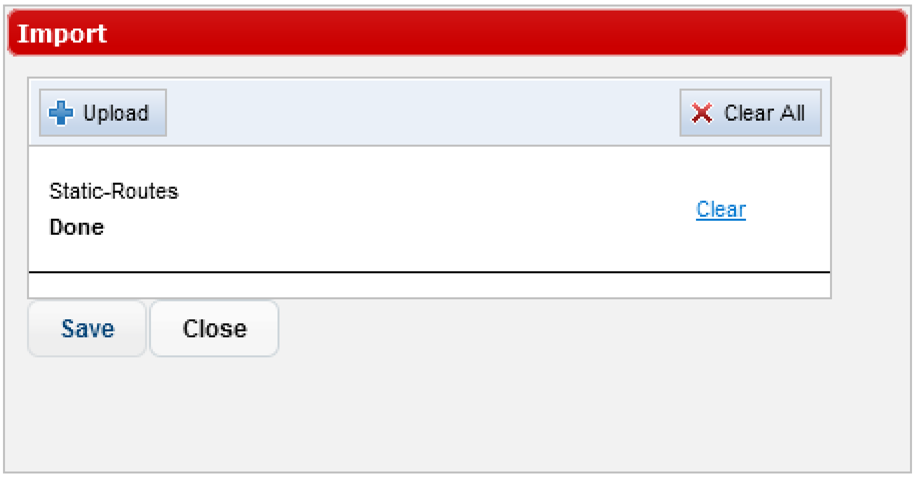
Host Name or IP Address	Gateway
192.168.199.1 /	10.100.129.2
192.168.199.1	10.100.129.2

The 'Import' dialog will be displayed.



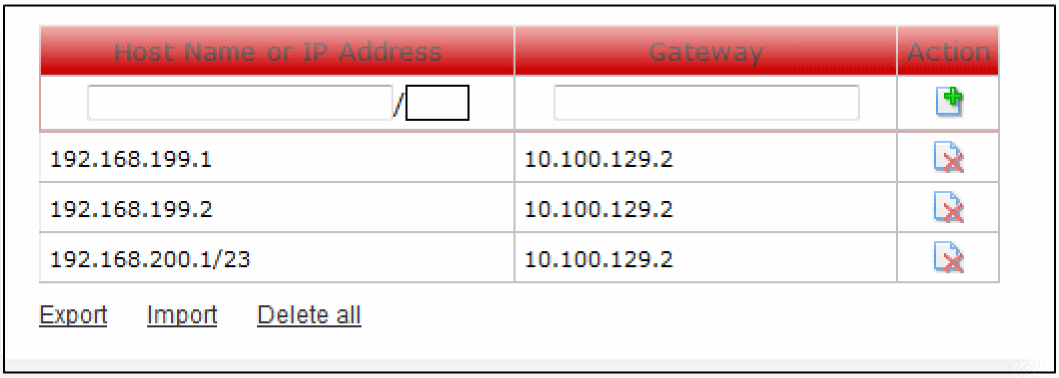
- Click the 'Upload' button, navigate to the the location where the file is saved, select it and click 'Open'.

The file will be added.



Static-Routes
Done
Clear

- Repeat the process to add more files.
- To remove a file, click the 'Clear' link beside it.
- To remove all the added files, click the 'Clear All' button at the top right.
- To import the machines from the files, click the 'Save' button.



Host Name or IP Address	Gateway	Action
/		✚
192.168.199.1	10.100.129.2	☒
192.168.199.2	10.100.129.2	☒
192.168.200.1/23	10.100.129.2	☒

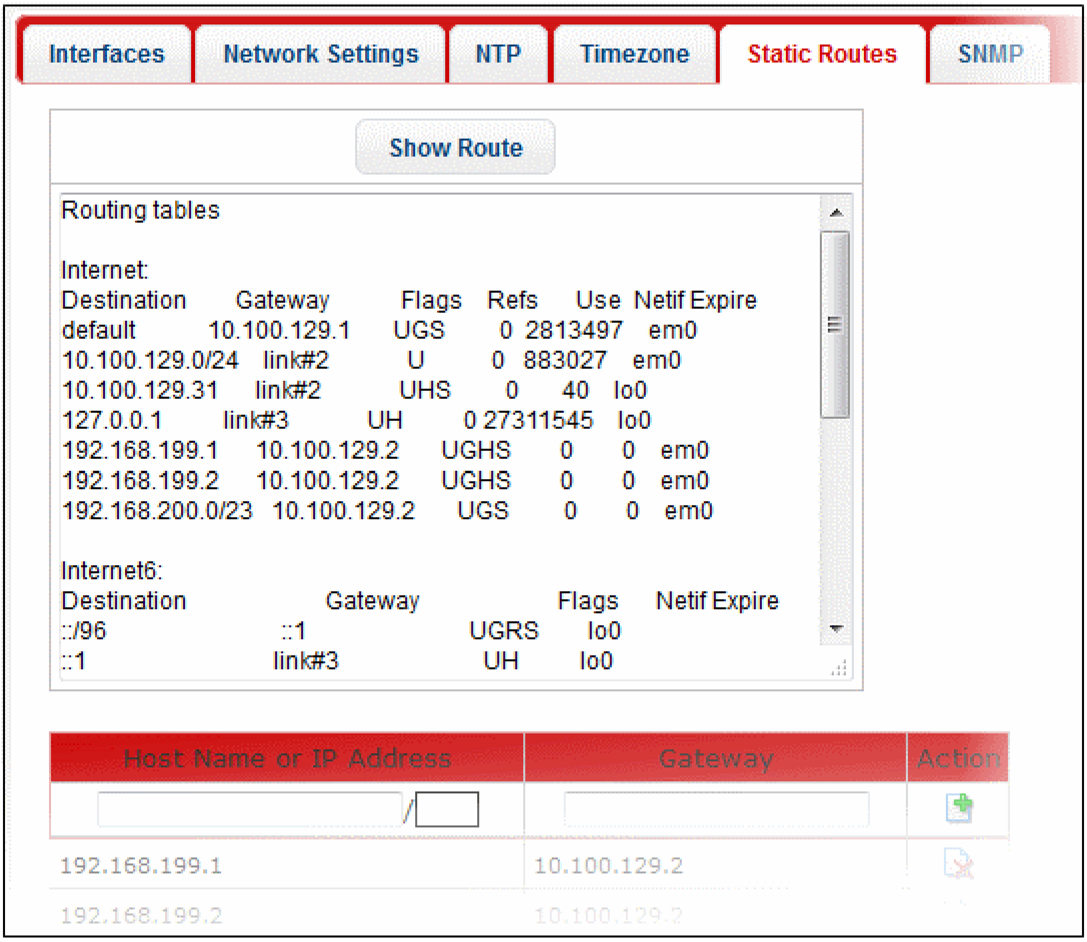
- To save the details of machines and gateway, click the 'Export' link and save it to your system.

To delete host names or IP address

- Click the ☒ beside a system to remove it from the static route and click 'OK' in the confirmation dialog.
- To remove all the machines from the list, click the 'Delete all' link at the bottom and click 'OK' in the confirmation dialog.

To view the network route

- Click the 'Show Route' to view the 'Routing tables' for the machines.



```
Routing tables

Internet:
Destination      Gateway         Flags   Refs     Use  Netif Expire
default          10.100.129.1    UGS        0  2813497   em0
10.100.129.0/24  link#2          U          0   883027   em0
10.100.129.31    link#2          UHS        0       40   lo0
127.0.0.1        link#3          UH         0 27311545   lo0
192.168.199.1    10.100.129.2    UGHS       0        0   em0
192.168.199.2    10.100.129.2    UGHS       0        0   em0
192.168.200.0/23 10.100.129.2    UGS        0        0   em0

Internet6:
Destination                Gateway               Flags      Netif Expire
::/96                      ::1                   UGRS       lo0
::1                        link#3                UH         lo0
```

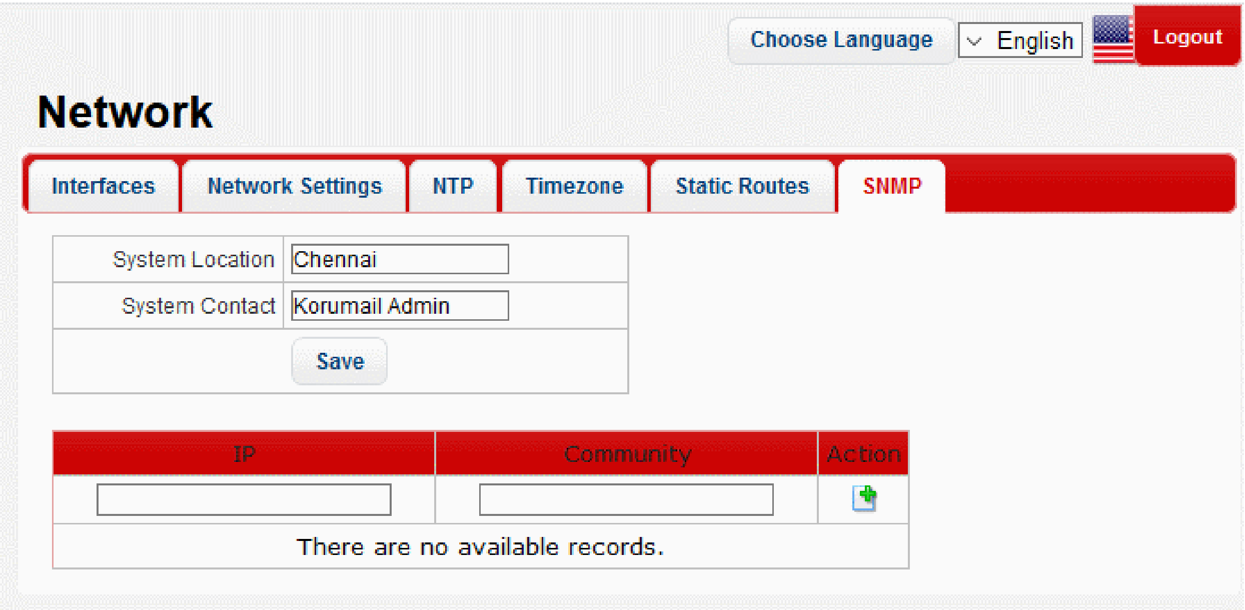
Host Name or IP Address	Gateway	Action
/		✚
192.168.199.1	10.100.129.2	☒
192.168.199.2	10.100.129.2	

6.1.6 Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) allows administrators to monitor network devices such as KoruMail. Before configuring the SNMP settings, download the SNMP agent and Management Information Base (MIB).

To configure SNMP settings,

- Click the 'System' tab on the left menu, then 'Network' and 'SNMP' from the 'Network' screen.



System Location	Chennai
System Contact	Korumail Admin

IP	Community	Action
		➕
There are no available records.		

- **System Location:** Name of the location where the KoruMail device is located.
- **System Contact:** The name, telephone number and/or email address of the system administrator to contact.

Click the 'Save' button.

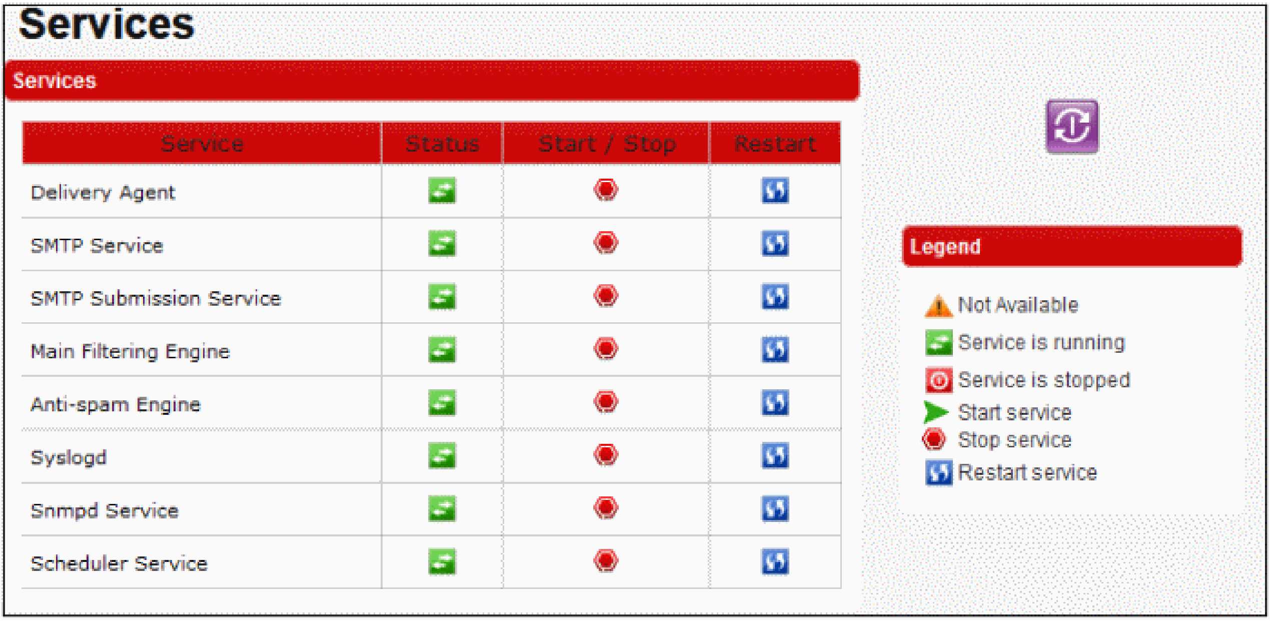
- **IP:** Enter the IP address of the SNMP Manager system
- **Community:** The community string that is defined between SNMP manger and the SNMP agent in KoruMail. It acts like a password to provide access to the agent in KoruMail.

Click the ➕ link to add the SNMP manager. You can add multiple SNMP managers. You can delete any currently SNMP access enabled hosts by clicking the ✖ link click 'OK' in the confirmation dialog.

6.2 Services

The 'Services' screen shows the current status of various KoruMail services. You can stop or restart a service, and also shutdown or reboot KoruMail.

- Click 'System' > 'Services' to view and configure KoruMail services:



Services

Services

Service	Status	Start / Stop	Restart
Delivery Agent	🟩	●	↻
SMTP Service	🟩	●	↻
SMTP Submission Service	🟩	●	↻
Main Filtering Engine	🟩	●	↻
Anti-spam Engine	🟩	●	↻
Syslogd	🟩	●	↻
Snmpd Service	🟩	●	↻
Scheduler Service	🟩	●	↻

Legend

- ⚠ Not Available
- 🟩 Service is running
- 🟥 Service is stopped
- ▶ Start service
- ● Stop service
- ↻ Restart service

The icons in the 'Legend' screen provides the status details of the services.

Description of the Services	
Column Header	**Description**
Delivery Agent	The service forwards emails processed by KoruMail to the target email server.
SMTP Service	• The service that filters emails on hosted domain names on KoruMail. • This service accepts incoming e-mail connections listening to port 25 of SMTP. • The SMTP service filters emails per the settings configured by the administrator (Reverse DNS, RBL, SRN, MX control the White List, Black List, Grey List, etc.) in SMTP level first and then the filtered emails are passed to the next stage - KoruMail Main Engine for spam and virus analysis.
SMTP Submission Service	• Ports 25 and 587 are mail delivery ports • You must have an account on the server to send mail through it.
Main Filtering Engine	• Emails that are filtered by the SMTP service are forwarded to the Korumail engine for spam and virus checks. • This module performs actions specified by the admin. These include quarantining the mail, blocking the mail, allowing the mail, or saving the mail to another area or address. • Mails which pass the Korumail filters are forwarded by the KoruMail delivery agent.
Anti-spam Engines	• The antispam engines scan your mail and assign spam scores based on Bayesian filters and thousands of spam signatures. • These scores are used to define a mail as spam.
Syslogd	The daemon service that stores system logs in rsyslog format.

Snmpd Service	It is an Simple Network Management Protocol (SNMP) agent which binds to port and acts on SNMP management application’s requests and sends the requested information to the requester.
Scheduler Service	This service organizes the programs that runs periodically. This feature in KoruMail Secure Email Gateway creates periodic reports and graphics about system usage.

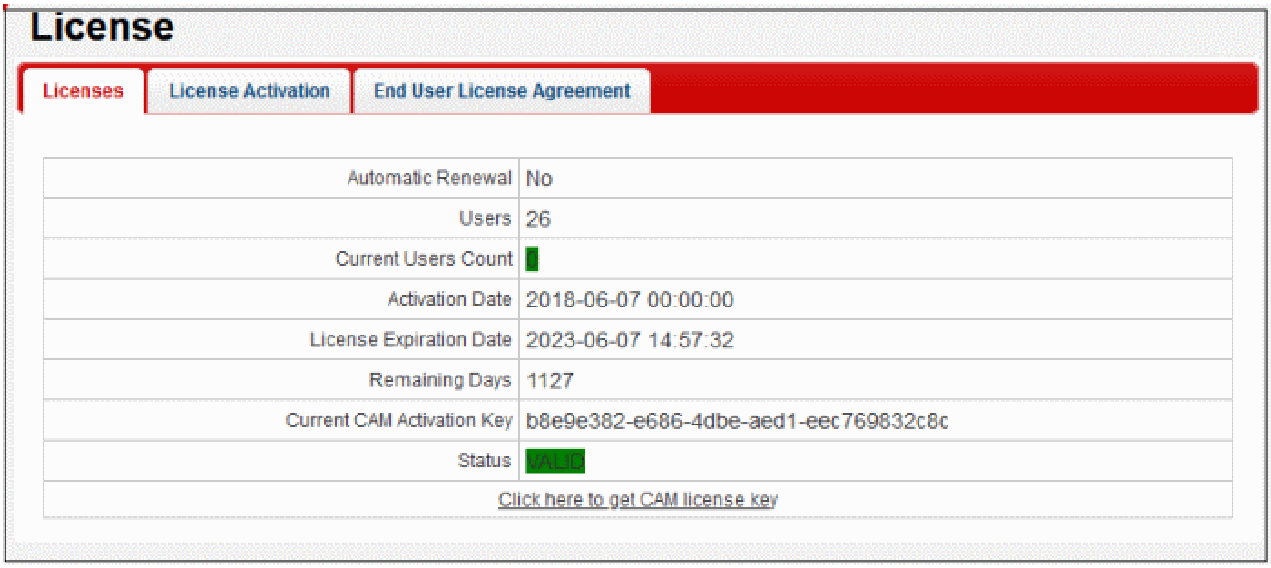
- To start or stop a service, click on the buttons beside it.

⇄	Indicates the service is running. Click on the 🛑 button under the 'Start / Stop' column to stop the service.
⏻	Indicates the service has stopped. Click on the ▶ button under the 'Start / Stop' column to start the service.

- To restart a service, click on the 🔄 button under the 'Restart' column. If the service is running, it will stop and restart again. If the service is stopped, then it will restart.
- To shutdown the KoruMail system, click the ⏻ button.
- To reboot the KoruMail system, click the 🔄 button.

6.3 License

- Click 'System'> 'License' in the left-hand menu
- The 'License' screen lets you view current license details, create a license request and install a new license.
- KoruMail licenses can be purchased by logging into your Comodo account at **https://accounts.comodo.com/account/login**
- Licenses are priced according to the number of users and license period.



License

Automatic Renewal	No
Users	26
Current Users Count	🟩
Activation Date	2018-06-07 00:00:00
License Expiration Date	2023-06-07 14:57:32
Remaining Days	1127
Current CAM Activation Key	b8e9e382-e686-4dbe-aed1-eec769832c8c
Status	VALID

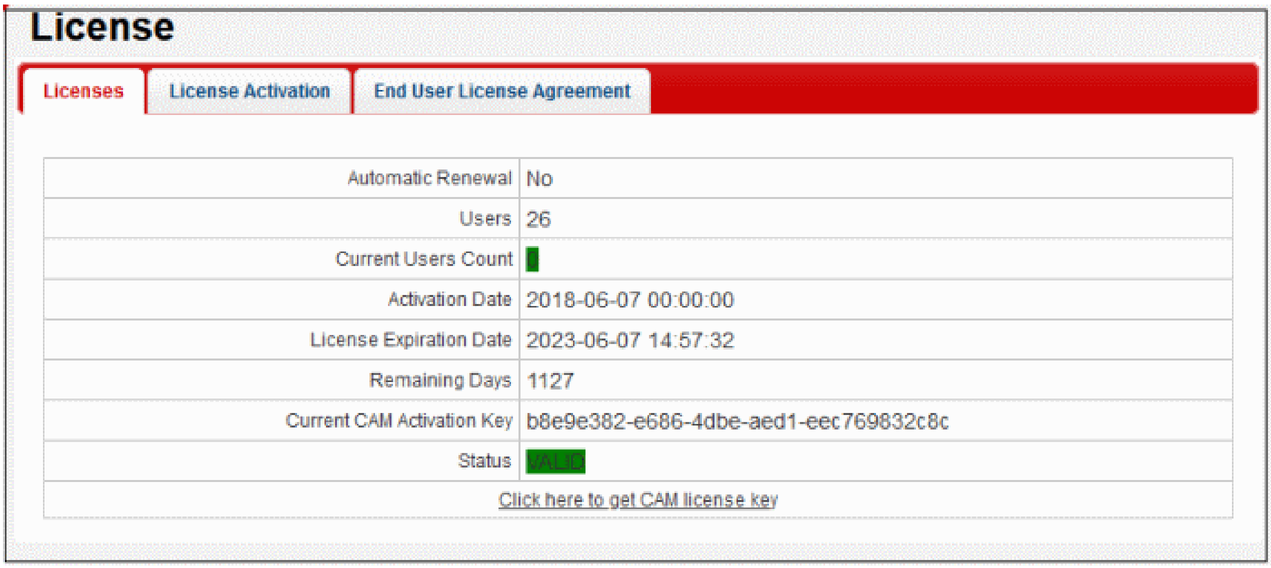
Click here to get CAM license key

From this screen you can:

- **View details of your current license**
- **Purchase a license**
- **Activate your license**
- **Read the End User License Agreement (EULA)**

To view the details of current license

- Click the 'Licenses' tab



License

Licenses
License Activation
End User License Agreement

Automatic Renewal	No
Users	26
Current Users Count	🟩
Activation Date	2018-06-07 00:00:00
License Expiration Date	2023-06-07 14:57:32
Remaining Days	1127
Current CAM Activation Key	b8e9e382-e686-4dbe-aed1-eec769832c8c
Status	VALID

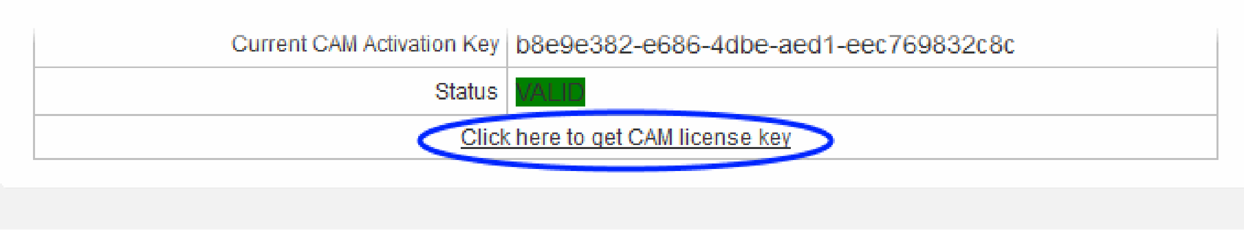
Click here to get CAM license key

License - Table of Column Descriptions	
Column Header	**Description**
Automatic Renewal	If enabled, Comodo will automatically renew your license for the same term/user count when it expires. Your payment card will be charged appropriately.
Users	Max. number of users that can be enrolled on the license.
Current User Count	Number of users currently using the product license

Activation Date	Start date of the license.
License Expiration Date	Date when the license expires.
Remaining Days	Number of days left until license expiry
Current CAM Activation Key	Key to activate your license.
Status	Can be 'Valid' (active) or 'Expired' (not active).

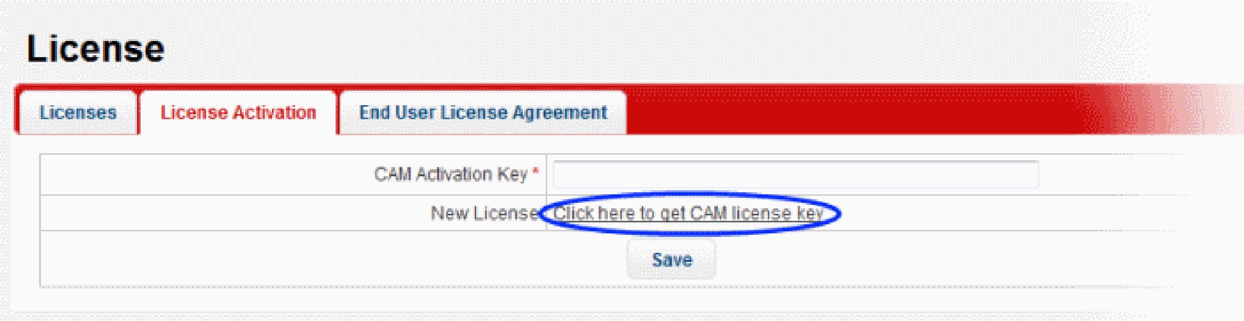
Purchase a license

- Click the 'Click here to get CAM license key' in the 'Licenses' tab...



Current CAM Activation Key	b8e9e382-e686-4dbe-aed1-eec769832c8c
Status	VALID
Click here to get CAM license key	

...or in the 'License Activation' tab.



CAM Activation Key *

New License Click here to get CAM license key

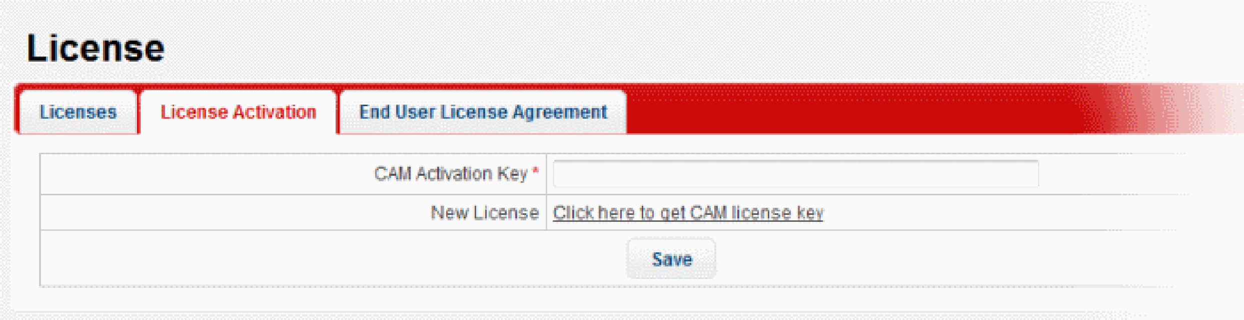
You will be taken to Comodo Accounts Manager (CAM) login page at **https://accounts.comodo.com/account/login**

- Login to your CAM account or create a new one and complete the KoruMail license purchase procedure.

A license key will be sent to your email address that was provided at the time of CAM sign-up.

Activate your license

- Click the 'License Activation' tab.



CAM Activation Key *

New License Click here to get CAM license key

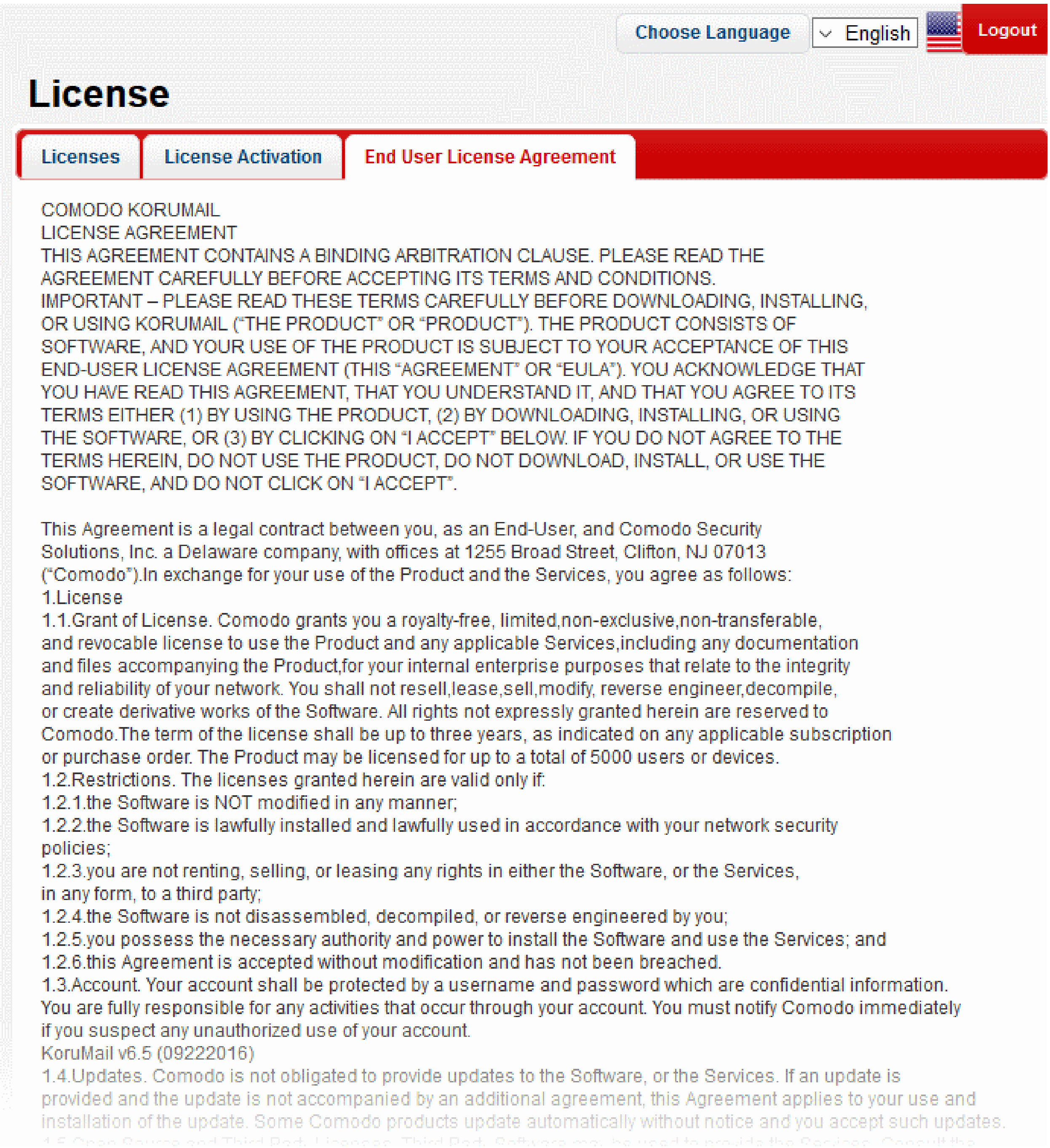
- Copy and paste the license key that was sent to your email address from Comodo in the 'CAM Activation Key' field.

- Click the 'Save' button.

The license key will be checked and if validated, the 'Licenses' interface will be updated accordingly.

End User License Agreement (EULA)

- Click the 'End User License Agreement' tab.

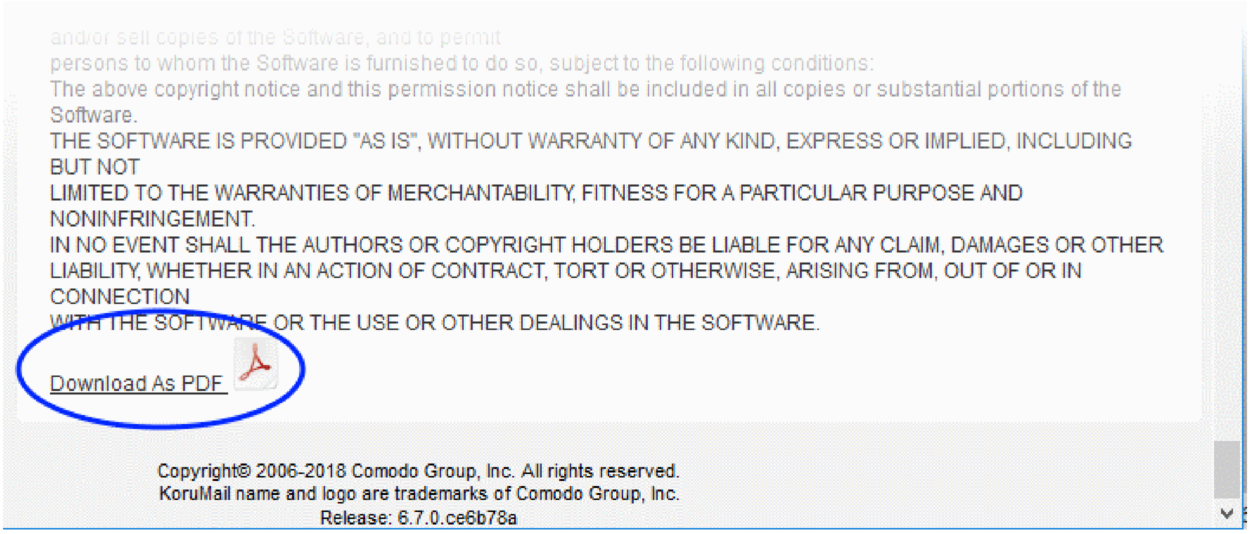


COMODO KORUMAIL
LICENSE AGREEMENT
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING ITS TERMS AND CONDITIONS.
IMPORTANT – PLEASE READ THESE TERMS CAREFULLY BEFORE DOWNLOADING, INSTALLING, OR USING KORUMAIL ("THE PRODUCT" OR "PRODUCT"). THE PRODUCT CONSISTS OF SOFTWARE, AND YOUR USE OF THE PRODUCT IS SUBJECT TO YOUR ACCEPTANCE OF THIS END-USER LICENSE AGREEMENT (THIS "AGREEMENT" OR "EULA"). YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO ITS TERMS EITHER (1) BY USING THE PRODUCT, (2) BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, OR (3) BY CLICKING ON "I ACCEPT" BELOW. IF YOU DO NOT AGREE TO THE TERMS HEREIN, DO NOT USE THE PRODUCT, DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND DO NOT CLICK ON "I ACCEPT".

This Agreement is a legal contract between you, as an End-User, and Comodo Security Solutions, Inc. a Delaware company, with offices at 1255 Broad Street, Clifton, NJ 07013 ("Comodo").In exchange for your use of the Product and the Services, you agree as follows:
1.License
1.1.Grant of License. Comodo grants you a royalty-free, limited,non-exclusive,non-transferable, and revocable license to use the Product and any applicable Services,including any documentation and files accompanying the Product,for your internal enterprise purposes that relate to the integrity and reliability of your network. You shall not resell,lease,sell,modify, reverse engineer,decompile, or create derivative works of the Software. All rights not expressly granted herein are reserved to Comodo.The term of the license shall be up to three years, as indicated on any applicable subscription or purchase order. The Product may be licensed for up to a total of 5000 users or devices.
1.2.Restrictions. The licenses granted herein are valid only if:
1.2.1.the Software is NOT modified in any manner;
1.2.2.the Software is lawfully installed and lawfully used in accordance with your network security policies;
1.2.3.you are not renting, selling, or leasing any rights in either the Software, or the Services, in any form, to a third party;
1.2.4.the Software is not disassembled, decompiled, or reverse engineered by you;
1.2.5.you possess the necessary authority and power to install the Software and use the Services; and
1.2.6.this Agreement is accepted without modification and has not been breached.
1.3.Account. Your account shall be protected by a username and password which are confidential information. You are fully responsible for any activities that occur through your account. You must notify Comodo immediately if you suspect any unauthorized use of your account.
KoruMail v6.5 (09222016)
1.4.Updates. Comodo is not obligated to provide updates to the Software, or the Services. If an update is provided and the update is not accompanied by an additional agreement, this Agreement applies to your use and installation of the update. Some Comodo products update automatically without notice and you accept such updates.
1.5.Open Source and Third Party Licenses. Third Party Software may be used to provide the Services. Consult the

- Read the EULA fully.

You can also download the EULA from the screen by clicking the 'Download As PDF' link at the bottom.



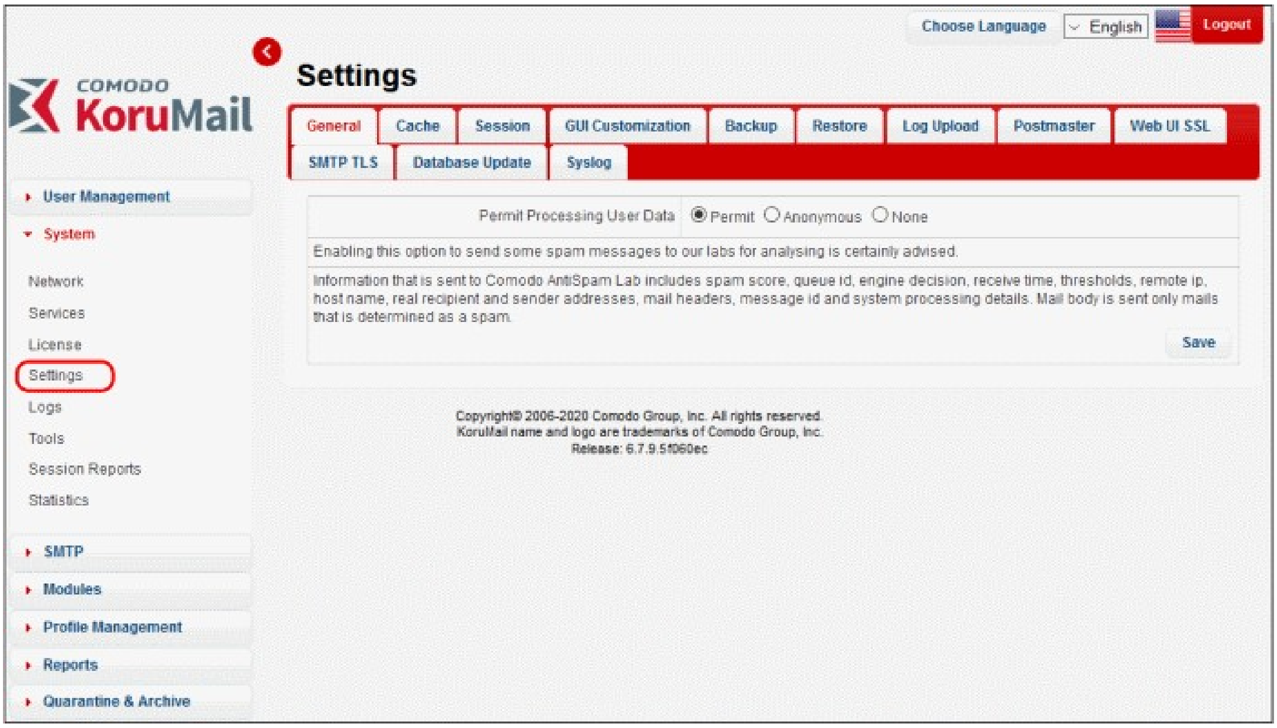
and/or sell copies of the Software, and to permit
persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT
LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

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

6.4 Configure System Settings

The 'Settings' interface allows you to configure all aspects of Korumail.

- Click 'System' > 'Settings' on the left menu:



Permit Processing User Data ● Permit ○ Anonymous ○ None

Enabling this option to send some spam messages to our labs for analysing is certainly advised.

Information that is sent to Comodo AntiSpam Lab includes spam score, queue id, engine decision, receive time, thresholds, remote ip, host name, real recipient and sender addresses, mail headers, message id and system processing details. Mail body is sent only mails that is determined as a spam.

Copyright© 2006-2020 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 6.7.9.5f060ec

Click the following links for more details:

- General
- Cache
- Session Settings
- GUI Customization
- System Backup
- System Restore
- Log Upload Settings

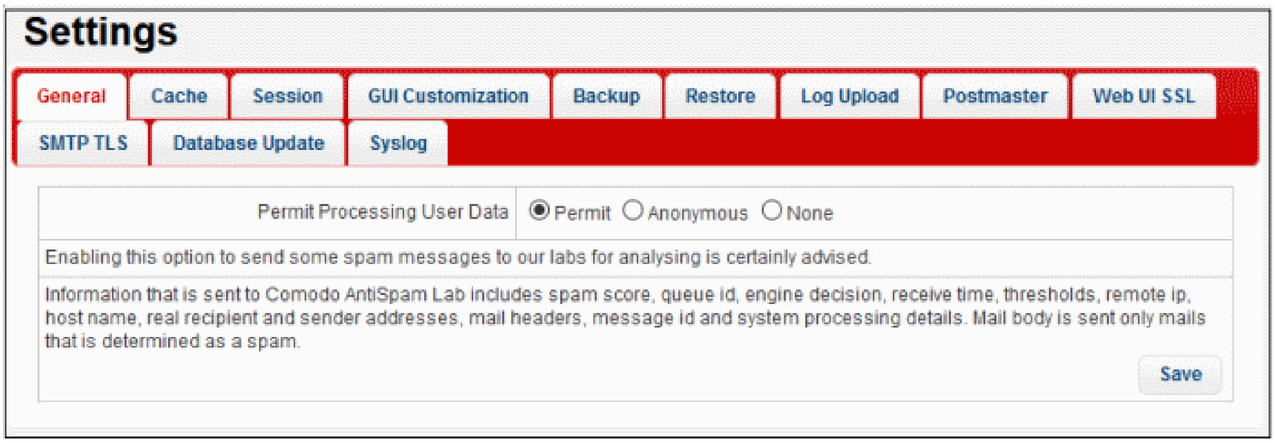
- Postmaster Settings
- Web UI SSL Certificate
- SMTP TLS Settings
- Update Database
- Syslog Server

6.4.1 System General Settings

The 'General' settings tab allows administrators to enable/disable the option to upload spam messages detected by KoruMail to Comodo labs for analytical purposes.

To open the 'General' settings interface,

- Click the 'System' tab from the left menu, then 'Settings' > 'General' tab.



Permit Processing User Data ● Permit ○ Anonymous ○ None

Enabling this option to send some spam messages to our labs for analysing is certainly advised.

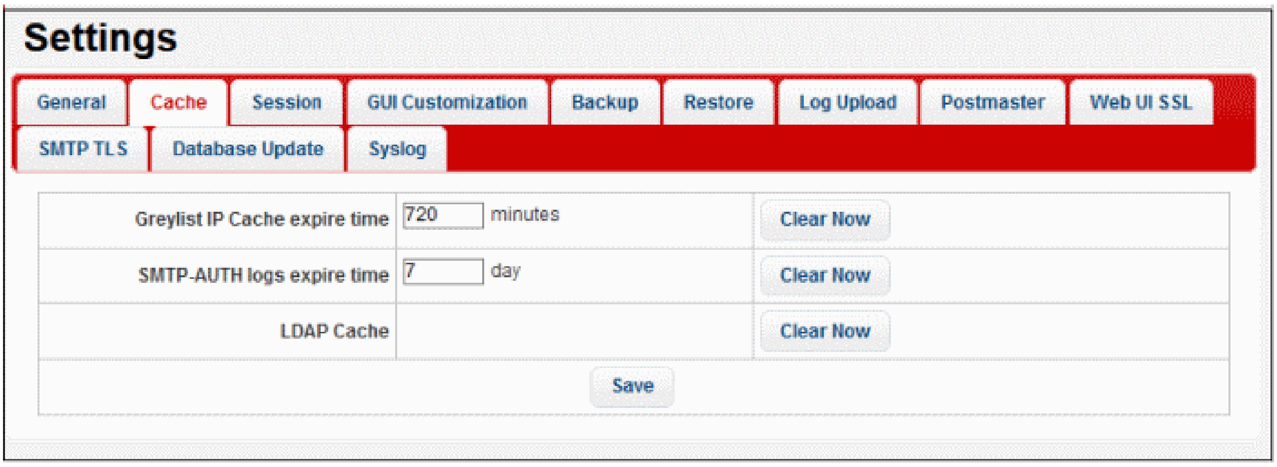
Information that is sent to Comodo AntiSpam Lab includes spam score, queue id, engine decision, receive time, thresholds, remote ip, host name, real recipient and sender addresses, mail headers, message id and system processing details. Mail body is sent only mails that is determined as a spam.

- **Permit Processing User Data:**
  - Permit - If enabled, spam messages detected by KoruMail will be uploaded to Comodo labs for analysis.
  - Anonymous - If enabled, spam messages detected by Korumail will be uploaded anonymously to Comodo labs for analysis.
  - None - If enabled, spam messages detected by Korumail, will not be uploaded to Comodo.
- Click 'Save' to apply your changes.

6.4.2 Cache Settings

The 'Cache' settings tab allow admins to set the cache expire time for greylisted IP addresses, SMTP Auth logs and LDAP.

- Click 'System' > 'Settings' on the left-menu
- Click the 'Cache' tab:



Greylist IP Cache expire time	720 minutes	Clear Now
SMTP-AUTH logs expire time	7 day	Clear Now
LDAP Cache		Clear Now

- **Greylist IP cache expire time**. The length of time that the IP address of an unknown sender will be held on the greylist.
  - Greylisting is a method of spam control whereby Korumail will initially reject any mail from an unknown sender. If the mail is legitimate, the originating server will resend the mail. Korumail will accept the mail on this second attempt and remove the sender from the greylist. This helps prevent junk mail as it is often too expensive for spam servers to send this second attempt.

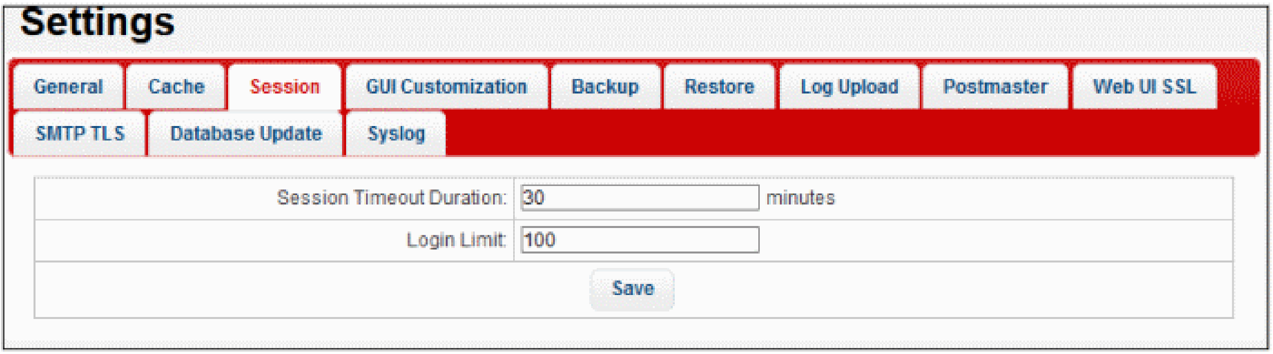
  If this time elapses with no response then the IP address returns to 'unknown' status. The next mail from the server will be subject to the greylisting process again.
- **SMTP AUTH logs expire time:** The end user authentication log details of SMTP clients are cached for the entered days and after that they are deleted.
- **LDAP Cache:** LDAP authentication details are cached and KoruMail does not query the LDAP server.

- Click the 'Clear Now' beside an item to clear the cache immediately.
- Click 'Save' to apply your changes.

6.4.3 Session Settings

The 'Session' settings tab allows administrators to configure the session inactivity period as well as to limit the number of times an administrator can log into the web console before the login password has to be changed.

- To open the 'Session' settings interface, click the 'System' tab on the left menu, then 'Settings' and 'Session' tab.



Session Timeout Duration: 30 minutes

Login Limit: 100

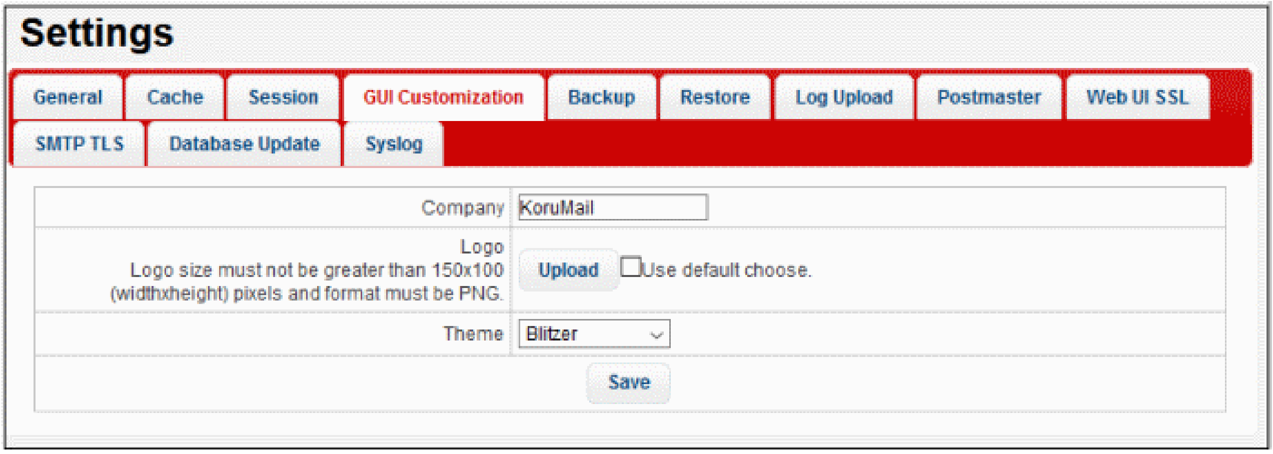
- **Session Timeout Duration:** Enter the period of session inactivity after which the administrator has to login again.
- **Login Limit:** Enter the number of users that can login to the portal at the same time.
- Click 'Save' to apply your changes.

6.4.4 GUI Customization

The 'GUI Customization' tab lets you customize the look and feel of KoruMail web console according to your preferences. You can also change the name and the logo to be displayed in the interface.

Open the 'GUI Customization' settings interface,

- Click the 'System' tab on the left menu, then 'Settings' > 'GUI Customization' tab



Company: KoruMail

Logo
Logo size must not be greater than 150x100 (widthxheight) pixels and format must be PNG.
□Use default choose.

Theme: Blitzer

- **Company:** Enter the name of the company to be displayed
- **Logo:** Upload your company logo. The logo will be shown in the interface to all users. Images should be in .png format and no larger than 150 px L x 100 px H.
  - Click ‘Upload’, choose file then again click ‘Upload’
  - To remove the logo, click the 'Clear' link.
  - Click 'Save' to upload the logo.
- **Theme:** The 'Themes' drop-down allows you to choose the colors and appearance of the GUI as you prefer *(Default = Blitzer Theme)*.
- Click 'Save' to apply your changes.

6.4.5 System Backup

The 'Backup' tab allow administrators to backup all configurations and logs. You can also automate the backup process by scheduling the backup dates and time. You can restore the stored back up in case the need arises.

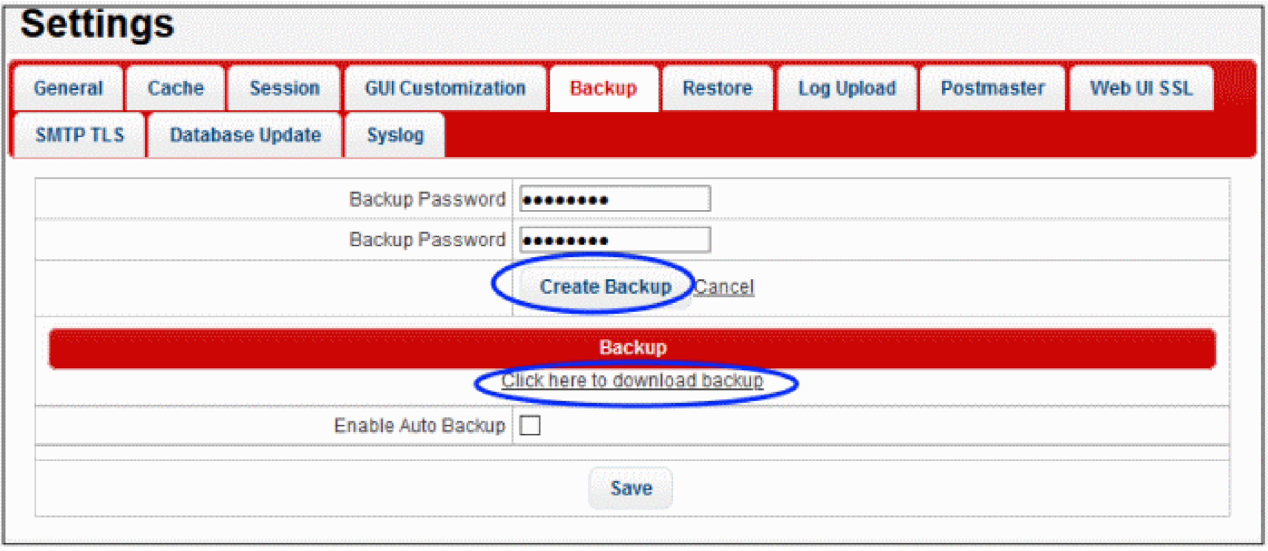
To open the 'Backup' settings interface,

- Click the 'System' tab on the left menu, then 'Settings' > 'Backup' tab.

Instant Backup

- To take an instant backup, enter the password, confirm it and click the 'Create Backup' button.

The system will backup the files and the backup download link will be displayed.



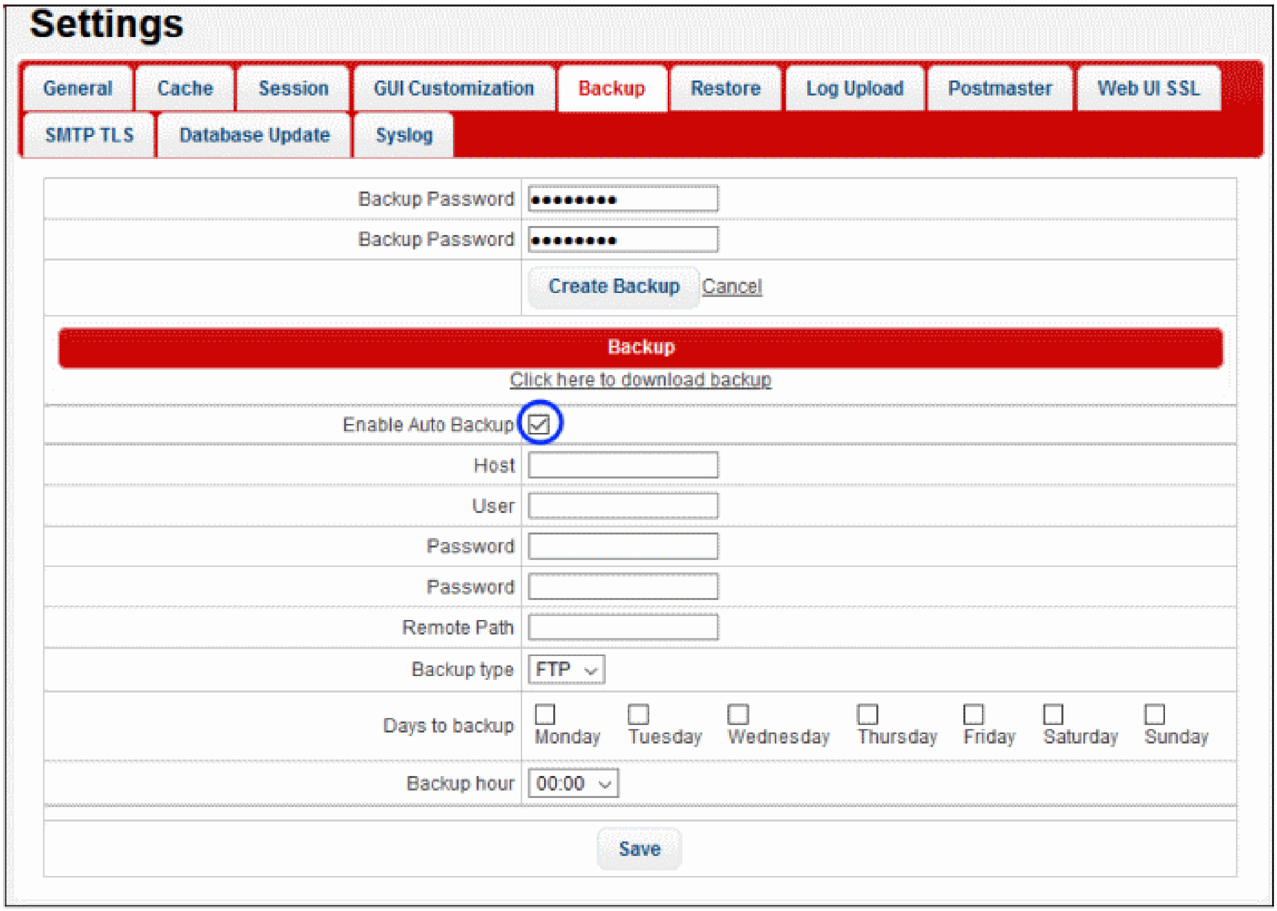
- 'Click here to download backup' – Click this link to save the backup.

The file is downloaded to your system. The 'Backup' file can be restored later from the '**Restore**' tab.

Scheduled Backup

You can automate the backup process by scheduling the jobs.

- To schedule a backup job, select the 'Enable Auto Backup' check box.



- **Host:** The name or IP of the system where the data should be backed up.
- **User:** The user name of the system
- **Password:** Enter the password to access the system

- **Remote Path:** Enter the remote path of the system including the folder name. Leaving the field blank means the backup will be uploaded to the default FTP folder.
- **Backup type:** Select the backup type from the drop-down. Currently only FTP option is available.
- **Days to backup:** Schedule the backup day(s) from the options.
- **Backup hour:** Select the hour when the scheduled backup should run on the selected backup day(s)

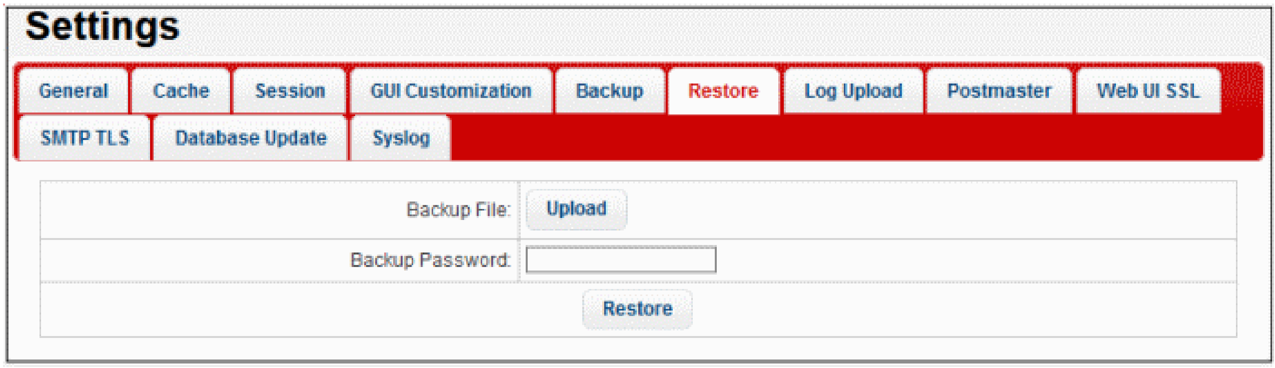
- Click 'Save'. The scheduled job will be saved. To change the schedule or the backup location, edit the settings accordingly and click 'Save'.

6.4.6 System Restore

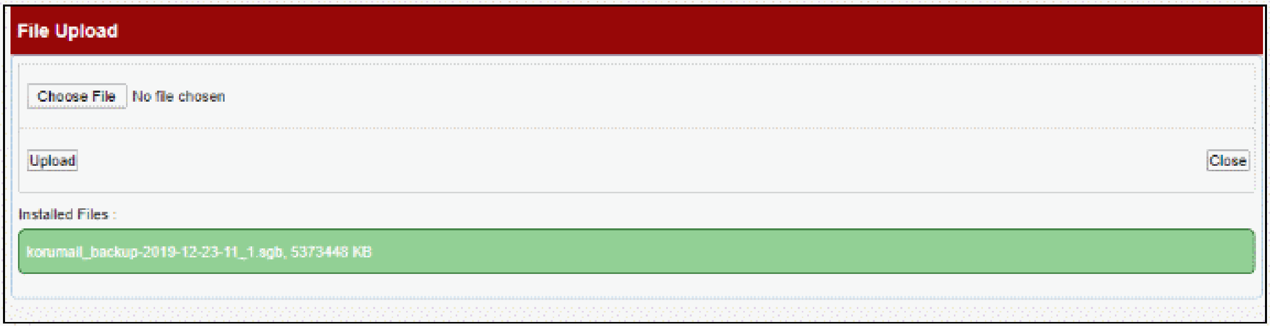
You can restore KoruMail configurations and logs using the 'Restore' feature. Please note that for a restore operation to be completed, KoruMail has to be rebooted.

To open the 'Restore' settings interface,

- Click the 'System' tab on the left menu, then 'Settings' > 'Restore' tab

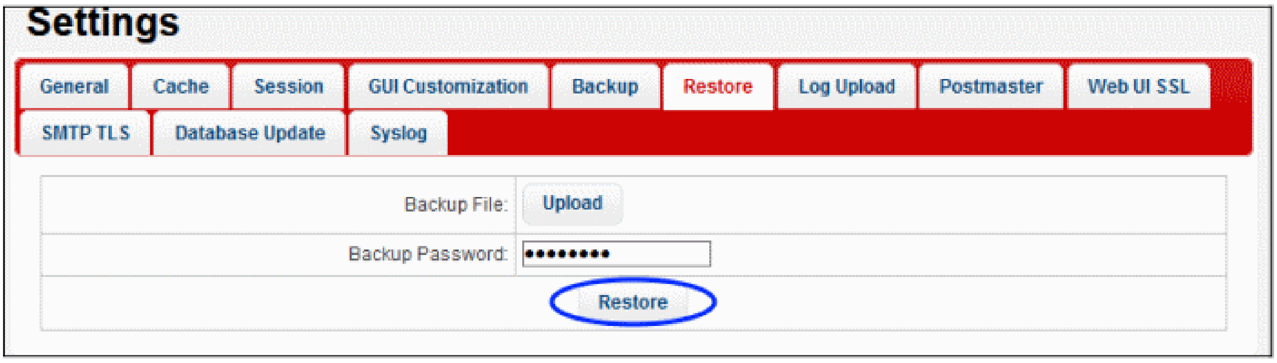


- Backup Password – Enter the password that you provided while backing up.
- Click the 'Upload' button
- Click ‘Choose File’, navigate to the location and click ‘Upload’



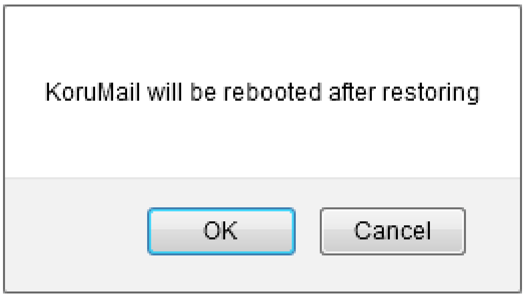
korumail_backup-2019-12-23-11_1.sgb, 5373448 KB

- Click ‘Restore’



Backup File:	Upload
Backup Password:	••••••••

The console has to be rebooted to complete the restore operation.


KoruMail will be rebooted after restoring

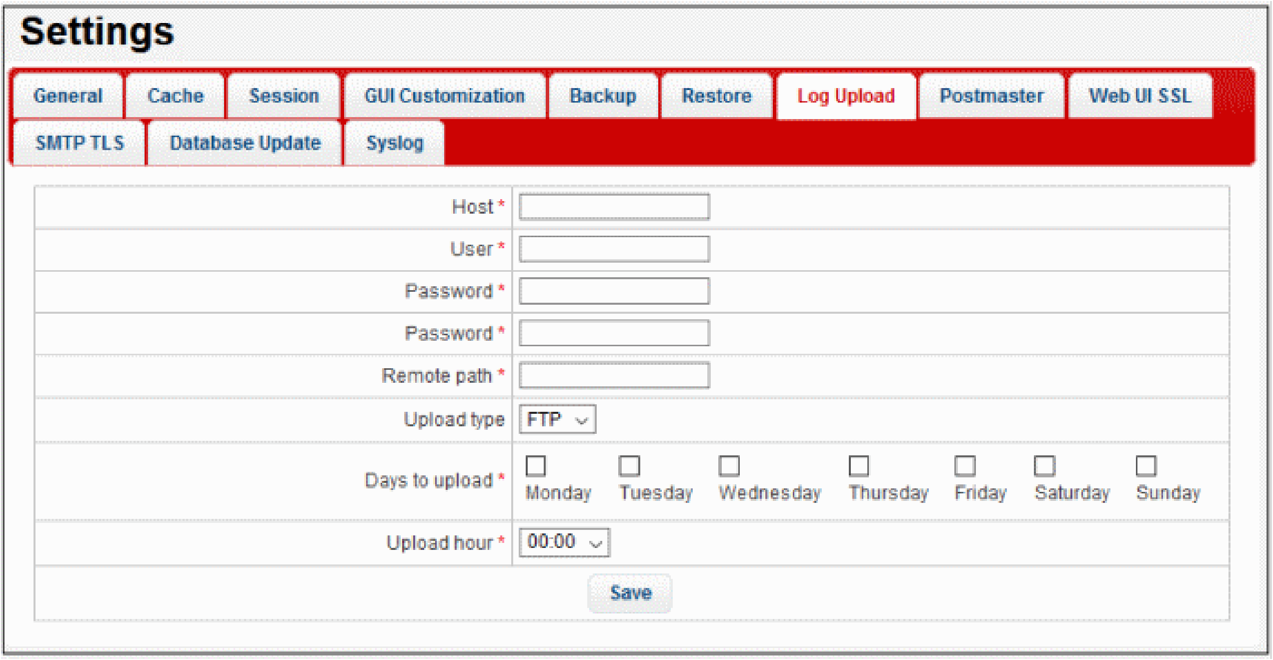
- Click 'OK' to confirm.

6.4.7 Log Upload Settings

The 'Log Upload' tab allows admins to configure the automated upload of various types of KoruMail logs.

To open the 'Log Upload' settings interface,

- Click the 'System' tab on the left menu, then 'Settings' > 'Log Upload' tab



Host *	
User *	
Password *	
Password *	
Remote path *	
Upload type	FTP
Days to upload *	□ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday
Upload hour *	00:00

- **Host:** The name or IP of the system where the logs should be uploaded.

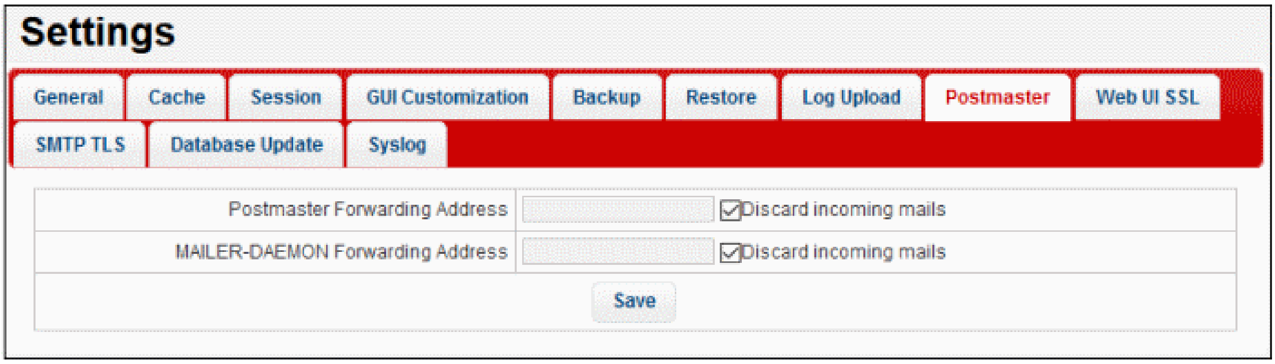
- **User:** The user name of the system
- **Password:** Enter the password to access the system
- **Remote Path:** Enter the remote path of the system including the folder name. Leaving the field blank means the logs will be uploaded to the default FTP folder.
- **Upload type:** Select the upload type from the drop-down. Currently only FTP option is available.
- **Days to upload:** Schedule the upload day(s) from the options.
- **Upload hour:** Select the hour when the scheduled upload should run on the selected upload day(s)
- Click 'Save'. The scheduled job will be saved. To change the schedule or the upload location, edit the settings accordingly and click the 'Save' button.

6.4.8 Postmaster Settings

- It is a statutory requirement to set a postmaster address to which email errors will be directed for an SMTP domain. Postmaster addresses are commonly targeted by spammers to send unsolicited messages.
- Similarly, spammers also use the mailer-daemon route to flood users with spam messages.
- KoruMail allow administrators to forward these to other addresses and /or reject emails sent to these addresses.

To open the 'Postmaster' settings interface,

- Click the 'System' tab on the left menu, then click 'Settings' > 'Postmaster' tab.



Postmaster Forwarding Address ☑Discard incoming mails

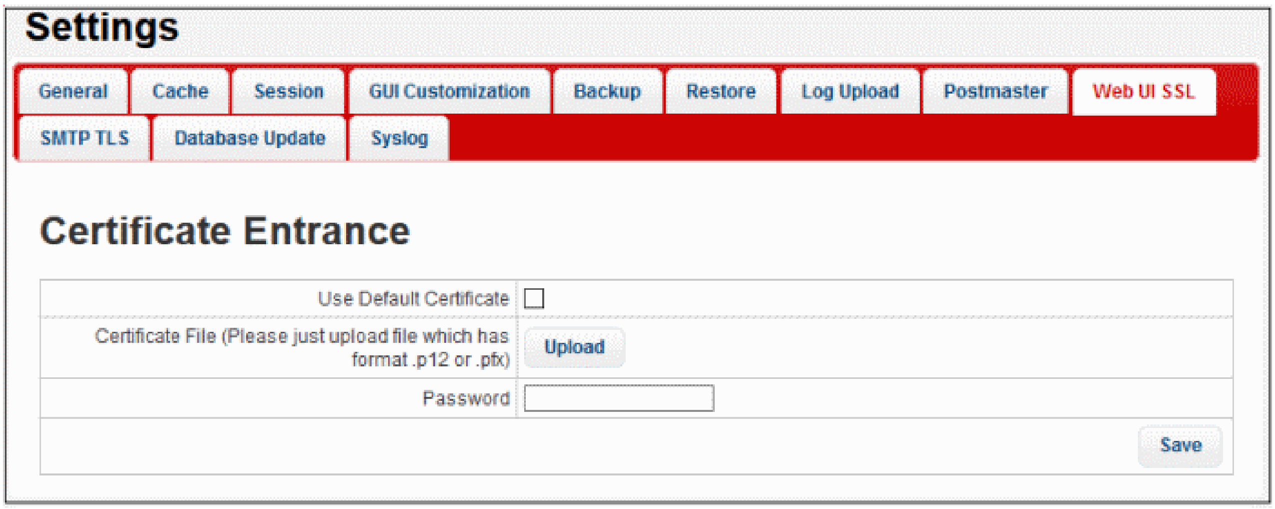
MAILER-DAEMON Forwarding Address ☑Discard incoming mails

- **Postmaster Forwarding Address:** Enter the forwarding address to which the email to postmaster are directed.
- **MAILER-DAEMON Forwarding Address:** Enter the forwarding address to which the Mailer Daemon notifications are to be directed.
- **Discard incoming mails:** Select the check box if the mails to the forwarded address is to be rejected.
- Click the 'Save' button.

6.4.9 Web UI SSL

An SSL certificate is required to provide secure, HTTPS access to your KoruMail admin console. You can choose to upload an SSL certificate from this interface or in the **dashboard**. The latest certificate that you uploaded from either of the interfaces is active.

- Click System' on the left then ‘Settings’ > ‘Postmaster’



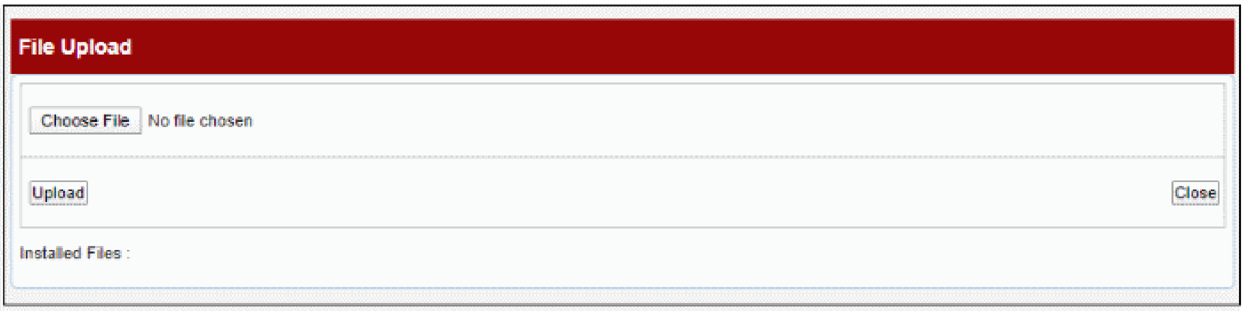
Certificate Entrance

Use Default Certificate □

Certificate File (Please just upload file which has format .p12 or .pfx) Upload

Password

- **Use Default Certificate** – This is a KoruMail self-signed certificate. KoruMail will automatically install a self-signed certificate on your console. Your connection to the console will be just as secure as above, but your browser will show error messages as the certificate is not signed by a trusted certificate authority. You can bypass these errors and create an exception in your browser to avoid these messages in future.
- **Certificate File** - Upload a certificate you have on file. Ideally, this will be a certificate which you have obtained from a trusted certificate authority. Using such a certificate means you will not see browser error messages when you access the admin console.
  - Click ‘Upload’



No file chosen

Installed Files :

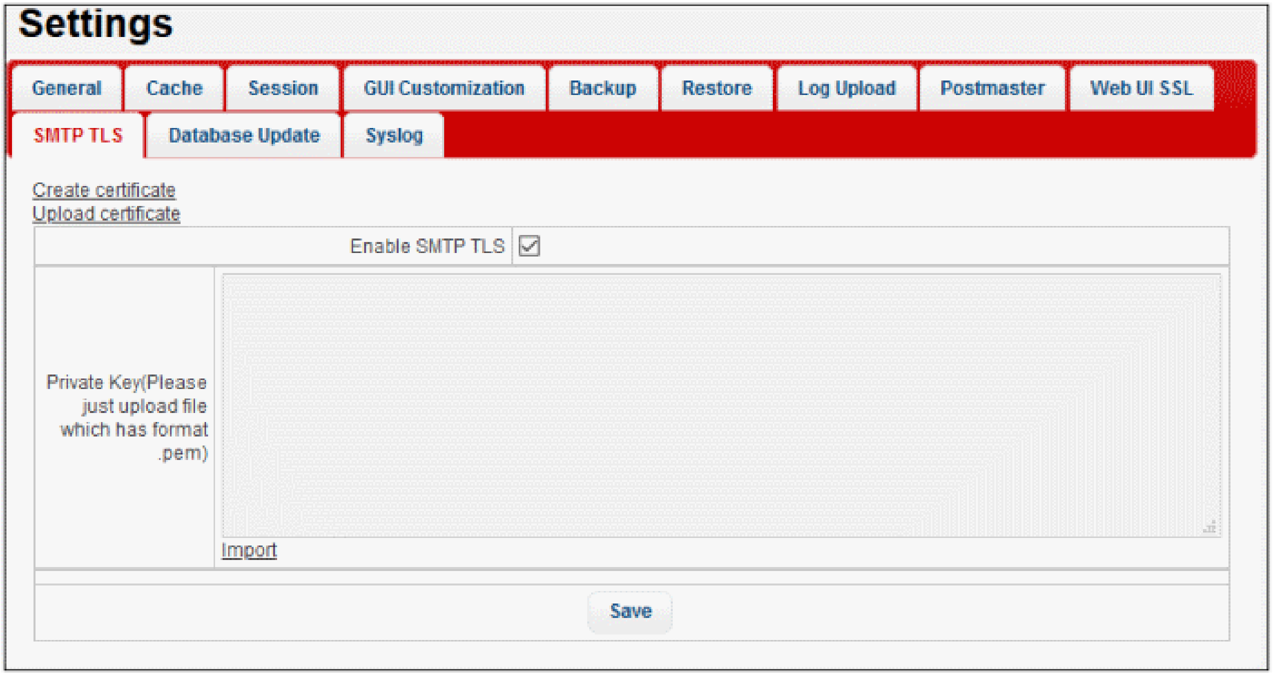
  - Click ‘Choose File’ then select the cert file and click ‘Upload’
- Enter the certificate password in the KoruMail interface
- Click ‘Save’

6.4.10 SMTP TLS Settings

- Transport layer security (TLS) is a cryptographic protocol which provides encryption and privacy for email traffic.
- You need to install a certificate on your mail server in order to enable TLS.
- The 'SMTP TLS' area lets you create a new certificate or upload an existing certificate.

Open the 'SMTP TLS' settings interface

- Click 'System' > 'Settings' > 'SMTP TLS' tab.

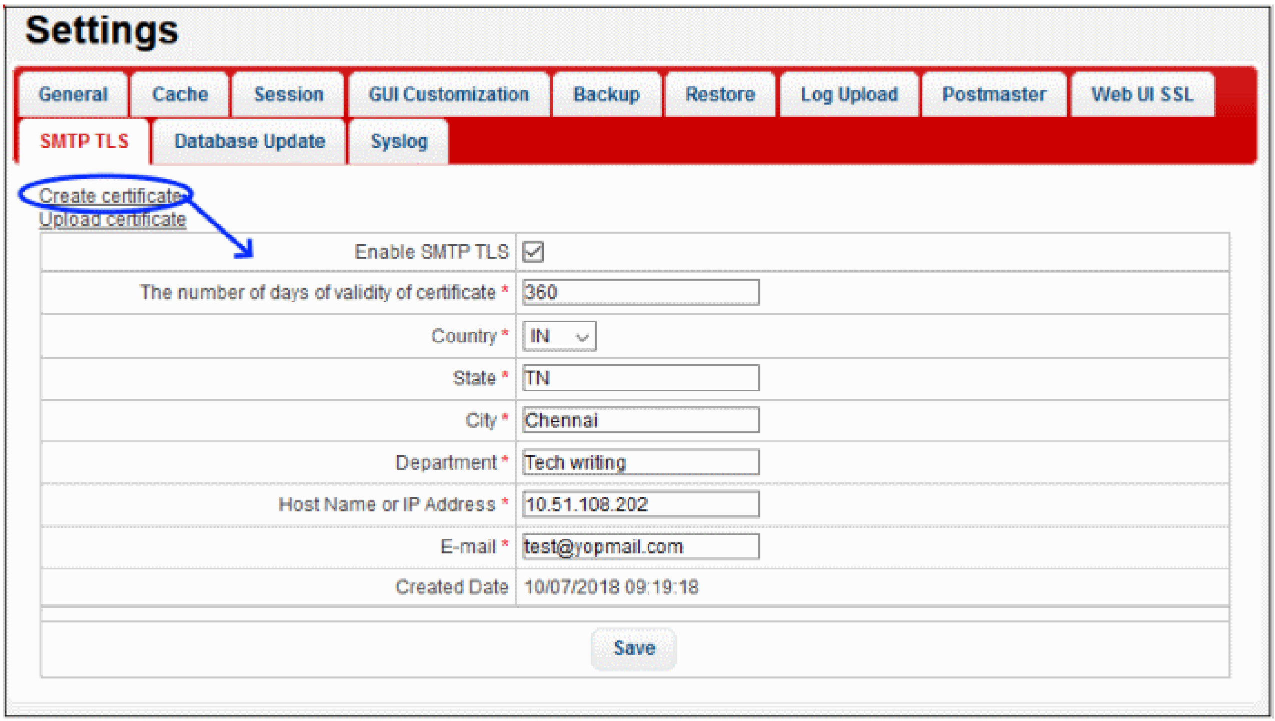


Enable SMTP TLS	☑
Private Key(Please just upload file which has format .pem)	

- Enable SMTP TLS – Select to activate SMTP TLS

Create a certificate

- Click the 'Create certificate' link and enter the mandatory details:



Enable SMTP TLS	☑
The number of days of validity of certificate *	360
Country *	IN
State *	TN
City *	Chennai
Department *	Tech writing
Host Name or IP Address *	10.51.108.202
E-mail *	test@yopmail.com
Created Date	10/07/2018 09:19:18

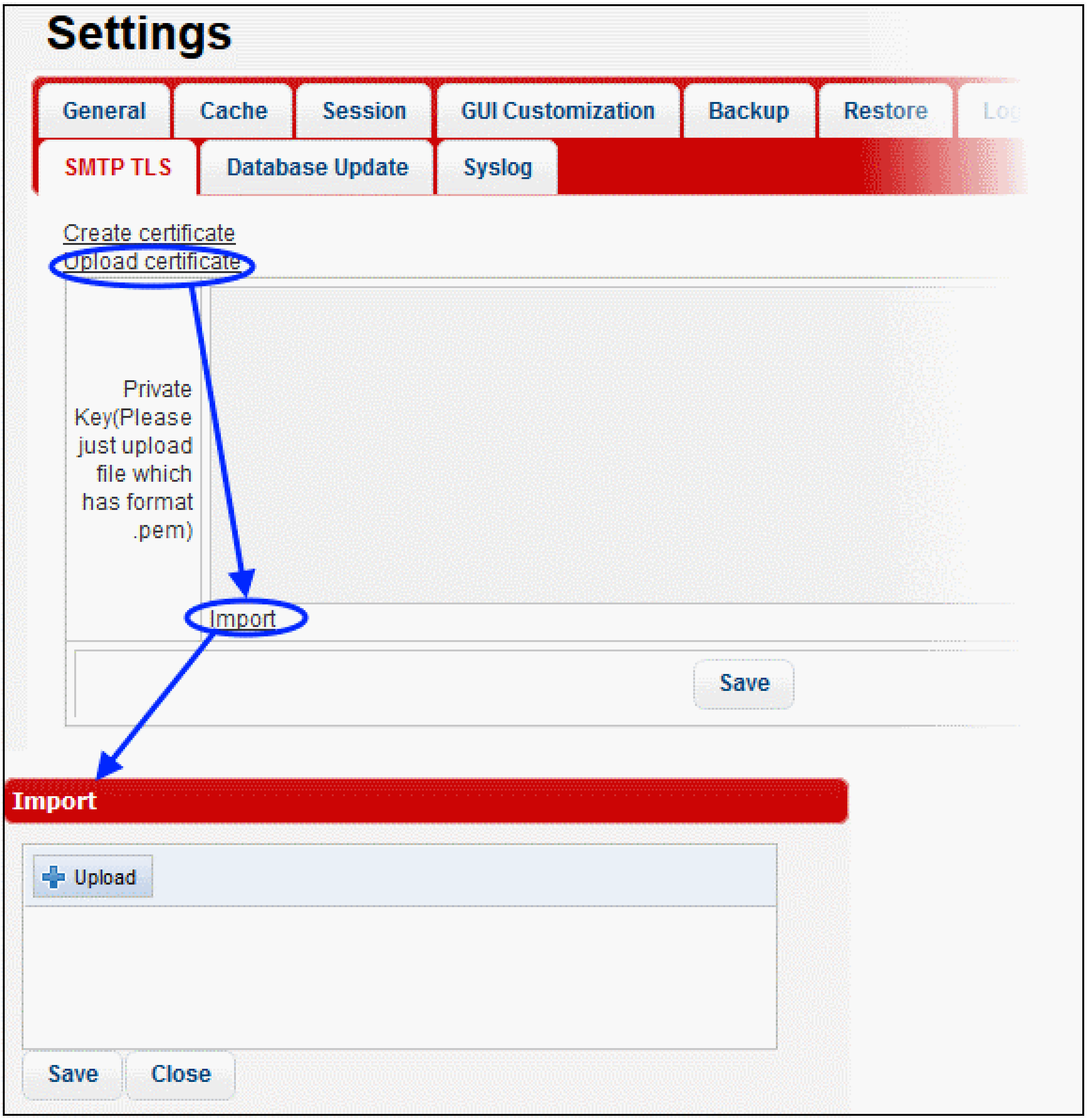
- Validity - Specify the term length of the certificate in days. Note - certificates for public-facing websites have a maximum term length of 720 days.
- Country - Select the two-character code for your country.
- State - Two character code of the state/province in which your organization is located.
- City/Locality - The name of the city in which your organization is located
- Department - Name of the department

- E-mail - Your contact email address
- Host or IP address - Type the domain, hostname or IP address of the server you want to secure

- Click 'Save' to create the certificate.

Upload a certificate

- Click 'Upload certificate' then click 'Import'



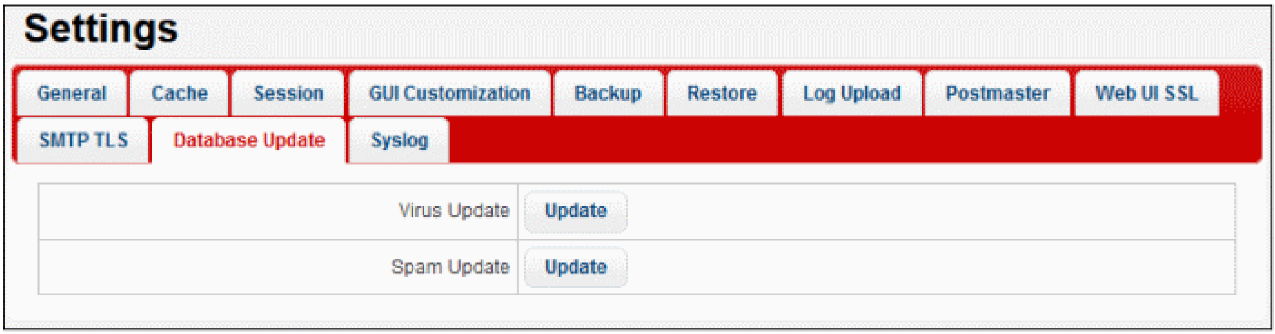
- Click the upload button to browse for the certificate you wish to import
- Click 'Save'.

6.4.11 Update Database

KoruMail updates virus and spam databases once per day. If required, the databases can be updated instantly from 'Database Update' tab.

To open the 'Database Update' settings interface,

- Click the 'System' tab on the left menu then click 'Settings' > 'Database Update'.



Virus Update

Spam Update

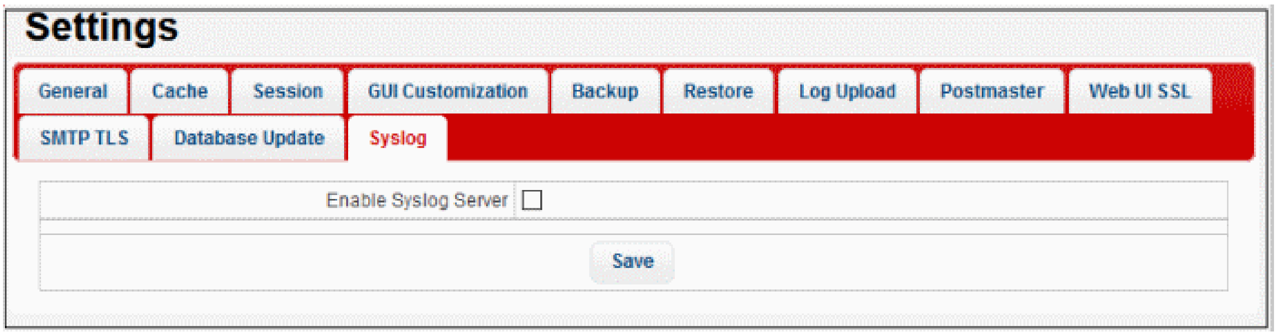
- **Virus Update:** Click the 'Update' button to update the virus database
- **Spam Update:** Click the 'Update' button to update the spam database

6.4.12 Syslog Server

KoruMail has the ability to forward logs pertaining to various operations and configuration changes to a remote Syslog server. Administrators can integrate the module with the remote Syslog server used by the organization for easy analysis of the logs and to conserve disk space.

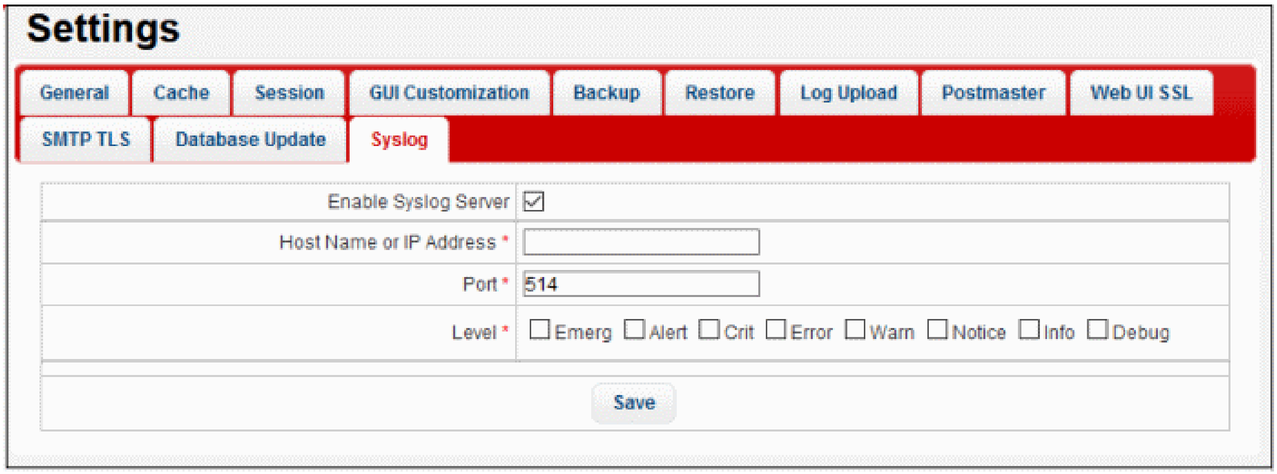
To open the 'Syslog' settings interface,

- Click the 'System' tab on the left menu then click 'Settings' > 'Syslog' tab



Enable Syslog Server □

- **Enable Syslog Server:** Select the check box to store the logs in a remote server. If selected, the details of the Syslog server should be entered in the fields.



Enable Syslog Server	☑
Host Name or IP Address *	
Port *	514
Level *	□ Emerg □ Alert □ Crit □ Error □ Warn □ Notice □ Info □ Debug

- **Host Name or IP Address:** Enter the host name or the IP address of the remote logging server to which the logs are to be passed.

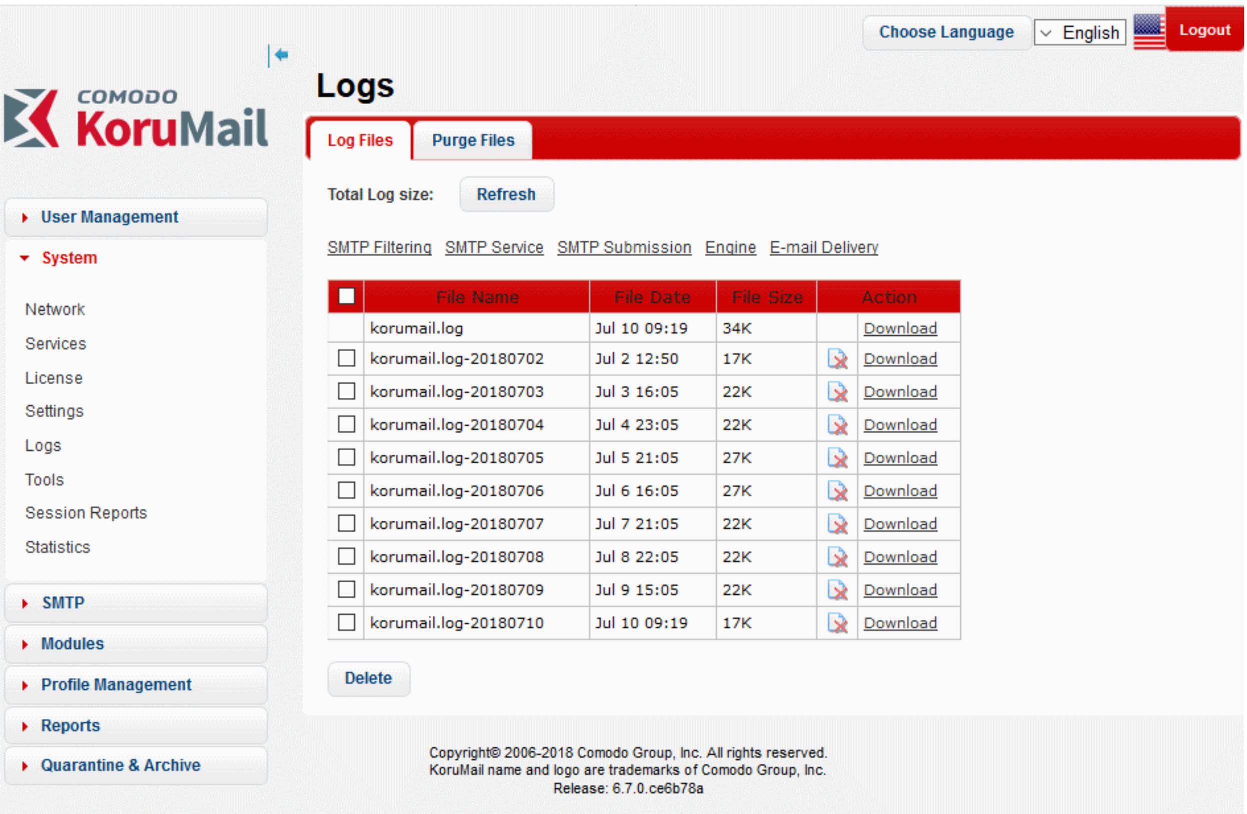
- **Port:** Enter the port number through which the server receives the logs. Default is 514.
- **Level:** Select the log level that has to be passed to the remote logging server.
- Click 'Save'

6.5 Logs

KoruMail stores log files for various activities and connections in the local database and uploads the logs to the server as specified under 'System' > 'Settings' > 'Log Upload'. Administrators can download logs from the database through the 'Logs' interface. The logs interface also allows administrators to delete unwanted logs.

To open the 'Logs' interface,

- Click the 'System' tab and then the 'Logs' sub tab.



Logs

Total Log size:

SMTP Filtering SMTP Service SMTP Submission Engine E-mail Delivery

☐	File Name	File Date	File Size	Action
	korumail.log	Jul 10 09:19	34K	Download
☐	korumail.log-20180702	Jul 2 12:50	17K	✗ Download
☐	korumail.log-20180703	Jul 3 16:05	22K	✗ Download
☐	korumail.log-20180704	Jul 4 23:05	22K	✗ Download
☐	korumail.log-20180705	Jul 5 21:05	27K	✗ Download
☐	korumail.log-20180706	Jul 6 16:05	27K	✗ Download
☐	korumail.log-20180707	Jul 7 21:05	22K	✗ Download
☐	korumail.log-20180708	Jul 8 22:05	22K	✗ Download
☐	korumail.log-20180709	Jul 9 15:05	22K	✗ Download
☐	korumail.log-20180710	Jul 10 09:19	17K	✗ Download

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 'Logs' interface has the following tabs:

- **Log Files**
- **Purge Files**

6.5.1 Log Files

The 'Log Files' tab contains logs of different activities and connection attempts. These include:

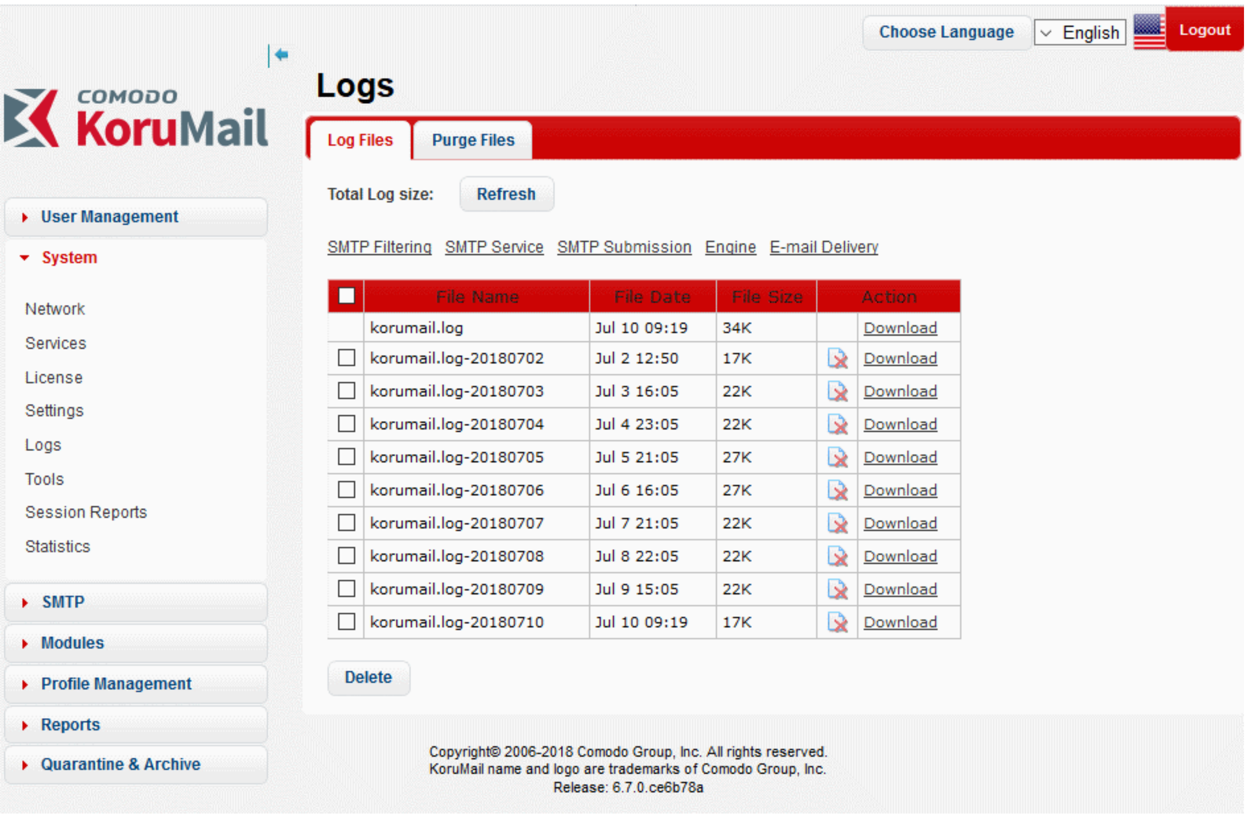
- SMTP Filtering
- SMTP Services
- SMTP Submission
- Engine Activities
- E-mail Delivery

Each logs contains granular details about a particular activity. You can download specific logs and delete unwanted logs from this interface.

Tip: You can also view real-time logs in the 'Reports' interface. See **Reports** for more details.

To open the 'Log Files' interface

- Click the 'System' > 'Logs' > 'Log Files' tab:



□	File Name	File Date	File Size	Action
	korumail.log	Jul 10 09:19	34K	Download
□	korumail.log-20180702	Jul 2 12:50	17K	Download
□	korumail.log-20180703	Jul 3 16:05	22K	Download
□	korumail.log-20180704	Jul 4 23:05	22K	Download
□	korumail.log-20180705	Jul 5 21:05	27K	Download
□	korumail.log-20180706	Jul 6 16:05	27K	Download
□	korumail.log-20180707	Jul 7 21:05	22K	Download
□	korumail.log-20180708	Jul 8 22:05	22K	Download
□	korumail.log-20180709	Jul 9 15:05	22K	Download
□	korumail.log-20180710	Jul 10 09:19	17K	Download

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

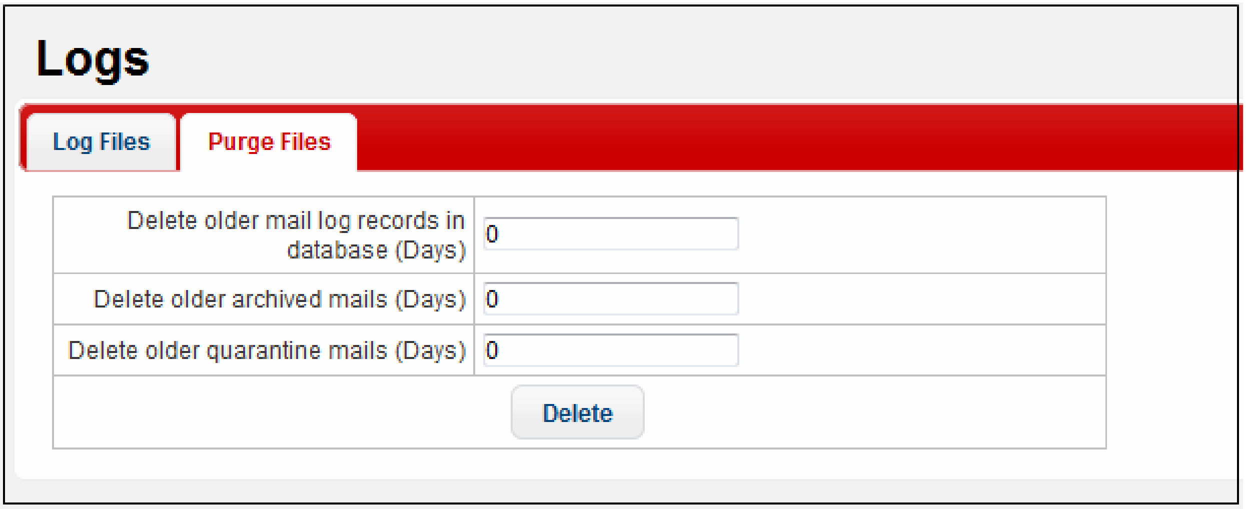
- Click 'Refresh' to reload the list and view the latest logs.
- Use the links above the table to change the type of log files shown in the list

6.5.2 Purge Files

The purge files interface lets you configure how long to keep log files, archived mails and quarantined mails. Items older than the period specified will be automatically deleted.

To open the 'Purge Files' interface,

- Click 'System'> 'Logs' > 'Purge Files' tab:



Logs

Delete older mail log records in database (Days)	0
Delete older archived mails (Days)	0
Delete older quarantine mails (Days)	0

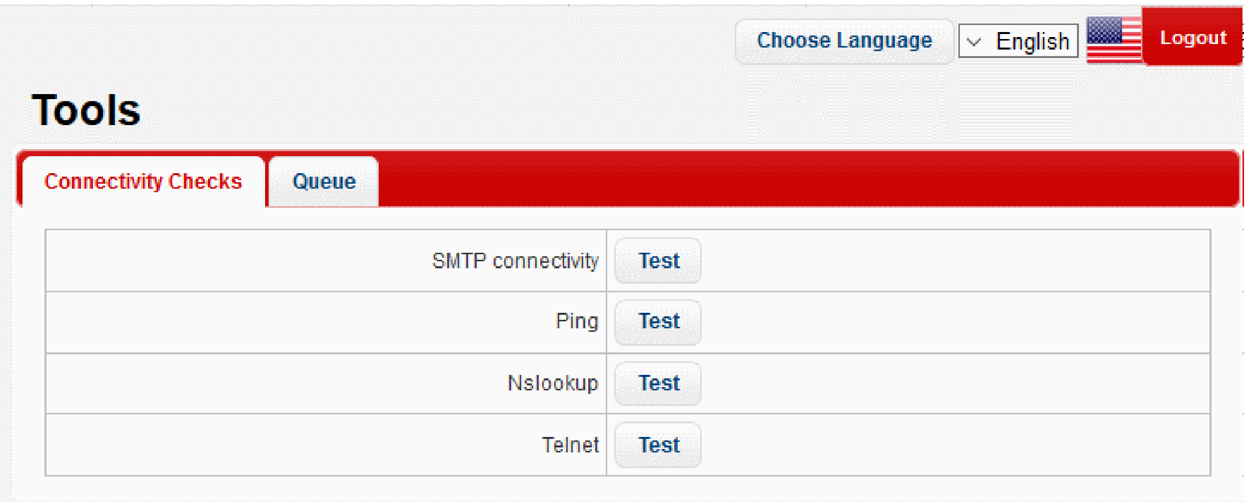
- Delete older mail log records in database (Days) - Specify the number of days to store the log files. The log files older than the days specified here will be automatically deleted.
- Delete older archived mails (Days) - Specify the number of days for which the quarantined mails are to be retained in the local database. Mails older than the days specified here, will be automatically deleted.
- Delete older quarantine mails (Days) - Specify the number of days for which the quarantined mails are to be preserved in the local database for review by the administrators. Mails older than the days specified here, will be automatically deleted.
- To instantly remove all the saved logs, archived mails and quarantined mails, click 'Delete'.

6.5.3 Tools

KoruMail has built-in tools to quickly check the connectivity to the mail servers and clients and to clear the mails in the SMTP delivery queue.

To open the 'Tools' interface,

- Click the 'System' tab on the left menu and then click 'Tools' from the sub-menu.



The 'Tools' interface has two tabs:

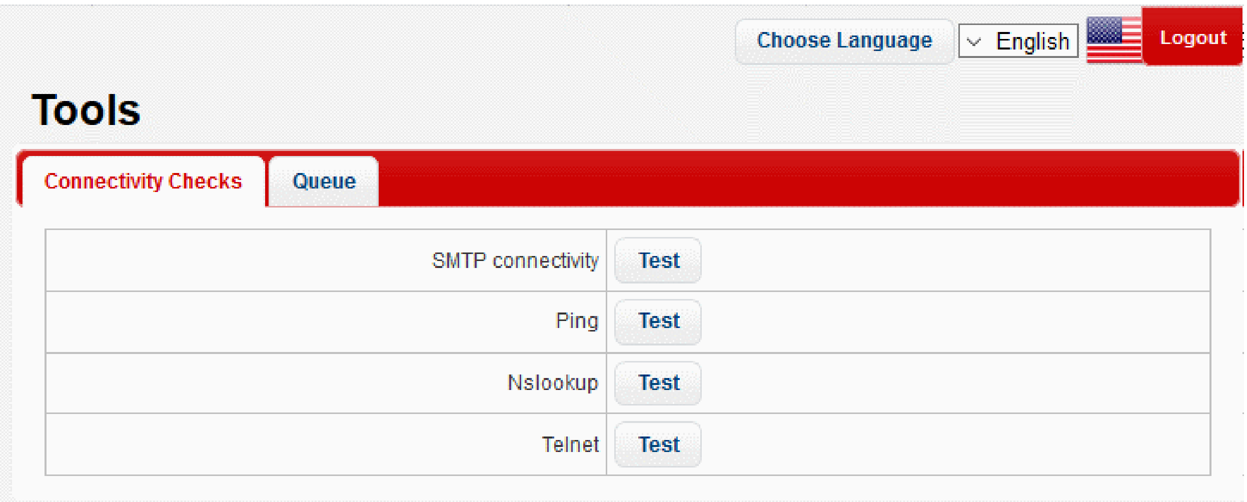
- Connectivity Check
- SMTP Queue

6.5.3.1 Check Connectivity

Allows administrators to check the connection status of KoruMail to external mail servers and clients, make name server lookups and check telnet connectivity to a remote host.

To open the 'Connectivity Checks' interface,

- Click the 'System' tab on the left menu then 'Tools' then the 'Connectivity Checks' tab.



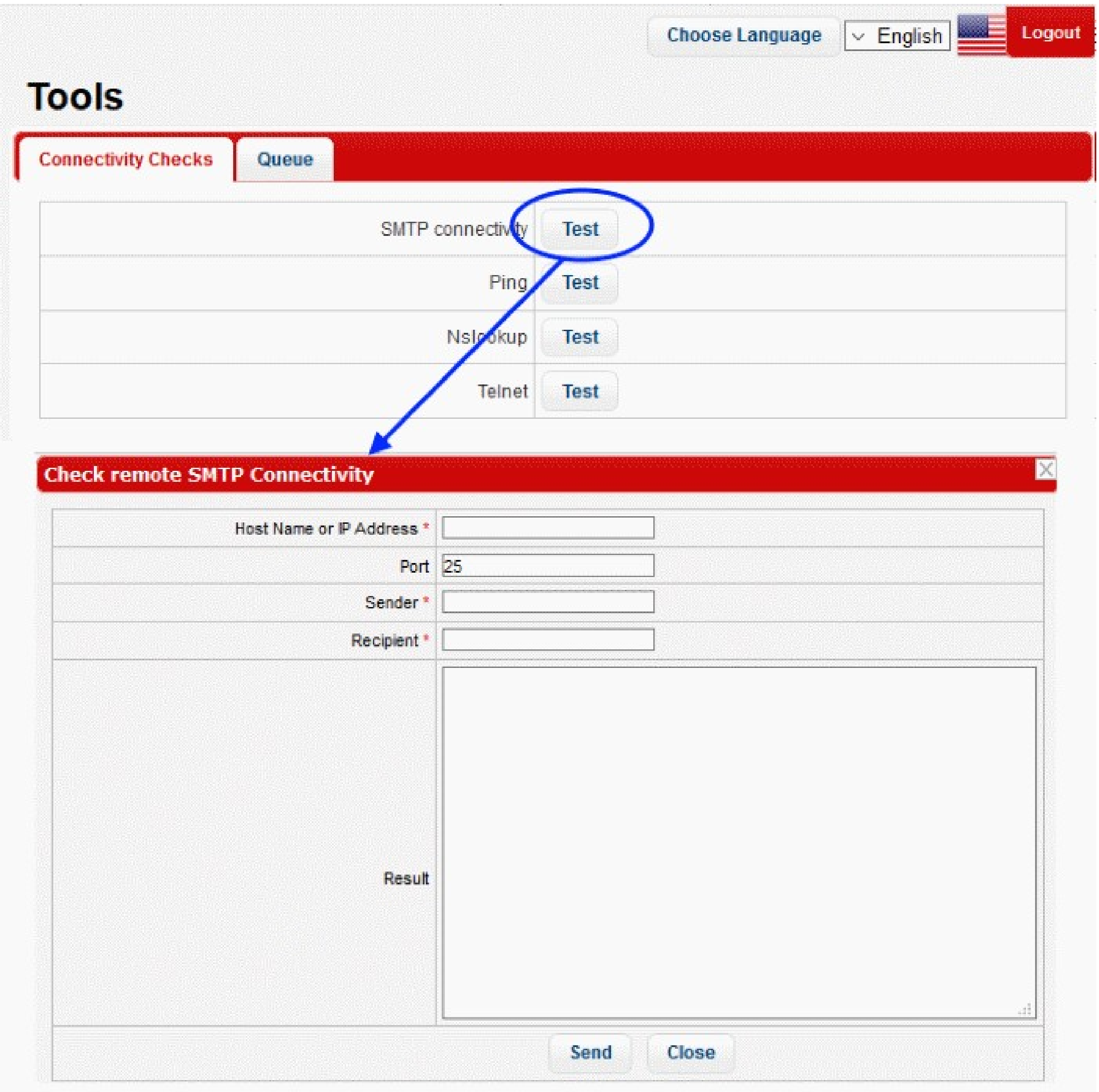
SMTP connectivity	Test
Ping	Test
Nslookup	Test
Telnet	Test

You can check for the following:

- Connectivity to a remote SMTP server
- Connectivity to a remote host
- Name server lookup for a remote host or a mail server
- Telnet connectivity for a remote host

To check connection to a SMTP server

- Click 'Test' beside 'SMTP connectivity' from the 'Connectivity Checks' interface.



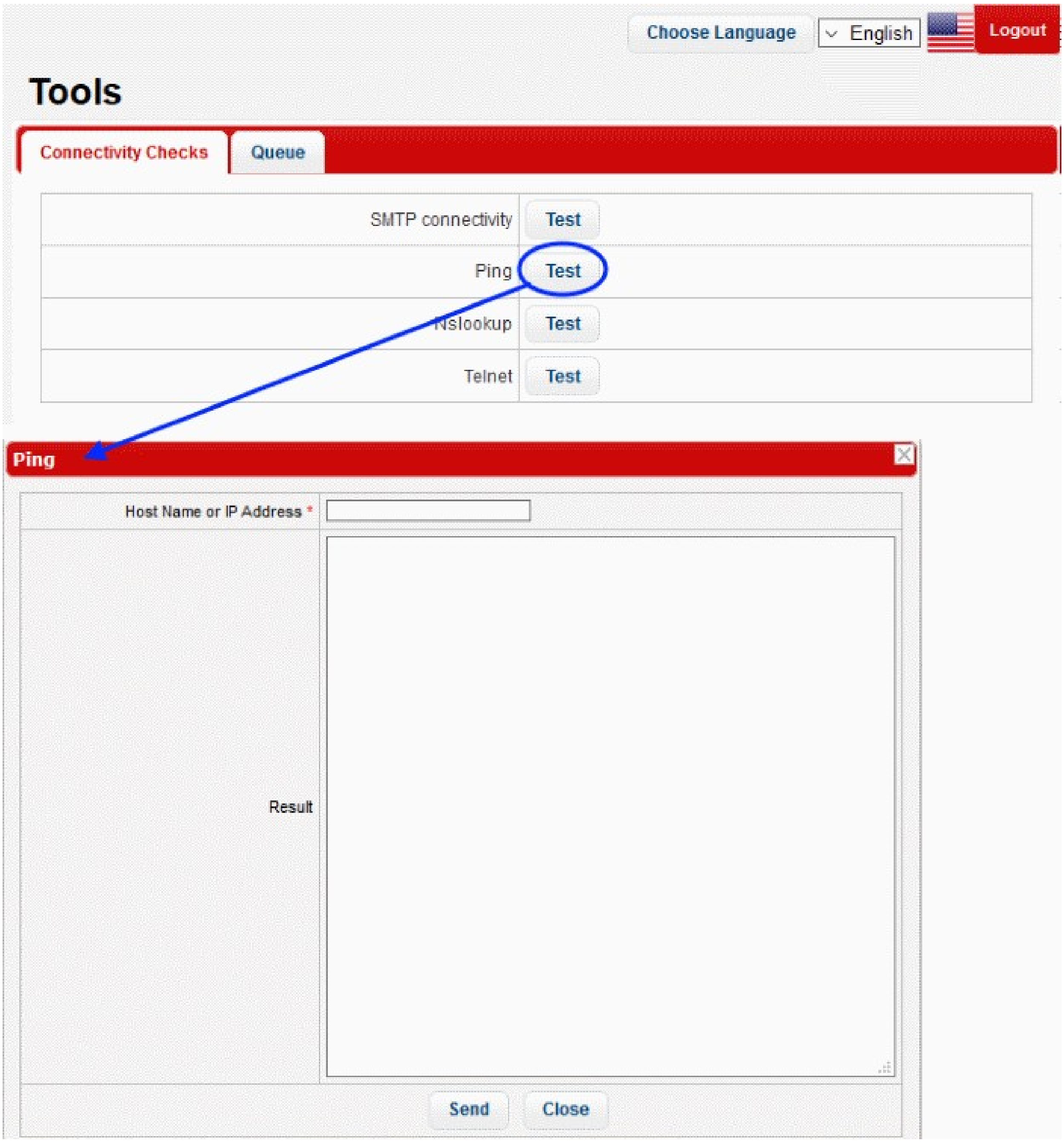
The 'Check remote SMTP Connectivity' interface will appear.

- Enter the details of the external or remote mail server as given below:
  - Host Name or IP Address - The hostname or IP address of the remote SMTP server
  - Port - The port used by the server for SMTP connections. This depends on whether or not the server uses SSL for SMTP connections (Default = 25)
  - Sender - A valid email address at the local SMTP server to send a test mail to the remote server for testing
  - Recipient - A valid email address at the remote SMTP server to which the test email needs to be sent
- Click 'Send'

KoruMail will send a test email to check the connectivity and display the results in the 'Result' field.

To check connectivity to a remote host

- Click 'Test' beside 'Ping' from the 'Connectivity Checks' interface.



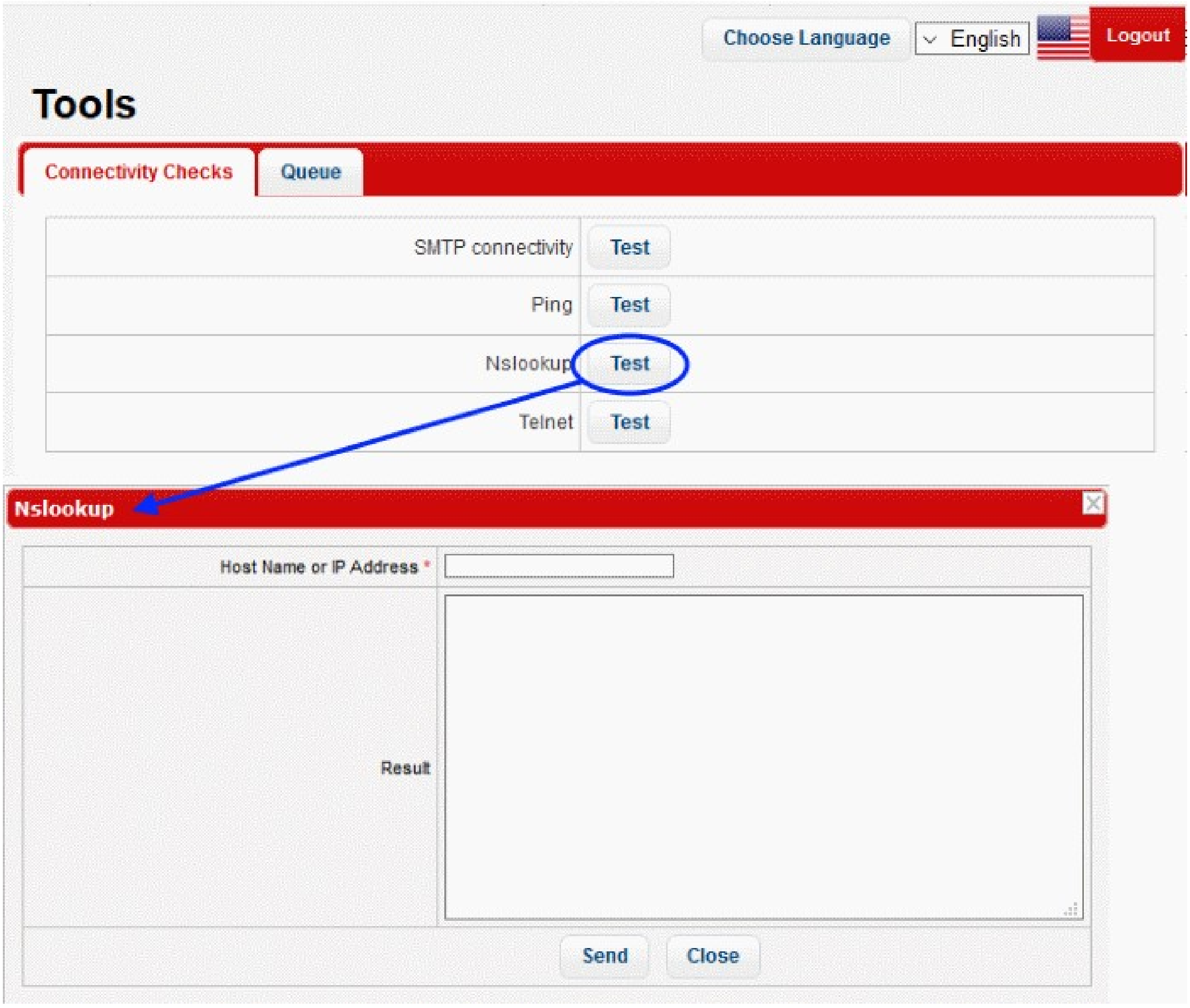
The 'Ping' interface will appear.

- Enter the hostname or IP address of the remote host to check whether it can be reached by KoruMail
- Click 'Send'

KoruMail will ping the remote host and display the results in the 'Result' field.

To lookup name server for a remote host

- Click 'Test' beside 'Nslookup' from the 'Connectivity Checks' interface.



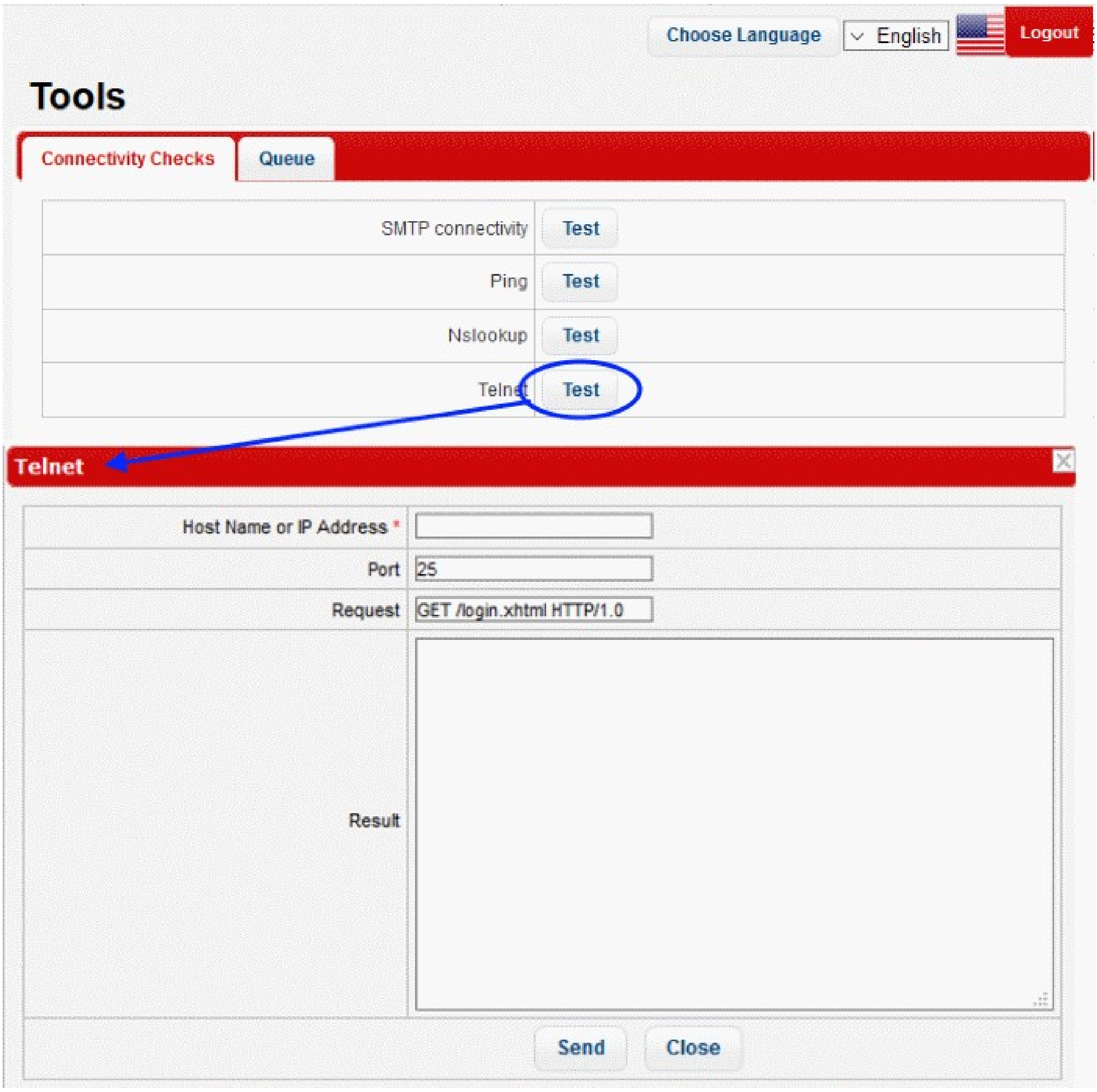
The 'Nslookup' interface will appear.

- Enter the hostname or IP address of the remote host to check the domain name associated with it
- Click 'Send'

KoruMail will lookup the name server to identify the domain name associated with the IP address or the hostname and display the results in the 'Result' field.

To check Telnet connectivity to a remote host

- Click 'Test' beside 'Telnet' from the 'Connectivity Checks' interface.



Port: 25

Request: GET /login.xhtml HTTP/1.0

The 'Telnet' interface will appear.

- Enter the hostname or IP address of the remote host to check whether it is connecting through Telnet protocol
- Enter the port use by the remote host for Telnet connections (Default = 25).
- KoruMail send a request 'GET /login.xhtml HTTP/1.0' to the remote host to check the connectivity, If you wish to send a custom request, edit the same in the 'Request' field.
- Click 'Send'

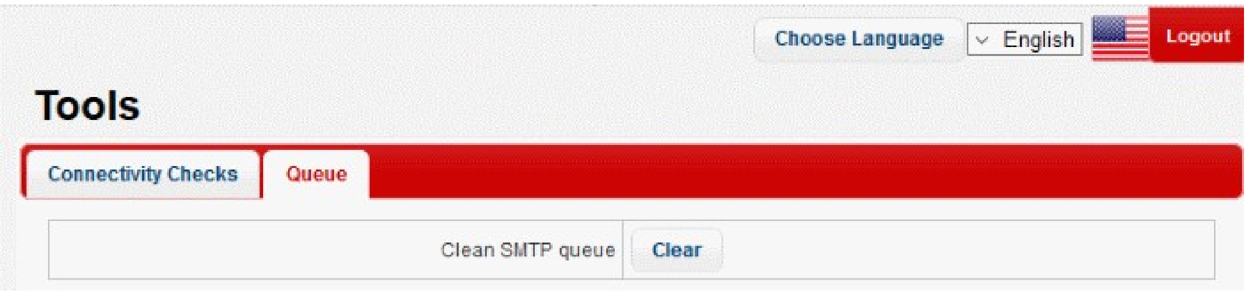
KoruMail will send the request to the remote host for checking the Telnet connectivity and display the results in the 'Result' field.

6.5.3.2 Clear SMTP Queue

The Queue tab under the Tools interface allows the administrator to remove the mails that are in queue for SMTP forwarding.

To clear the SMTP queue

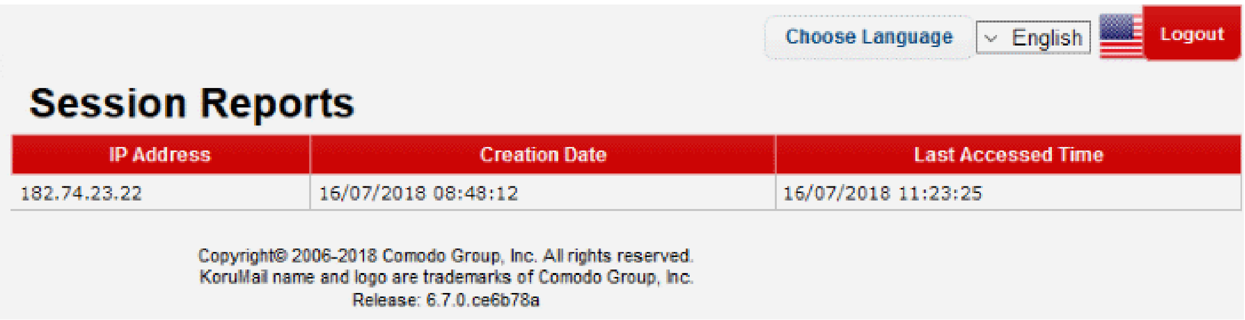
- Click the 'System' tab from the left, then 'Tools' > 'Queue' tab.



- Click 'Clear' beside 'CLEAN SMTP queue'.

6.6 Session Reports

- Click the 'System' tab from the left, then click 'Session Reports'.
- Session reports show all currently active logins.
- Details include the IP address of the user, the last login time and the details of last activity performed on the user interface.



Session Reports

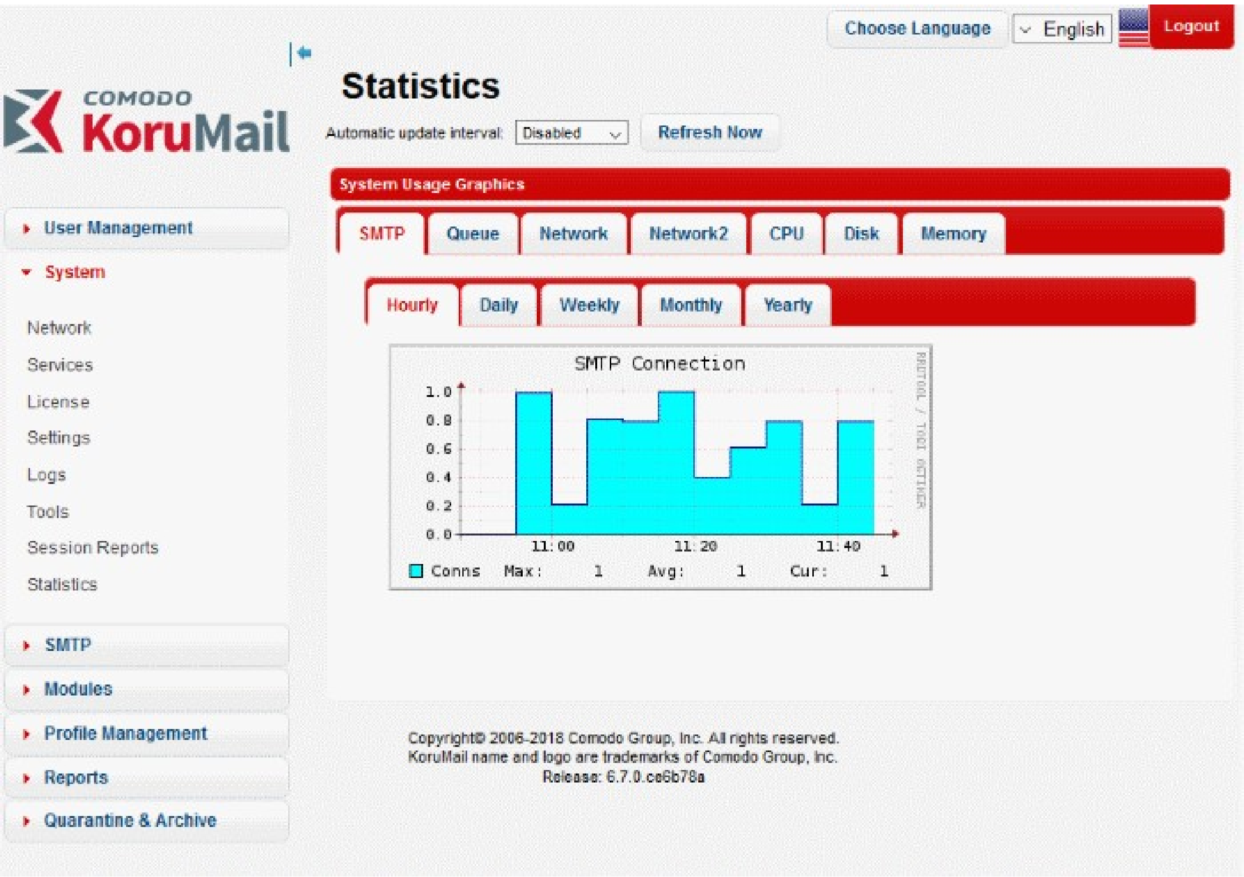
IP Address	Creation Date	Last Accessed Time
182.74.23.22	16/07/2018 08:48:12	16/07/2018 11:23:25

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

6.7 System Usage Statistics

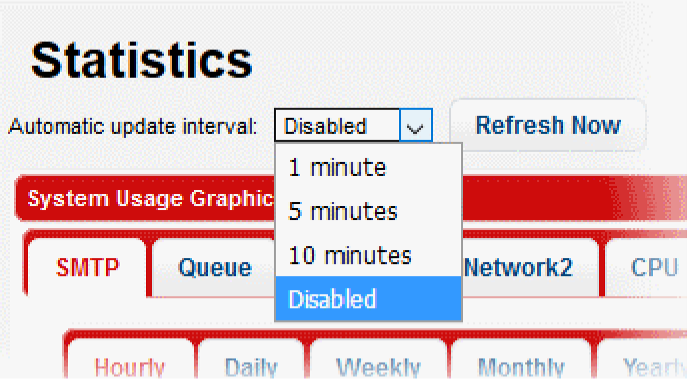
KoruMail displays SMTP connection statistics, mail statistics and utilization statistics of hardware and software resources like network, CPU, hard disks and system memory as graphs in the 'Statistics' interface.

- To open the 'Statistics' interface, click the 'System' tab and then the 'Statistics' sub tab.



The administrator can set the update interval for the statistics or can instantly update the statistics to view the real-time usage graphs.

- To set the update interval, choose the interval from the 'Automatic update interval' drop-down.



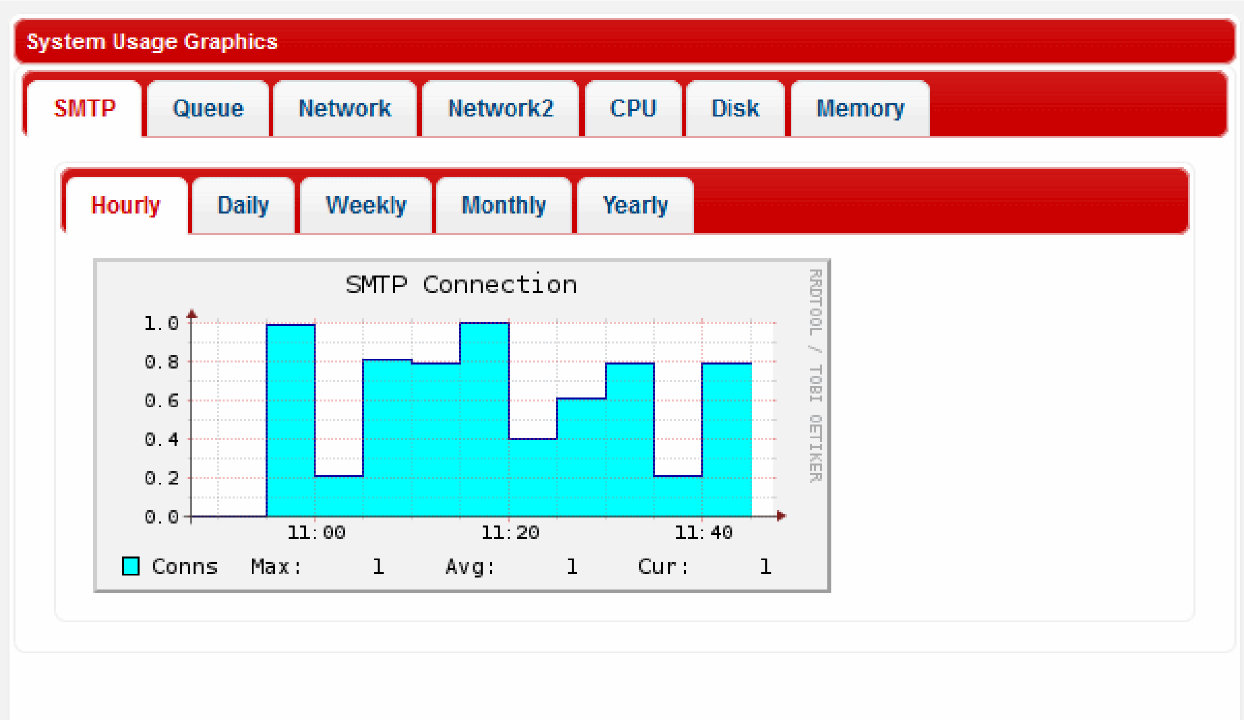
- To instantly update the statistics, click the 'Refresh Now' button.

The 'System Usage Graphics' area displays the connection and usage statistics graphs under the following tabs:

- **SMTP**: A graphical representation of the number of SMTP connections between KoruMail and different mail servers during the selected time period. Shows data for both for incoming and outgoing mails.
- **Queue:** Displays the graphical representation of number of mails that were in queue for processing and delivering to the mail servers, during the selected time period.
- **Network and Network2:** Shows network utilization statistics through various network interfaces for the selected period.
- **CPU:** Shows the load on the KoruMail CPU over the selected period.
- **Disk:** Shows disk access levels over the selected period.
- **Memory:** Shows system memory usage over the selected period.

SMTP

The 'SMTP' tab displays the numbers of SMTP connections made to different mail servers over the period chosen from the sub tabs:

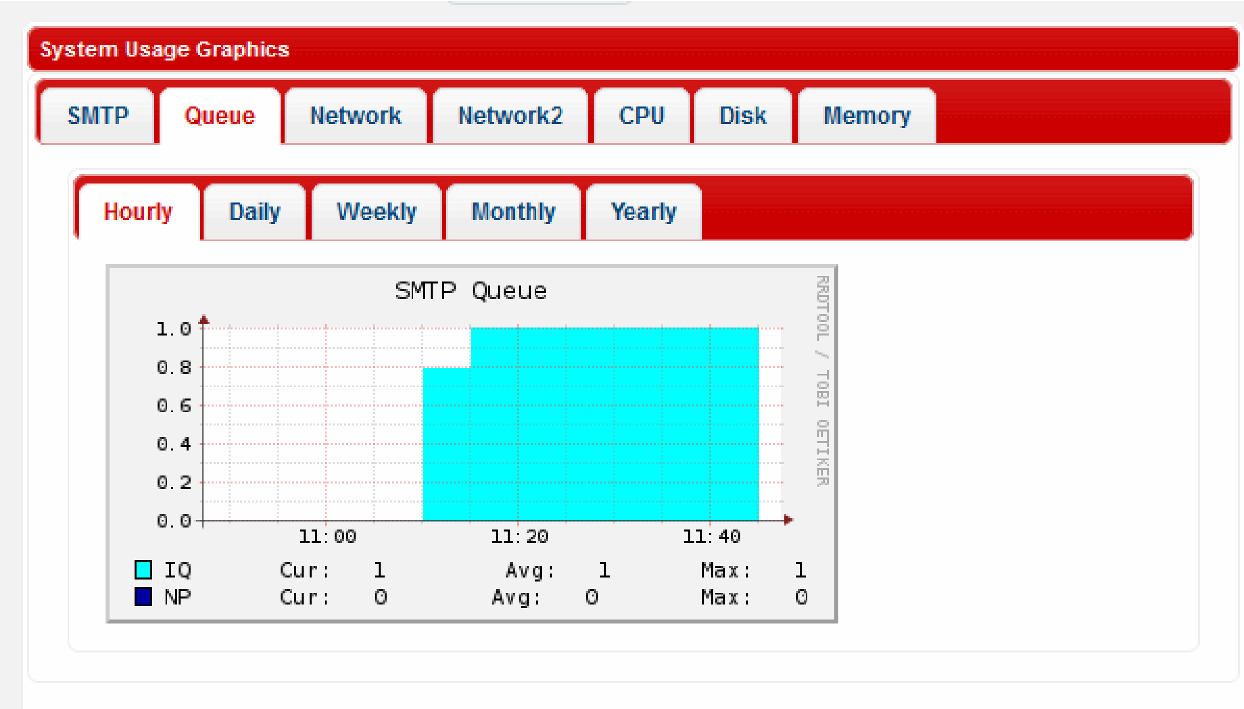


- Hourly - Shows the log of connections for the past one hour
- Daily - Shows the log of connections for the past 24 hours
- Weekly - Shows the log of connections for the past seven days
- Monthly - Shows the log of connections for the past four weeks
- Yearly - Shows the log of connections for the past twelve months

The numbers of maximum and average connections within the selected period and the current number of connections are displayed below the graph.

Queue

KoruMail receives all the emails and analyzes them for spam filtering, virus scanning, content filtering and so on, before delivering it to the mail servers. The 'Queue' tab displays the log of mails that were under processing and not delivered to the mail servers during the selected period.

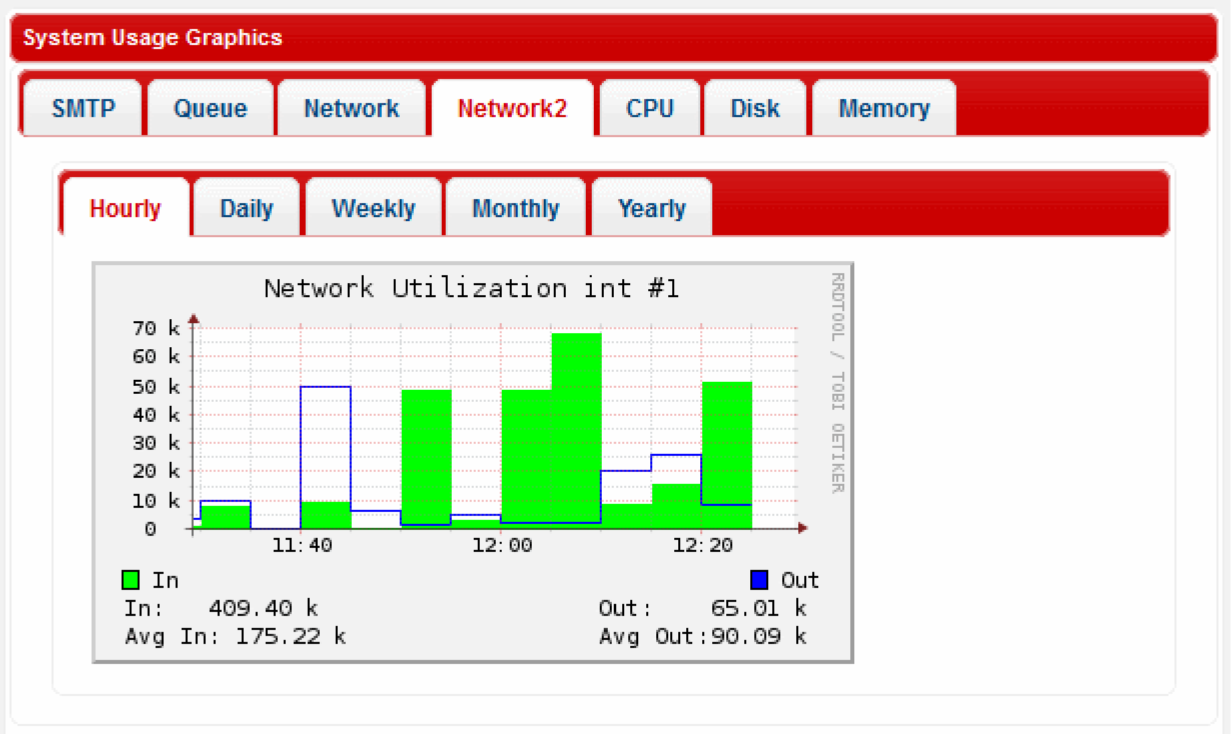


You can choose the time period for which you wish to see the logs from the sub tabs:

- Hourly - Shows the log of number of mails in queue for the past one hour
- Daily - Shows the log of number of mails in queue for the past 24 hours
- Weekly - Shows the log of number of mails in queue for the past seven days
- Monthly - Shows the log of number of mails in queue for the past four weeks
- Yearly - Shows the log of number of mails in queue for the past twelve months

Network and Network2

The Network tabs display the log of network resource utilization through the respective interface, for the period chosen from the sub-tabs.



- Hourly - Shows the log of network usage for the past one hour
- Daily - Shows the log of network usage for the past 24 hours
- Weekly - Shows the log of network usage for the past seven days
- Monthly - Shows the log of network usage for the past four weeks
- Yearly - Shows the log of network usage for the past twelve months

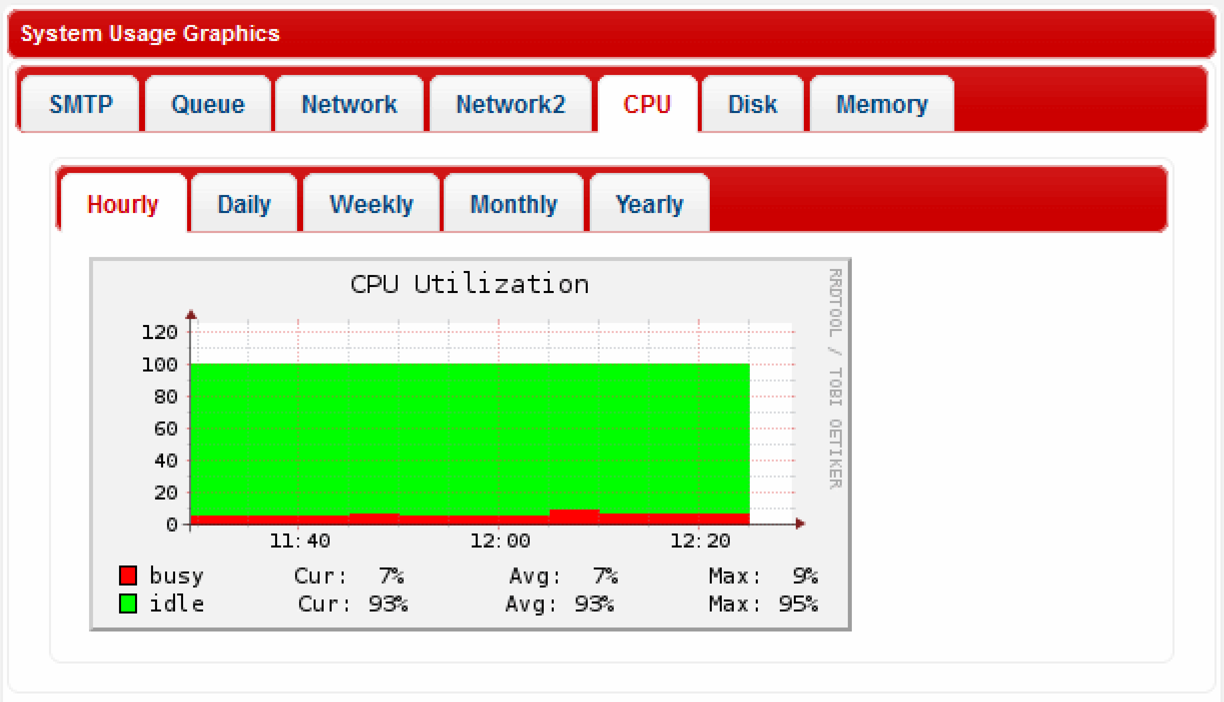
The incoming and outgoing traffic are represented with different colors in the graph.

- Green - Incoming traffic
- Blue - Outgoing traffic

The current incoming/outgoing traffic and the average incoming and outgoing traffic for the selected period of time are indicated below the graph.

CPU

The CPU tab displays the log of load on KoruMail CPU, for the period chosen from the sub-tabs.



🟥 busy	Cur: 7%	Avg: 7%	Max: 9%
🟩 idle	Cur: 93%	Avg: 93%	Max: 95%

- Hourly - Shows the CPU usage for the past one hour
- Daily - Shows the CPU usage for the past 24 hours
- Weekly - Shows the CPU usage for the past seven days
- Monthly - Shows the CPU usage for the past four weeks
- Yearly - Shows the CPU usage for the past twelve months

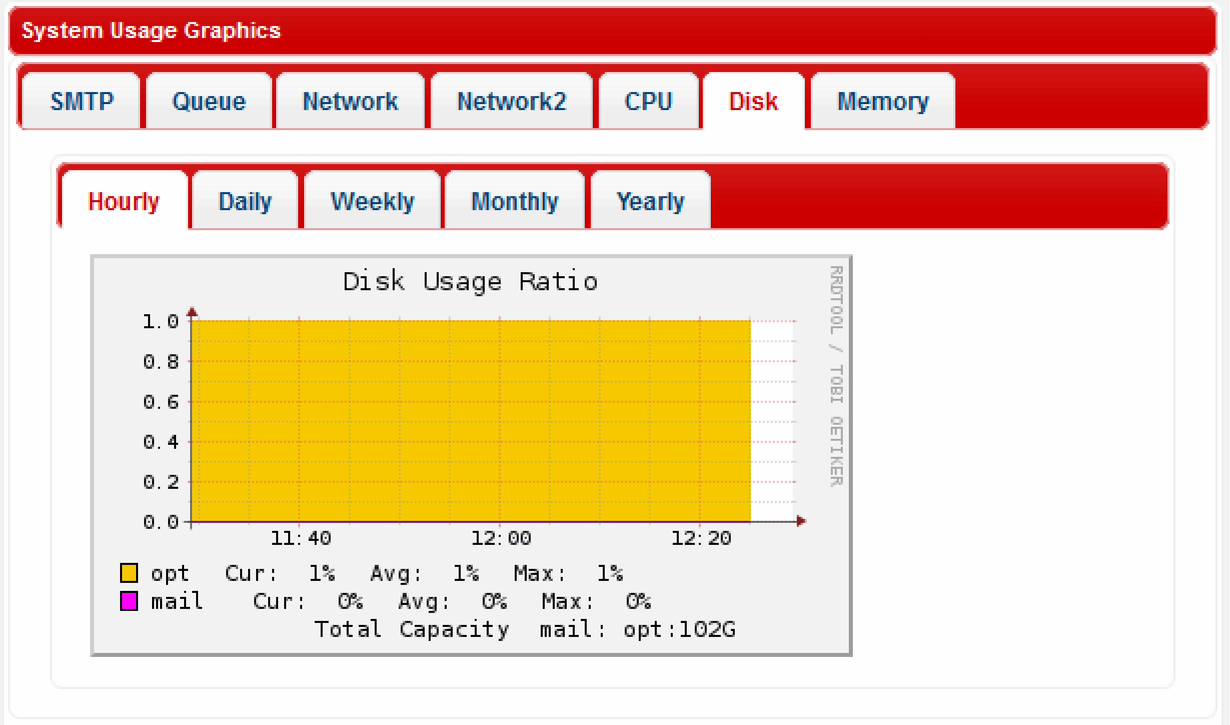
The processes that are responsible for CPU usage are indicated with different colors.

- Green - Idle, CPU was not used by any of the processes
- Red - System processes

The table below the graph shows the current, average and maximum load of the CPU for the selected period from the respective processes.

Disk

The 'Disk' tab displays a graphical representation of the log of the ratio of disk usage with respect to total disk space in KoruMail, for the period chosen from the sub-tabs.



```
🟨 opt   Cur:  1%   Avg:  1%   Max:  1%
🟪 mail   Cur:  0%   Avg:  0%   Max:  0%
       Total Capacity  mail: opt:102G
```

- Hourly - Shows the disk usage for the past one hour
- Daily - Shows the disk usage for the past 24 hours
- Weekly - Shows the disk usage for the past seven days
- Monthly - Shows the disk usage for the past four weeks
- Yearly - Shows the disk usage for the past twelve months

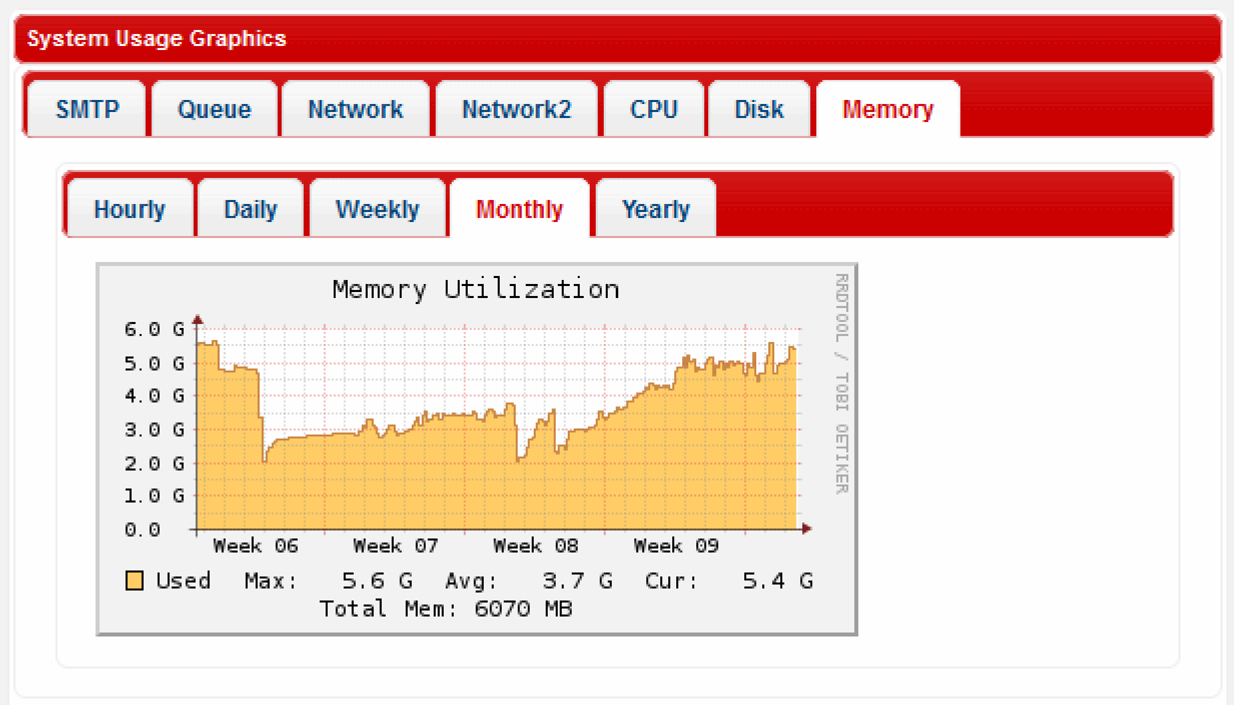
The disk usage by different types of data are indicated with different colors.

- Yellow - Space occupied by system configuration
- Magenta - Space occupied by mail archive

The table below the graph shows the current, average and maximum disk usages for the selected period.

Memory

The 'Memory' tab displays a graphical representation of the usage of system memory of KoruMail, for the period chosen from the sub-tabs.

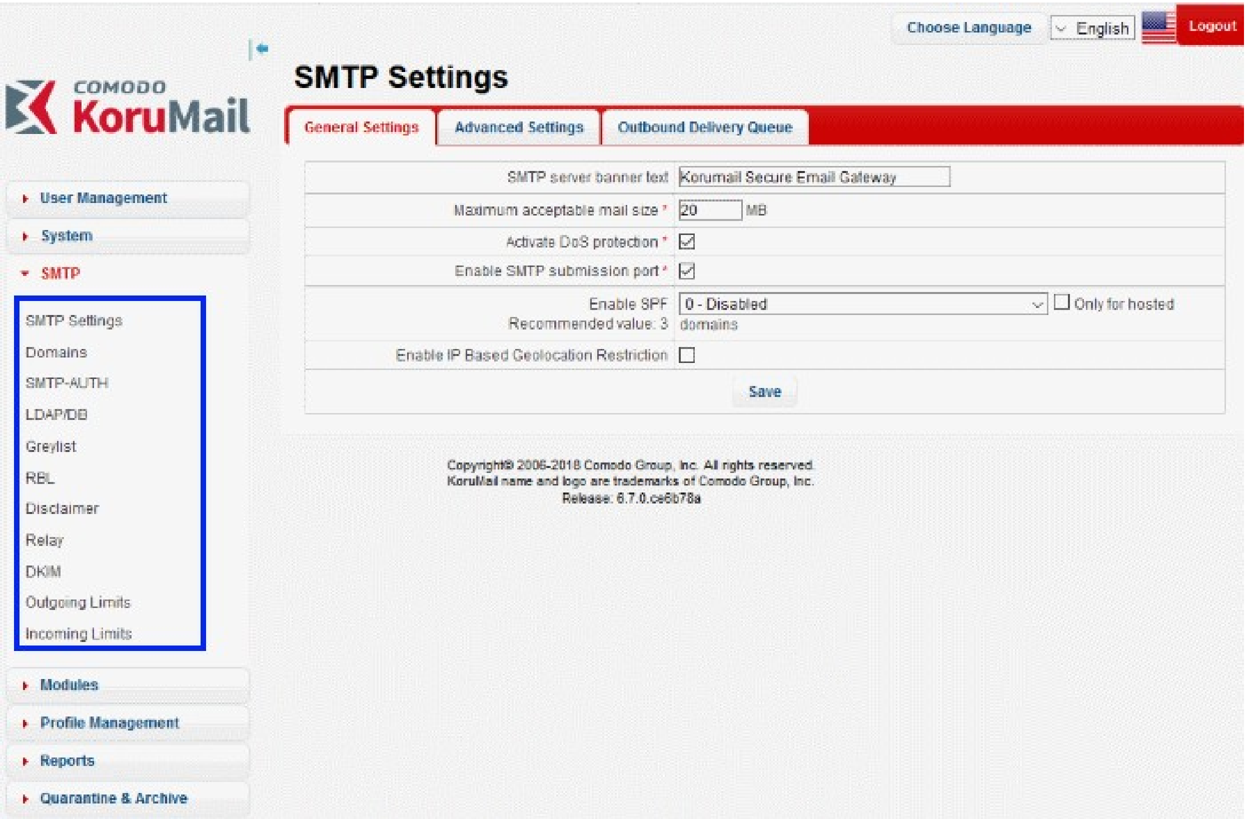


- Hourly - Shows the memory usage for the past one hour
- Daily - Shows the memory usage for the past 24 hours
- Weekly - Shows the memory usage for the past seven days
- Monthly - Shows the memory usage for the past four weeks
- Yearly - Shows the memory usage for the past twelve months

The maximum, average and current memory usage statistics are indicated below the graph.

7 SMTP Configuration

The 'SMTP' area allow administrators to configure settings for outgoing mails such as SMTP settings, set outgoing limits, manage domains, SMTP-Auth settings, block users and more.



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

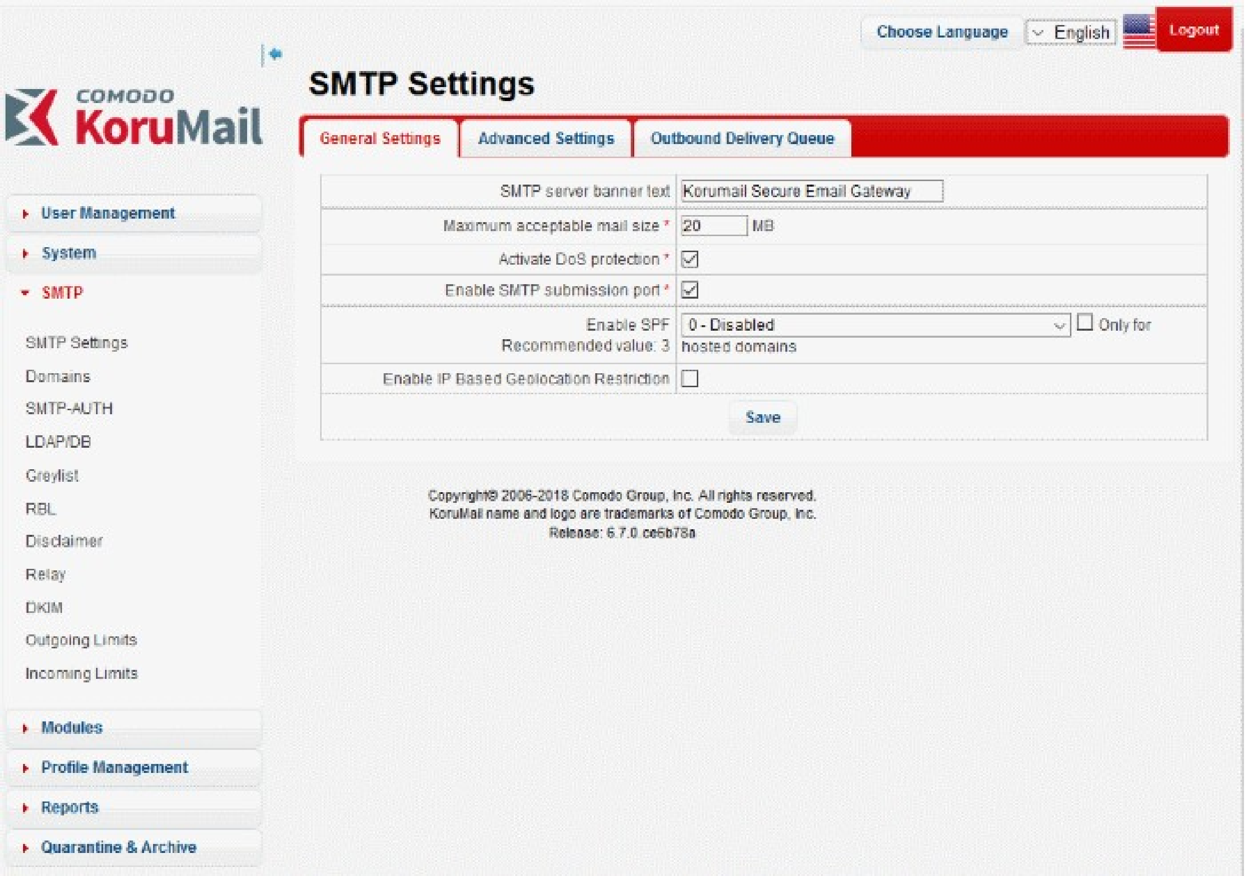
Click the following links for more details:

- **SMTP Settings**
- **Manage Domains**
- **KoruMail SMTP AUTH Connector**
- **LDAP/Local DB/MySQL User Database**
- **Greylisting**
- **Manage RBL Servers**
- **Disclaimer**
- **SMPT Relay**
- **DomainKeys Identified Mail (DKIM)**
- **Outgoing SMTP Limits**
- **Incoming SMTP Limits**

7.1 SMTP (Send E-Mail Protocol) Settings

The 'SMTP' settings area allow administrators to configure items such as SMTP connection response message, activate DoS protection, configure minimum and maximum number of sub processes the main filtering engine can be utilized. The area also allows you to set the number of mails that can be queued and sent at a time for a particular domain.

- To open the 'SMTP' screen, click the 'SMTP-Auth' tab on the left menu and click 'SMTP'.



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

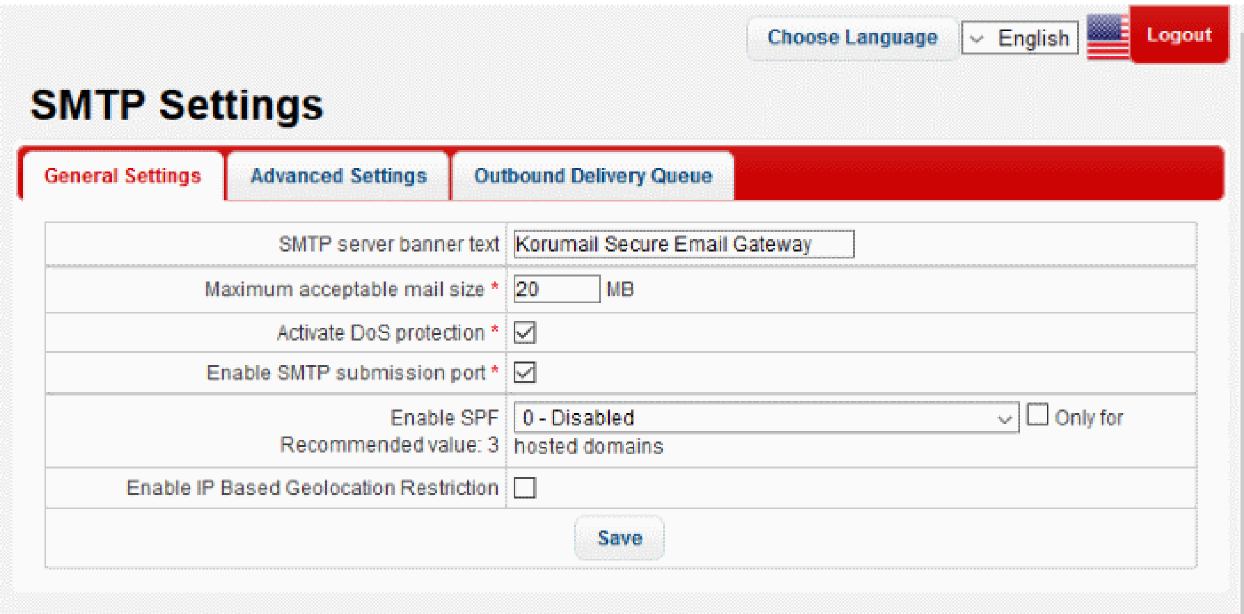
Click the following links for more details:

- **General Settings**
- **Advanced Settings**
- **Outbound Delivery Queue**

7.1.1 General Settings

The 'General Settings' lets you configure the max. size of mails that can be sent, enable denial of service (DoS) protection, and configure sender policy framework (SPF).

- Click 'SMTP' > 'SMTP' > 'General Settings' to open the settings interface:



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	☐

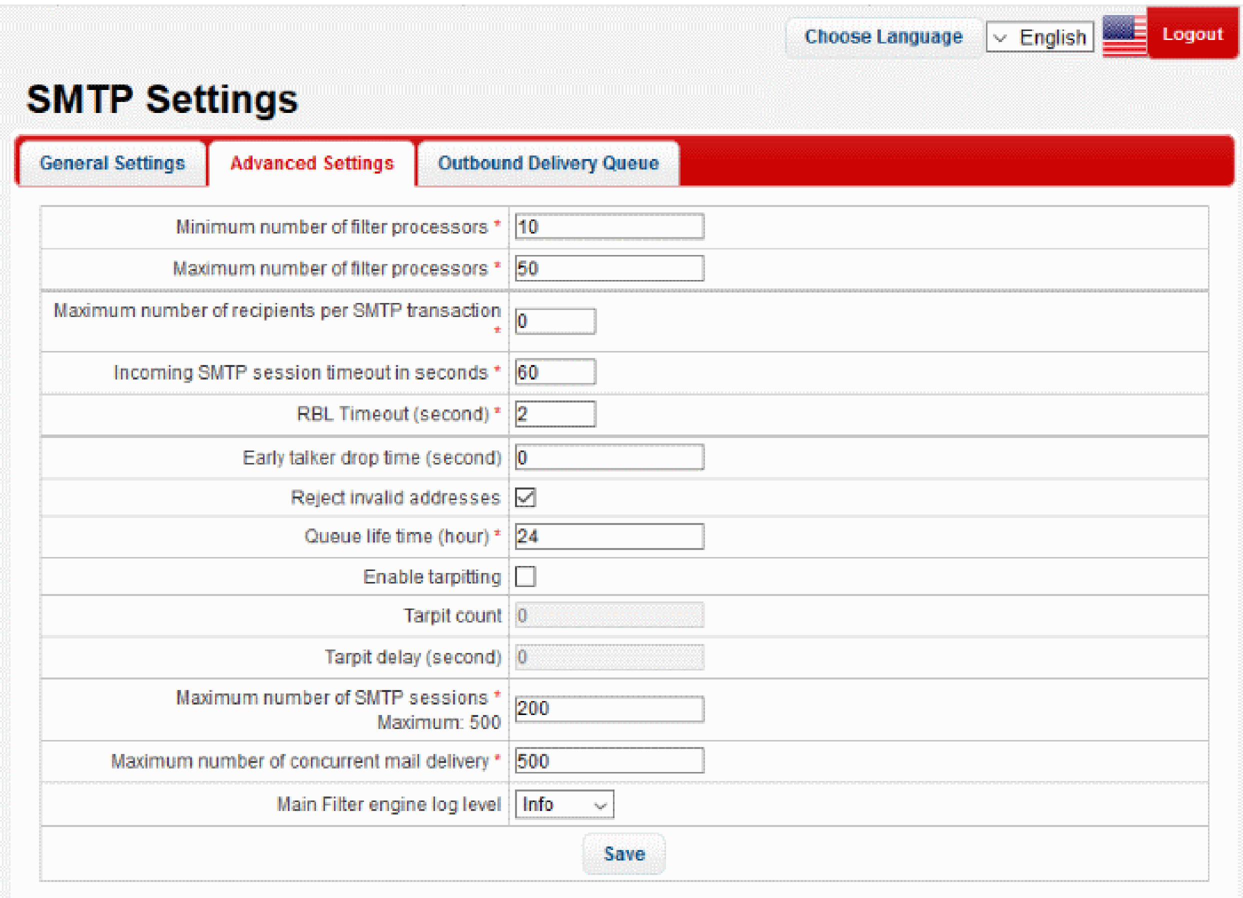
SMTP Settings - General Settings Table of Parameters	
Parameter	**Description**
SMTP server banner text	The welcome message shown on the server after connection to KoruMail port 25 is established.
Maximum acceptable mail size (MB)	The maximum permitted size of a single email + attachments. The default 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 doesn't accept outgoing messages from unauthenticated sources. This helps protect your network and users from spam emails.
Enable SPF Recommended value: 3	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	Detects the location of the sender from their IP address. This should be enabled in order to activate the geo-location restriction settings in incoming profiles. Mails from restricted countries will be rejected. See 'Geolocation Restriction' settings in **incoming profile settings** to specify countries from which you want to reject email.

- Click 'Save' to apply your changes.

7.1.2 Advanced Settings

The SMTP 'Advanced Settings' area allows administrators to configure settings such as the minimum and maximum number of processes that the main filtering engine should use, the number of recipients per SMTP transactions and more.

- To open the SMTP 'Advanced Settings' interface, click the 'SMTP' tab and then the 'SMTP' sub tab > 'Advanced Settings'.



Minimum number of filter processors *	10
Maximum number of filter processors *	50
Maximum number of recipients per SMTP transaction *	0
Incoming SMTP session timeout in seconds *	60
RBL Timeout (second) *	2
Early talker drop time (second)	0
Reject invalid addresses	☑
Queue life time (hour) *	24
Enable tarpitting	□
Tarpit count	0
Tarpit delay (second)	0
Maximum number of SMTP sessions * Maximum: 500	200
Maximum number of concurrent mail delivery *	500
Main Filter engine log level	Info

SMTP Settings - Advanced Settings Table of Parameters	
Parameter	**Description**
Minimum number of filter processors	The lowest amount of processes that Korumail should use to filter mail. 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 Korumail should use to filter mail. Filter processors are threads used to scan and handle mail. • More processors = Higher resource overhead / better performance

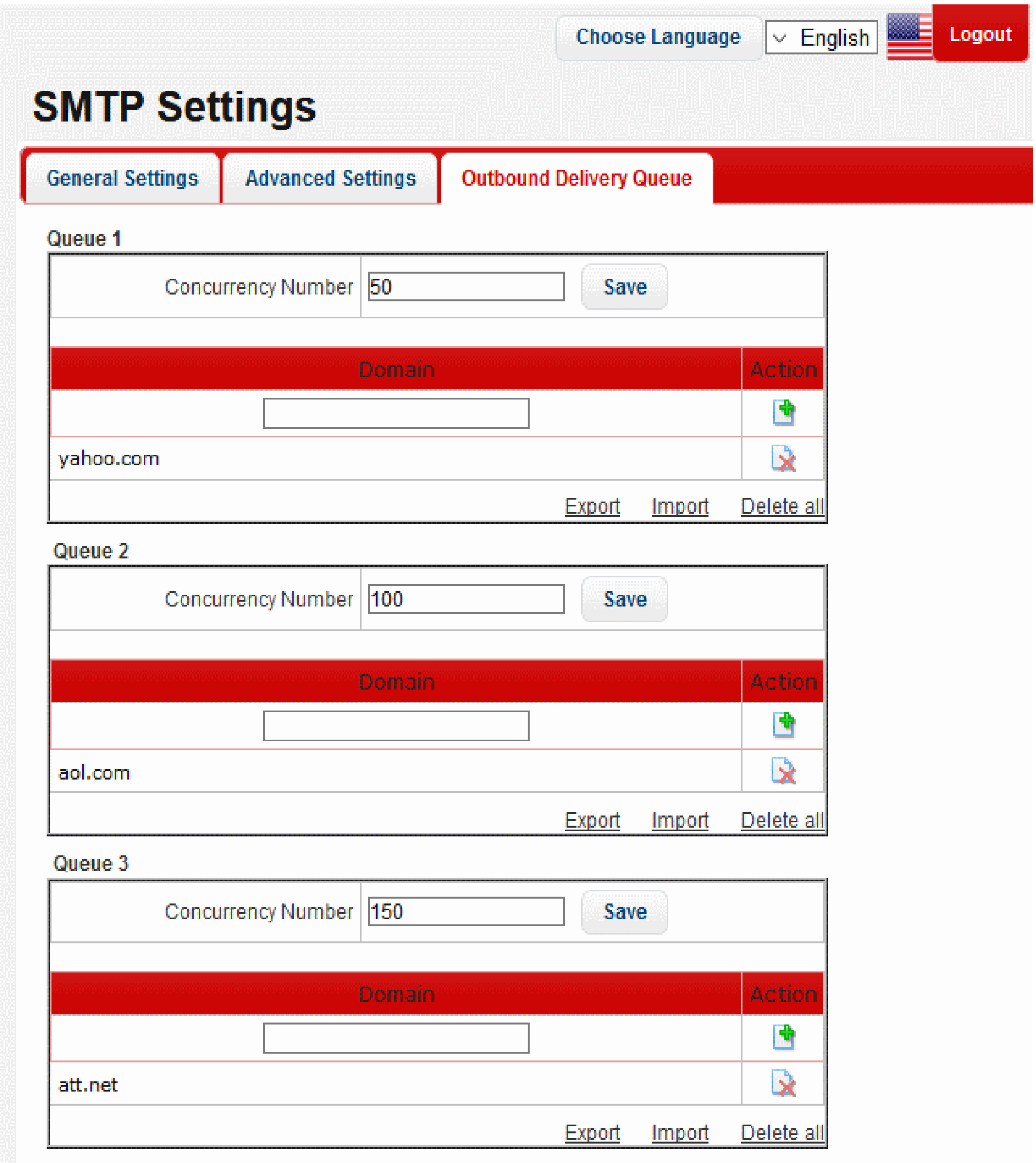
Maximum number of recipients per SMTP transaction	The highest number of mailboxes to which Dome Antispam will forward mail per transaction.
Incoming SMTP session timeout (seconds)	Timeout duration of each SMTP session.
RBL Timeout (seconds)	If this time is exceed, the RBL query is canceled and next filter 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 recieves the response before it sends the greeting, then there is a high chance the client is a spammer. 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, outgoing 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 concurrent SMTP sessions.
Maximum number of concurrent mail delivery	Maximum number of concurrent messages that can be sent by SMTP server.
Main Filter engine log level	Select the level of main filtering engine event that should be logged. Selecting 'Notset' will log all the levels.

- Click 'Save' to apply your changes.

7.1.3 Outbound Delivery Queue

Some domains have restrictions on how many email recipients that can be delivered concurrently from a source. KoruMail has the feature to queue outbound mails per domain so that only the specified number of mails will be delivered at a time.

- To open the SMTP 'Outbound Delivery Queue' interface, click the 'SMTP' tab and then the 'SMTP' sub tab > 'Outbound Delivery Queue'.



SMTP Settings

Queue 1

Concurrency Number	50

Domain	Action
	+
yahoo.com	✗

Queue 2

Concurrency Number	100

Domain	Action
	+
aol.com	✗

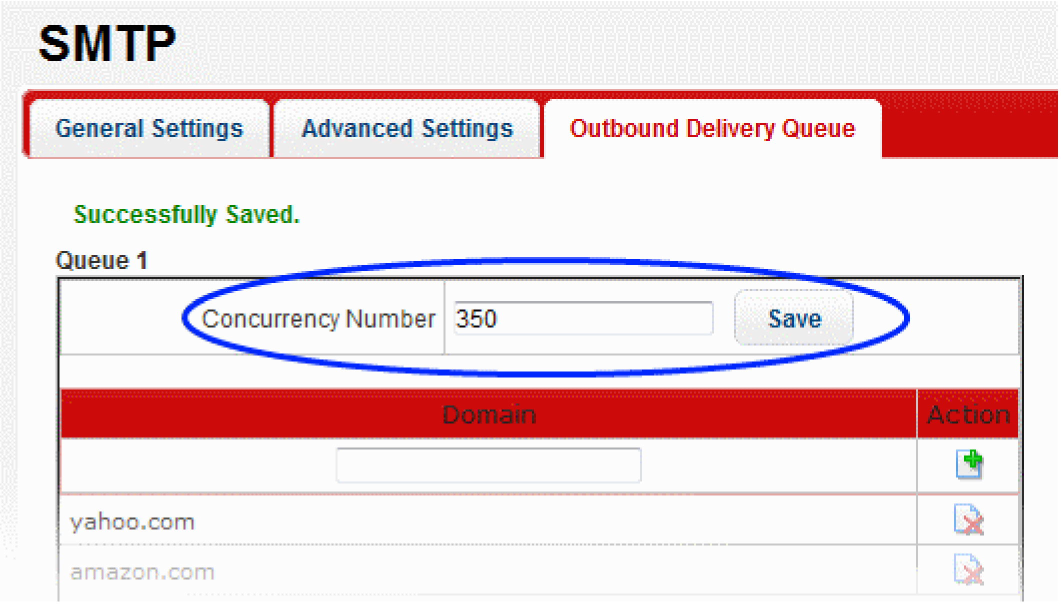
Queue 3

Concurrency Number	150

Domain	Action
	+
att.net	✗

The interface has three preset delivery queue numbers that can be configured according to your organizational needs. The 'Concurrency Number' for each of the queue can be changed.

- To set the number of emails that can be sent at a time, enter the number in the 'Concurrency Number' field and click the 'Save' button.



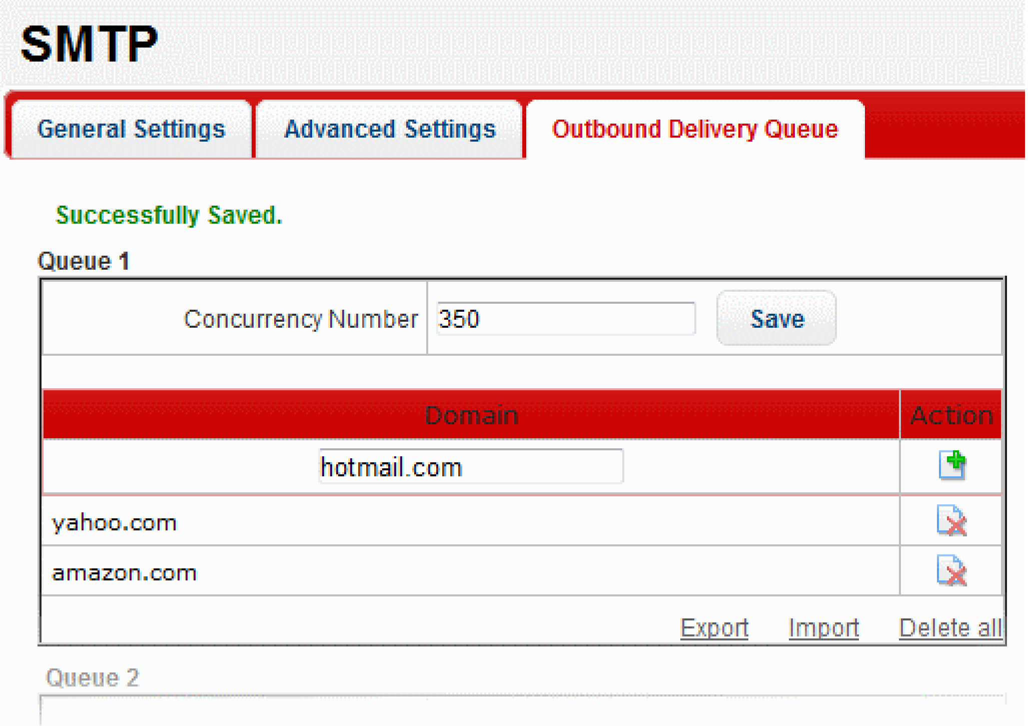
Successfully Saved.

Queue 1

Concurrency Number: 350

Domain	Action
	➕
yahoo.com	✗
amazon.com	✗

- To add a domain for which the number of outgoing mails should be restricted and queued depending on the 'Concurrency Number', enter the domain name in the filed and click the ➕ button under the 'Action' column.



Successfully Saved.

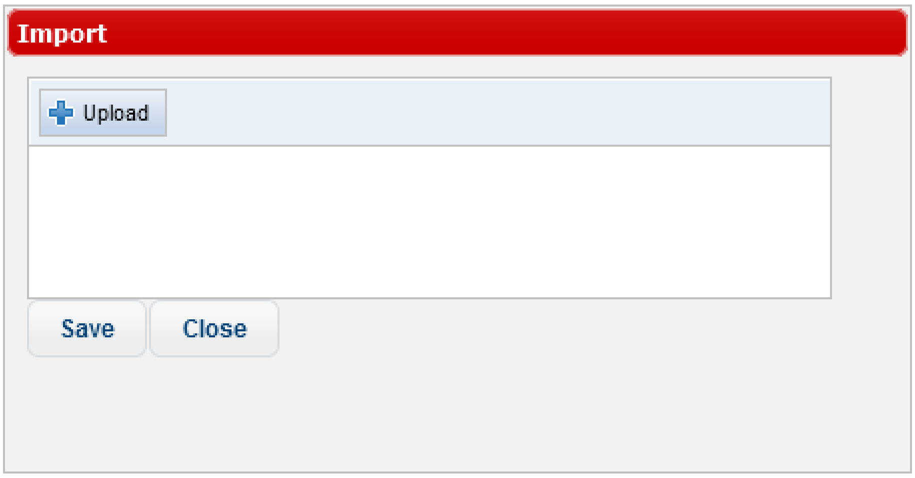
Queue 1

Concurrency Number: 350

Domain	Action
hotmail.com	➕
yahoo.com	✗
amazon.com	✗

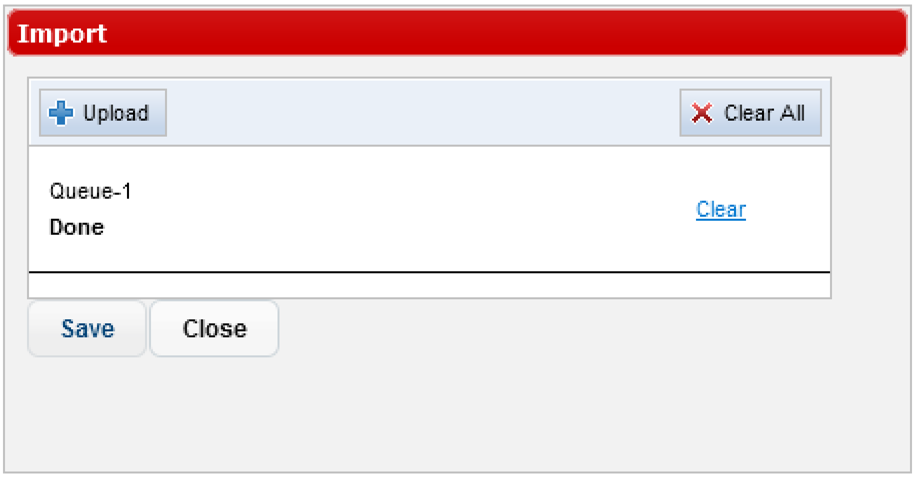
Queue 2

- 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'.
- To save the list of domains in a 'Queue', click the 'Export' link and save it to your system.
- To import a list of domains, click the 'Import' link. The 'Import' dialog will be displayed:



- Click the 'Upload' button, browse to the location where the file is saved and click 'Open'.

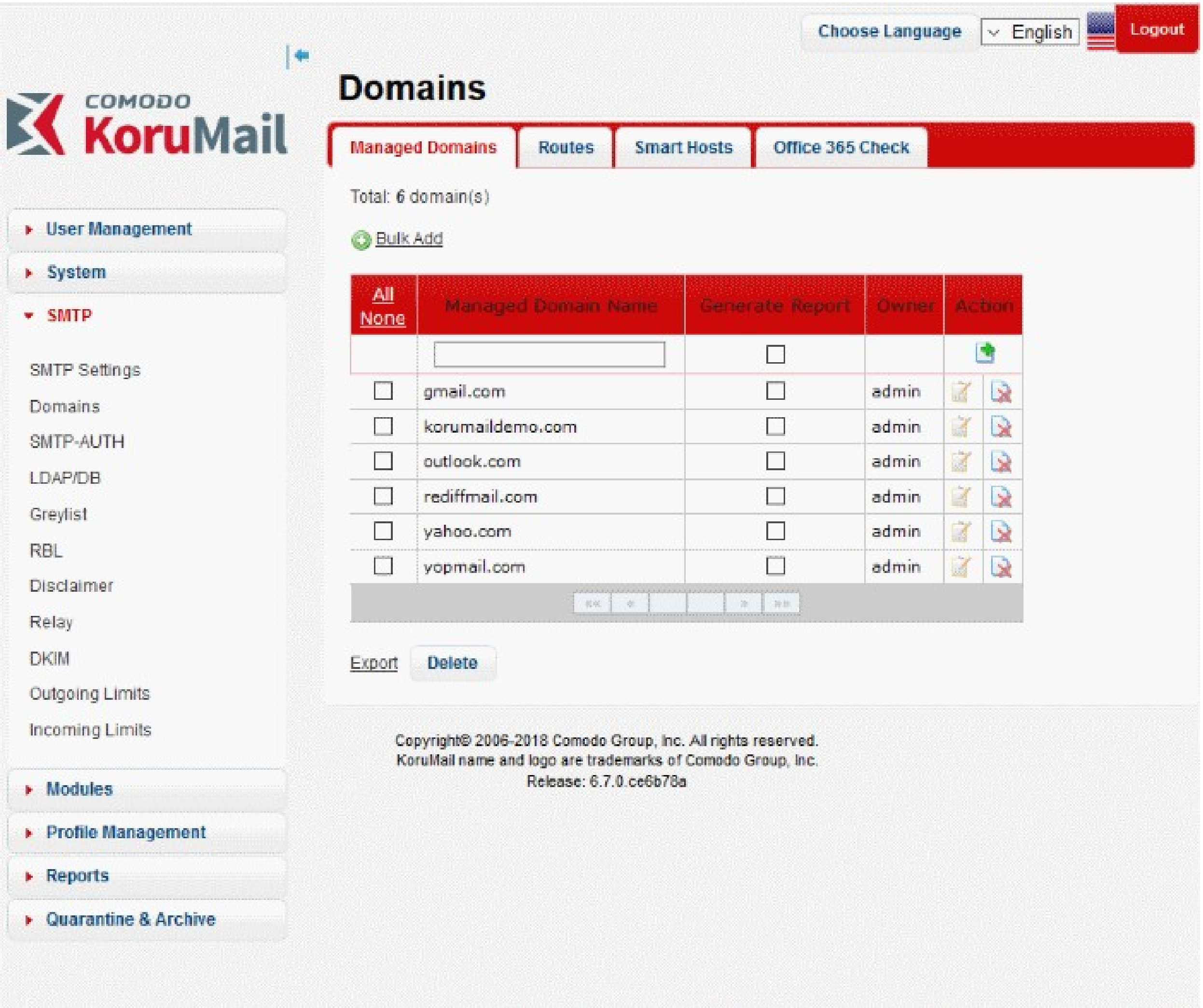
The file will be added.



- Repeat the process to add more files.
- To remove a file, click the 'Clear' link beside it.
- To remove all the added files, click the 'Clear All' button at the top right.
- To import the list of domains from the files, click the 'Save' button.

7.2 Manage Domains

- The 'Manage Domains' area allows you to add, edit and view the domains you wish to filter.
- You can also configure routes, SMTP servers and add 'Smart Hosts', so mail is routed to an intermediate/ relay server rather than direct to the recipient server.
- Click 'SMTP' left then 'Domains' to open this interface:



Domains

Total: 6 domain(s)

All None	Managed Domain Name	Generate Report	Owner	Action
		□		
□	gmail.com	□	admin	
□	korumaildemo.com	□	admin	
□	outlook.com	□	admin	
□	rediffmail.com	□	admin	
□	yahoo.com	□	admin	
□	yopmail.com	□	admin	

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

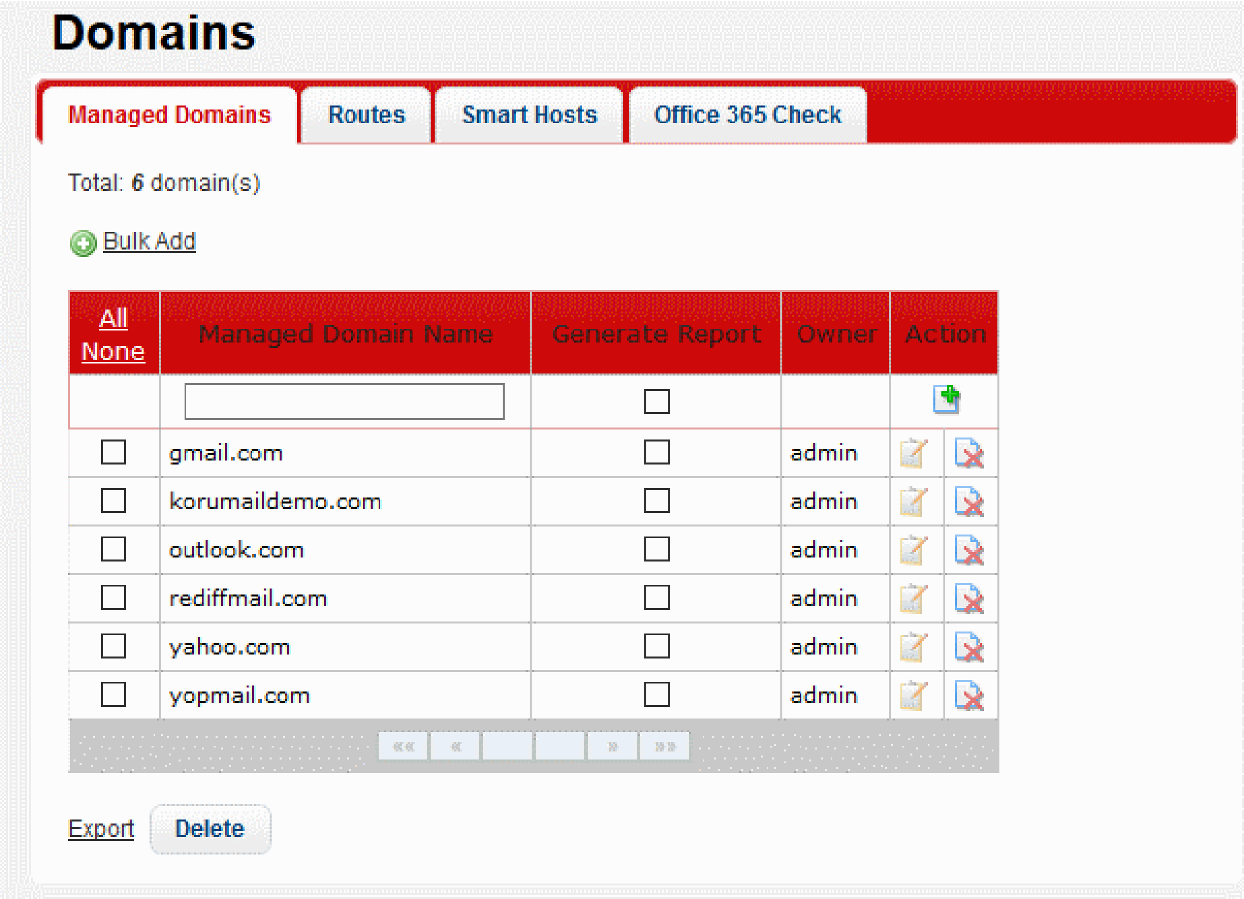
Click the following the links for more details:

- Manage domain names
- Manage domain routes
- Manage smart hosts
- Default domain routing

7.2.1 Manage Domain Names

The 'Managed Domain Names' tab lets you view, add and edit your protected domains.

- Click 'SMTP' > 'Domains' on the left
- Click the 'Managed Domains' tab



Domains

Total: 6 domain(s)

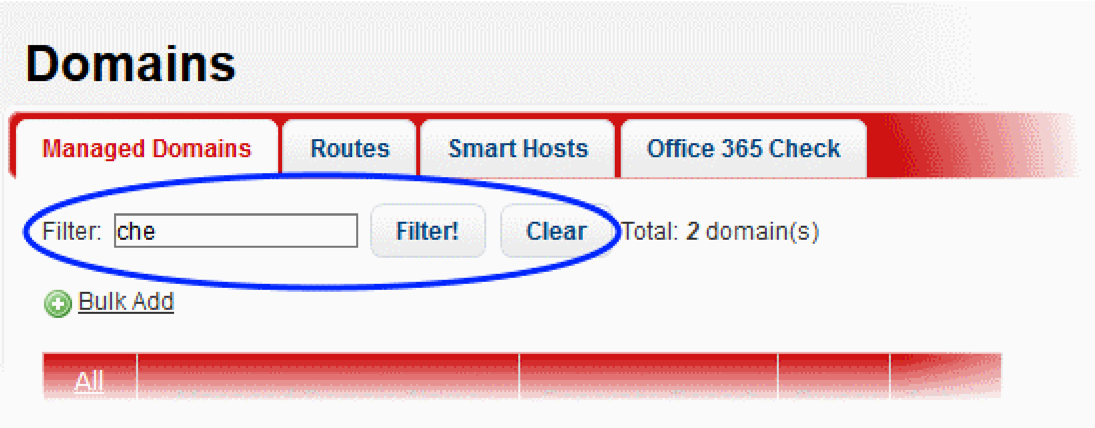
Bulk Add

All None	Managed Domain Name	Generate Report	Owner	Action
		□		
□	gmail.com	□	admin	
□	korumaildemo.com	□	admin	
□	outlook.com	□	admin	
□	rediffmail.com	□	admin	
□	yahoo.com	□	admin	
□	yopmail.com	□	admin	

Managed Domains - Table of Column Descriptions		
Column Header	**Description**	
Managed Domain Name	The name of the domain added to KoruMail	
Generate Report	If enabled, KoruMail displays related email statistics of the selected domain name in '**Domain Reports**'	
Owner	The name of the administrator who added the domain.	
Actions		To add a domain, click this button after entering the details in the field under 'Managed Domain Name' column.
		Allows the administrators to delete a domain from the list.
		Allows the administrators to change the name of the 'Owner'

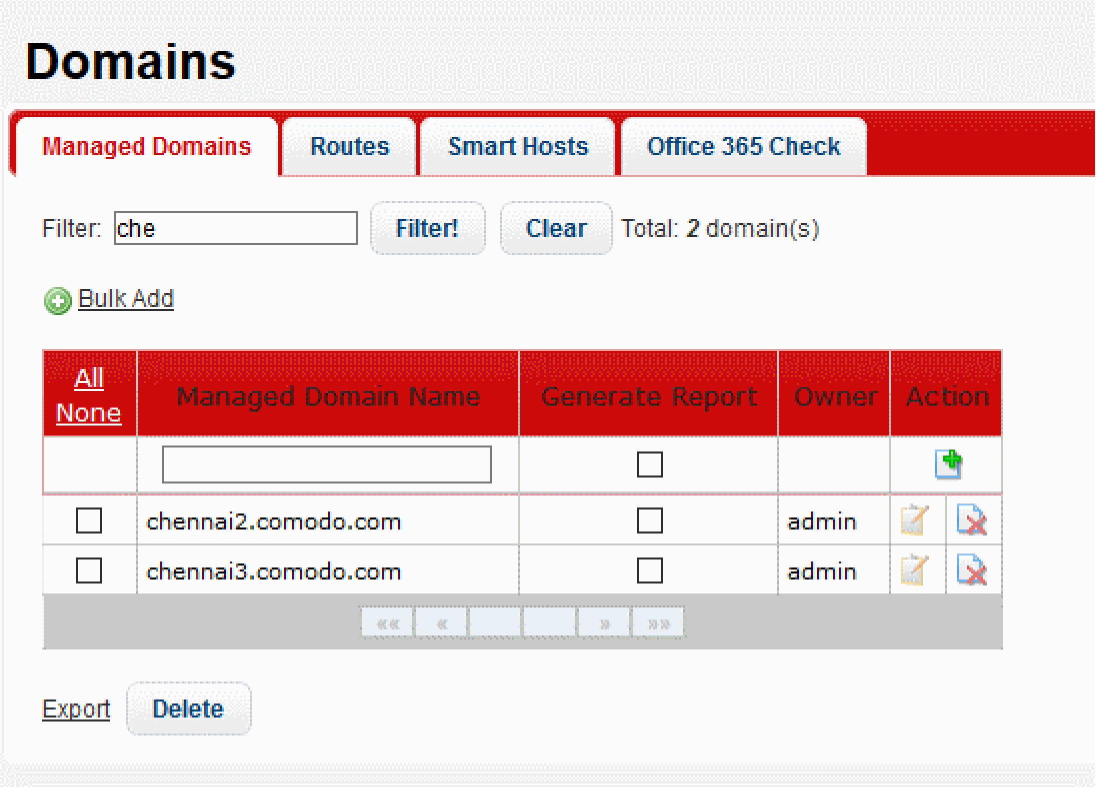
Search Options

You can search for a particular domain(s) by using the filter.



- Enter the name of the domain fully or partially in the filter field and click the 'Filter' button.

Domains that match the entered search text will be displayed.



All None	Managed Domain Name	Generate Report	Owner	Action
		□		
□	chennai2.comodo.com	□	admin	
□	chennai3.comodo.com	□	admin	

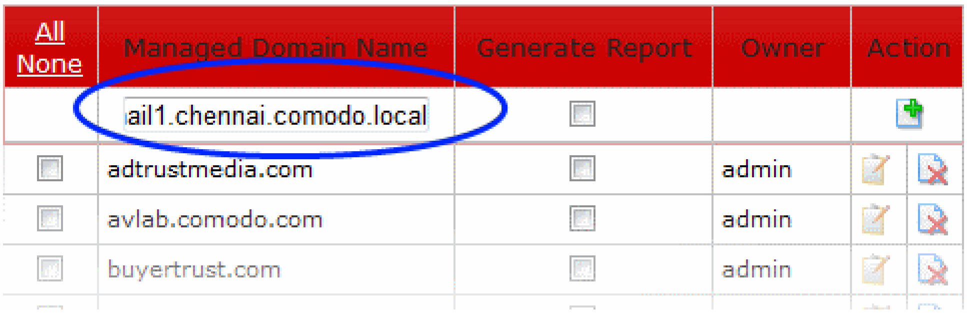
- To display all the managed domains, click the 'Clear' button.

The interface allows you to:

- **Add a domain name**
- **Add multiple domain names**
- **Edit a domain owner**
- **Delete domain names**
- **Export domain names**

To add a domain name

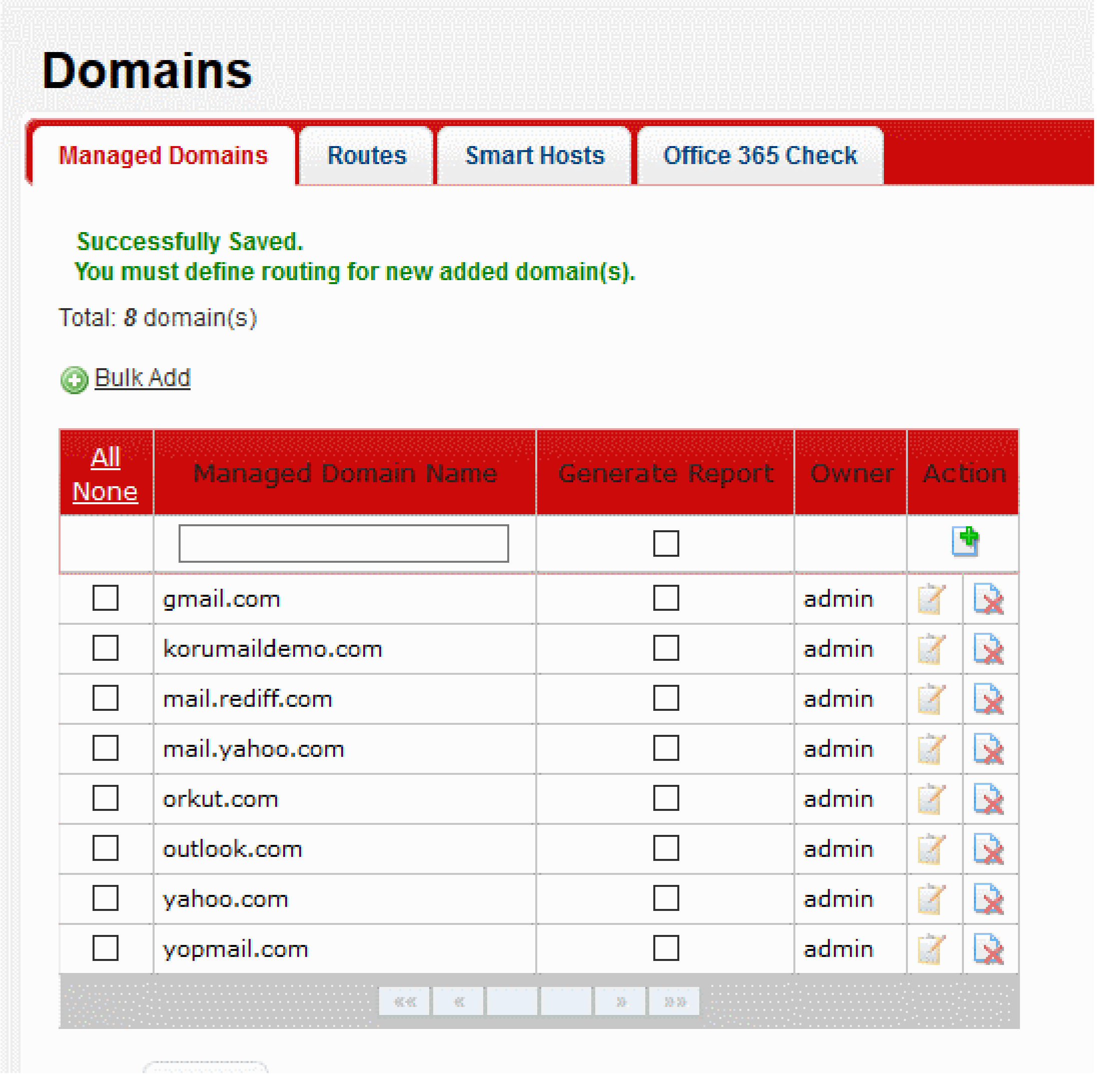
- Enter the domain name in the field under 'Managed Domain Name' column



All None	Managed Domain Name	Generate Report	Owner	Action
	ail1.chennai.comodo.local	☐		➕
☐	adtrustmedia.com	☐	admin	✎ ✗
☐	avlab.comodo.com	☐	admin	✎ ✗
☐	buyertrust.com	☐	admin	✎ ✗

- Select the 'Generate Report' check box if you want to display email statistics of the domain name in '**Domain Reports**'
- Click the ➕ button under the 'Action' column.

The domain will be added and the next step is to define route for the added domain. If left undefined, then the default route will apply for the domain.



Domains

Successfully Saved.
You must define routing for new added domain(s).

Total: *8* domain(s)

Bulk Add

All None	Managed Domain Name	Generate Report	Owner	Action
		☐		➕
☐	gmail.com	☐	admin	✎ ✗
☐	korumaildemo.com	☐	admin	✎ ✗
☐	mail.rediff.com	☐	admin	✎ ✗
☐	mail.yahoo.com	☐	admin	✎ ✗
☐	orkut.com	☐	admin	✎ ✗
☐	outlook.com	☐	admin	✎ ✗
☐	yahoo.com	☐	admin	✎ ✗
☐	yopmail.com	☐	admin	✎ ✗

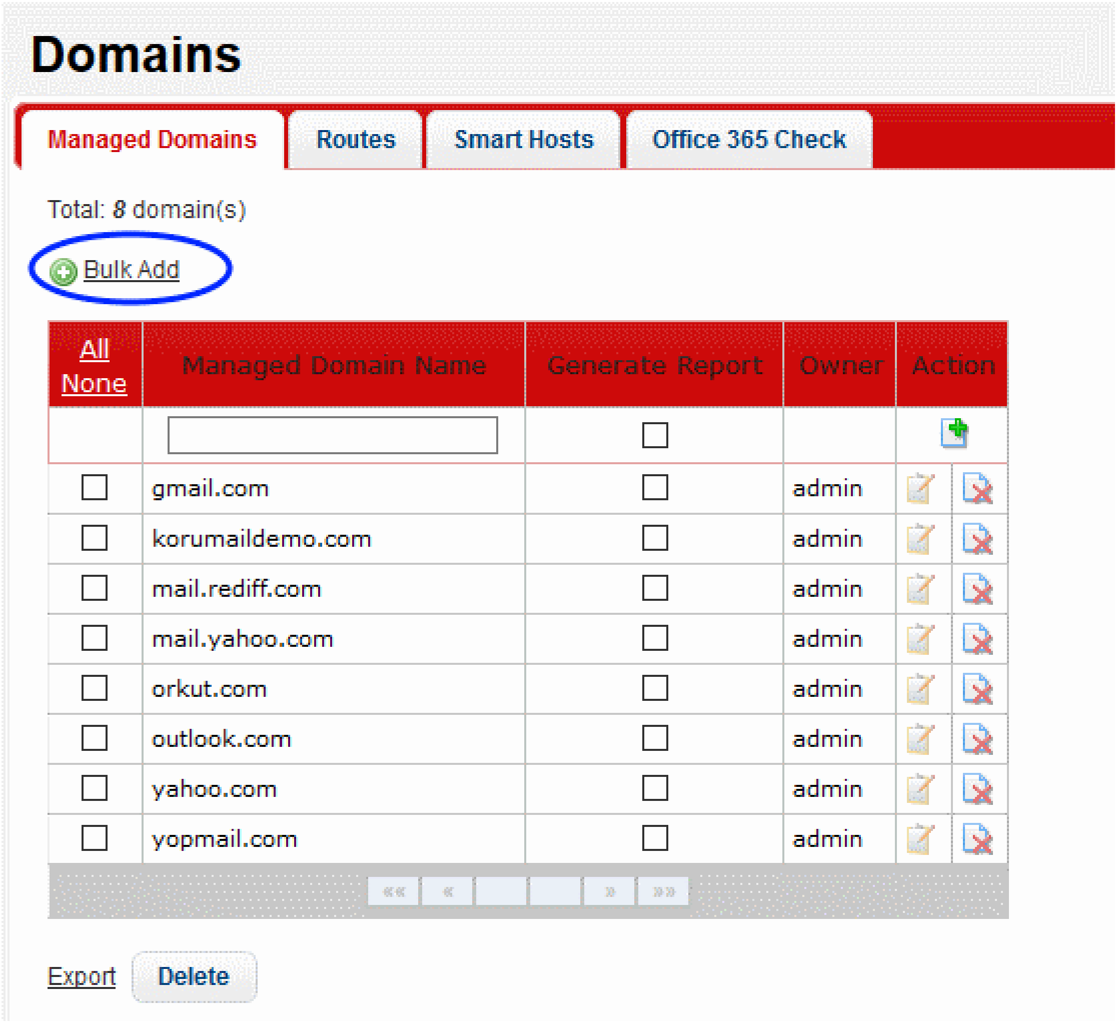
See '**Manage Routes**' on how to add routes.

To add multiple domain names

When you add the domain name, you can also route the domain name at the same time. To do this, you must specify the domain name, target IP address, port and LDAP profile name in one line.

- Separate each item with a semi-colon as follows:
    - Domain; Destination IP; Port; LDAP Profile Name
- If destination IP address is blank then no routing is done for the domain
- If the port field is blank, port 25 is used as default.

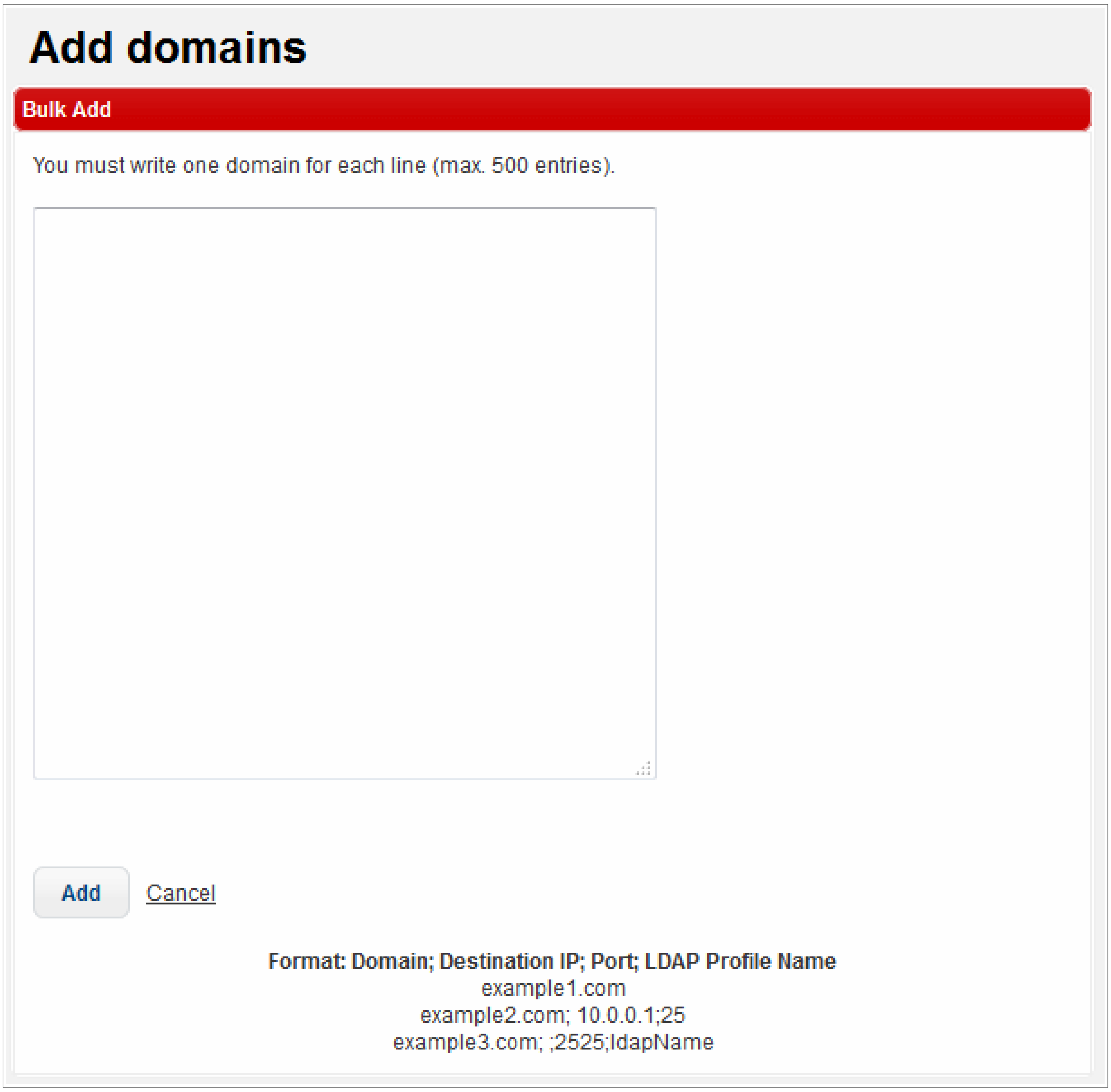
Click the 'Bulk Add' link in the 'Managed Domains' screen:



Total: 8 domain(s)

All None	Managed Domain Name	Generate Report	Owner	Action
		□		✚
□	gmail.com	□	admin	✎ ✗
□	korumaildemo.com	□	admin	✎ ✗
□	mail.rediff.com	□	admin	✎ ✗
□	mail.yahoo.com	□	admin	✎ ✗
□	orkut.com	□	admin	✎ ✗
□	outlook.com	□	admin	✎ ✗
□	yahoo.com	□	admin	✎ ✗
□	yopmail.com	□	admin	✎ ✗

The 'Bulk Add' screen will open:



Add domains

Bulk Add

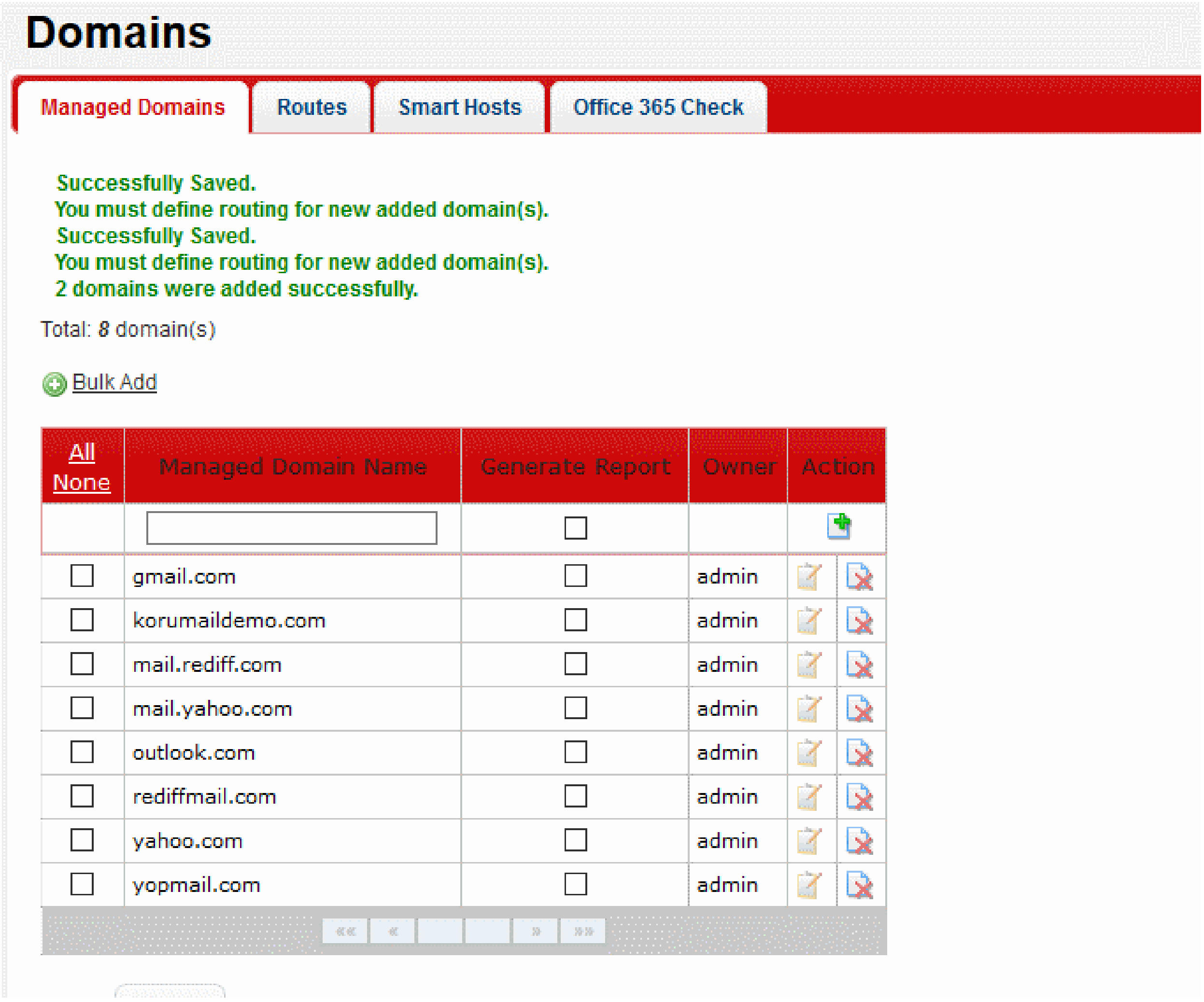
You must write one domain for each line (max. 500 entries).

Format: Domain; Destination IP; Port; LDAP Profile Name
example1.com
example2.com; 10.0.0.1;25
example3.com; ;2525;ldapName

- Enter the domain names each per line.
- You can also define routes, port number and LDAP profile name here for the domains. The items should be separated by a semicolon as shown in the screen.

- Click the 'Add' button.

The domains will be added and the next step is to define routes for the added domains if not defined while entering the domain names. If left undefined, then the default route will apply for the domains.



Domains

Successfully Saved.
You must define routing for new added domain(s).
Successfully Saved.
You must define routing for new added domain(s).
2 domains were added successfully.

Total: 8 domain(s)

Bulk Add

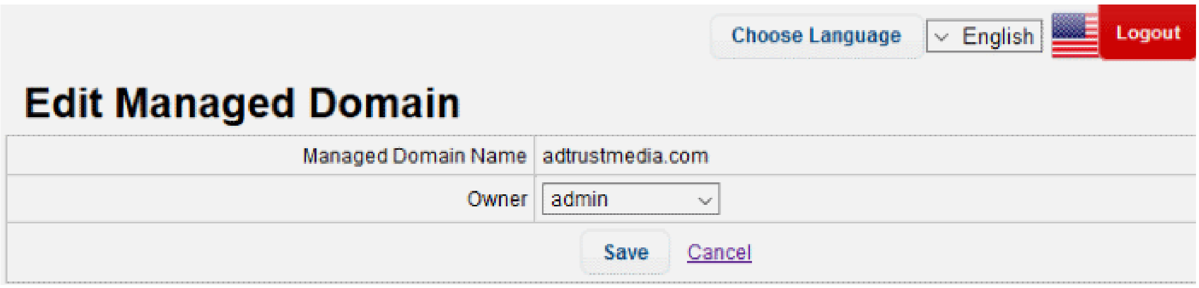
All None	Managed Domain Name	Generate Report	Owner	Action	
		□			
□	gmail.com	□	admin		
□	korumaildemo.com	□	admin		
□	mail.rediff.com	□	admin		
□	mail.yahoo.com	□	admin		
□	outlook.com	□	admin		
□	rediffmail.com	□	admin		
□	yahoo.com	□	admin		
□	yopmail.com	□	admin		

To edit a domain owner

When an administrator adds a domain name, his/her user name will be displayed in the screen under the 'Owner' column header.

- To change the name of domain owner, click the button beside the 'Owner' name.

The 'Edit Managed Domain' screen will be displayed.



Edit Managed Domain

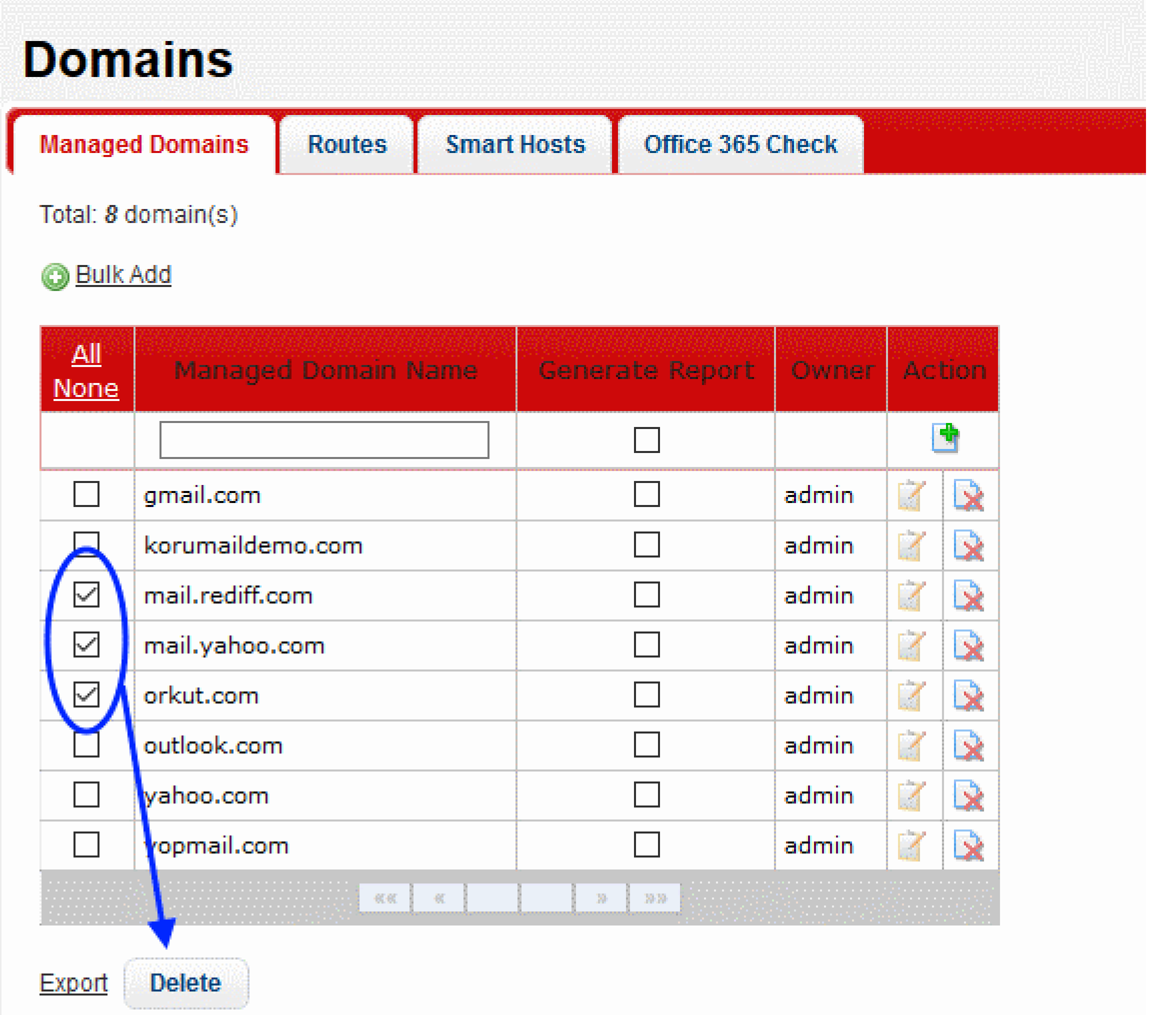
Managed Domain Name	adtrustmedia.com
Owner	admin

- Select the name that you want to change as the owner from the 'Owner' drop-down
- Click the 'Save' button

To delete domain names

- To delete domain names one at a time, click the button under the 'Action' column header and confirm the deletion in 'Confirmation' dialog.

- To delete multiple domain names, select the check boxes beside them and click the 'Delete' button at the bottom.



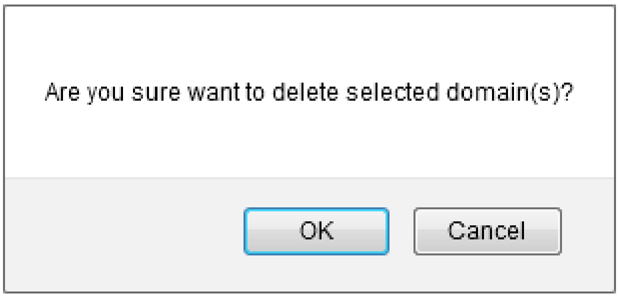
Domains

Total: 8 domain(s)

Bulk Add

All None	Managed Domain Name	Generate Report	Owner	Action
		□		
□	gmail.com	□	admin	
□	korumaildemo.com	□	admin	
☑	mail.rediff.com	□	admin	
☑	mail.yahoo.com	□	admin	
☑	orkut.com	□	admin	
□	outlook.com	□	admin	
□	yahoo.com	□	admin	
□	yopmail.com	□	admin	

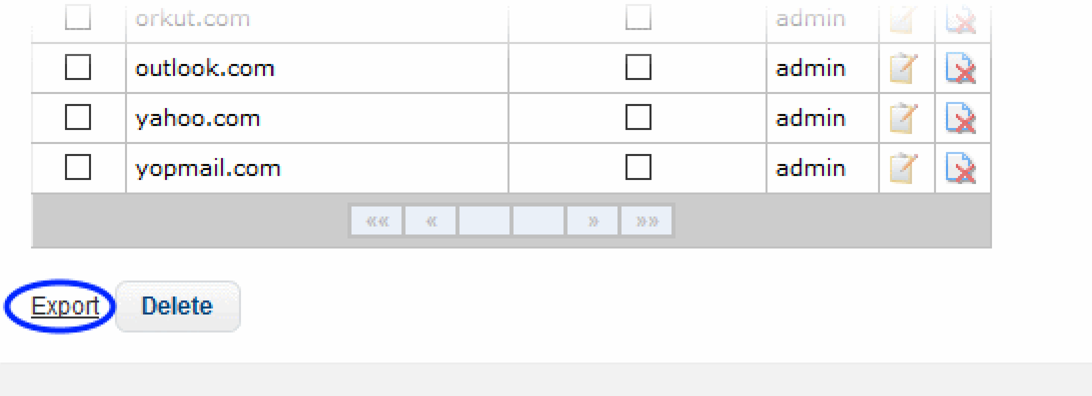
- Click 'OK' to confirm the removal of the selected domains.



Are you sure want to delete selected domain(s)?

To export the domain names

- Click the 'Export' link at the bottom of the screen



□	orkut.com		□	admin		
□	outlook.com		□	admin		
□	yahoo.com		□	admin		
□	yopmail.com		□	admin		

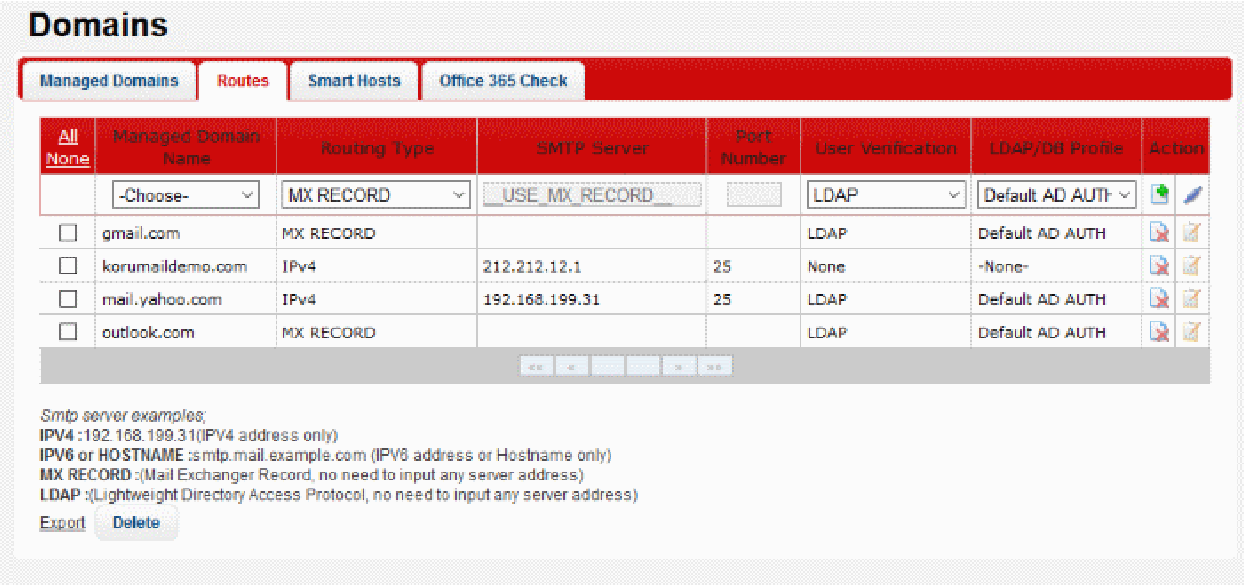
- Download and save the domains list as a text file to your system.

7.2.2 Manage Domain Routes

- Once you have added the domains you wish to manage as explained in the previous section, you can define the route each domain should use to deliver mail after KoruMail has filtered them.
- If no route is defined, then the default domain route will apply. See '**Default Domain Routing**' for more details.

To open the 'Routes' screen

- Click the 'SMTP' tab on the left menu, click 'Domains' > then 'Routes'.



All None	Managed Domain Name	Routing Type	SMTP Server	Port Number	User Verification	LDAP/DB Profile	Action
	-Choose-	MX RECORD	__USE_MX_RECORD__		LDAP	Default AD AUTH	
□	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	

Smtp server examples;
IPV4 :192.168.199.31(IPV4 address only)
IPV6 or HOSTNAME :smtp.mail.example.com (IPV6 address or Hostname only)
MX RECORD :(Mail Exchanger Record, no need to input any server address)
LDAP :(Lightweight Directory Access Protocol, no need to input any server address)

Domain Route - Table of Column Descriptions

Column Header	Description
Managed Domain Name	The name of the domain added to KoruMail
Routing Type	Select the routing type that should be used to send mail to the SMTP server. The options available are: • IPv4 • IPv6 Hostname • MX Record

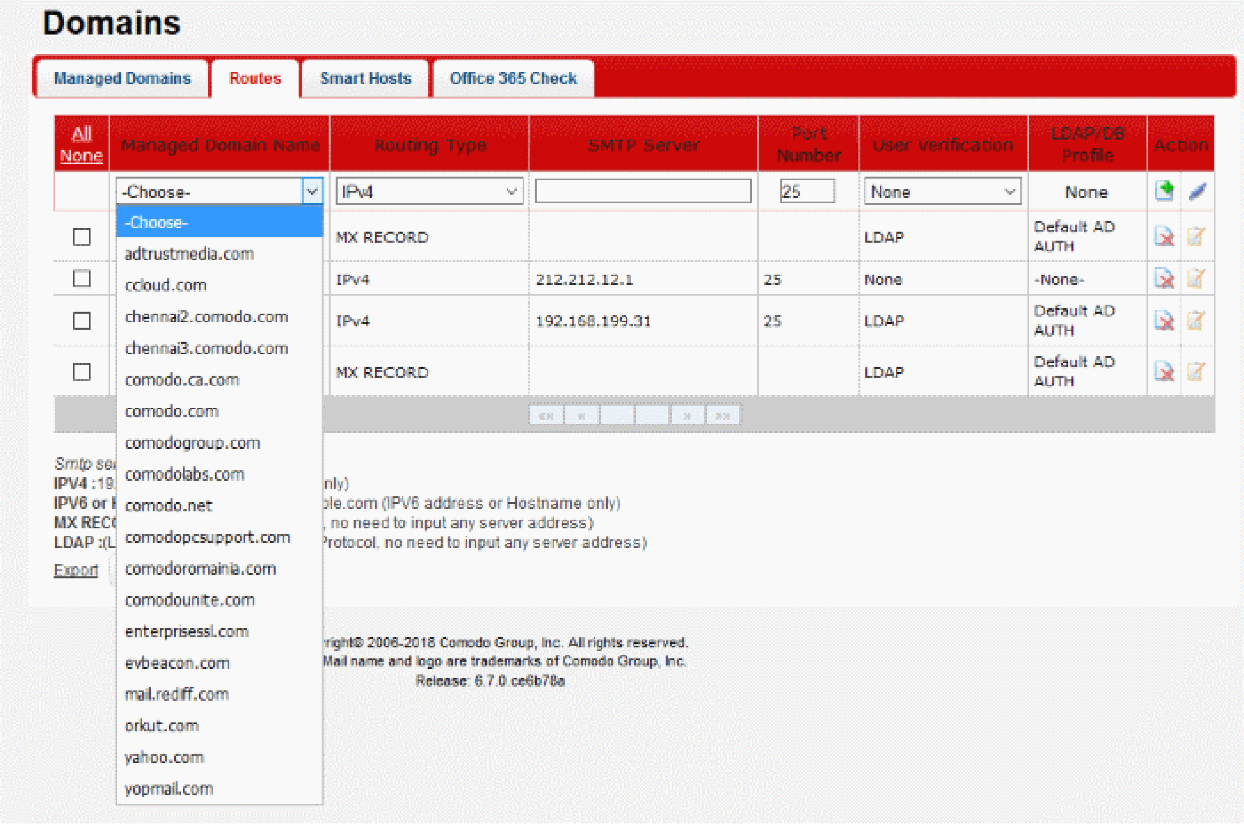
	• LDAP	
SMTP Server	Enter the IP address or the SMTP server name	
Port Number	The port number to which the KoruMail should forward the mail	
User Verification	The type of user verification that KoruMail should use before forwarding the mails. The options available are: • None • Local User DB • My SQL • LDAP	
LDAP/DB Profile	This field will be populated depending on the type of 'User Verification' selected. If 'LDAP' is chosen, then the option to choose the LDAP type will be available from the drop-down.	
Action	➕	To add the domain route, click this button after entering/selecting all the routing details.
	🔌	Click this button to check the connectivity between KoruMail and the SMTP server.
	✖	Allows the administrators to delete a domain route from the list.
	✎	Allows the administrators to edit the domain route.

The interface allow administrators to:

- **Configure domain route for the added domains**
- **Edit a domain route**
- **Delete domain routes**
- **Export domain routes**

To configure a domain route

- Click the 'Choose' drop-down and select the **added domain** for which you want to configure the route.



Domains

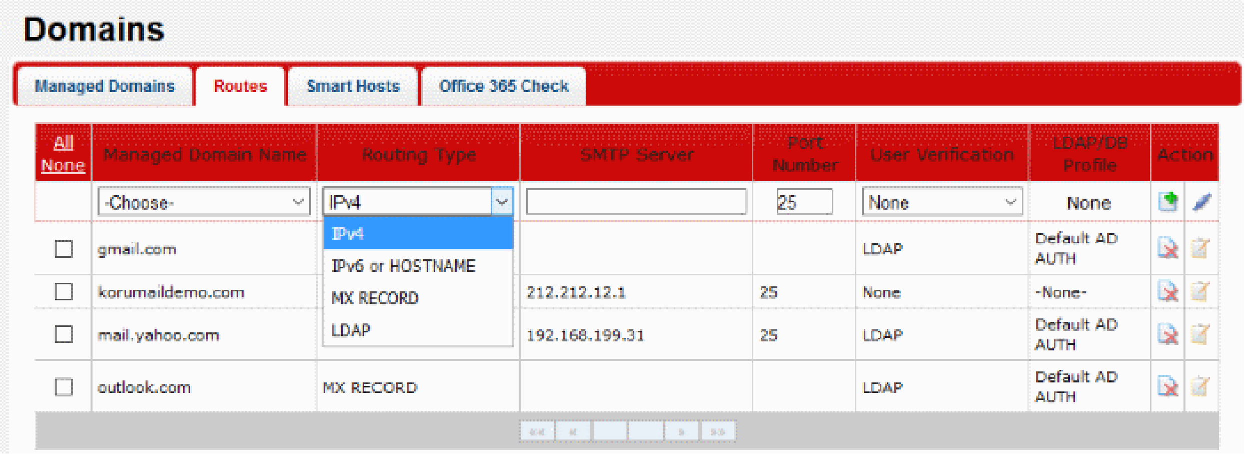
All None	Managed Domain Name	Routing Type	SMTP Server	Port Number	User Verification	LDAP/DB Profile	Action
	-Choose-	IPv4		25	None	None	
□		MX RECORD			LDAP	Default AD AUTH	
□		IPv4	212.212.12.1	25	None	-None-	
□		IPv4	192.168.199.31	25	LDAP	Default AD AUTH	
□		MX RECORD			LDAP	Default AD AUTH	

-Choose-
adtrustmedia.com
ccloud.com
chennai2.comodo.com
chennai3.comodo.com
comodo.ca.com
comodo.com
comodogroup.com
comodolabs.com
comodo.net
comodopcsupport.com
comodoromainia.com
comodounite.com
enterprisessl.com
evbeacon.com
mail.rediff.com
orkut.com
yahoo.com
yopmail.com

Smtp se
IPV4 :19 nly)
IPV6 or ble.com (IPV6 address or Hostname only)
MX REC , no need to input any server address)
LDAP :(L Protocol, no need to input any server address)
Export

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

- Select the routing type that should be used to send mail to the SMTP server.

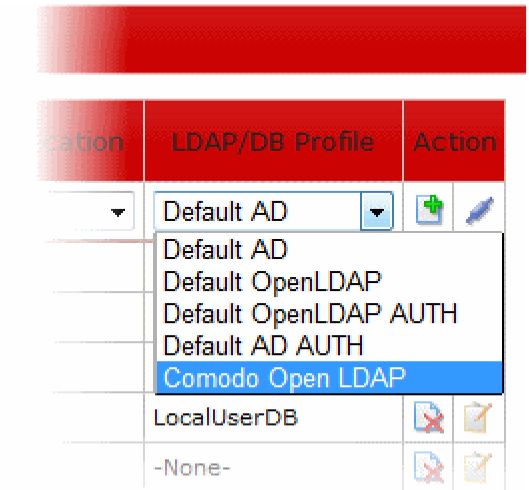


Domains

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

IPv4
IPv6 or HOSTNAME
MX RECORD
LDAP

- Enter the server name or IP address of the SMTP server to which KoruMail should forward the mails to in the filed under 'SMTP Server'
- Enter the port number to which the KoruMail should forward the mail
- Select the verification type that the KoruMail should use before forwarding the mails. The options available are: Local User DB, My SQL and LDAP. These are configured in **LDAP/DB** section.
- 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 displayed from the drop-down. Select the LDAP profile from the options.



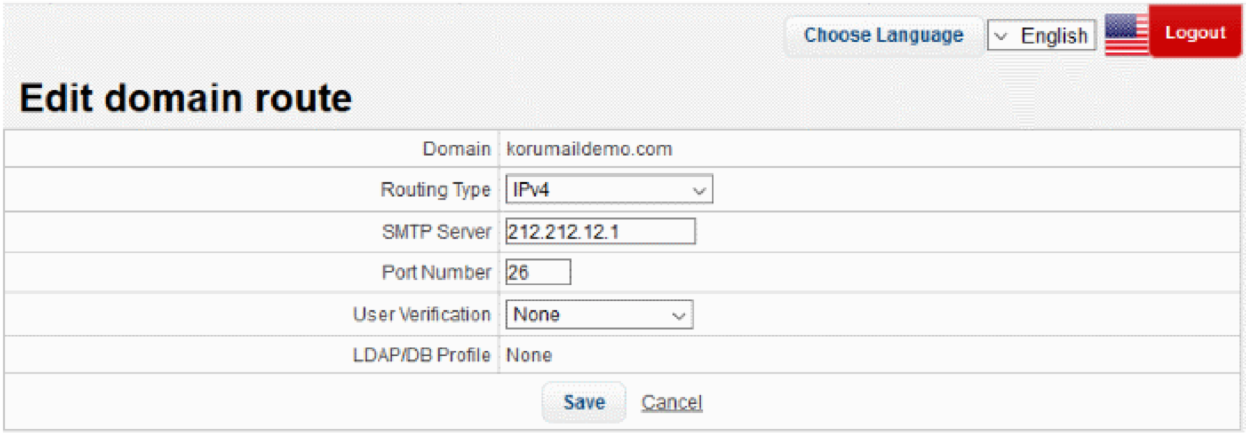
- To check the connectivity between KoruMail and the configured remote server, click the button under the 'Action' column header. The connection will be checked and the result displayed at the top.
- To add a domain route to the list, click the button under the 'Action' column header.

The configured domain route will be added for the domain and displayed in the list.

To edit a domain route

- Click the button under the 'Action' column header for the domain route that you want to edit.

The 'Edit domain route' screen will be displayed.



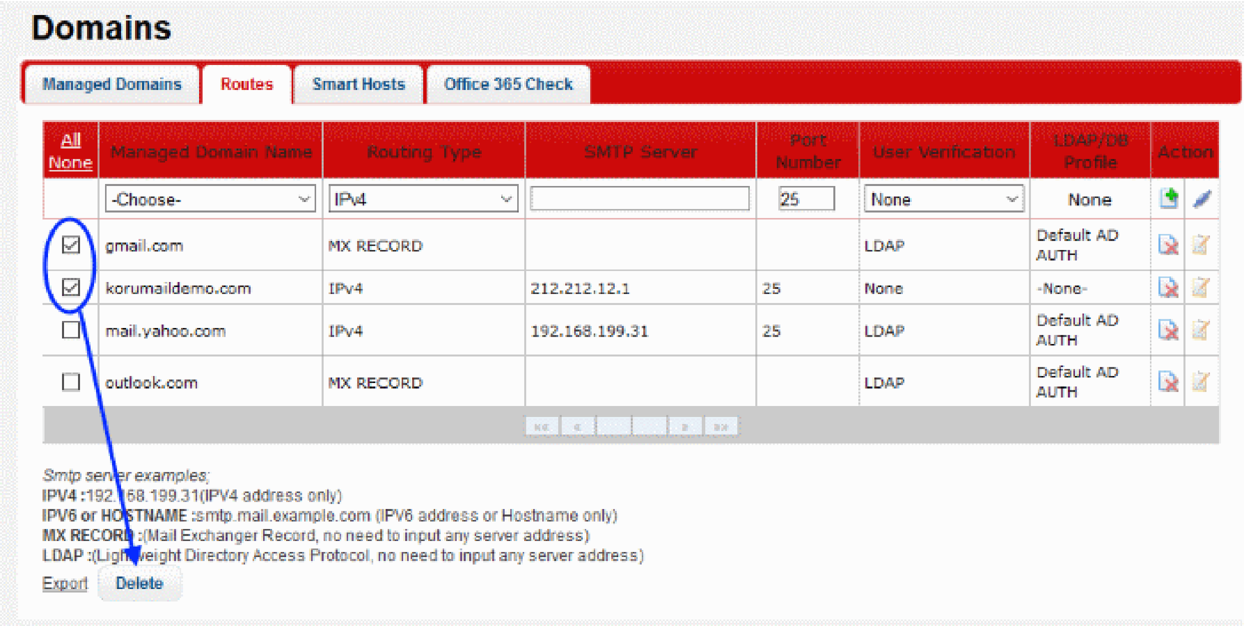
Edit domain route

Domain	korumaildemo.com
Routing Type	IPv4
SMTP Server	212.212.12.1
Port Number	26
User Verification	None
LDAP/DB Profile	None

- Edit the required parameters. This is similar to the method explained in the '**Add**' section.
- Click 'Save' to apply your changes.

To delete domain routes

- Delete individual routes - Click the button under the 'Action' column header.
- Delete multiple routes - Select the check box each domain and click the 'Delete' button at the bottom.

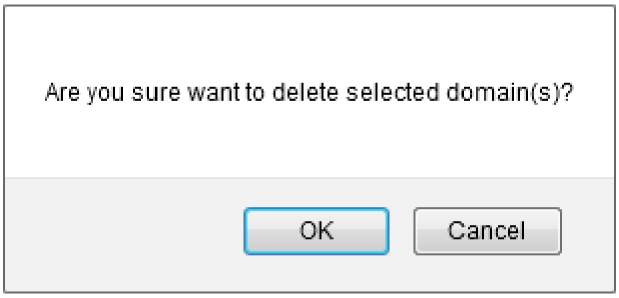


Domains

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	

Smtp server examples;
IPV4 :192.168.199.31(IPV4 address only)
IPV6 or HOSTNAME :smtp.mail.example.com (IPV6 address or Hostname only)
MX RECORD :(Mail Exchanger Record, no need to input any server address)
LDAP :(Lightweight Directory Access Protocol, no need to input any server address)

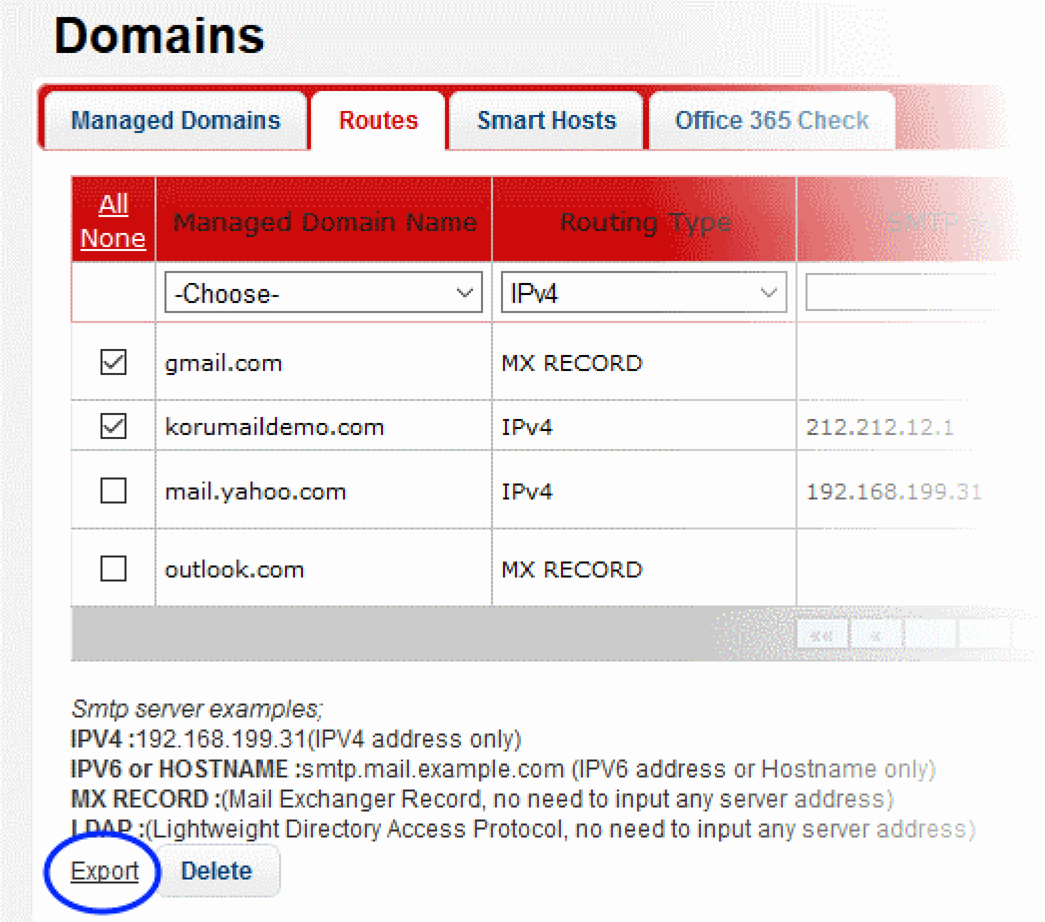
- Click 'OK' to confirm the deletion of the selected domain routes



Are you sure want to delete selected domain(s)?

To export the domain routes to a file

- Click the 'Export' link at the bottom of the screen



Domains

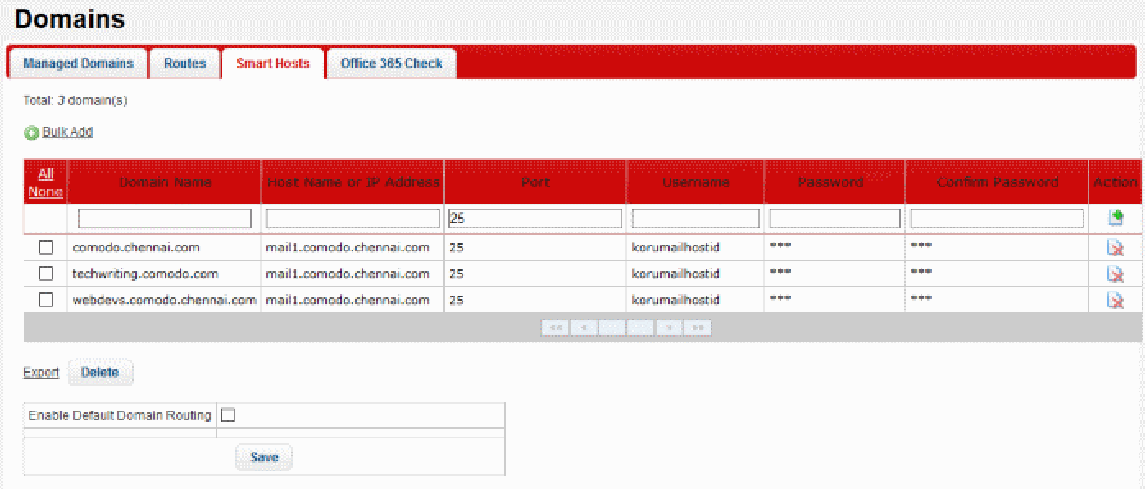
All None	Managed Domain Name	Routing Type	SMTP
	-Choose-	IPv4	
☑	gmail.com	MX RECORD	
☑	korumaildemo.com	IPv4	212.212.12.1
□	mail.yahoo.com	IPv4	192.168.199.31
□	outlook.com	MX RECORD	

Smtp server examples;
IPV4 :192.168.199.31(IPV4 address only)
IPV6 or HOSTNAME :smtp.mail.example.com (IPV6 address or Hostname only)
MX RECORD :(Mail Exchanger Record, no need to input any server address)
LDAP :(Lightweight Directory Access Protocol, no need to input any server address)

- Download and save the domain routes list as a text file to your system.

7.2.3 Manage Smart Hosts

- Smart hosts are an intermediate mail server that receive mail from an SMTP server and, after applying their own policy, forward them to end-user mail boxes.
- Smart hosts require authentication from the sender to verify that the sender is allowed to forward mails through the smart host. This differs from an open mail relay which forwards mail directly to the recipient server without authentication.
  - Please note that a domain added under 'Managed Domains' cannot be added for 'Smart Host' routing.
- The interface also allows admins to configure default domain routing.



Domains

Total: 3 domain(s)

All None	Domain Name	Host Name or IP Address	Port	Username	Password	Confirm Password	Action
			25				
□	comodo.chennai.com	mail1.comodo.chennai.com	25	korumailhostid	***	***	
□	techwriting.comodo.com	mail1.comodo.chennai.com	25	korumailhostid	***	***	
□	webdevs.comodo.chennai.com	mail1.comodo.chennai.com	25	korumailhostid	***	***	

Enable Default Domain Routing □

  - This applies to 'Managed Domains' whose routing has not been configured. See '**Default Domain**

Routing' for more details.

To open the 'Smart Hosts' screen

- Click 'SMTP' > 'Domains' on the left
- Click the 'Smart Hosts' tab.

<table>
<tr><th colspan="3">Smart Hosts - Table of Column Descriptions</th></tr>
<tr><th>Column Header</th><th colspan="2">Description</th></tr>
<tr><td>Domain Name</td><td colspan="2">The URL of the domain added to KoruMail.</td></tr>
<tr><td>Host Name or IP Address</td><td colspan="2">Host Name or IP address of the smart host.</td></tr>
<tr><td>Port</td><td colspan="2">The port number to which the KoruMail should forward the mail.</td></tr>
<tr><td>Username</td><td colspan="2">Enter a username for the corresponding domain name.</td></tr>
<tr><td>Password</td><td colspan="2">Enter a password for the corresponding domain name.</td></tr>
<tr><td>Confirm Password</td><td colspan="2">Enter the password again to set it for the domain name.</td></tr>
<tr><td rowspan="2">Action</td><td>➕</td><td>To route the domain to a 'Smart Host', click this button after entering all the routing details.</td></tr>
<tr><td>❌</td><td>Allows the administrators to delete a domain 'Smart Host' route from the list.</td></tr>
</table>

The interface allow administrators to:

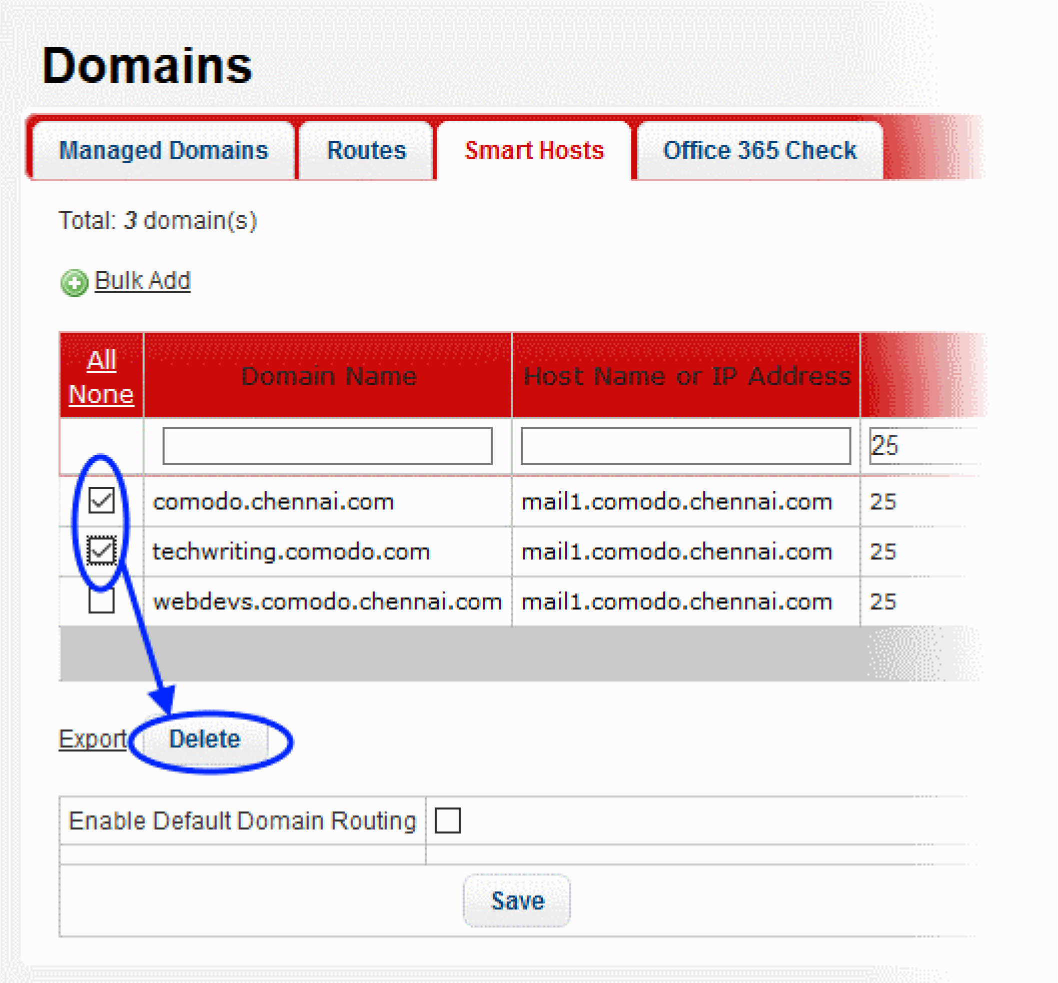
- **Configure 'Smart Host' route for domains**
- **Delete 'Smart Host' routes for domains**
- **Export 'Smart Host' routes list for domains**

To configure 'Smart Host' route for domains

- Enter the domain whose mail you wish to route to a smart host in the 'Domain Name' column
- Enter the host name or IP address of the smart host you wish to use for that domain
- Add the port number to which KoruMail should forward the mail
- To add the 'Smart Host' route to the list, click ➕ under the 'Action' column header.

To delete 'Smart Host' route for domains

- To delete 'Smart Host' routes one at a time, click ❌ under the 'Action' column header and confirm the deletion in 'Confirmation' dialog.
- To delete 'Smart Host' routes, select the check boxes beside them and click 'Delete' at the bottom.



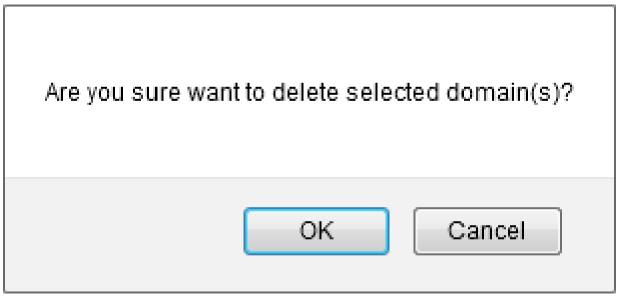
Domains

Total: 3 domain(s)

All None	Domain Name	Host Name or IP Address	
			25
☑	comodo.chennai.com	mail1.comodo.chennai.com	25
☑	techwriting.comodo.com	mail1.comodo.chennai.com	25
☐	webdevs.comodo.chennai.com	mail1.comodo.chennai.com	25

Enable Default Domain Routing ☐

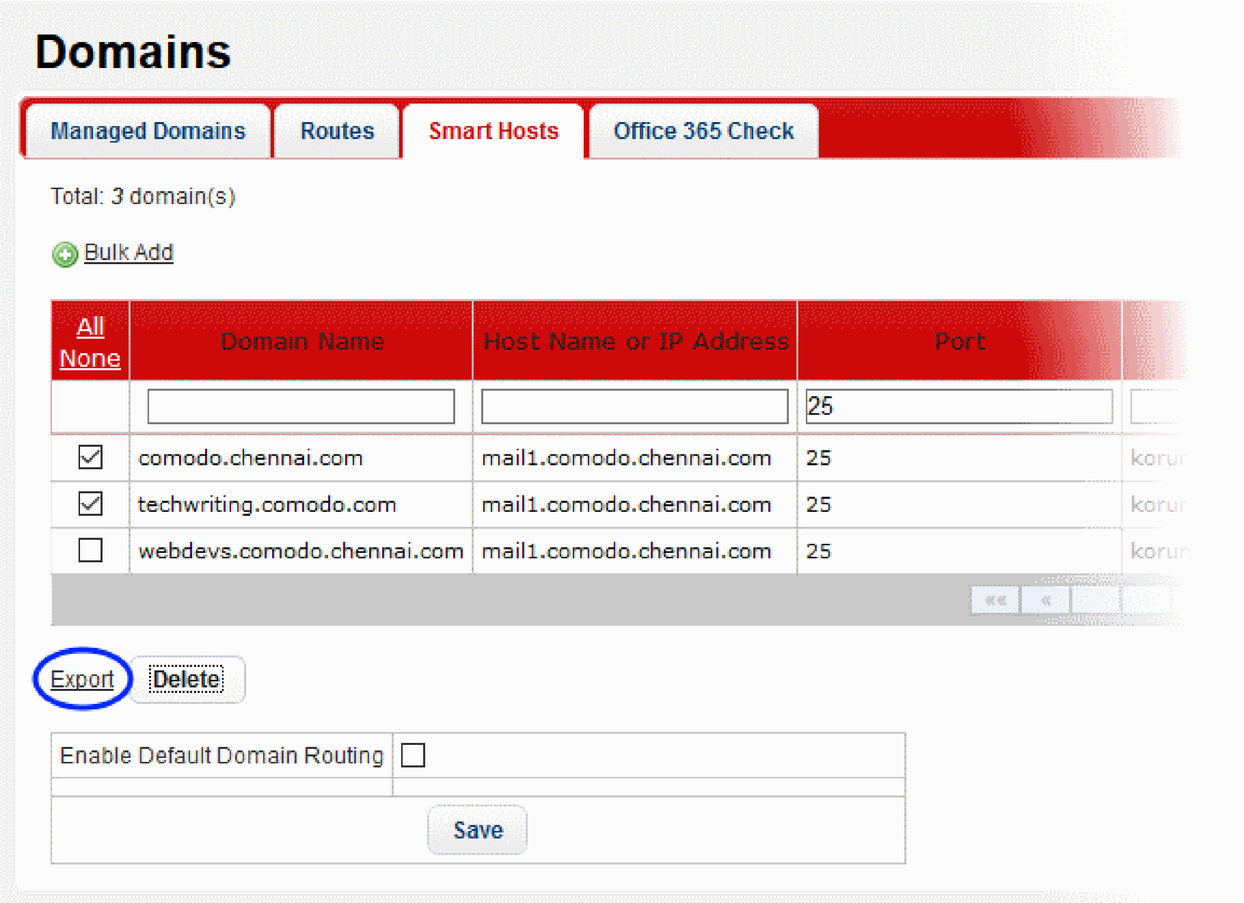
- Click 'OK' to confirm the deletion of the selected 'Smart Host' routes



Are you sure want to delete selected domain(s)?

To export 'Smart Host' routes list for domains

- Click the 'Export' link at the bottom of the screen



Domains

Total: 3 domain(s)

Bulk Add

All None	Domain Name	Host Name or IP Address	Port	
			25	
☑	comodo.chennai.com	mail1.comodo.chennai.com	25	korur
☑	techwriting.comodo.com	mail1.comodo.chennai.com	25	korur
☐	webdevs.comodo.chennai.com	mail1.comodo.chennai.com	25	korur

Enable Default Domain Routing	☐

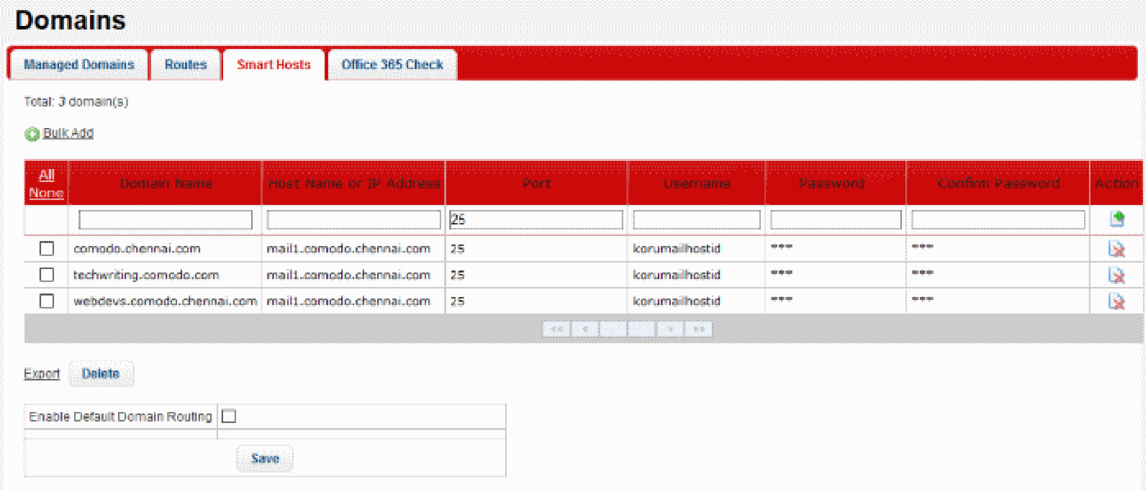
- Download and save the 'Smart Host' routes list as a text file to your system.

7.2.4 Default Domain Routing

- KoruMail allows admins to configure routing for '**Managed Domains**' that are protected by its filtering engine.
- See '**Manage Domain Routes**' to find out how to configure routing for managed domains. If no custom routing is defined then the default routing scheme is applied.
- The default settings can be configured in the 'Smart Hosts' section.

To open the 'Smart Hosts' screen,

- Click 'SMTP' > 'Domains' on the left
- Select the 'Smart Hosts' tab



Domains

Total: 3 domain(s)

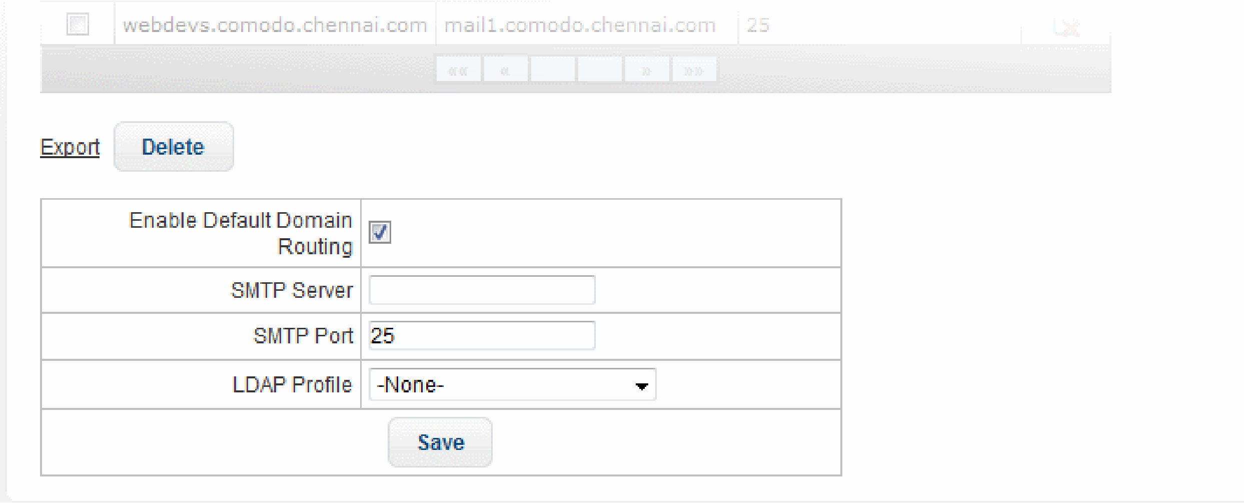
Bulk Add

All None	Domain Name	Host Name or IP Address	Port	Username	Password	Confirm Password	Action
			25				
☐	comodo.chennai.com	mail1.comodo.chennai.com	25	korumailhostid	***	***	
☐	techwriting.comodo.com	mail1.comodo.chennai.com	25	korumailhostid	***	***	
☐	webdevs.comodo.chennai.com	mail1.comodo.chennai.com	25	korumailhostid	***	***	

Enable Default Domain Routing	☐

- Select the 'Enable Default Domain Routing' check box

The fields for entering/selecting the routing details will be displayed.



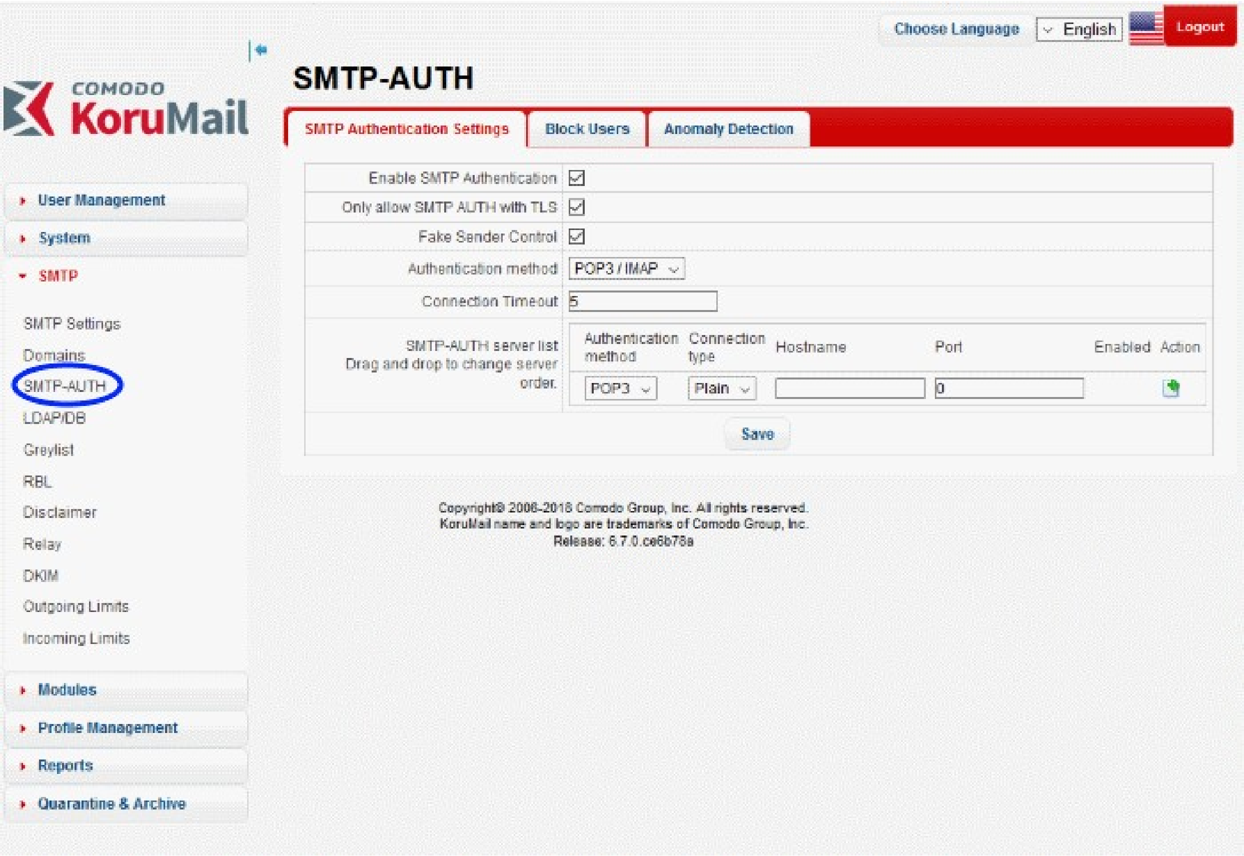
Enable Default Domain Routing	☑
SMTP Server	
SMTP Port	25
LDAP Profile	-None-

  - **SMTP Server:** Enter the server name or IP address of the SMTP server to which KoruMail should forward the mails
  - **SMTP Port:** Enter the port number to which KoruMail should forward the mails
  - **LDAP Profile:** Select the LDAP Profile that KoruMail should use for user verification before forwarding the mails. The LDAP Profiles are configured in **LDAP/DB** section.
- Click 'Save' to apply your changes.

7.3 KoruMail SMTP AUTH Connector

The 'SMTP-AUTH' section lets admins block users, configure authentication settings for outgoing mails, and configure anomaly detection. Anomaly detection lets you track which IP addresses are used to send out mails for an email address.

- Click 'SMTP' > 'SMTP-AUTH' to open the interface:



Enable SMTP Authentication	☑
Only allow SMTP AUTH with TLS	☑
Fake Sender Control	☑
Authentication method	POP3 / IMAP
Connection Timeout	5

SMTP-AUTH server list
Drag and drop to change server order.

Authentication method	Connection type	Hostname	Port	Enabled	Action
POP3	Plain		0		

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

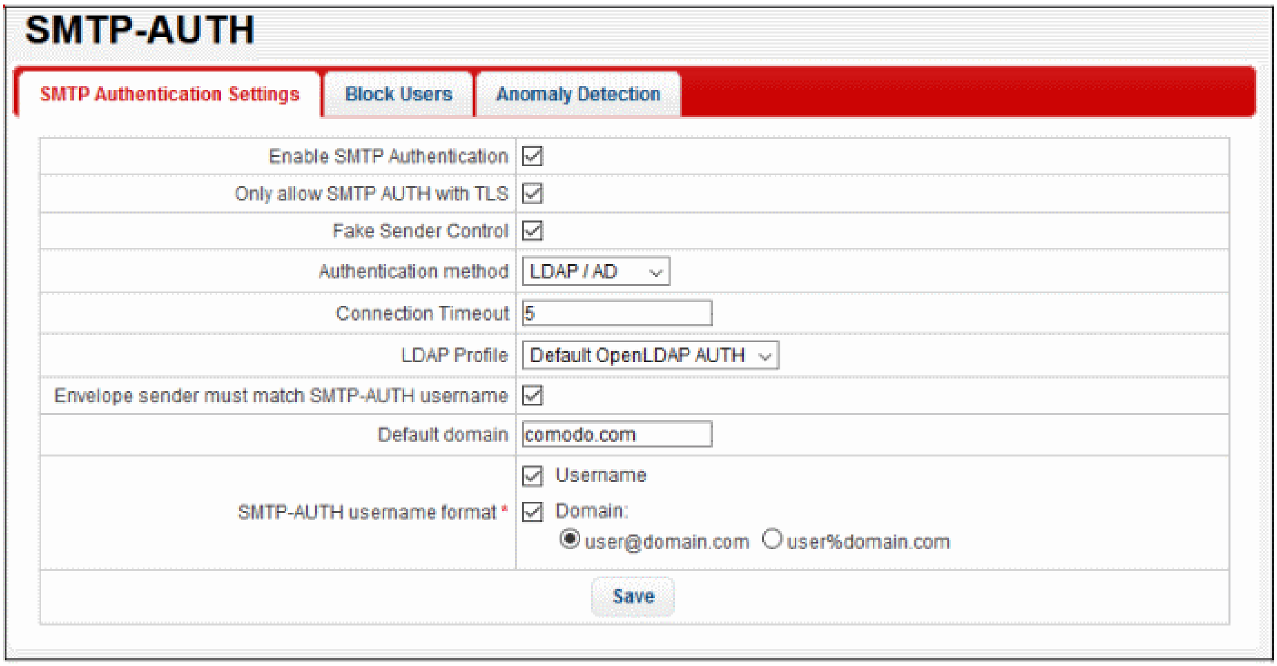
Click the following links for more details:

- SMTP Authentication Settings
- Block Users
- Anomaly Detection

7.3.1 SMTP Authentication Settings

The 'SMTP Authentication Settings' screen allows administrators to configure the user authentication type for outgoing mails.

- To open the 'SMTP Authentication Settings' screen, click the 'SMTP' menu item on the left then 'SMTP-AUTH' then open the 'SMTP Authentication Settings' tab.



SMTP-AUTH

Enable SMTP Authentication	☑
Only allow SMTP AUTH with TLS	☑
Fake Sender Control	☑
Authentication method	LDAP / AD
Connection Timeout	5
LDAP Profile	Default OpenLDAP AUTH
Envelope sender must match SMTP-AUTH username	☑
Default domain	comodo.com
SMTP-AUTH username format *	☑ Username ☑ Domain: ● user@domain.com ○ user%domain.com

SMTP Authentication Settings - Table of Parameters		
Parameter	**Description**	
Enable SMTP Authentication	If enabled, admins can use this interface to configure an SMTP authentication method for senders.	
Only allow SMTP AUTH with TLS	If enabled, authentication must be conducted over a secure TLS connection.	
Fake Sender Control	Will block fake senders	
Authentication Method	Select the user authentication method from the drop-down. The options available are POP3/IMAP and LDAP/AD. The settings fields depend on the options chosen. Refer to '**POP3/IMAP Authentication Method**' and '**LDAP Authentication Method**' for details on the respective settings.	
Connection Timeout	Enter the time in seconds during which authentication between the client and the POP3/IMAP/LDAP server must be completed. The user will be prompted to enter credentials again if the time elapses.	
Envelope sender must match SMTP-AUTH username	KoruMail checks whether the envelope sender name and username is same. KoruMail authenticates the users via the servers added in the SMTP-AUTH server list. If enabled, you have to select any of the authentication type below: SMTP-AUTH username format: • Username – Enter the domain in the default domain field. KoruMail appends the domain to the username and checks in the SMTP auth servers. • Domain – Select the domain format. KoruMail checks the usernames for all domains in the SMTP auth servers.	
POP3/IMAP Authentication Method		
SMTP-AUTH server list	Authentication method	Select authentication method - either POP3 or IMAP.
	Connection type	Select the type of connection (clear text or encrypted SSL/TLS).

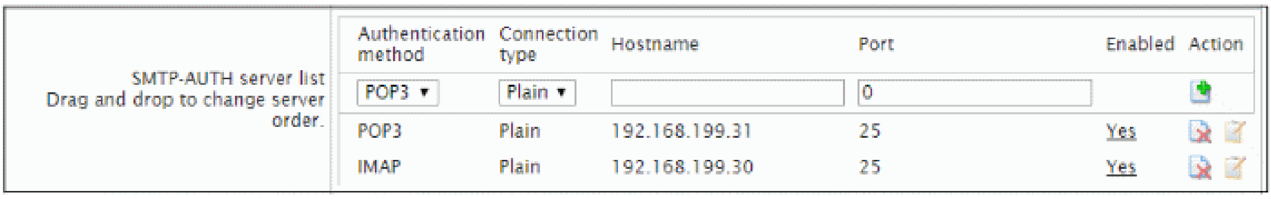
	Hostname	Enter the server name or IP address of the SMTP-AUTH server.	
	Port	Enter the port of the server to which KoruMail should connect to.	
	Enabled	Activate or disable the server.	
	Action	➕	Click this button to add an SMTP-AUTH server to the list after configuring all parameters.
		❌	Allows administrators to delete an auth server from the list.
		✎	Allows administrators to edit the parameters of an auth server.
LDAP/AD Authentication Method			
LDAP Profile	Select the type of LDAP profile from the drop-down. The profiles available are configured in **LDAP/DB** section.		

Configure SMTP authentication settings

- Select the 'Enable SMTP Authentication' check box
- Select the 'Only allow SMTP AUTH with TLS' check box to allow only encrypted SMTP AUTH sessions
- Select the 'Fake Sender Control' to block fake sender email address in the SMTP Server.
- Select the type of authentication method from the 'Authentication method' drop-down. The options available are POP3 / IMAP and LDAP. Refer to '**POP3/IMAP Authentication Method**' and '**LDAP Authentication Method**' for details on the respective settings.
- Enter the time in seconds after which the SMTP Auth session will end.

POP3/IMAP Authentication Method

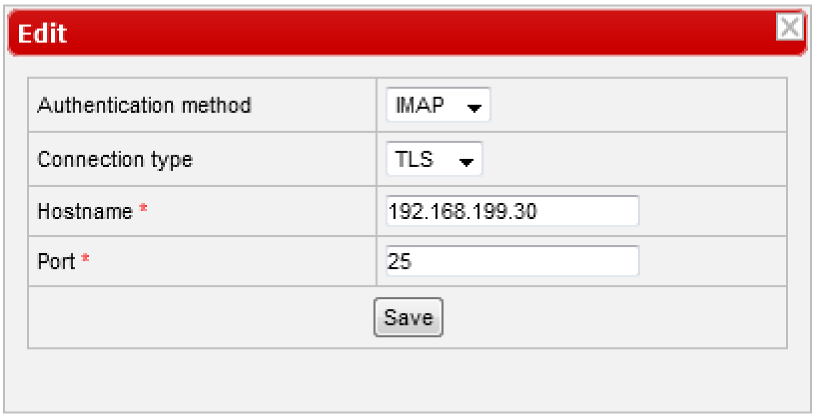
- Authentication method - Select the POP3 or IMAP type of authentication method from the drop-down.
- Connection type - Selection the type of connection, whether it should clear text or encrypted. The options available are 'Plain', 'SSL' and 'TLS'.
- Hostname - Enter the IP address or the server name of the SMTP AUTH server.
- Port - Enter the port of the server to which KoruMail should connect to.
- Click the ➕ button to add the server to the list.
- Repeat the process to add more auth servers.



SMTP-AUTH server list
Drag and drop to change server order.

Authentication method	Connection type	Hostname	Port	Enabled	Action
POP3 ▾	Plain ▾		0		➕
POP3	Plain	192.168.199.31	25	Yes	❌ ✎
IMAP	Plain	192.168.199.30	25	Yes	❌ ✎

- You can change the server order by dragging and dropping them.
- To edit the details of an auth server, click the ✎ button.



Edit

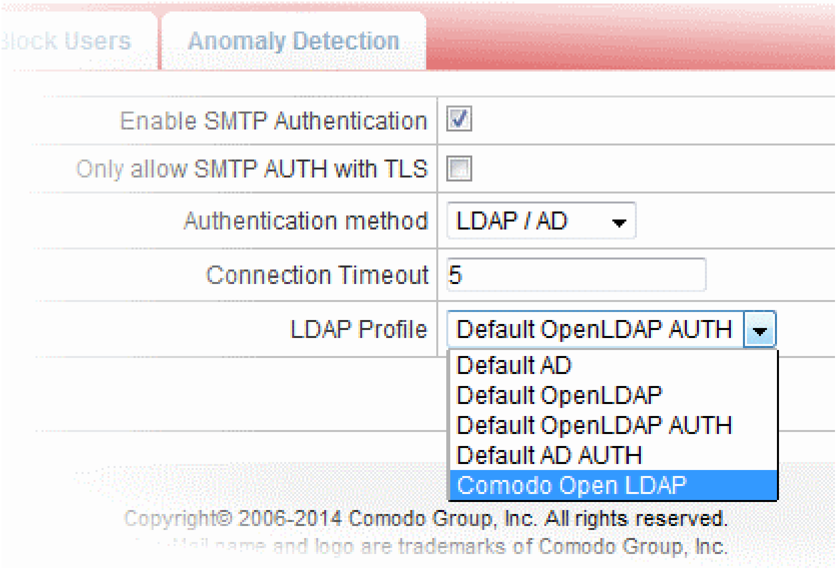
Authentication method	IMAP
Connection type	TLS
Hostname *	192.168.199.30
Port *	25

- Edit the parameters as required and click the 'Save' button.
- To delete an auth server from the list, click the ☒ button and click 'OK' in the confirmation dialog.

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

LDAP Authentication Method

- LDAP Profile - Select the type of LDAP profile from the drop-down. The profiles available here are configured in **LDAP/DB** section.



Enable SMTP Authentication	☑
Only allow SMTP AUTH with TLS	□
Authentication method	LDAP / AD
Connection Timeout	5
LDAP Profile	Default OpenLDAP AUTH

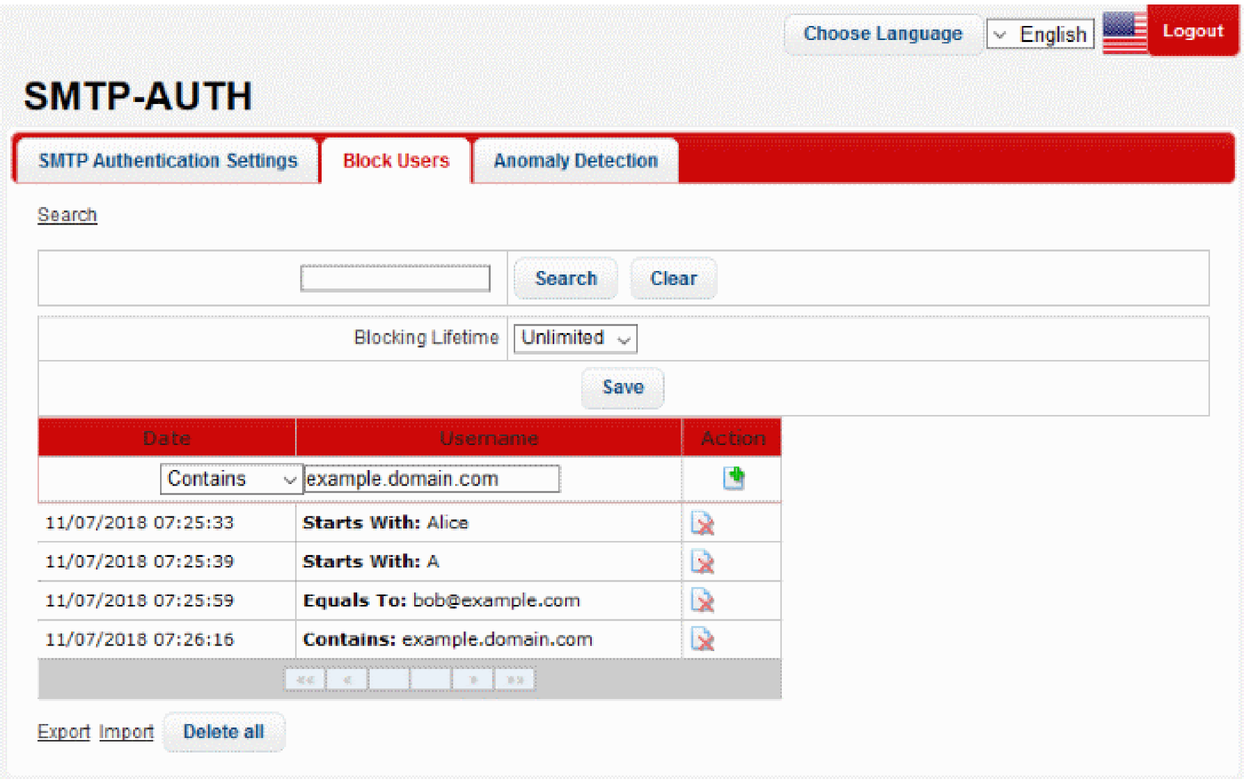
Copyright© 2006-2014 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.

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

7.3.2 Block Users

Administrators can block outgoing mails from users that are routed via KoruMail. The 'Block Users' interface also allows you to search for blocked users and domains.

- To open the 'Block Users' screen, click the 'SMTP' tab on the left and click 'SMTP-AUTH' then 'Block Users'.



Blocking Lifetime: Unlimited

Date	Username	Action
Contains	example.domain.com	
11/07/2018 07:25:33	**Starts With:** Alice	
11/07/2018 07:25:39	**Starts With:** A	
11/07/2018 07:25:59	**Equals To:** bob@example.com	
11/07/2018 07:26:16	**Contains:** example.domain.com	

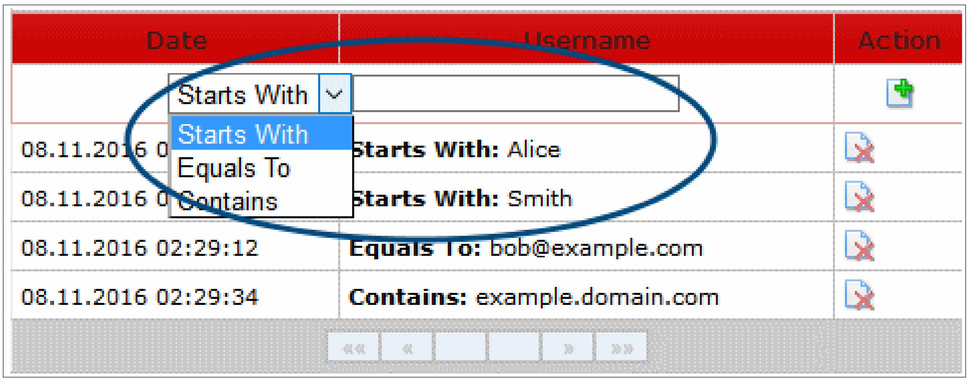
The interface allow administrators to:

- Add blocked users
- Block Lifetime
- Remove users from the blocked list
- Search for blocked users
- Export lists of blocked users
- Import lists of blocked users from file

Add a Blocked User

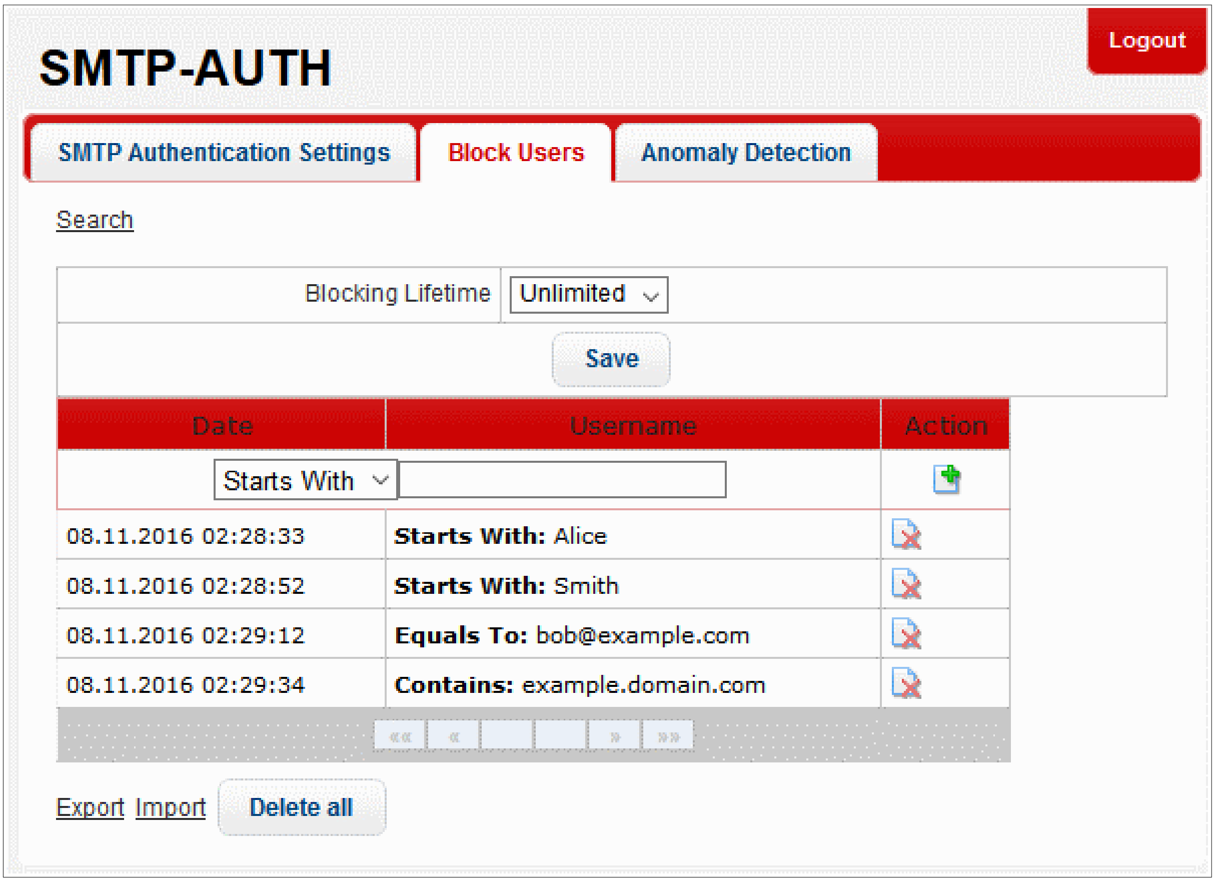
Type the username (or part of the username) of the user you wish to block in the 'Username' field. You can then set how the rule should be applied using the drop-down menu:

- Starts With - Blocks users whose names begin with the entered text
- Equals To - Blocks users whose names exactly match the entered text
- Contains - Blocks users whose names contain the entered text somewhere in their name. Will also block exact matches



Date	Username	Action
08.11.2016 0	**Starts With:** Alice	
08.11.2016 0	**Starts With:** Smith	
08.11.2016 02:29:12	**Equals To:** bob@example.com	
08.11.2016 02:29:34	**Contains:** example.domain.com	

- Click the 'Add' button to apply your choice. The item will be added to the list with the category type displaying on the left side.



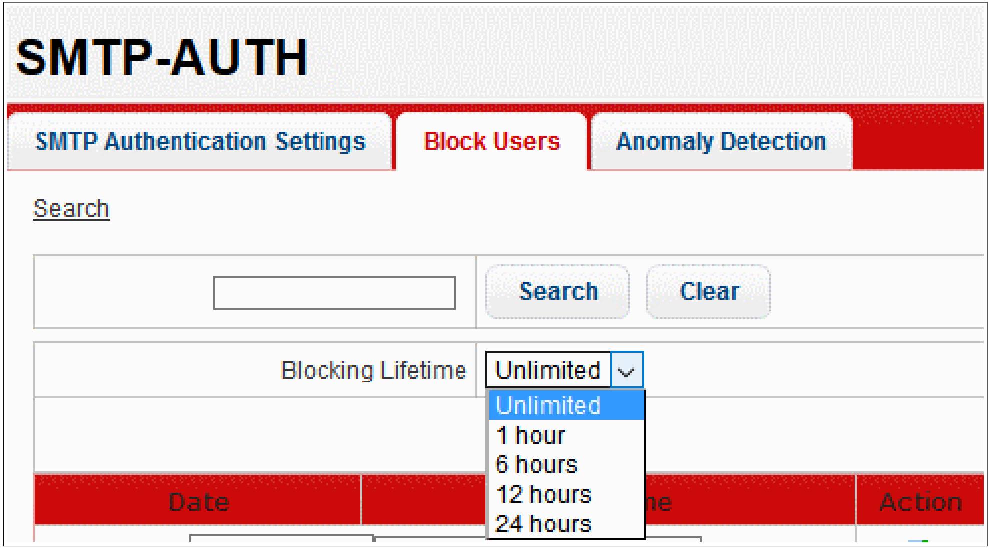
SMTP-AUTH

Blocking Lifetime: Unlimited

Date	Username	Action
	Starts With	
08.11.2016 02:28:33	**Starts With:** Alice	
08.11.2016 02:28:52	**Starts With:** Smith	
08.11.2016 02:29:12	**Equals To:** bob@example.com	
08.11.2016 02:29:34	**Contains:** example.domain.com	

Block Lifetime

The 'Blocking lifetime' refers to the number of hours the email address will remain blocked at the SMTP Server. The available intervals are 'Unlimited', '1 hour', '6 hours', '12 hours' and '24 hours'.

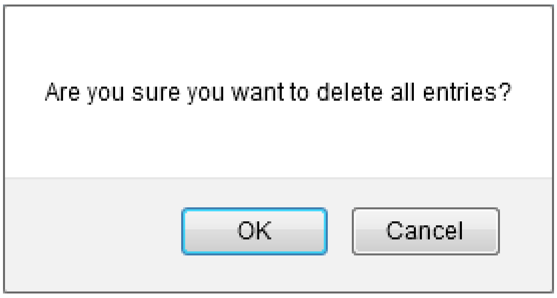


SMTP-AUTH

Blocking Lifetime: Unlimited

To remove users from the blocked list

- To remove users one at a time, click the button under the 'Action' column header and confirm the deletion in the 'Confirmation' dialog.
- To delete all the blocked users in the list, click the 'Delete all' button at the bottom.

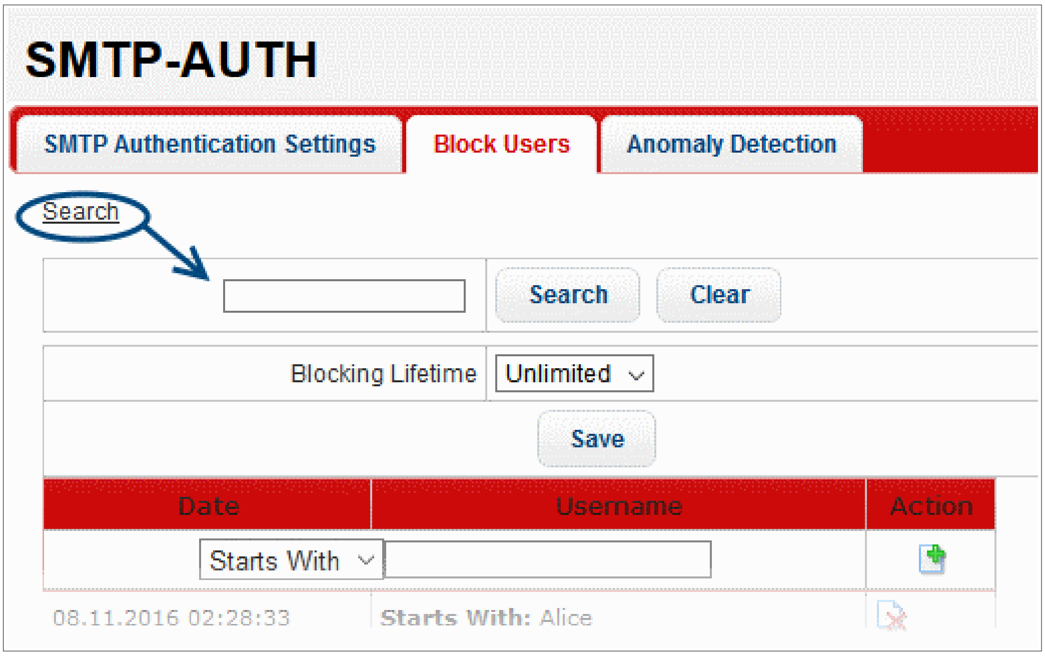


Are you sure you want to delete all entries?

- Click 'OK' to confirm the deletion of all blocked users.

To search for blocked users

- Click the 'Search' link at the top of the interface

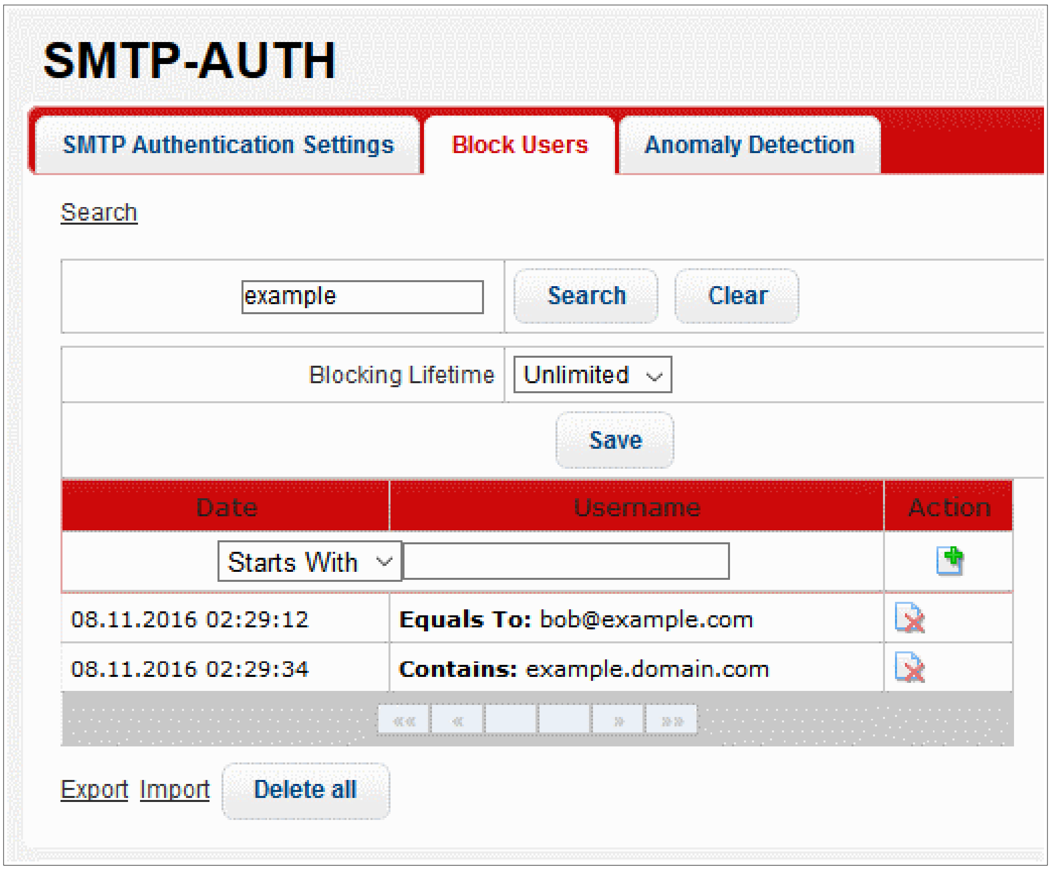


Blocking Lifetime: Unlimited

Date	Username	Action
Starts With		
08.11.2016 02:28:33	Starts With: Alice	

- In the search field, enter a full or partial name and click the 'Search' button.

The items that contain the entered search text will be displayed.



Search field: example

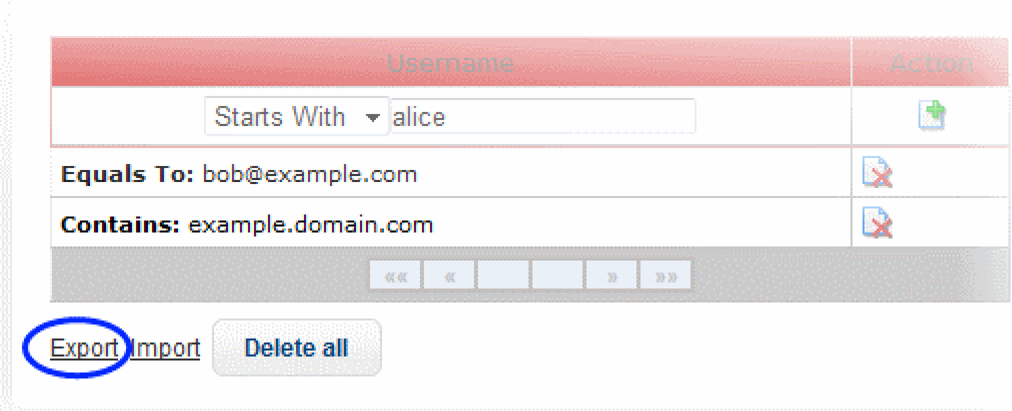
Blocking Lifetime: Unlimited

Date	Username	Action
	Starts With	
08.11.2016 02:29:12	**Equals To:** bob@example.com	
08.11.2016 02:29:34	**Contains:** example.domain.com	

- To display all the items again, click the 'Clear' button.
- To remove the search field, click the 'Search' link again.

To export blocked users to file

- Click the 'Export' link at the bottom of the screen

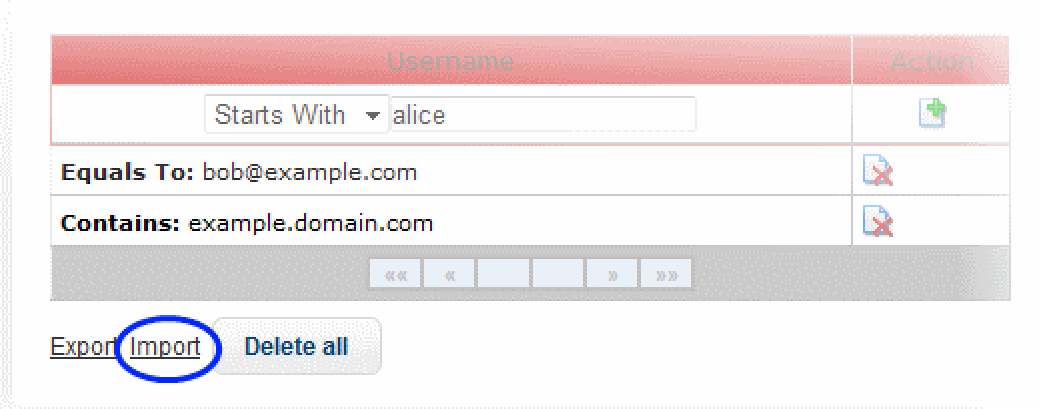


Username	Action
Starts With alice	
Equals To: bob@example.com	
Contains: example.domain.com	

- Download and save the blocked user list as a text file to your system.

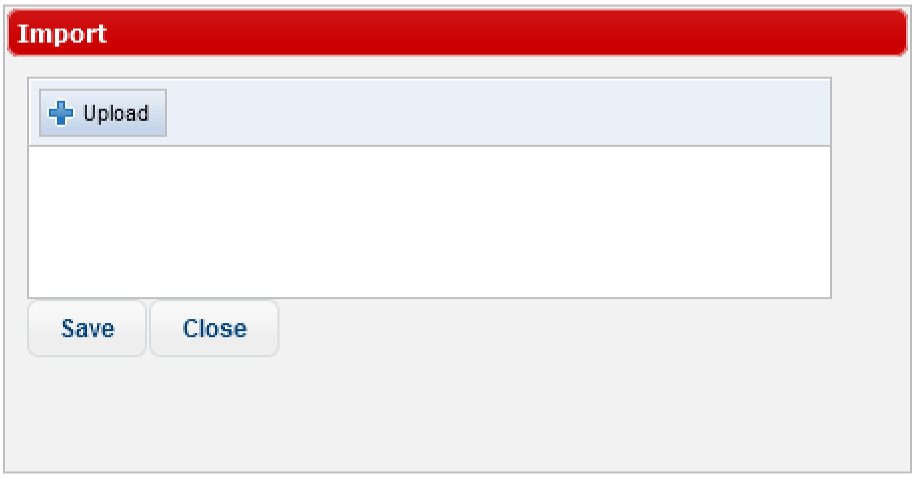
To import blocked users from file

- Click the 'Import' link at the bottom of the screen

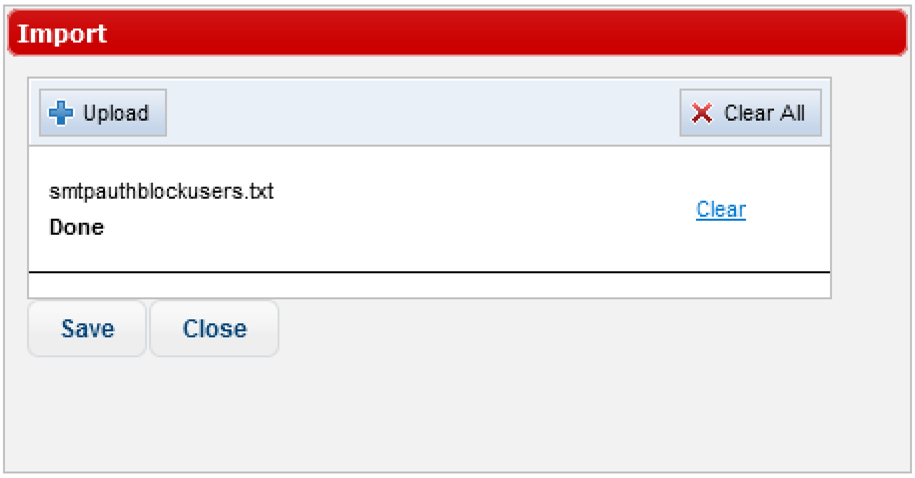


Username	Action
Starts With ▾ alice	
Equals To: bob@example.com	
Contains: example.domain.com	

The 'Import' dialog will be displayed.



- Click the 'Upload' button, navigate to the the location where the file is saved, select it and click 'Open'.



smtpauthblockusers.txt

Done

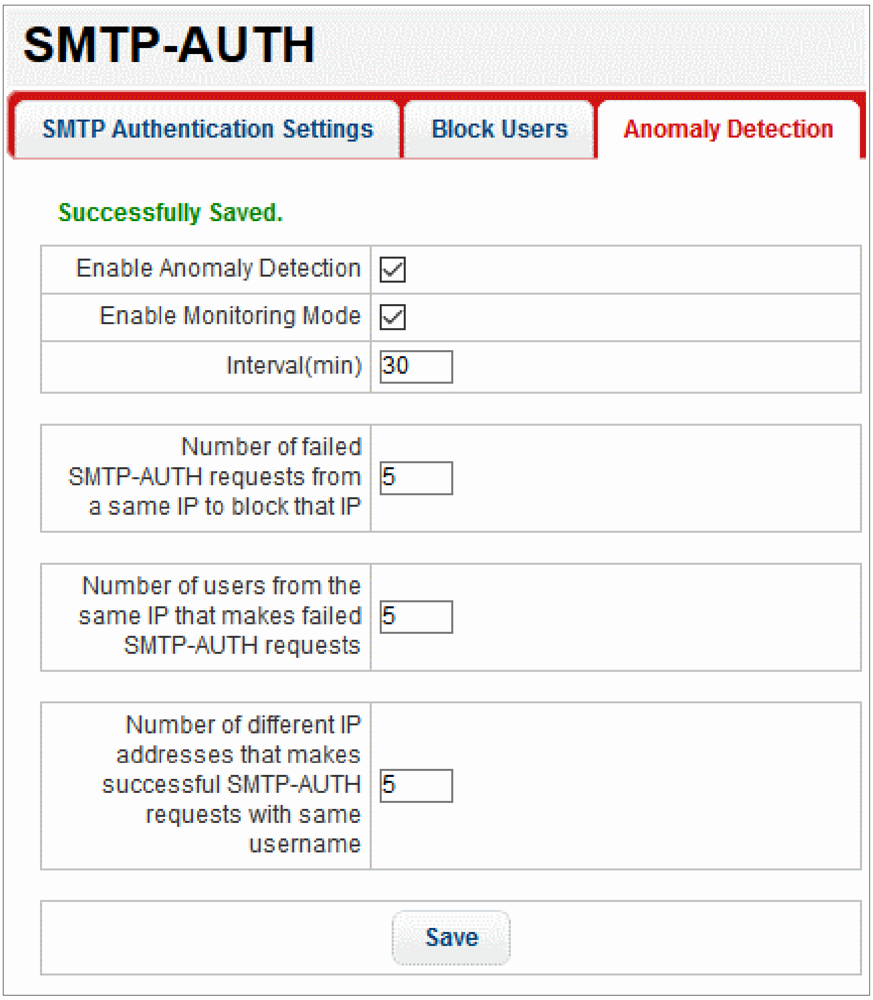
- Repeat the process to add more files.
- To remove a file, click the 'Clear' link beside it.
- To remove all added files, click the 'Clear All' button at top right.
- To finalize the import, click the 'Save' button.

7.3.3 Anomaly Detection

- Allows you to receive alerts when KoruMail detects a user/email address has sent messages from multiple IP addresses within a set time interval.
- You can choose to block these users if the outgoing mail IP addresses exceed the number set in this tab.
- This value can not be '0', therefore administrators are expected to set a value between 1 and 10,000 to block users, IP addresses or SMTP Auth requests.

To open the 'Anomaly Detection' screen,

- Click 'SMTP' > 'SMTP-AUTH' on the left
- Open the 'Anomaly Detection' tab.



SMTP-AUTH

Successfully Saved.

Enable Anomaly Detection	☑
Enable Monitoring Mode	☑
Interval(min)	30
Number of failed SMTP-AUTH requests from a same IP to block that IP	5
Number of users from the same IP that makes failed SMTP-AUTH requests	5
Number of different IP addresses that makes successful SMTP-AUTH requests with same username	5

Anomaly Detection Settings - Table of Parameters	
Parameter	**Description**
Enable Anomaly Detection	Enables anomaly detection with the parameters listed directly below this setting.
Enable monitoring mode	If enabled, the SMTP-AUTH controller monitors authorization requests from the specified IP addresses.
Interval (min)	The auditing time period for anomaly detection. To use the default settings as an example, a user will be blocked if detected IP addresses exceed 100 in any 30 minute period. Administrators will receive an alert if more than 30 IPs are detected in 30 minutes.
Number of failed SMTP-	Number of failed SMTP-AUTH requests from a particular IP before it is rejected.

AUTH requests from a same IP to block that IP	
Number of users from the same IP that makes failed SMTP-AUTH requests	The minimum number of users with same IP address that can make failed SMTP-AUTH requests. Any request beyond the threshold set will not be processed
Number of different IP addresses that makes successful SMTP-AUTH requests with same username	The minimum number of different IP addresses that can make successful SMTP-AUTH requests with the same username. Any request beyond the threshold set will not be processed

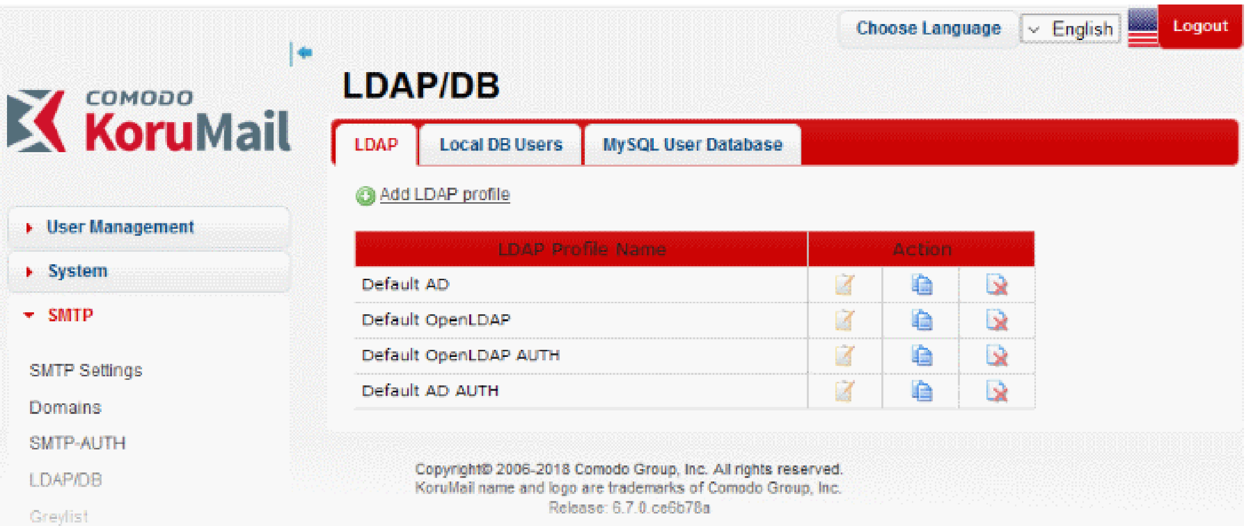
- Click the 'Save' button to apply your changes.

7.4 LDAP/Local DB/My SQL User Database

- KoruMail can be configured to check the validity of a recipient before filtering so that resources are not wasted on invalid recipients.
- If the email servers behind KoruMail are integrated with LDAP, Local DB and/or MY SQL database, then KoruMail will check the validity of recipients. If they are not valid the mails will be rejected at the SMTP level.

To open the 'LDAP/DB' screen:

- Click 'SMTP' > 'LDAP/DB' on the left menu



LDAP Profile Name	Action		
Default AD			
Default OpenLDAP			
Default OpenLDAP AUTH			
Default AD AUTH			

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

See the following sections for more details:

- **LDAP (Lightweight Directory Access Protocol)**
- **Local DB Users**
- **MySQL User Database**

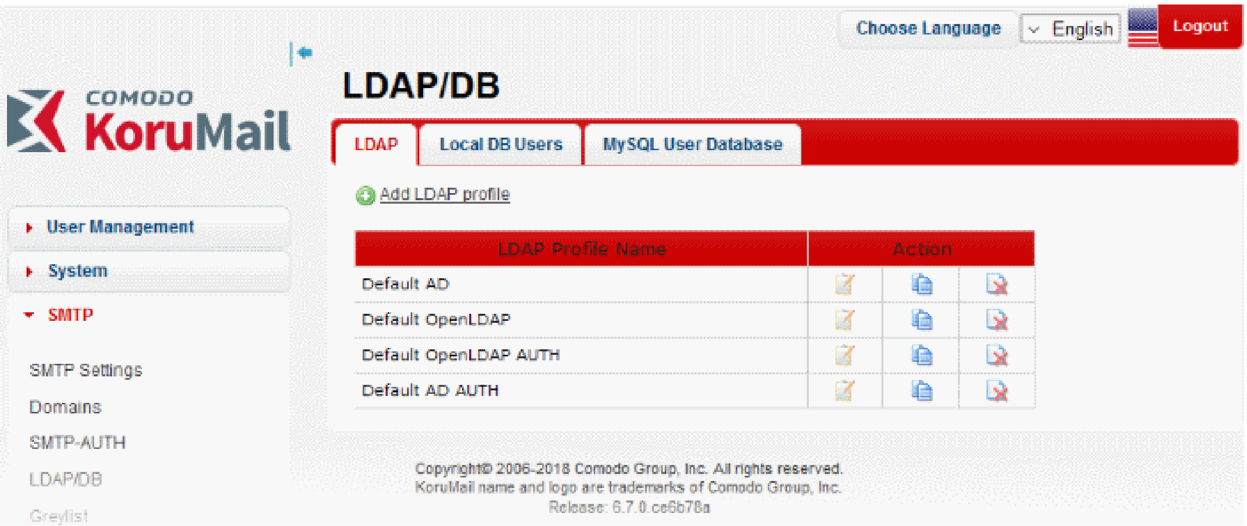
7.4.1 LDAP Profile

- The Lightweight Directory Access Protocol (LDAP) is used to query and modify data using directory services running over TCP/IP.
- If the email servers behind KoruMail are integrated with a directory service via an LDAP profile, KoruMail can check whether the recipient is a valid user in the directory.
- If the recipient is not a valid user then the email is rejected at the SMTP level. This avoids wasting resources by filtering mail for for invalid recipients.

- The LDAP profiles added here are available for selection in interfaces such as '**Managed Domains** > **Routes**' and '**SMTP AUTH** > **SMTP Authentication Settings**'.

To open the 'LDAP' screen

- Click the 'SMTP' tab on the left and click 'LDAP/DB' then 'LDAP'.



LDAP Profile Name	Action		
Default AD	✎	⎘	✖
Default OpenLDAP	✎	⎘	✖
Default OpenLDAP AUTH	✎	⎘	✖
Default AD AUTH	✎	⎘	✖

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

LDAP Profile - Table of Column Descriptions		
Column Header	**Description**	
LDAP Profile Name	The name of the LDAP profile added to KoruMail	
Action	✎	Allows the administrators to edit the details of a LDAP profile
	⎘	Allows administrators to copy a LDAP profile so it can be used as the basis for a new profile.
	✖	Allows the administrators to delete a LDAP profile from the list.

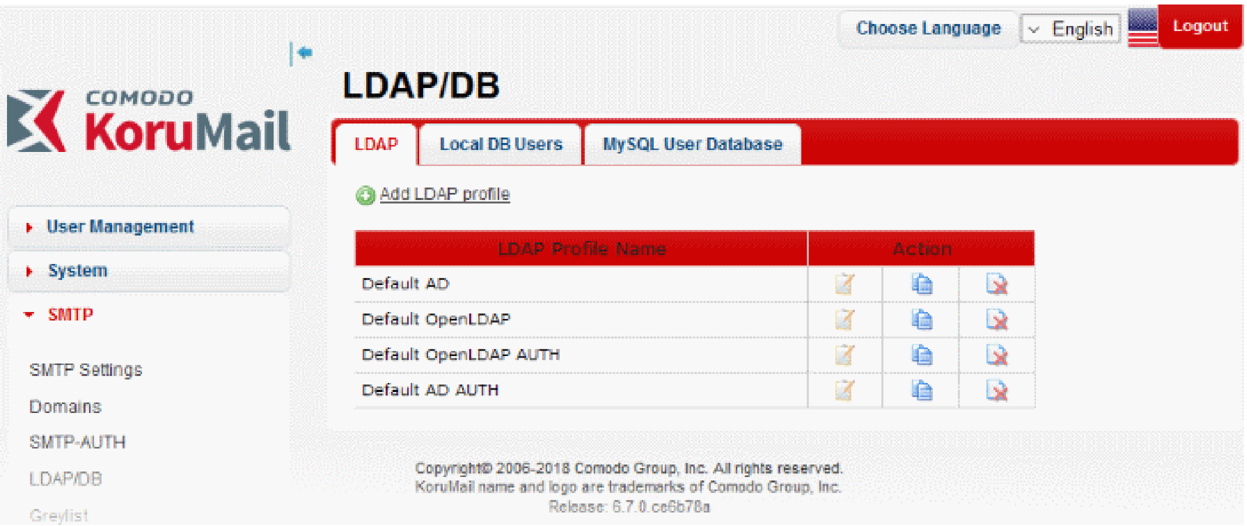
From this screen administrators can:

- **Create and add a new LDAP profile**
- **Edit a LDAP profile**
- **Delete a LDAP profile**

To create a new LDAP profile

You can create a new LDAP profile in two ways:

- By clicking the copy button ⎘ beside an LDAP profile. This will open the 'New LDAP Profile' screen with details pre-populated for the copied profile.
- By clicking the 'Add LDAP profile' link at the top



LDAP Profile Name	Action		
Default AD			
Default OpenLDAP			
Default OpenLDAP AUTH			
Default AD AUTH			

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

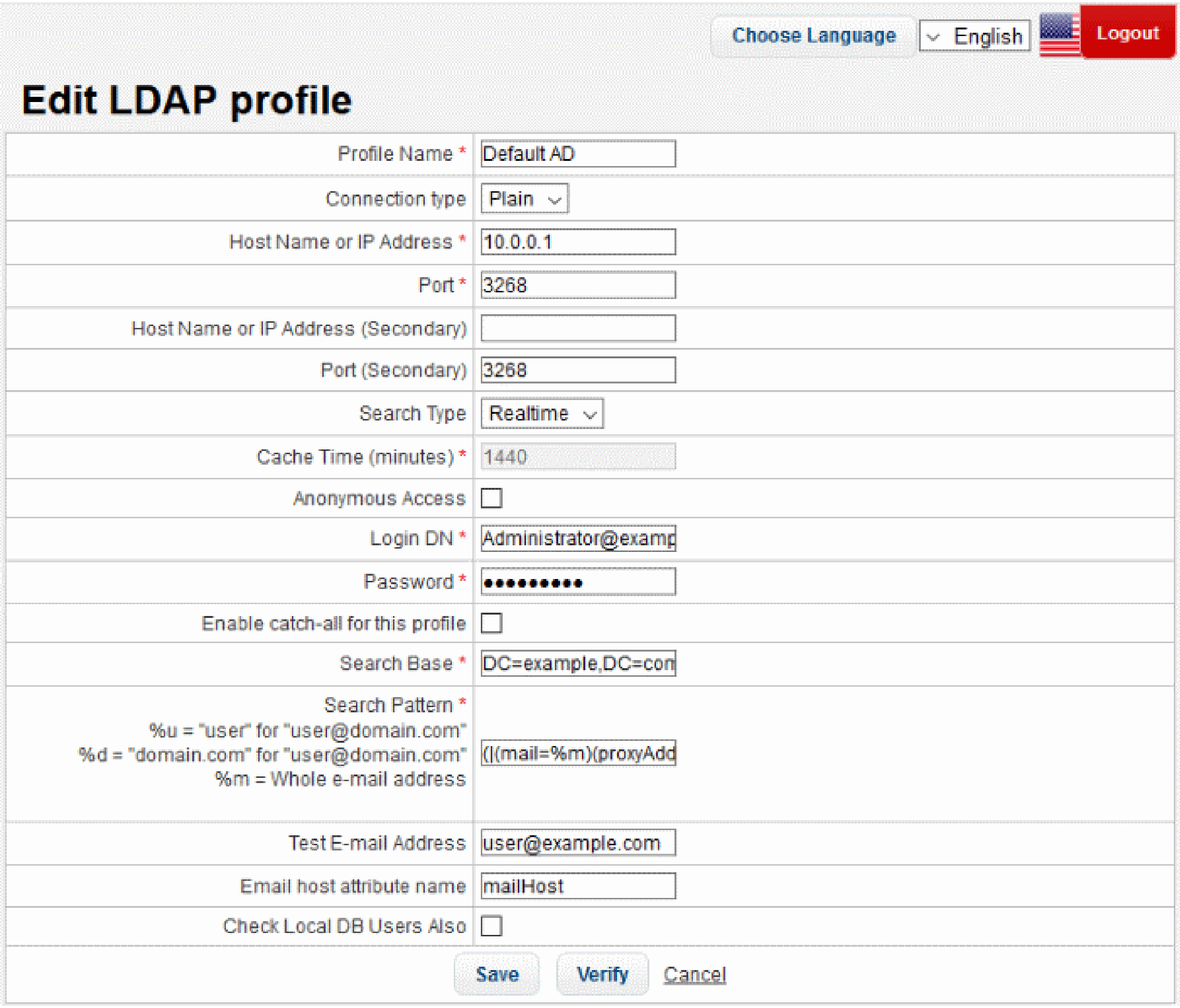
LDAP Profile -Table of Parameters	
Parameter	**Description**
Profile Name	Enter the name of the new LDAP profile
Connection type	Determines how KoruMail should connect to the LDAP server. The options available are: • Plain (Not encrypted) • TLS (Encrypted with the TLS protocol. Recommended) • SSL (Encrypted using the SSL protocol. Use if your systems have compatibility issues with TLS)
Host Name or IP Address	Enter the hostname or IP address of the LDAP/Active Directory. KoruMail will first check the primary server and will check the secondary server if the primary is not available.
Port	Specify the LDAP server port number. If you use 'Active Directory' then, instead of the default LDAP port 389, port 3826 must be used as Active Directory Catalog port.
Search Type	Select the type of search from the drop-down. The options available are: Realtime - Checks the AD server each time for user validity Cache - Checks the user validity from the system's cache memory and if not available checks the AD server.
Cache Time (minutes)	If the 'Cache' option is enabled as 'Search Type', this field becomes active. Enter the time in minutes the details of users are cached after which they are wiped out.
Anonymous Access	If this feature is enabled, the connection to LDAP server will be created anonymously so that username and password are not required.
Login DN	LDAP username to connect LDAP / Active Directory server.
Password	Enter the LDAP user password.
Enable catch-all for this profile	When this feature is enabled, if the recipient's address is value1-value2-value3@domain.com then KoruMail first checks whether this address is registered in LDAP. If it does not find it, it deletes value1 and checks the remaining value2-value3@domain.com address. If it does not find it again then it delete value2 and checks value3@domain.com
Search Base	Specify the search starting criteria to be used in LDAP tree.
Search Pattern	Determines which LDAP attributes will be searched in search base.

Test E-Mail Address	Enter the email address to test the LDAP connection.
Email host attribute name	Enter the mail host attribute name for the LDAP / Active Directory server.
Check Local DB Users Also	Checks for users in Local Data base users list as well.

- Click the 'Verify' button to check the entered parameters and connectivity are correct. If verification fails, the error message will be displayed.
- Click the 'Save' button to apply your changes.

To edit a LDAP profile

- Click the 📝 button beside a LDAP profile that you want to edit.



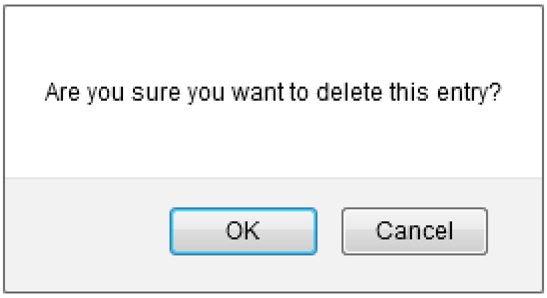
Edit LDAP profile

Profile Name *	Default AD
Connection type	Plain
Host Name or IP Address *	10.0.0.1
Port *	3268
Host Name or IP Address (Secondary)	
Port (Secondary)	3268
Search Type	Realtime
Cache Time (minutes) *	1440
Anonymous Access	□
Login DN *	Administrator@examp
Password *	••••••••••
Enable catch-all for this profile	□
Search Base *	DC=example,DC=con
Search Pattern * %u = "user" for "user@domain.com" %d = "domain.com" for "user@domain.com" %m = Whole e-mail address	(|(mail=%m)(proxyAdd
Test E-mail Address	user@example.com
Email host attribute name	mailHost
Check Local DB Users Also	□

- Edit the required parameters. This is similar to the method explained in the '**Add**' section.
- Click 'Save' to apply your changes.

To delete a LDAP profile

- Click the delete button ☒ beside a LDAP profile that you want to remove.



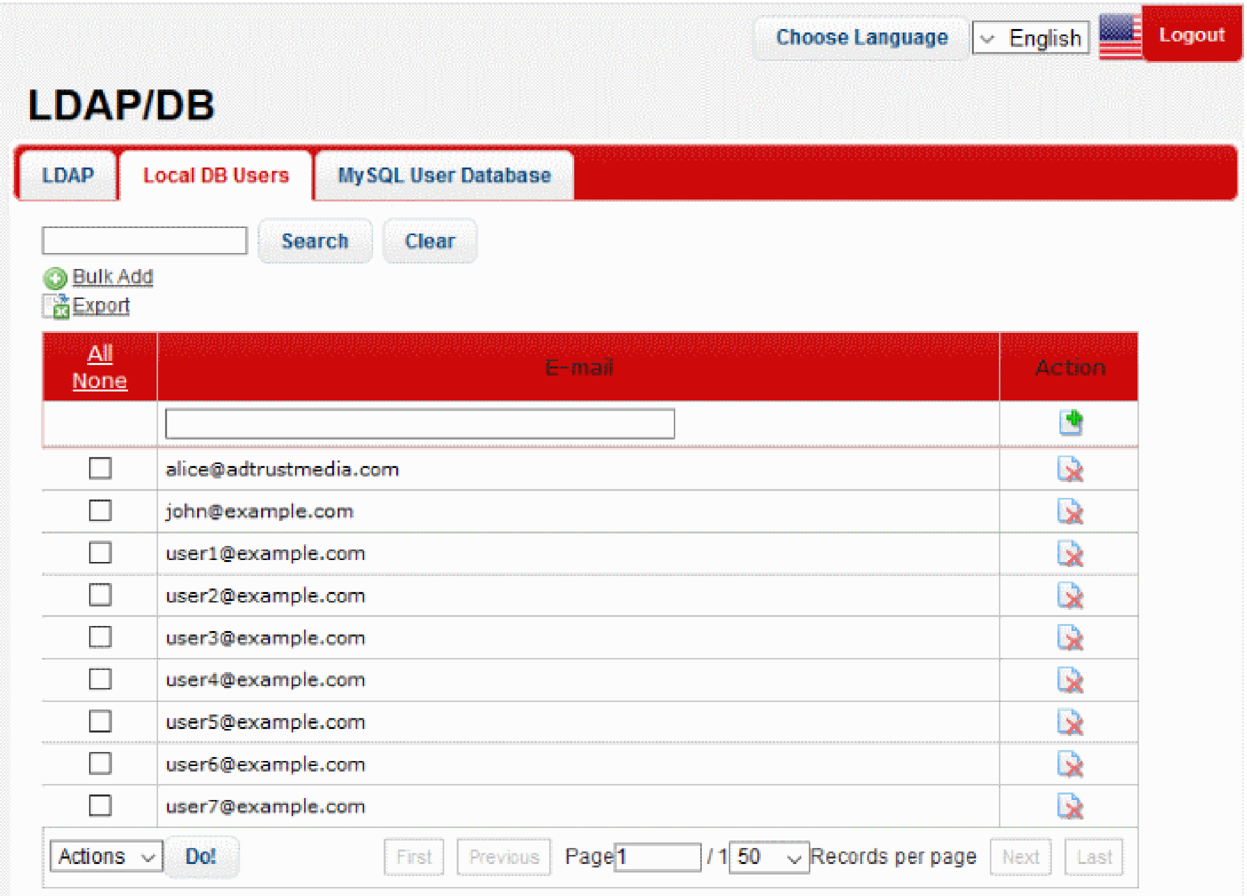
Are you sure you want to delete this entry?

- Click 'OK' to confirm the deletion.

7.4.2 Local DB Users

KoruMail allows you to add users to its local database for managed domains. This saves resources by making sure emails to invalid recipients are rejected before filtering begins. Users added here are available for selection in interfaces such as '**Managed Domains** > **Routes**'.

- Click 'SMTP' > 'LDAP/DB' on the left
- Open the 'Local DB Users' tab

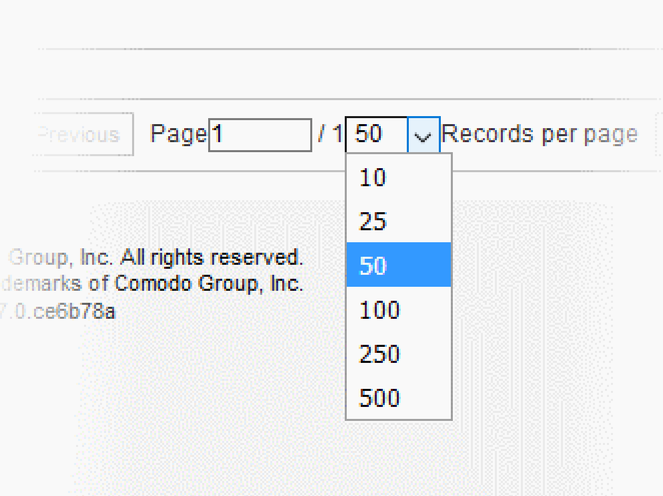


All None	E-mail	Action
□	alice@adtrustmedia.com	
□	john@example.com	
□	user1@example.com	
□	user2@example.com	
□	user3@example.com	
□	user4@example.com	
□	user5@example.com	
□	user6@example.com	
□	user7@example.com	

Local DB Users - Table of Column Descriptions		
Column Header	**Description**	
Email	The address of the user added to KoruMail.	
Actions	✚	Add a user. Enter the user's email address in the field provided then click this button.

	✗	Delete a user from the list. Use the check-boxes on the left to select users.

The number of users to be displayed on the screen can be set from the 'Records per page' drop-down field.



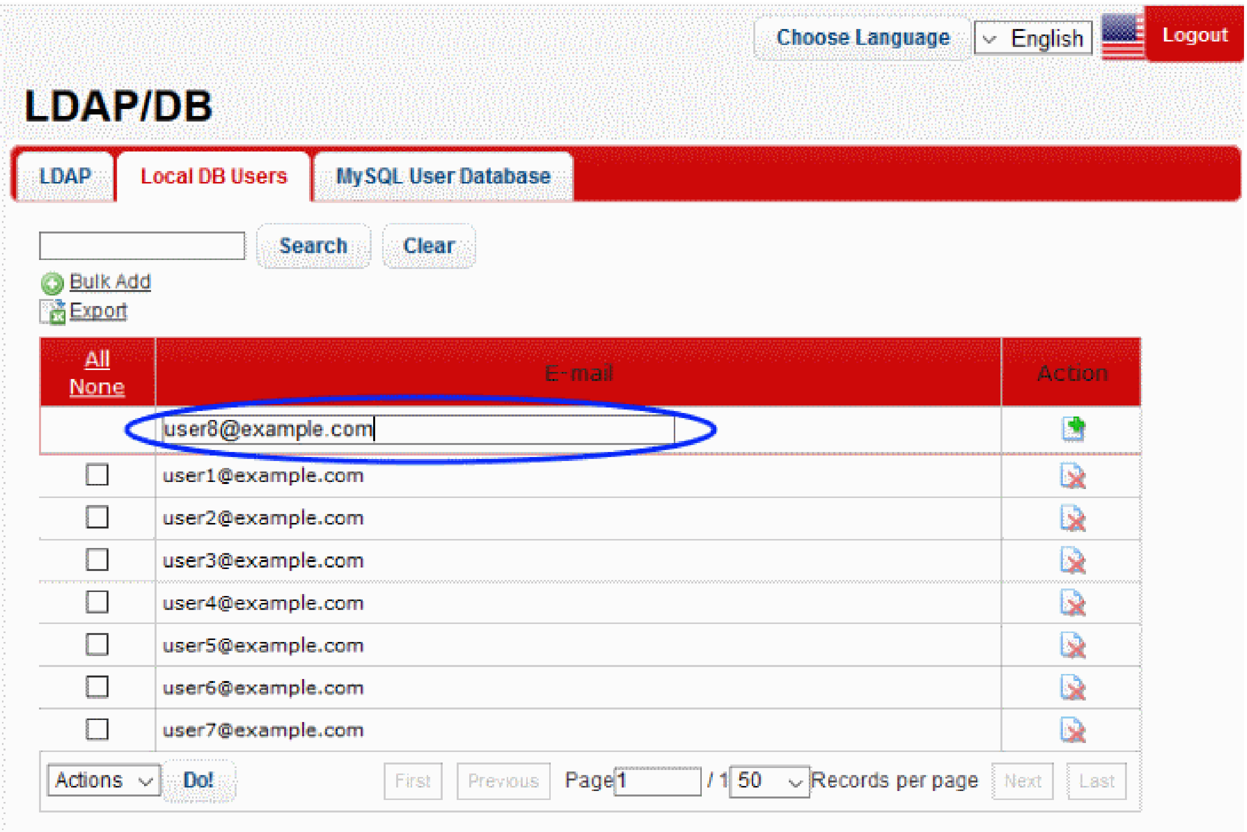
Click the 'First, Previous, Next and Last' buttons to view all the items in the list.

The interface allows administrators to:

- **Add a user**
- **Add multiple users**
- **Search for users**
- **Delete users**
- **Export user list**

To add a user

- Enter the user's email address in the field under 'E-mail' column



LDAP/DB

All None	E-mail	Action
	user8@example.com	
□	user1@example.com	
□	user2@example.com	
□	user3@example.com	
□	user4@example.com	
□	user5@example.com	
□	user6@example.com	
□	user7@example.com	

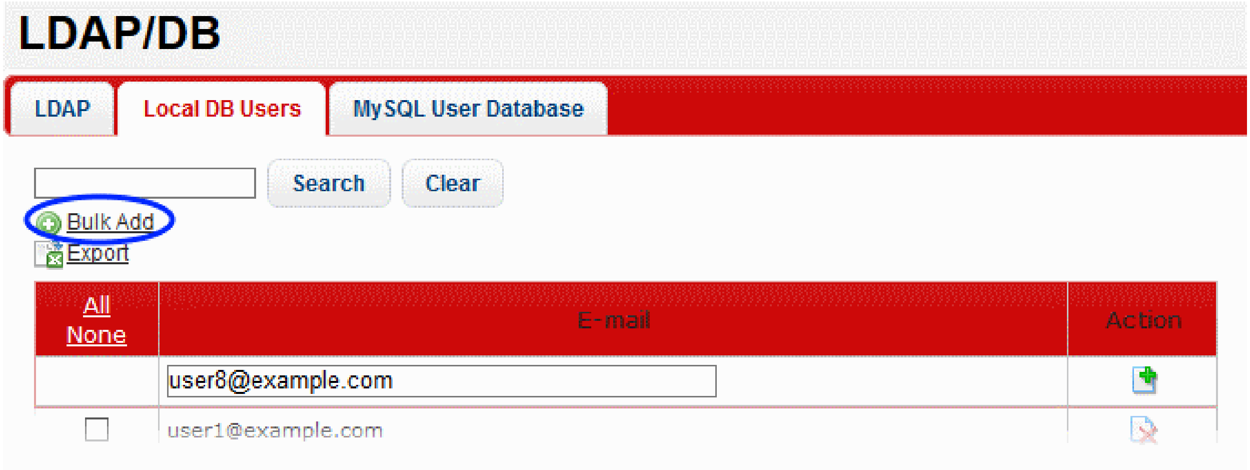
- Click the button under the 'Action' column.

Note: You can add users for managed domains only.

The user will be added and displayed in the list. You can also add multiple users at a time. See the next section '**To add multiple users**' for more details.

To add multiple users

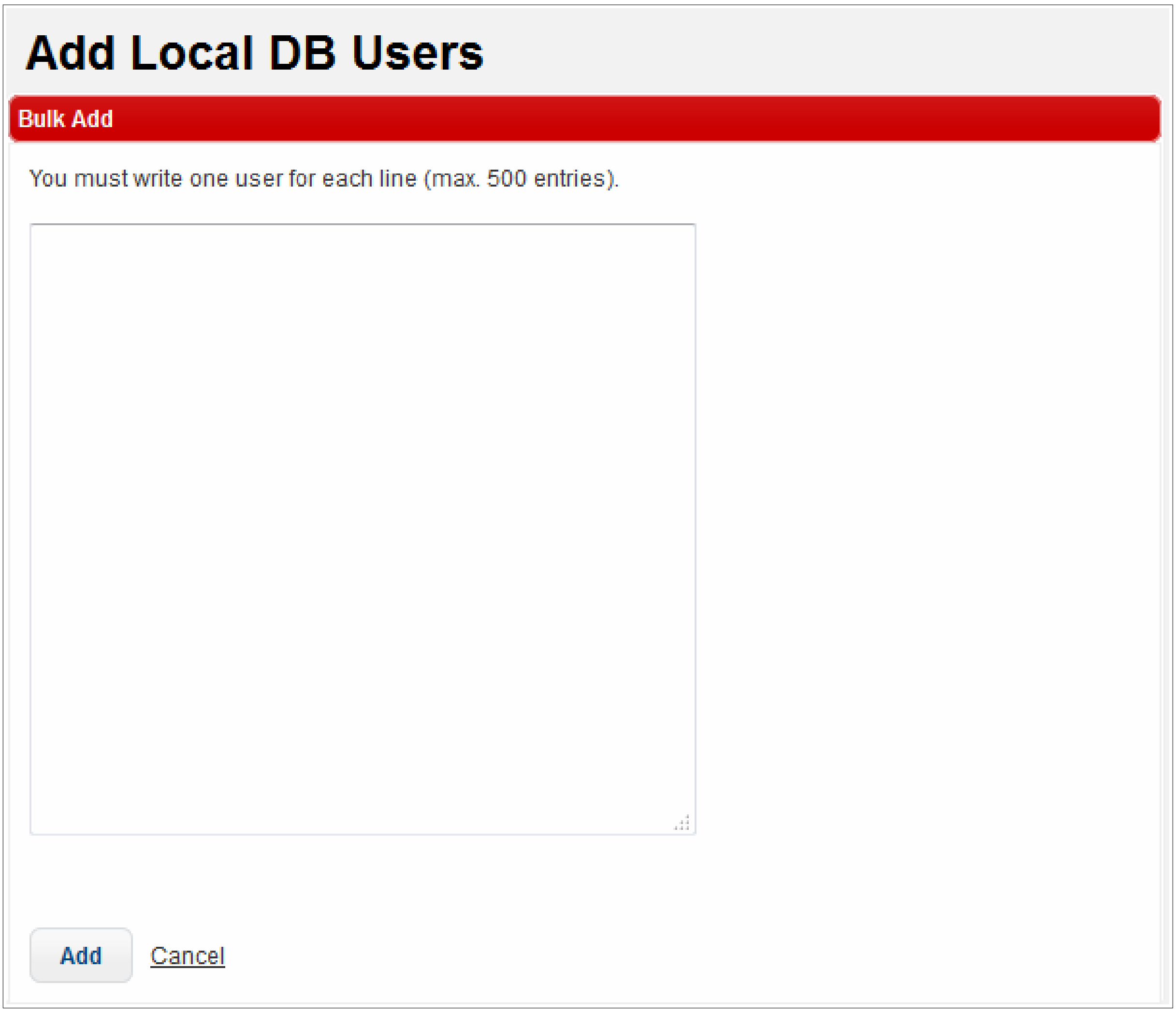
- Click the 'Bulk Add' link in the 'Local DB Users' screen



LDAP/DB

All None	E-mail	Action
	user8@example.com	
□	user1@example.com	

The 'Bulk Add' screen will be displayed.



Add Local DB Users

Bulk Add

You must write one user for each line (max. 500 entries).

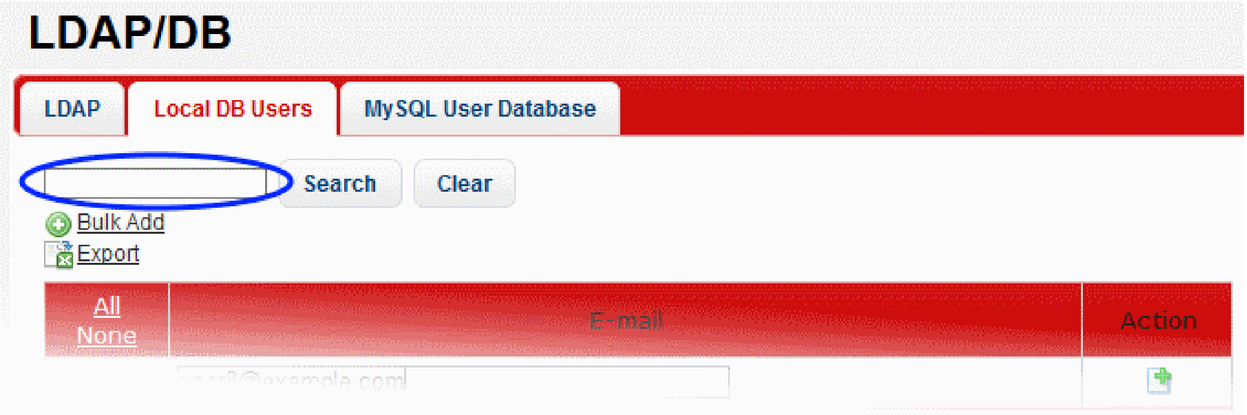
- Enter the users' email addresses each per line. The maximum allowed at a time is 500 users.
- Click the 'Add' button.

Note: You can add users for managed domains only.

The users will be added and displayed in the list.

To search for users

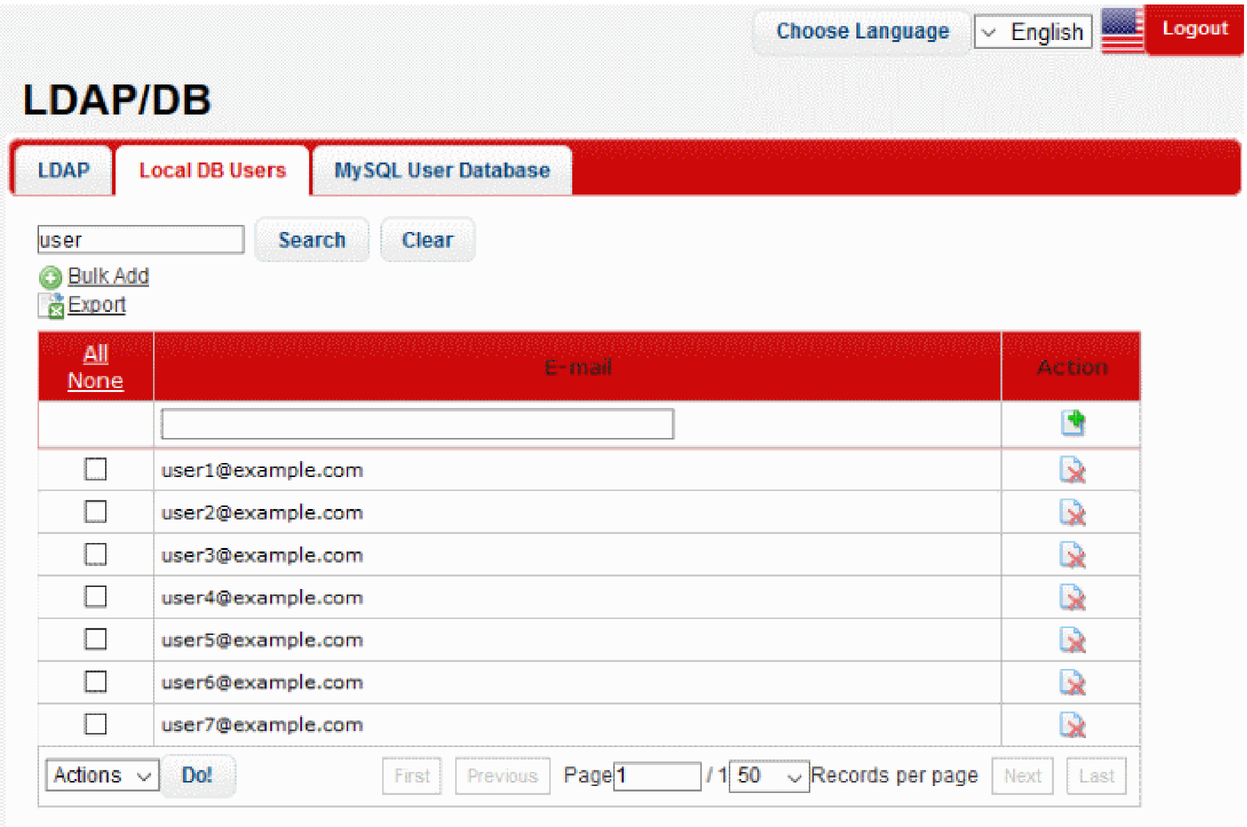
- In the search field, enter a full or partial name.



LDAP/DB

- Click the 'Search' button.

The items that contain the entered search text will be displayed.



Search: user

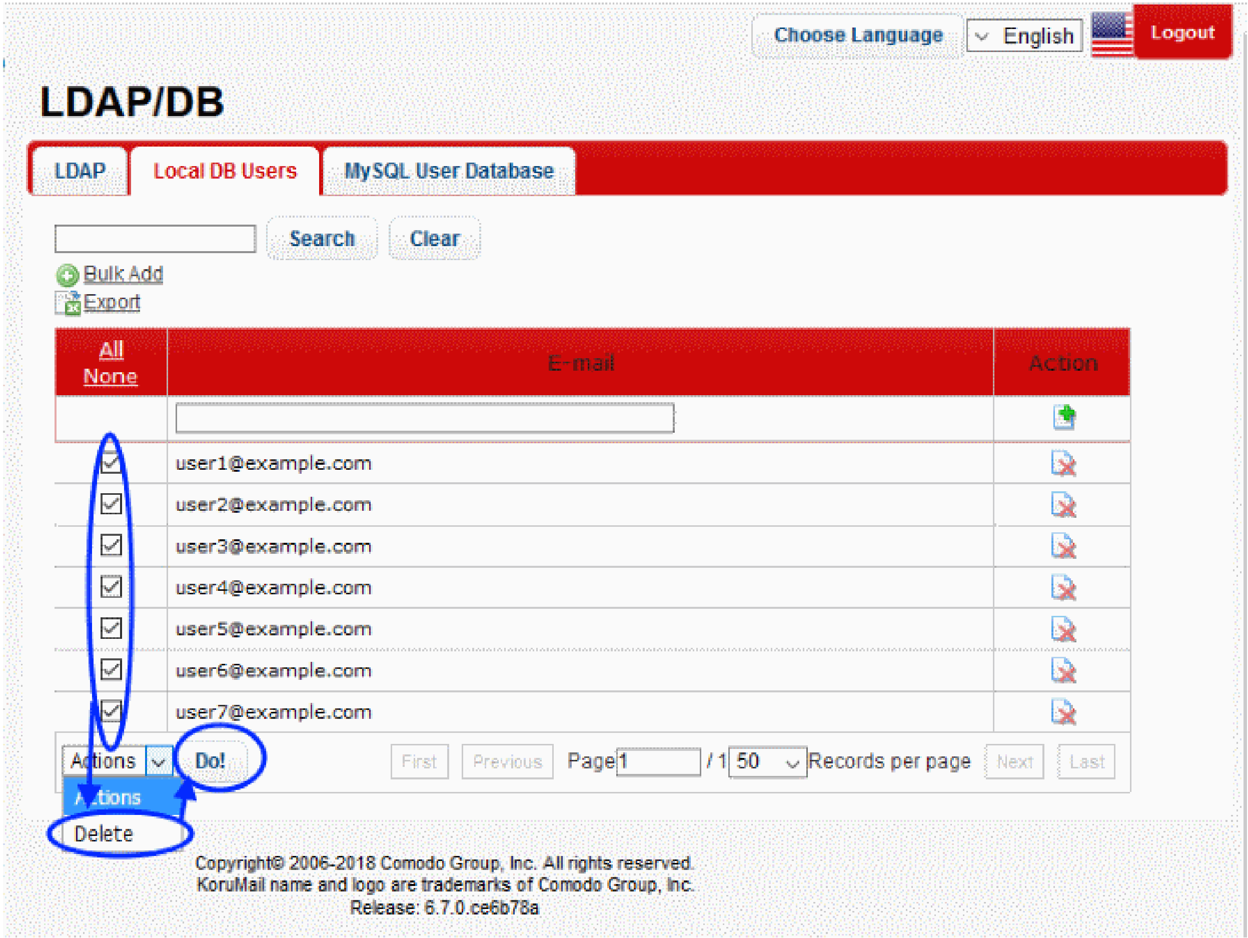
All None	E-mail	Action
□	user1@example.com	☒
□	user2@example.com	☒
□	user3@example.com	☒
□	user4@example.com	☒
□	user5@example.com	☒
□	user6@example.com	☒
□	user7@example.com	☒

Page 1 / 1 50 Records per page

- To display all the items again, click the 'Clear' button.

To delete users

- To remove users one at a time, click the ☒ button under the 'Action' column header and confirm the deletion in the 'Confirmation' dialog.
- To delete multiple users in the list in one go, select the check boxes beside them.



All None	E-mail	Action
☑	user1@example.com	
☑	user2@example.com	
☑	user3@example.com	
☑	user4@example.com	
☑	user5@example.com	
☑	user6@example.com	
☑	user7@example.com	

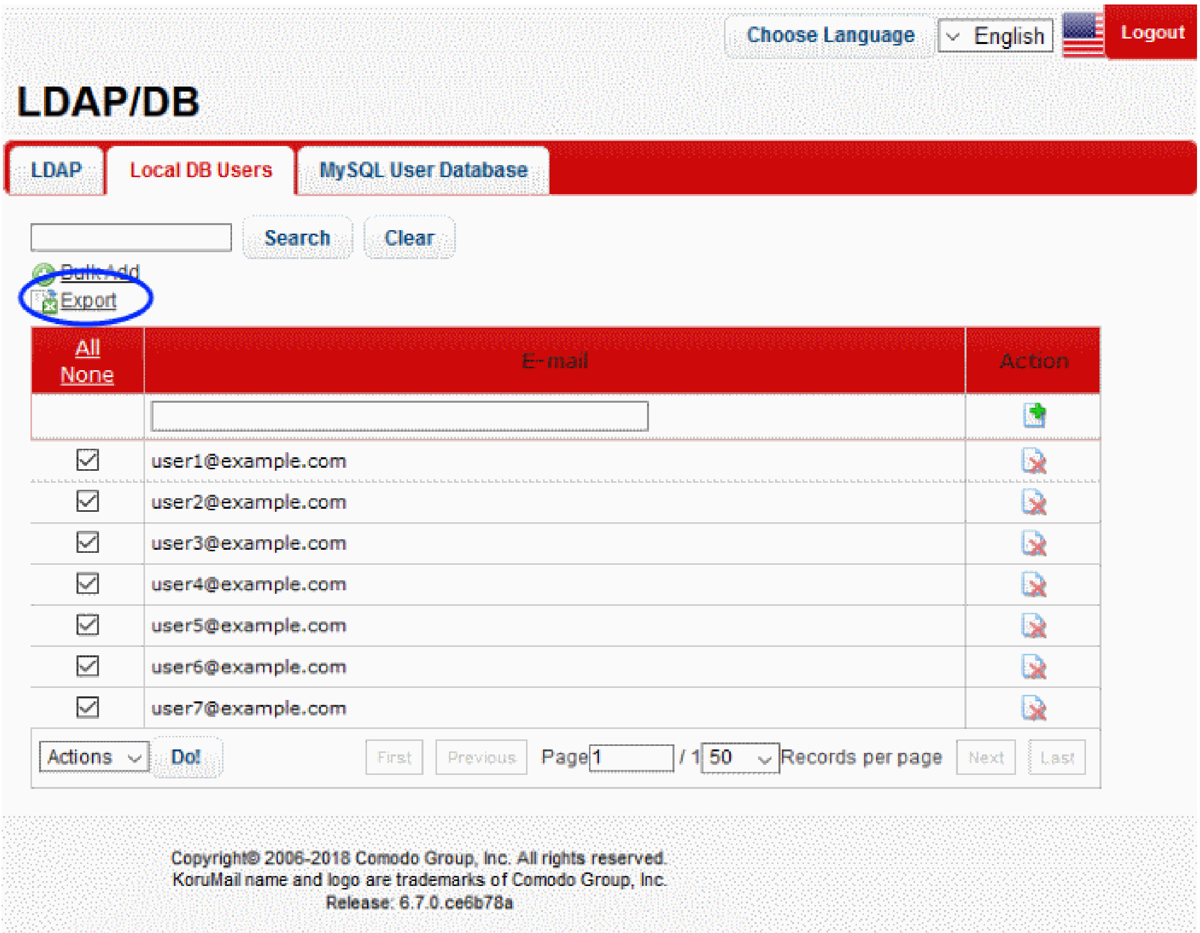
Copyright© 2006-2018 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 6.7.0.ce6b78a

- Select 'Delete' from the 'Actions' drop-down and click the 'Do!' button.

The selected users will be deleted from the list.

To export the user list to a file

- To export users one at a time, click the 'Export' link on the top left



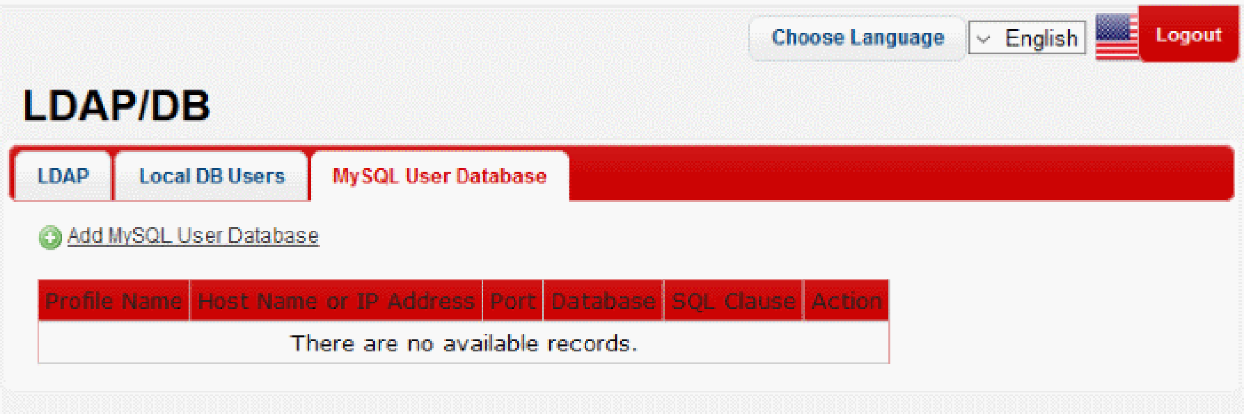
All None	E-mail	Action
☑	user1@example.com	
☑	user2@example.com	
☑	user3@example.com	
☑	user4@example.com	
☑	user5@example.com	
☑	user6@example.com	
☑	user7@example.com	

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

- Download and save the list as a text file to your system.

7.4.3 My SQL User Database

- KoruMail is capable of verifying the validity of users by referring to a 'MySQL User Database' located on a remote server.
- If the recipient is not a valid user then email is rejected in SMTP level. Since the sophisticated filtering process is not used for invalid recipients, KoruMail's resources are not wasted.
- The 'MySQL User Database profiles' added here are available for selection in interfaces such as '**Managed Domains** > **Routes**'.
- To open the 'MySQL User Database' screen, click the 'SMTP' tab on the left menu and click 'LDAP/DB' then 'MySQL User Database'.



Profile Name	Host Name or IP Address	Port	Database	SQL Clause	Action
There are no available records.					

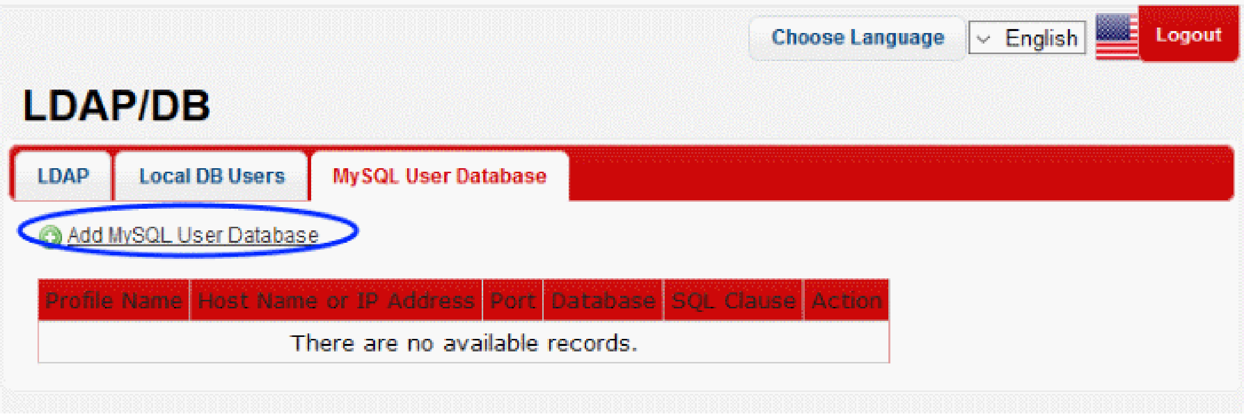
MySQL User Database Profile - Table of Column Descriptions		
Column Header	**Description**	
Profile Name	The name of the MySQL User Database profile added to KoruMail.	
Host Name or IP Address	Displays the address of the system where the 'MySQL User Database' is located.	
Port	Displays the port number to which KoruMail connects to.	
Database	The name of the 'MySQL User Database'.	
SQL Clause	The 'SQL clause' used to fetch the users' details.	
Action	✎	Allows the administrators to edit the details of a 'MySQL' profile
	✖	Allows the administrators to delete a 'MySQL' profile from the list.

From this screen administrators can:

- **Add a new MySQL profile**
- **Edit a MySQL profile**
- **Delete a MySQL profile**

To add a new MySQL profile

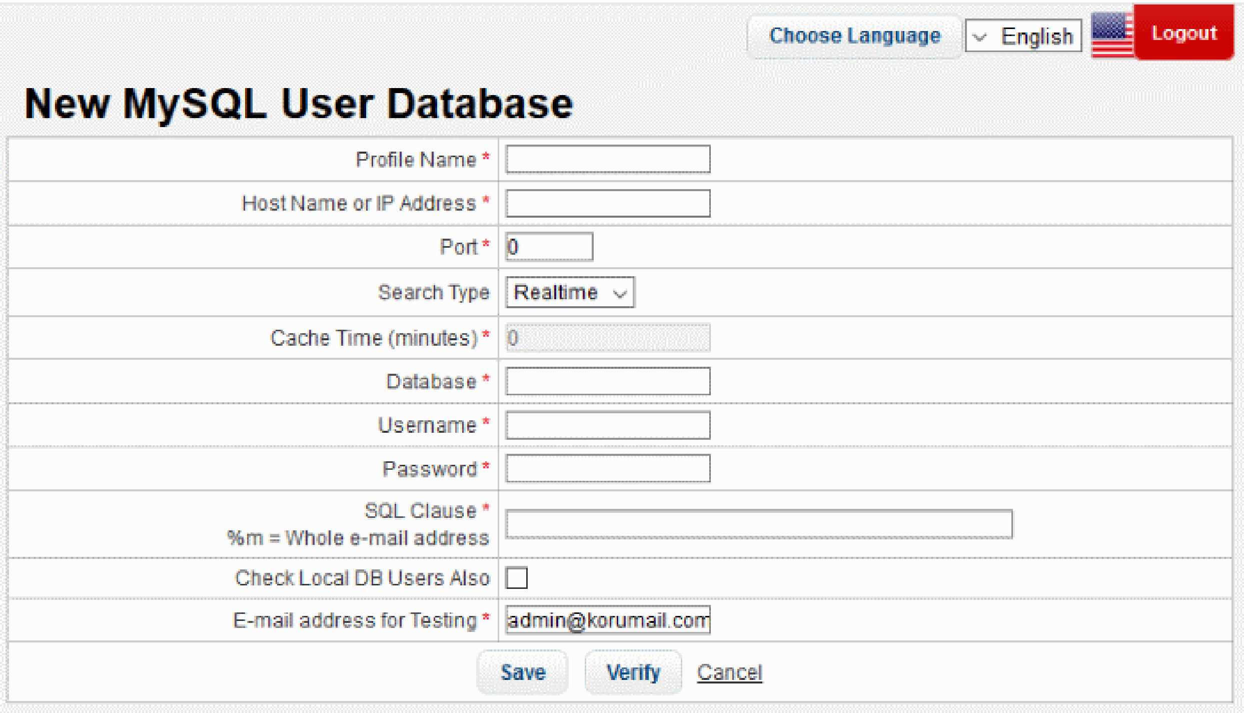
- Click 'Add MySQL User Database' link at the top of the screen.



LDAP/DB

Profile Name	Host Name or IP Address	Port	Database	SQL Clause	Action
There are no available records.					

The 'New MySQL User Database' screen will be displayed.



New MySQL User Database

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

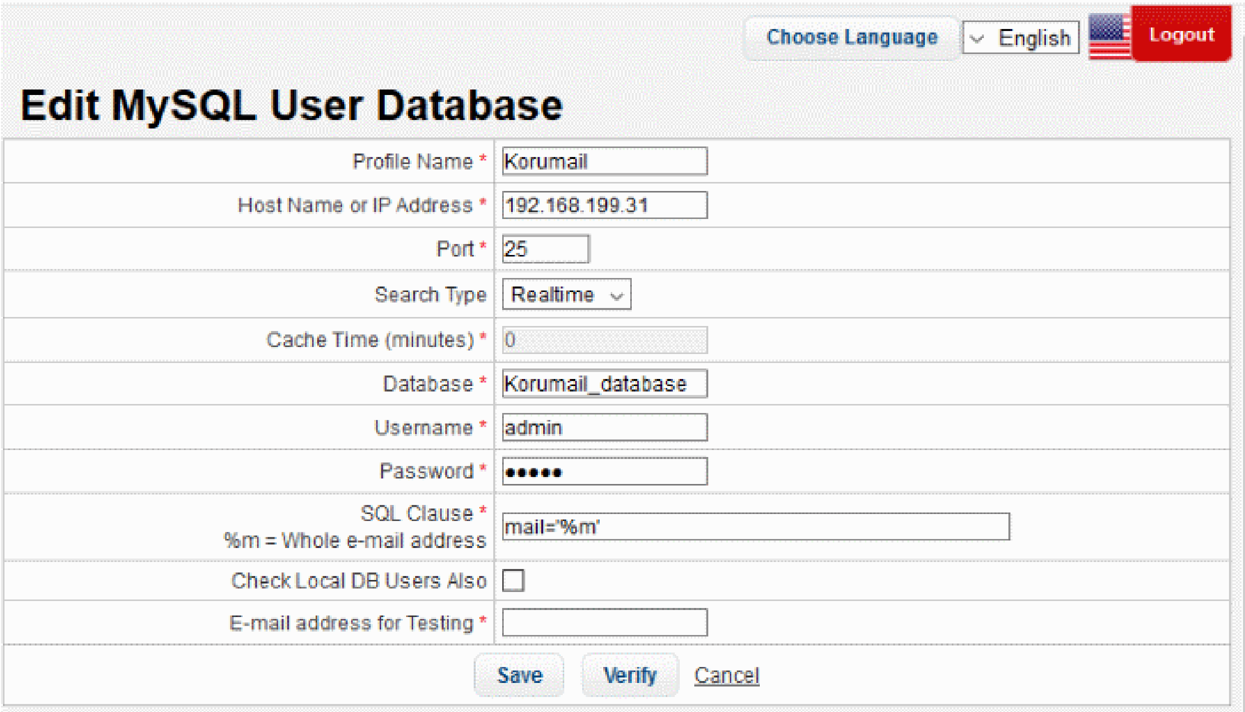
MySQL User Database Profile -Table of Parameters

Parameter	Description
Profile Name	Enter the name of the MySQL profile
Host Name or IP Address	Enter the hostname or IP address of the system where MySQL database is located.
Port	Enter the port number to which KoruMail should connect to.
Search Type	Select the type of search from the drop-down. The options available are: Realtime - Checks the MySQL server each time for user validity. Cache - Checks the user validity from the system's cache memory and if not available checks the MYSQL server.
Cache Time (minutes)	If the 'Cache' option is enabled as 'Search Type', this field becomes active. Enter the time in minutes the details of users are cached after which they are wiped out.
Database	Enter the MySQL database name.
Username	The username to access the MySQL server.
Password	Enter the password to access the MySQL server.
SQL Clause	The SQL clause to fetch the users' details.
Check Local DB Users Also	Checks for users in Local Data base users list as well.
E-Mail address for testing	Enter the email address to test the MySQL database connection.

- Click the 'Verify' button to check the entered parameters and connectivity are correct. If verification fails, the error message will be displayed.
- Click the 'Save' button to apply your changes.

To edit a MySQL profile

- Click the button beside a 'MySQL' profile that you want to edit.



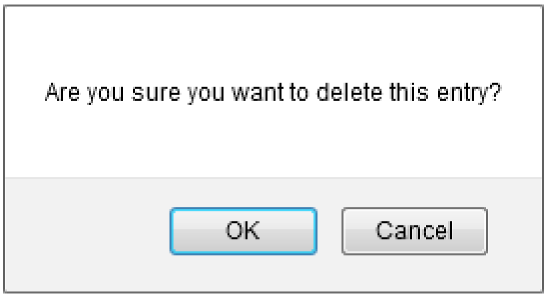
Edit MySQL User Database

Profile Name *	Korumail
Host Name or IP Address *	192.168.199.31
Port *	25
Search Type	Realtime
Cache Time (minutes) *	0
Database *	Korumail_database
Username *	admin
Password *	●●●●●
SQL Clause * %m = Whole e-mail address	mail='%m'
Check Local DB Users Also	□
E-mail address for Testing *	

- Edit the required parameters. This is similar to the method explained in the '**Add**' section.
- Click the 'Save' button to apply your changes.

To delete a MySQL profile

- Click the delete button beside a 'MySQL' profile that you want to remove.



Are you sure you want to delete this entry?

- Click 'OK' to confirm the deletion.

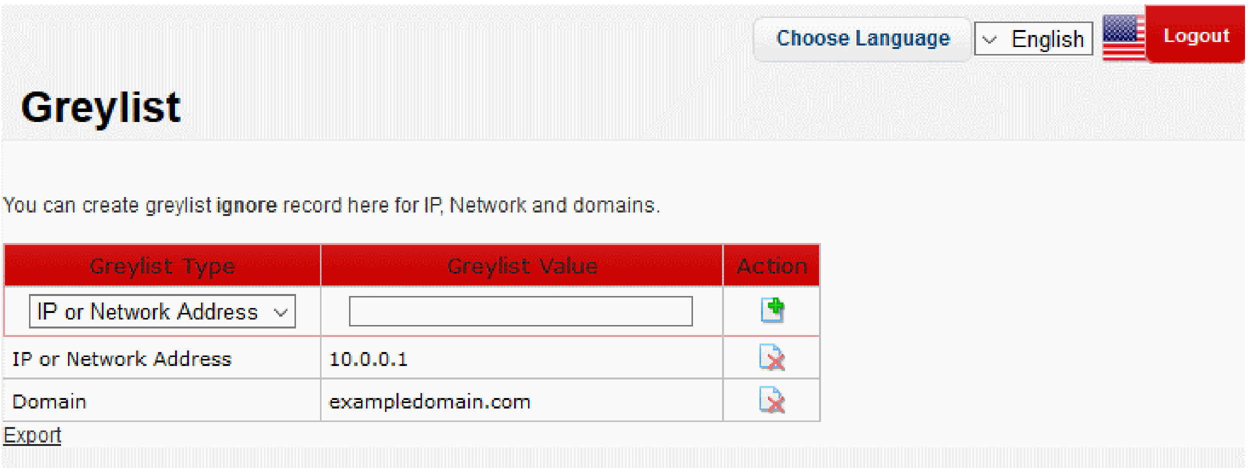
7.5 Greylist

- Greylisting is a form of spam control whereby Korumail will temporarily reject any email from senders it does not recognize.
- Upon receiving this 'try again later' message, legitimate mail servers will indeed try to resend the mail after a delay.
- Korumail will accept the resent mail providing it does not fall foul of its other filters.
- Spam servers are unlikely to perform this simple resend due to the prohibitive cost of re-sending millions of

mails. Thus, greylisting can be an effective way to block junk-mail at source.

To open the 'Greylist' screen

- Click 'SMTP' > 'Greylist' in the left menu



Greylist

You can create greylist **ignore** record here for IP, Network and domains.

Greylist Type	Greylist Value	Action
IP or Network Address		➕
IP or Network Address	10.0.0.1	✗
Domain	exampledomain.com	✗

Export

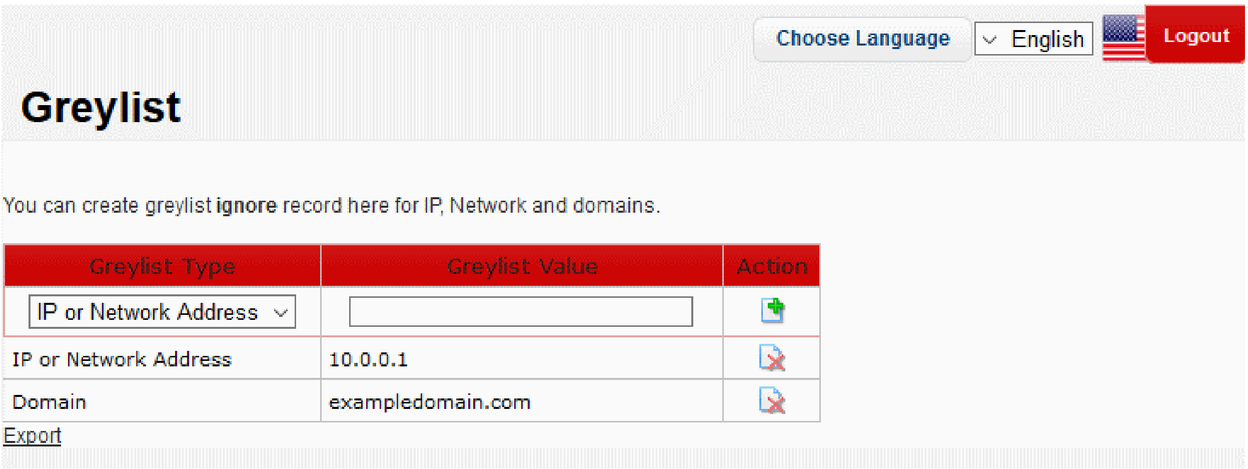
See '**Greylist Ignored IP Addresses/Domains**' for how to add domains, networks and IP addresses to Greylist ignored list.

7.5.1 Greylist Ignored IP Addresses/Domains

- Korumail allows you to add IP addresses and domains as exceptions to its greylisting policy.
- Mail from these addresses will be accepted immediately, without requiring the source mail server to resend. See the previous section if you'd like an explanation of greylisting.

To open the 'Greylist' screen

- Click SMTP' > 'Greylist' in the left-menu



Greylist

You can create greylist **ignore** record here for IP, Network and domains.

Greylist Type	Greylist Value	Action
IP or Network Address		➕
IP or Network Address	10.0.0.1	✗
Domain	exampledomain.com	✗

Export

Greylist Ignored Record List - Table of Column Descriptions		
Column Header	**Description**	
Greylist Type	The type of Greylist whether domain name or IP address added.	
Greylist Value	The domain name or the IP/Network address added.	
Action	➕	To add a email source to Greylist ignore record, click this button after selecting and entering the details in the fields under 'Greylist Type' and 'Greylist Value' columns respectively.

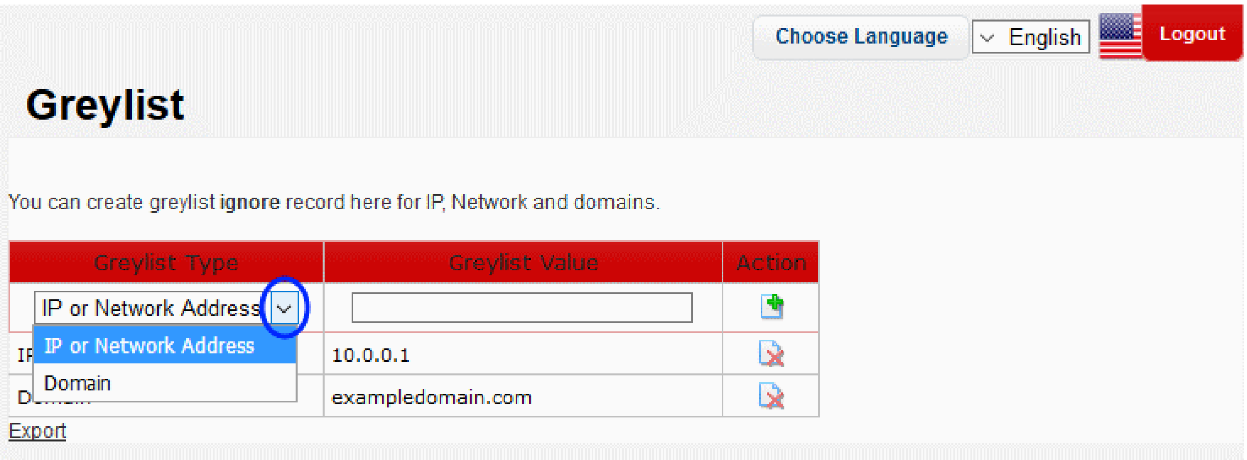
	☒	Allows the administrators to delete a record from the list.

The interface allows administrators to:

- Add an IP address/domain name to Greylist ignore list
- Delete an IP address/domain name from Greylist ignore list
- Export Greylist ignore list to a file

To add a domain name or IP address to Greylist ignore list

- Select the Greylist type that you want to add to the ignored list from the drop-down



Greylist

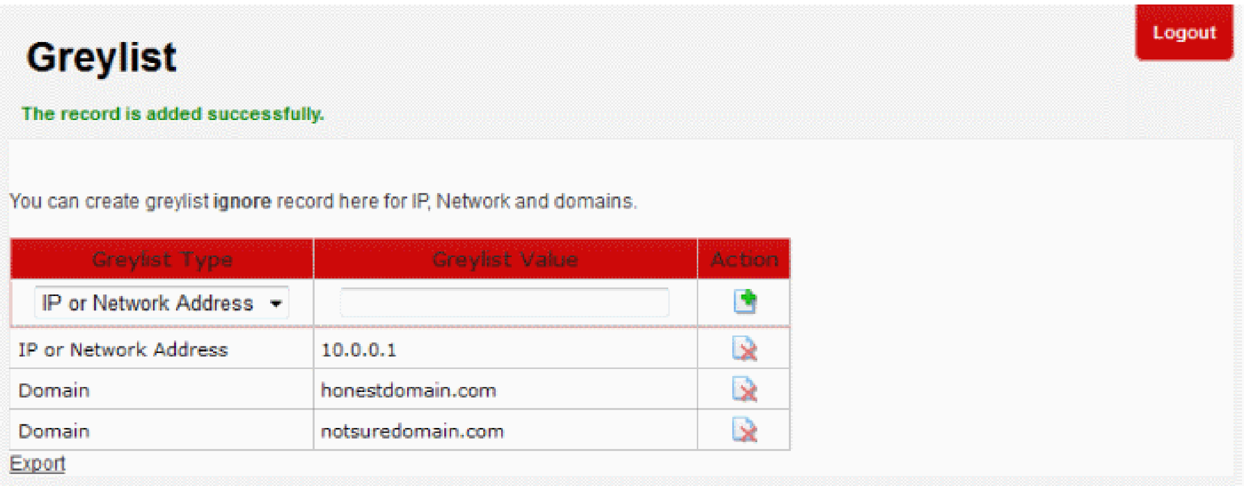
You can create greylist **ignore** record here for IP, Network and domains.

Greylist Type	Greylist Value	Action
IP or Network Address		
IP or Network Address Domain		
IP	10.0.0.1	
Domain	exampledomain.com	

Export

- Enter the value, domain name or IP address, in the field under 'Greylist Value'
- Click the ➕ button under the 'Action' column.

The domain name/IP address will be added and displayed in the list.



Greylist

The record is added successfully.

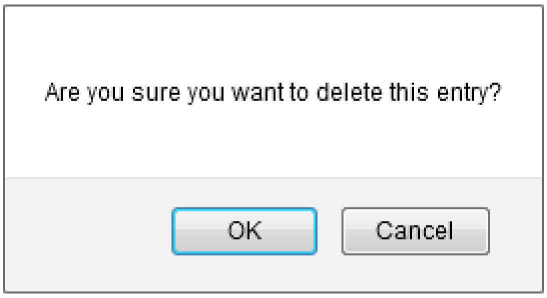
You can create greylist **ignore** record here for IP, Network and domains.

Greylist Type	Greylist Value	Action
IP or Network Address		
IP or Network Address	10.0.0.1	
Domain	honestdomain.com	
Domain	notsuredomain.com	

Export

To delete a domain name or IP address from Greylist ignore list

- To delete a domain name/IP address from the Greylist ignore list , click the ☒ button under the 'Action' column header.

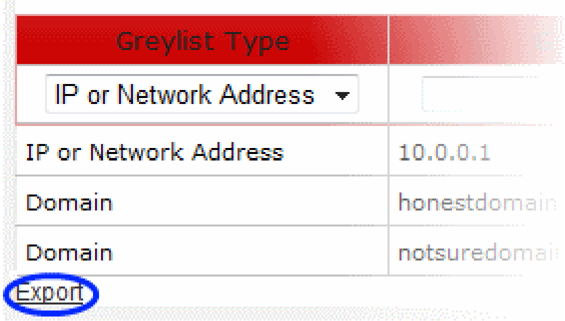


Are you sure you want to delete this entry?

- Click 'OK' to confirm the deletion.

To export Greylist ignore list to a file

- Click the 'Export' link at the bottom of the screen

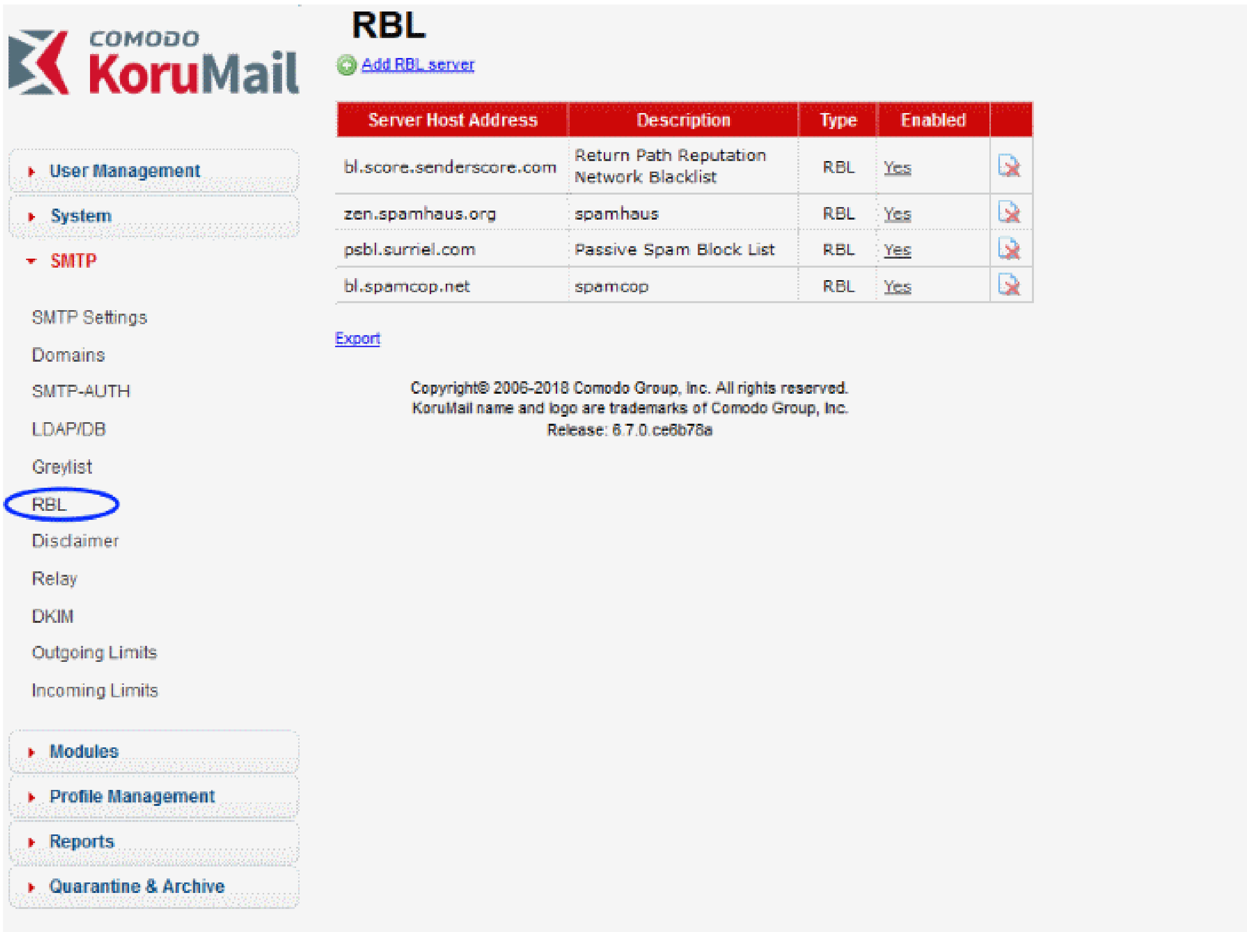


Greylist Type	
IP or Network Address ▾	
IP or Network Address	10.0.0.1
Domain	honestdomain
Domain	notsuredomai

- Download and save the list as a text file to your system.

7.6 Manage RBL Servers

- A realtime blackhole list (RBL) is a list of IP addresses that serve spam, act as spam relays, or have sent mails containing viruses.
- Korumail can block SMTP connections from addresses that are present in an RBL.
- You can add as many RBL servers as you wish. You can also enable or disable individual lists as required.
- Click 'SMTP' > 'RBL' in the left-hand menu to configure RBLs.



RBL

Server Host Address	Description	Type	Enabled	
bl.score.senderscore.com	Return Path Reputation Network Blacklist	RBL	Yes	✗
zen.spamhaus.org	spamhaus	RBL	Yes	✗
psbl.surriel.com	Passive Spam Block List	RBL	Yes	✗
bl.spamcop.net	spamcop	RBL	Yes	✗

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

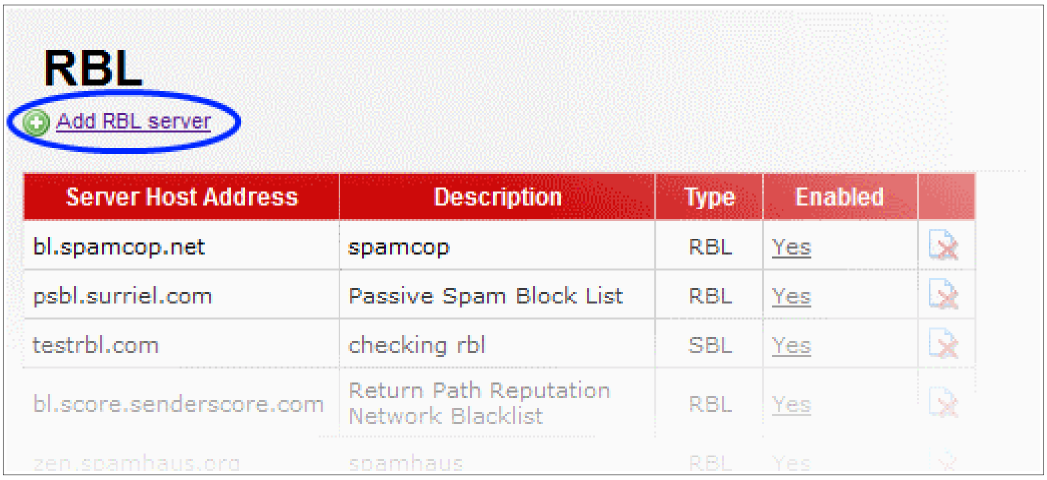
RBL Servers - Table of Column Descriptions		
Column Header	**Description**	
Server Host Address	The address of the RBL server.	
Description	The description provided at the time of adding the RBL server.	
Type	The type of block list selected.	
Enabled	Indicates whether the RBL server is enabled or not for the '**Profiles**'.	
Action	✗	Allows the administrators to delete a RBL server from the list.

The interface allow admins to:

- **Add a RBL server**
- **Enable/disable a RBL server**
- **Delete a RBL server**
- **Export RBL server list to a file**

To add a RBL server

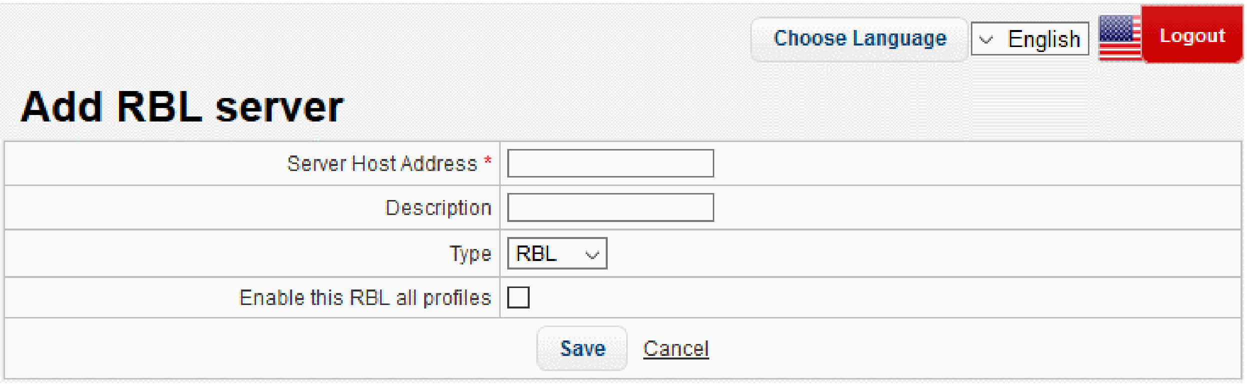
- Click the 'Add RBL Server' link at the top



RBL

Server Host Address	Description	Type	Enabled	
bl.spamcop.net	spamcop	RBL	Yes	
psbl.surriel.com	Passive Spam Block List	RBL	Yes	
testrbl.com	checking rbl	SBL	Yes	
bl.score.senderscore.com	Return Path Reputation Network Blacklist	RBL	Yes	
zen.spamhaus.org	spamhaus	RBL	Yes	

The 'Add RBL server' screen will be displayed:



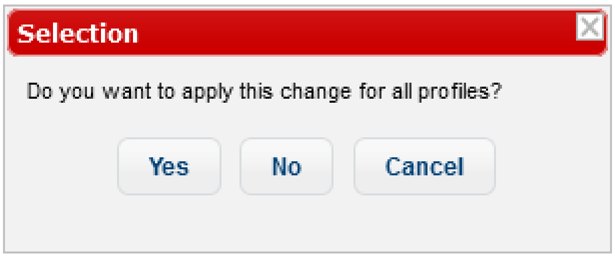
Add RBL server

Server Host Address *	
Description	
Type	RBL
Enable this RBL all profiles	□

- **Server Host Address:** Enter the address of the RBL server
- **Description:** Enter an appropriate description for the server
- **Type:** Select the type of block list from the options.
  - RBL - Realtime Black Hole Lists
  - SBL - Spamhaus Block List
  - XBL - Spamhaus Exploits List
  - SMTP - Email server List
- Enable this RBL for all profiles: If selected, the server will be enabled for all the profiles in KoruMail. See '**Profile Management**' for more details about profiles.
- Click 'Save' to add the new RBL server.

To enable/disable a RBL server

- Click the 'Yes/No' link under the 'Enabled' column



Selection

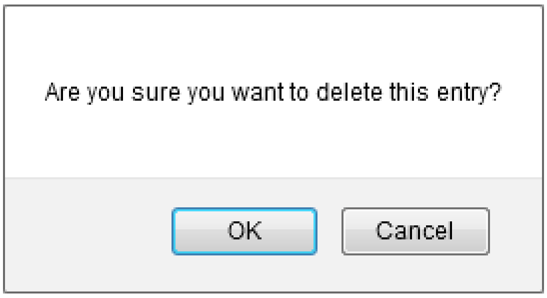
Do you want to apply this change for all profiles?

- Click 'Yes' to enable the server for all the profiles.
- Click 'No' to enable the server for the current profile.

The RBL servers can be enabled/disabled independently also for the profiles available in KoruMail. See '**Profile Management**' for more details.

To delete a RBL server

- To delete a RBL server from the list , click the ☒ button.

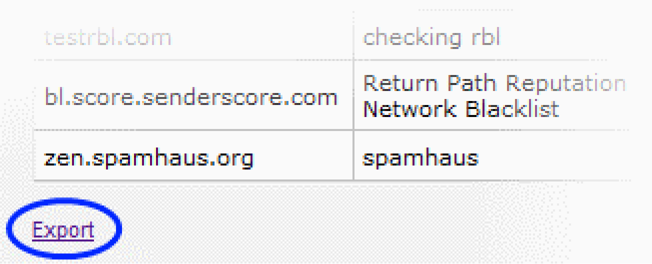


Are you sure you want to delete this entry?

- Click 'OK' to confirm the deletion.

To export RBL server list to a file

- Click the 'Export' link at the bottom of the screen



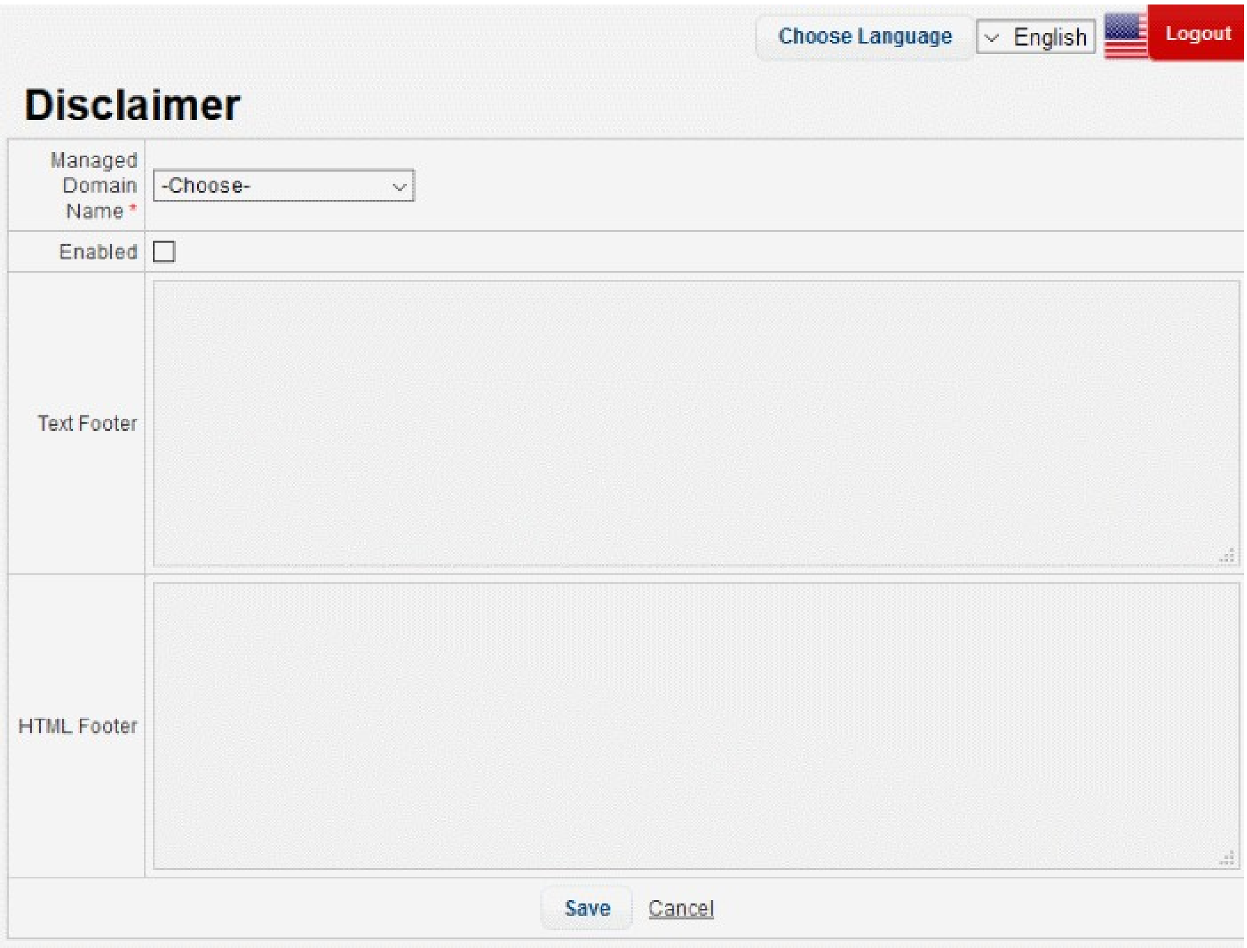
testrbl.com	checking rbl
bl.score.senderscore.com	Return Path Reputation Network Blacklist
zen.spamhaus.org	spamhaus

- Download and save the list as a text file to your system.

7.7 Disclaimer

KoruMail allows administrators to insert disclaimers in outgoings mails for the managed domains. The screen has two sections. 'Text Footer' and 'HTML Footer'. The 'Text Footer' is used to enter the disclaimer content for the selected domain and the 'HTML Footer' can be used to enter corporate messages.

- To open the 'Disclaimer' screen, click the 'SMTP' tab on the left menu, then click 'Disclaimer'.



- **Managed Domain Name:** Select the managed domain from the drop-down for which you want to add a disclaimer.
- **Enabled:** If selected, the messages will be inserted in the outgoing mails of the domain.
- **Text Footer:** Enter the disclaimer content in this field.
- **HTML Footer:** Enter content such as corporate message and so on in this field.
- Click 'Save'

To edit the disclaimer, open the screen, select the domain from the drop-down, edit the messages and click the 'Save' button to apply your changes.

7.8 SMPT Relay

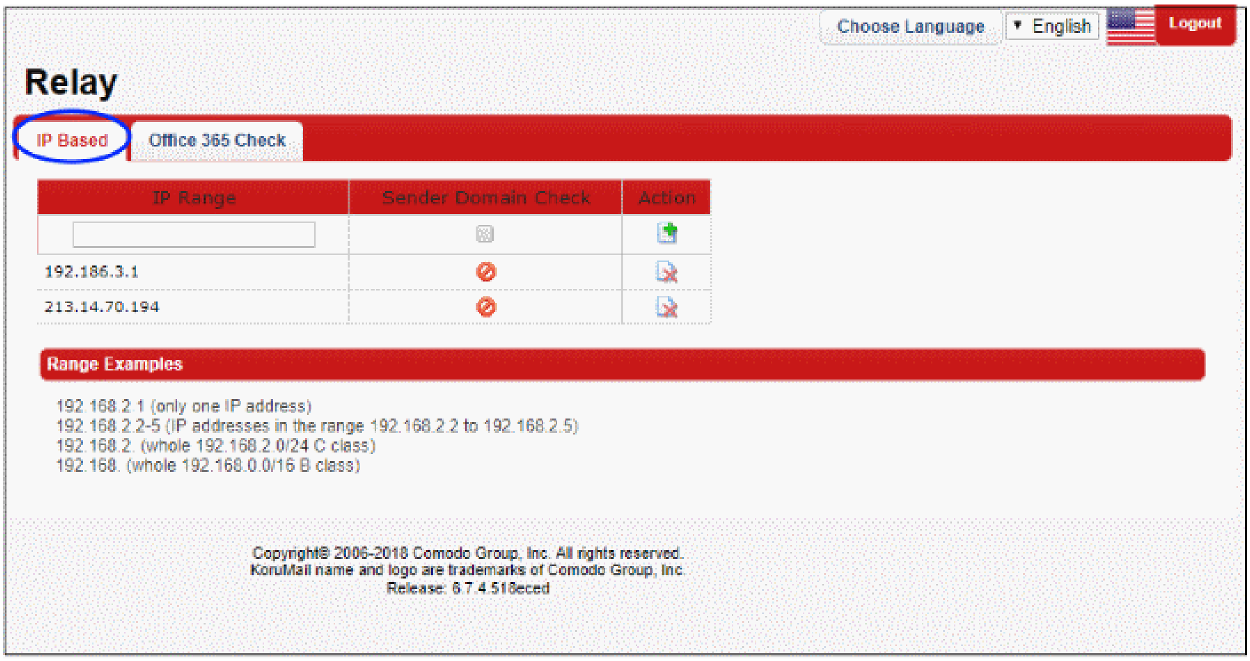
The 'Relay' interface allows you to configure so users not available in managed domains can send mails. You can also configure to manage mails to Office 365.

- **SMPT Relay**
- **Office 365 Check**

SMPT Relay

KoruMail allows you to define IPs from which mails can be sent by users who are not available on the mail server.

- Click 'SMTP' > 'Relay' then 'IP Based' tab



Relay

IP Range	Sender Domain Check	Action
	☐	✚
192.186.3.1	⊘	✖
213.14.70.194	⊘	✖

Range Examples

192.168.2.1 (only one IP address)
192.168.2.2-5 (IP addresses in the range 192.168.2.2 to 192.168.2.5)
192.168.2. (whole 192.168.2.0/24 C class)
192.168. (whole 192.168.0.0/16 B class)

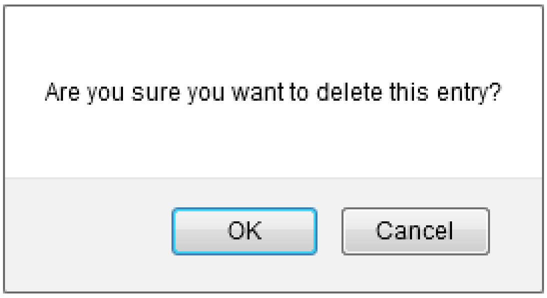
Copyright© 2006-2018 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 6.7.4.518eced

The screen allows you to add a single IP address, a range of IP addresses or a IP address class range.

- To add an IP address, range or class, enter the details in the field under 'IP Range' and click the ✚ button.

The IP address will be added and displayed.

- To remove an address, click the ✖ button.


Are you sure you want to delete this entry?

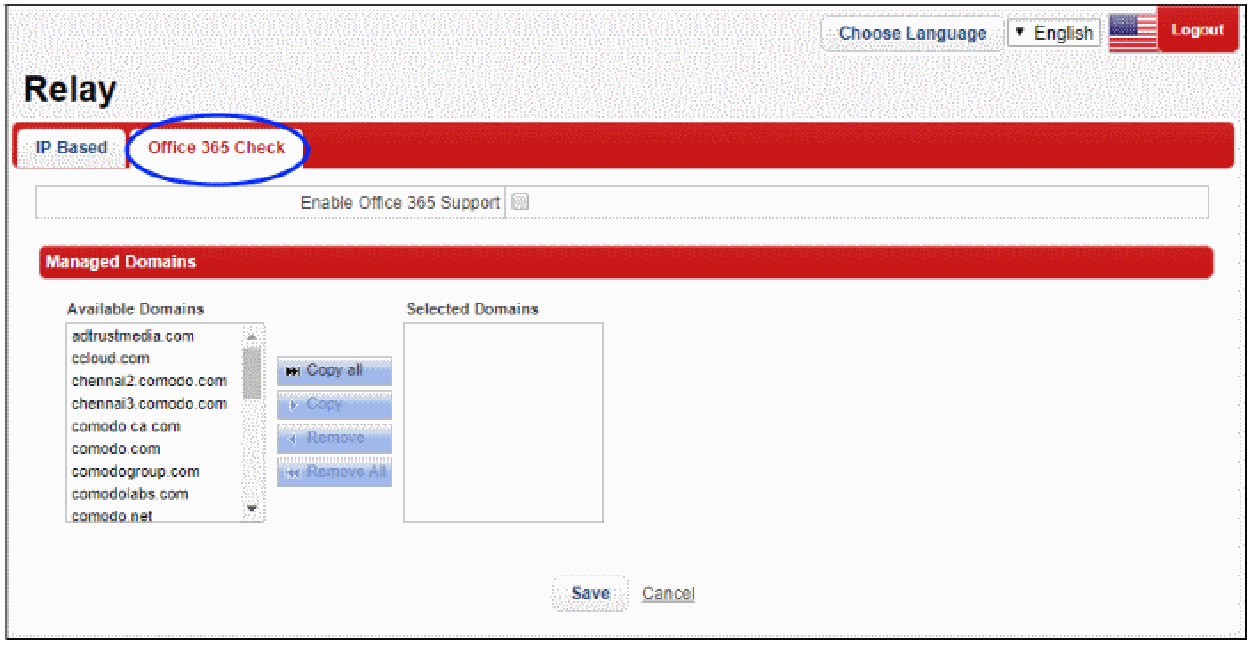
- Click 'OK' to confirm the deletion.

Manage Office 365

You can configure Korumail to route inbound emails sent to your domain to Office 365. You can create rules for inbound and outbound emails.

To configure Office 365 support:

- Click 'SMTP' > 'Relay' then 'Office 365 Check' tab



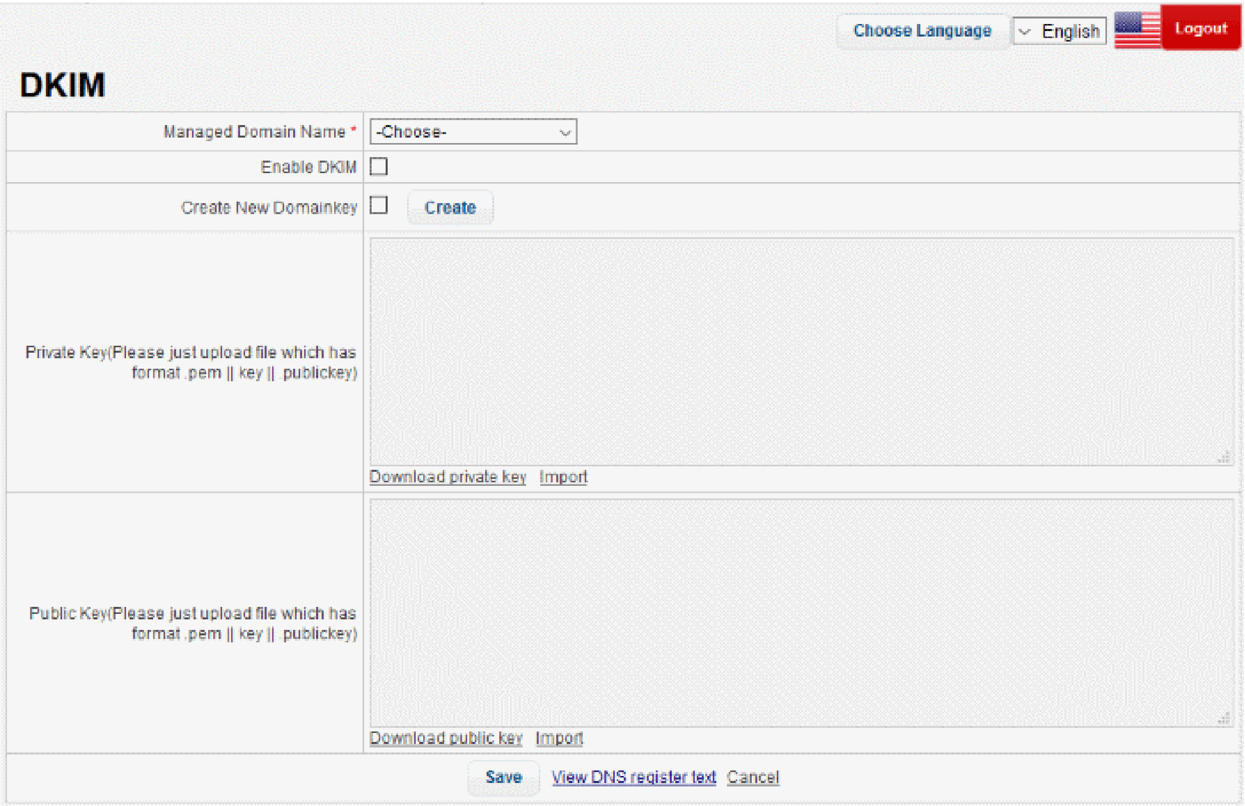
- Activate 'Enable Office 365 Support' to integrate your office 365 email rules.
- Select the domains you want to integrate with your Office 365 server then click 'Copy'.
- Click 'Save'.
- See '**Korumail Office 365 Integration Guide**' for a complete overview of Office 365 integration.

7.9 DomainKeys Identified Mail (DKIM)

- DomainKeys Identified Mail (DKIM) is another method of authenticating an outgoing mail that allows senders to associate a domain with an outgoing mail.
- It is an electronic signature that is inserted into the header of an outgoing mails identifying the source from where the message is sent. KoruMail allows administrators to create a new domain key for managed domains in order to authenticate mails that are sent from the domain.
- After the domain key is generated, it has to be entered in the DNS record. Please to your domain or web hosting documentation to add DKIM records for your domain.

To open the 'DKIM' screen,

- Click the 'SMTP' tab on the left menu, then click 'DKIM'.



Choose Language ⌄ English Logout

DKIM

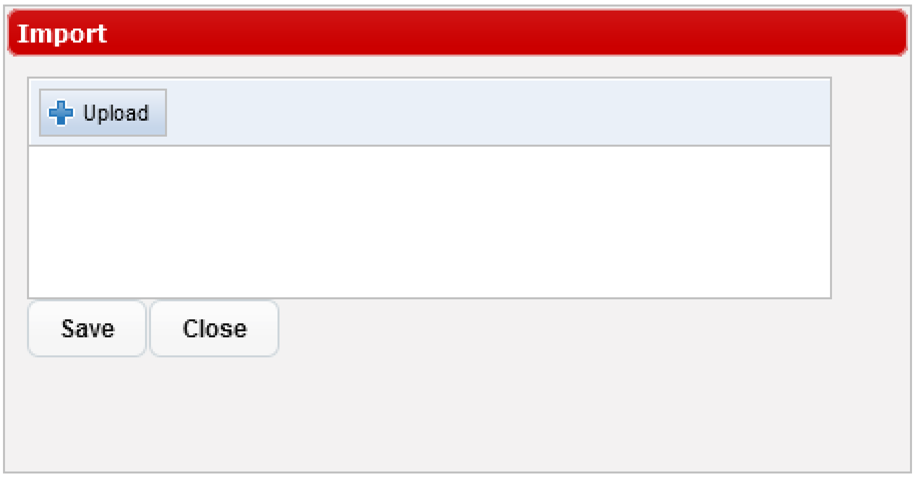
Managed Domain Name *	-Choose-
Enable DKIM	□
Create New Domainkey	□ Create
Private Key(Please just upload file which has format .pem || key || .publickey)	Download private key Import
Public Key(Please just upload file which has format .pem || key || .publickey)	Download public key Import

Save View DNS register text Cancel

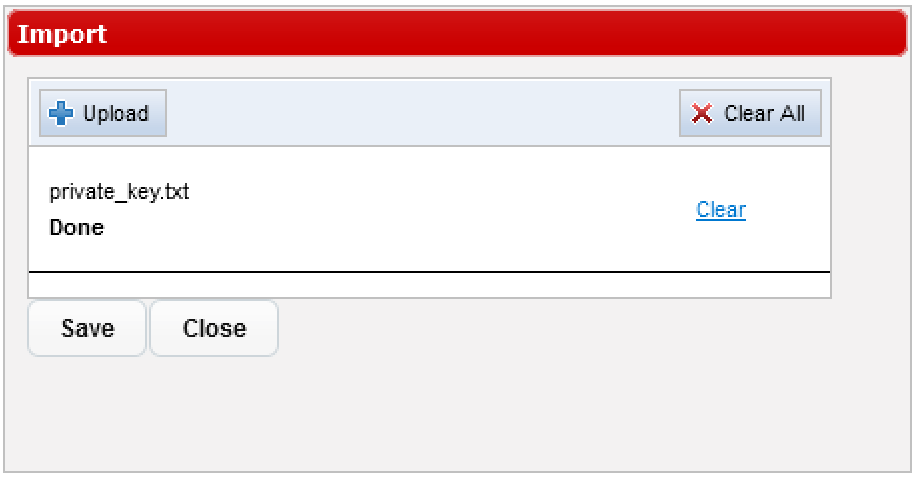
- Select the domain from the drop-down for which you authenticate with DKIM

If you have the domain key that needs to be associated with your mails, then follow the steps below:

- Leave the 'DKIM' check box, unchecked.
- Click the 'Import' link



- Click the 'Upload' link, navigate to the location where the private key for the selected domain is saved and click 'Open'

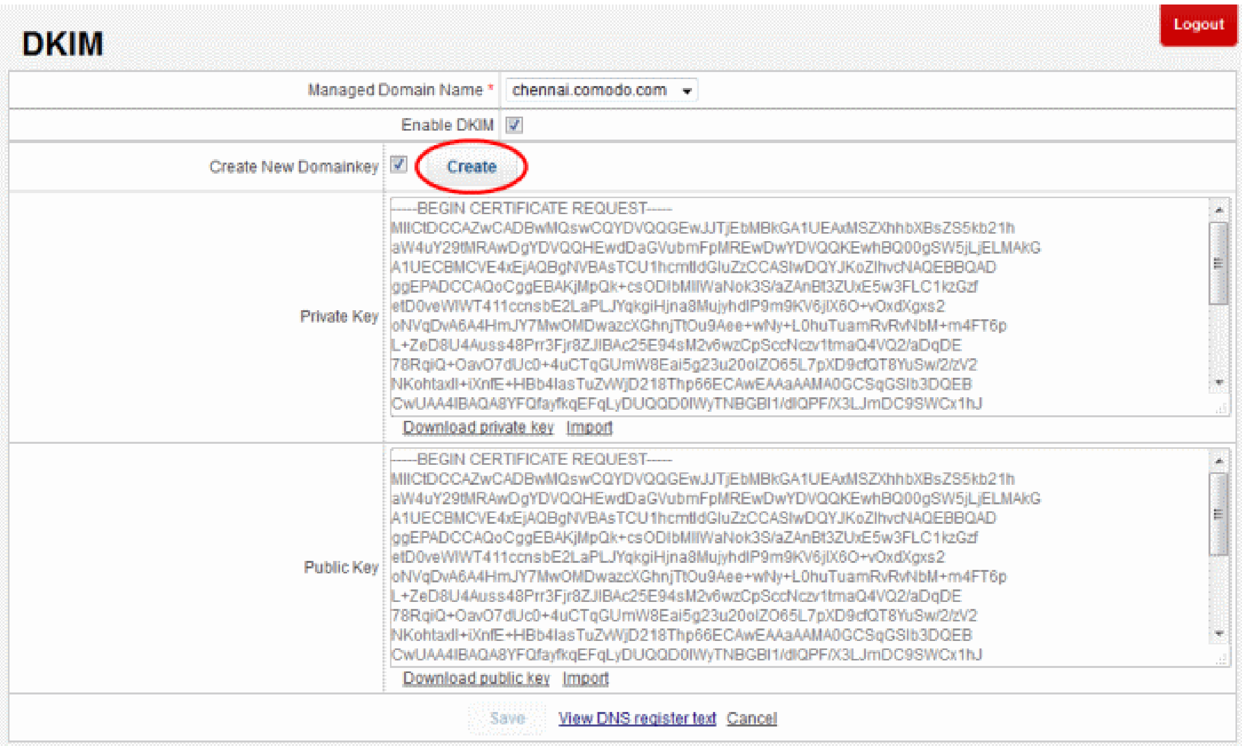


private_key.txt
Done

- To remove the selected file from the field, click 'Clear'
- To upload the private key, click 'Save'.
- Repeat the above steps to upload the public key.
- To download and save the private and public keys, click the respective download links.

If you do not have the domain key, then follow these steps:

- Enable 'Create New Domainkey'
- Click 'Create' to generate a new domain key for the selected domain.



Managed Domain Name * chennai.comodo.com

Enable DKIM ☑

Create New Domainkey ☑

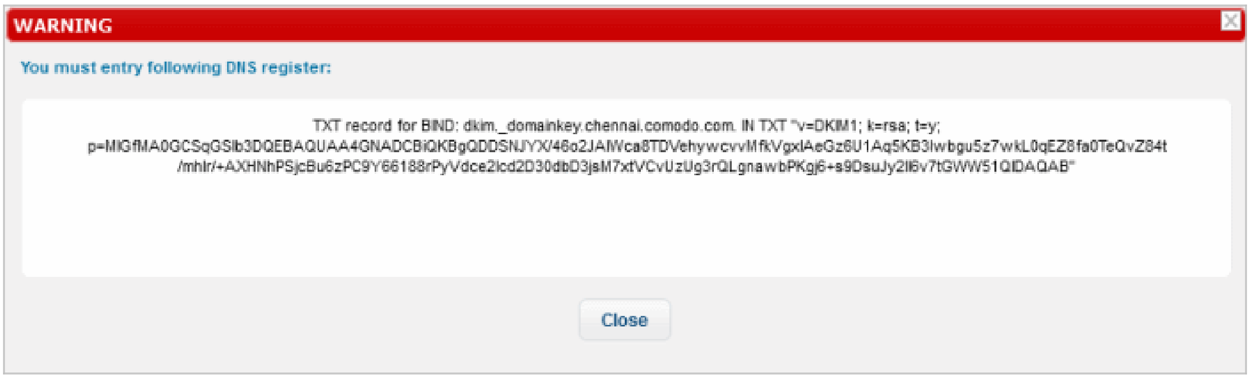
Private Key

```
-----BEGIN CERTIFICATE REQUEST-----
MIICtDCCAZwCADBwMQswCQYDVQQGEwJJTjEbMBkGA1UEAxMSZXhhbXBsZS5kb21h
aW4uY29tMRAwDgYDVQQHEwdDaGVubmFpMREwDwYDVQQKEwhBQ00gSW5jLjELMAkG
A1UECBMCVE4xEjAQBgNVBAsTCU1hcmtldGluZzCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAKjMpQk+csODIbMIIWaNok3S/aZAnBt3ZUxE5w3FLC1kzGzf
etD0veWIWT411ccnsbE2LaPLJYqkgiHjna8MujyhdIP9m9KV6jIX6O+vOxdXgxs2
oNVqDvA6A4HmJY7MwOMDwazcXGhnjTtOu9Aee+wNy+L0huTuamRvRvNbM+m4FT6p
L+ZeD8U4Auss48Prr3Fjr8ZJIBAc25E94sM2v6wzCpSccNczv1tmaQ4VQ2/aDqDE
78RqiQ+OavO7dUc0+4uCTqGUmW8Eai5g23u20oIZO65L7pXD9cfQT8YuSw/2/zV2
NKohtaxlI+iXnfE+HBb4lasTuZVWjD218Thp66ECAwEAAaAAMA0GCSqGSIb3DQEB
CwUAA4IBAQA8YFQfayfkqEFqLyDUQQD0lWyTNBGBI1/dlQPF/X3LJmDC9SWCx1hJ
```

Public Key

```
-----BEGIN CERTIFICATE REQUEST-----
MIICtDCCAZwCADBwMQswCQYDVQQGEwJJTjEbMBkGA1UEAxMSZXhhbXBsZS5kb21h
aW4uY29tMRAwDgYDVQQHEwdDaGVubmFpMREwDwYDVQQKEwhBQ00gSW5jLjELMAkG
A1UECBMCVE4xEjAQBgNVBAsTCU1hcmtldGluZzCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAKjMpQk+csODIbMIIWaNok3S/aZAnBt3ZUxE5w3FLC1kzGzf
etD0veWIWT411ccnsbE2LaPLJYqkgiHjna8MujyhdIP9m9KV6jIX6O+vOxdXgxs2
oNVqDvA6A4HmJY7MwOMDwazcXGhnjTtOu9Aee+wNy+L0huTuamRvRvNbM+m4FT6p
L+ZeD8U4Auss48Prr3Fjr8ZJIBAc25E94sM2v6wzCpSccNczv1tmaQ4VQ2/aDqDE
78RqiQ+OavO7dUc0+4uCTqGUmW8Eai5g23u20oIZO65L7pXD9cfQT8YuSw/2/zV2
NKohtaxlI+iXnfE+HBb4lasTuZVWjD218Thp66ECAwEAAaAAMA0GCSqGSIb3DQEB
CwUAA4IBAQA8YFQfayfkqEFqLyDUQQD0lWyTNBGBI1/dlQPF/X3LJmDC9SWCx1hJ
```

The domain key will be generated and the same must be entered in the DNS register for authenticating the domain.



WARNING

You must entry following DNS register:

TXT record for BIND: dkim._domainkey.chennai.comodo.com. IN TXT "v=DKIM1; k=rsa; t=y;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDDSNJYX/46o2JAIWca8TDVehywcvvMfkVgxIAeGz6U1Aq5KB3Iwbgu5z7wkL0qEZ8fa0TeQvZ84t
/mhIr/+AXHNhPSjcBu6zPC9Y66188rPyVdce2Icd2D30dbD3jsM7xtVCvUzUg3rQLgnawbPKgj6+s9DsuJy2Il6v7tGWW51QIDAQAB"

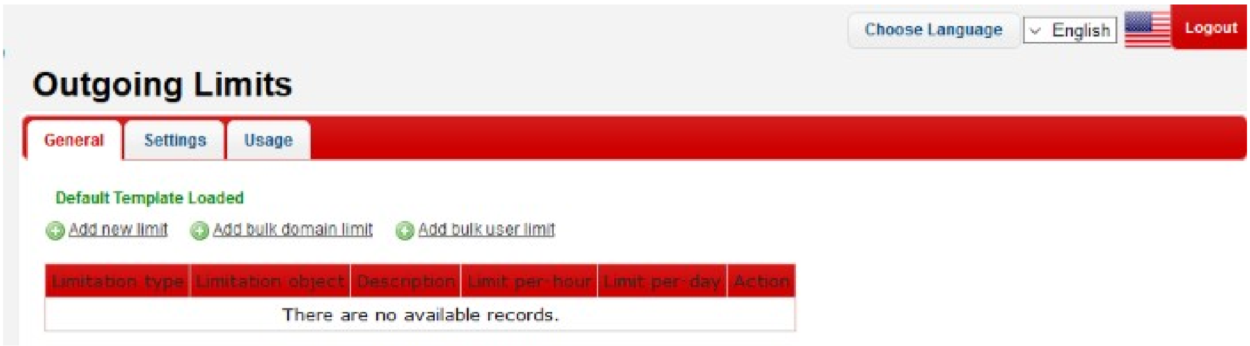
You can view and copy the details of domain key anytime by clicking the 'View DNS register text' link at the bottom. For more details about how to update the DNS record, refer to your domain or web hosting documentation.

7.10 Outgoing SMTP Limits

- KoruMail lets you limit how many outgoing mails can be sent by a user, or sent from a specific domain.
- You can configure the system to allow a certain number of outgoing mails per hour and per day.
- The interface lets you add domains or usernames individually or in bulk.

To open the 'Outgoing Limits' screen,

- Click the 'SMTP' tab on the left menu, then click 'Outgoing Limits'.



Default Template Loaded

Limitation type	Limitation object	Description	Limit per hour	Limit per day	Action
There are no available records.					

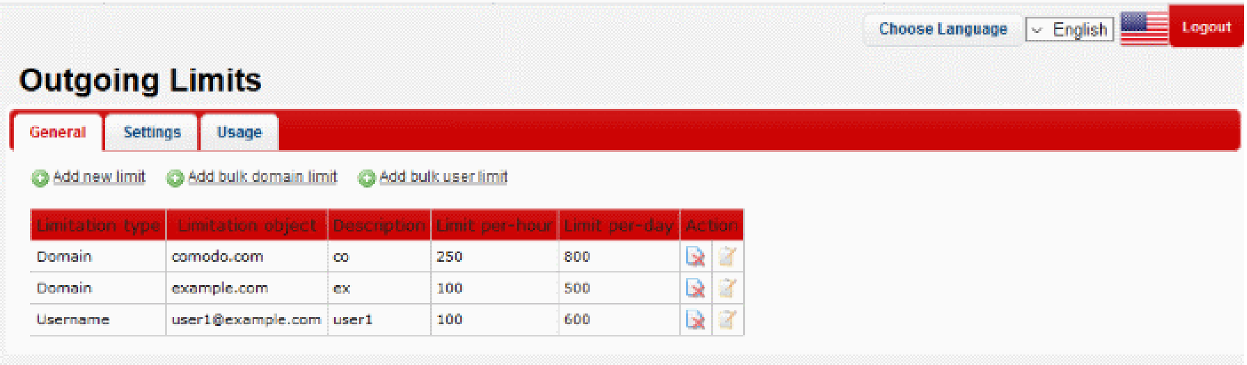
The interface allows administrators to:

- **Set outgoing limits for domains and users**
- **Configure outgoing limits settings**
- **View outgoing mail usage details for domains and users**

Configure outgoing limits for domains and users

To configure outgoing limits for domains and users:

- Click the 'General' tab



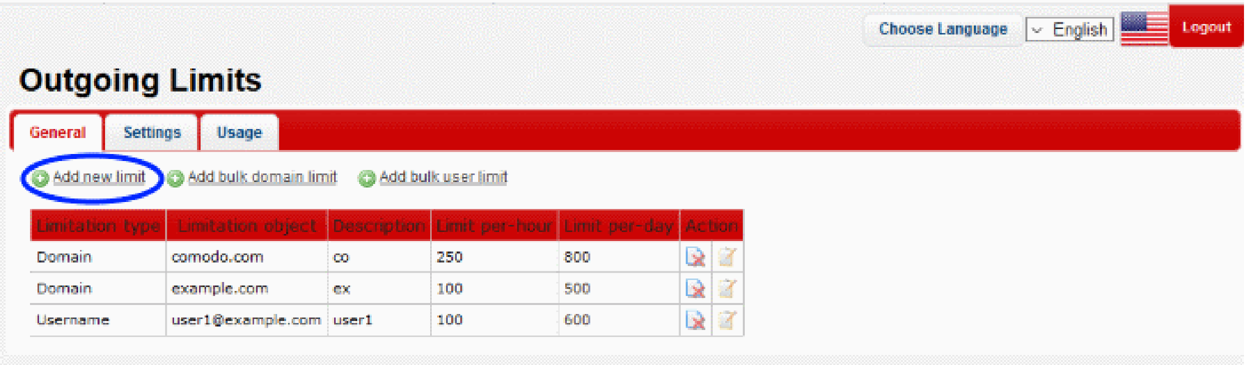
Outgoing Limits

Limitation type	Limitation object	Description	Limit per-hour	Limit per-day	Action
Domain	comodo.com	co	250	800	✗ ✎
Domain	example.com	ex	100	500	✗ ✎
Username	user1@example.com	user1	100	600	✗ ✎

Outgoing Limits: General - Table of Column Descriptions

Column Header	Description	
Limitation Type	Whether the limitation is for a domain or for a user	
Limitation Object	The details of the domain or the user	
Description	Enter a description of the limit if required.	
Limit per-hour	The number of outgoing mails allowed per hour	
Limit per-day	The number of outgoing mails allowed per day	
Action	✗	Delete a limitation.
	✎	Edit a limitation.

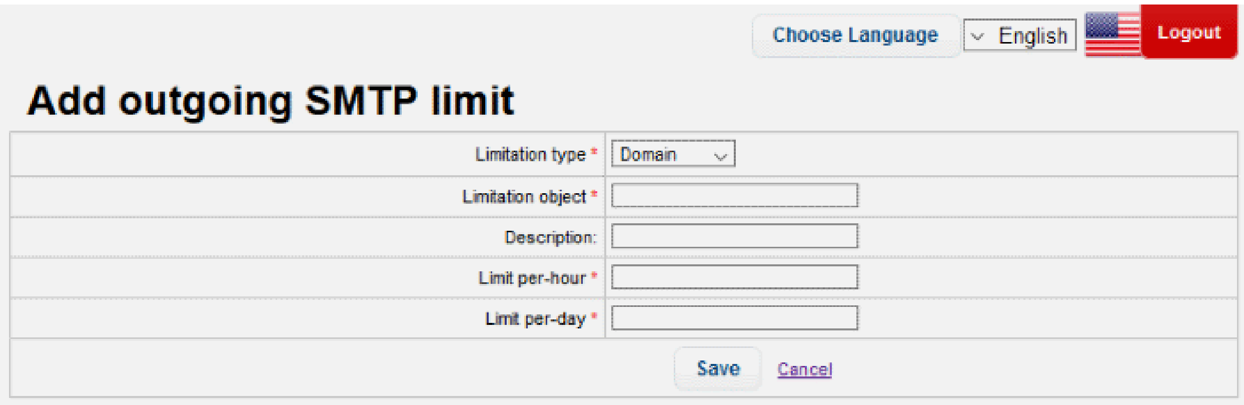
- To set a limitation for a domain or user individually, click the 'Add new limit' link at the top



Outgoing Limits

Limitation type	Limitation object	Description	Limit per-hour	Limit per-day	Action
Domain	comodo.com	co	250	800	✗ ✎
Domain	example.com	ex	100	500	✗ ✎
Username	user1@example.com	user1	100	600	✗ ✎

The 'Add outgoing SMTP limit' screen will be displayed.



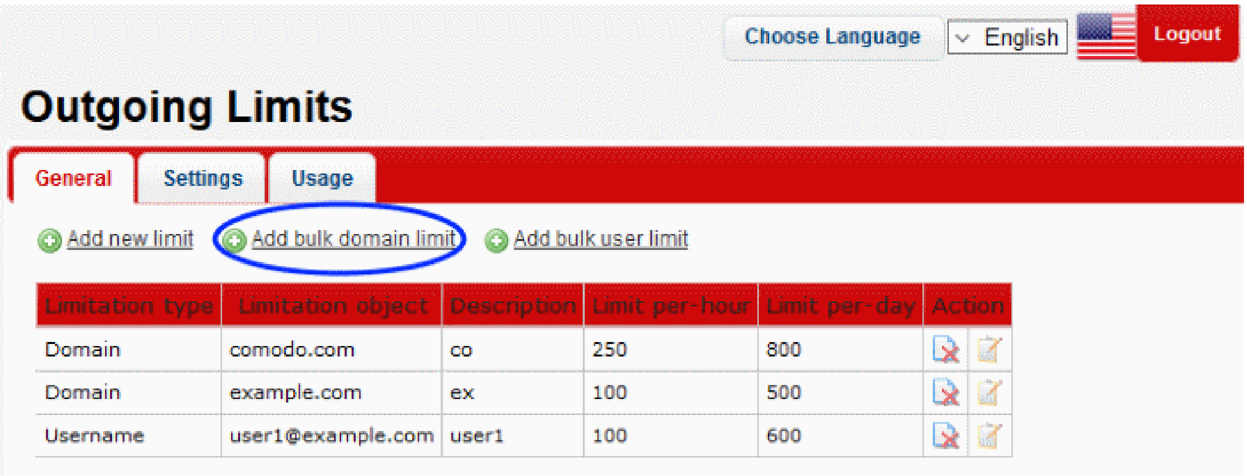
Add outgoing SMTP limit

Limitation type *	Domain
Limitation object *	
Description:	
Limit per-hour *	
Limit per-day *	

- **Limitation type:** Select whether you want to configure the limit for a domain or user from the drop-down
- **Limitation object:** Enter the name of the domain or username depending on your 'Limitation type' selection
- **Description:** Enter an appropriate description for the limitation
- **Limit per-hour:** Enter the number of outgoing mails allowed per hour for a domain or user
- **Limit per-day:** Enter the number of outgoing mails allowed per day for a domain or user

Click 'Save'. The newly added limitation will be displayed in the list.

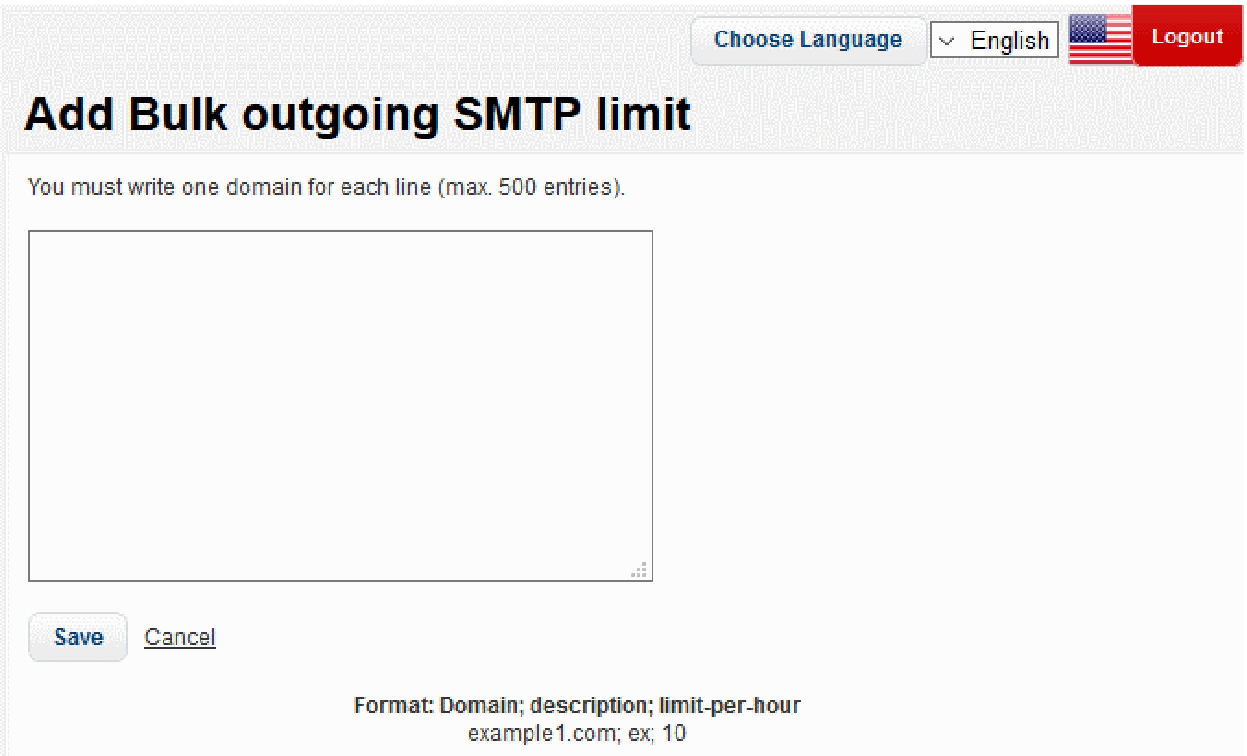
- To set a limitation for multiple domains at a time, click the 'Add bulk domain limit' link at the top



Outgoing Limits

Limitation type	Limitation object	Description	Limit per-hour	Limit per-day	Action
Domain	comodo.com	co	250	800	
Domain	example.com	ex	100	500	
Username	user1@example.com	user1	100	600	

The 'Add Bulk outgoing SMTP limit' screen will be displayed.



Add Bulk outgoing SMTP limit

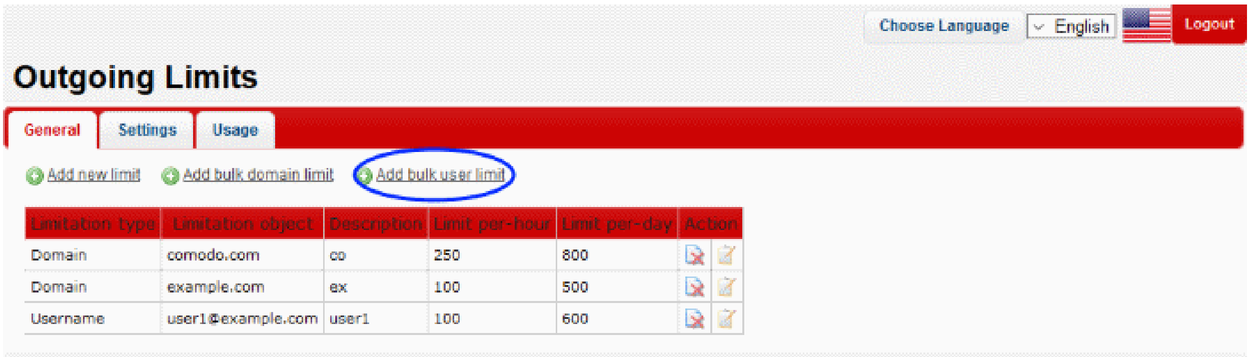
You must write one domain for each line (max. 500 entries).

Format: Domain; description; limit-per-hour
example1.com; ex; 10

- Enter the limitation for each domain per line as per the format shown in the screen..
- Click 'Save'.

The limitations for the added domains will be displayed in the 'General' screen.

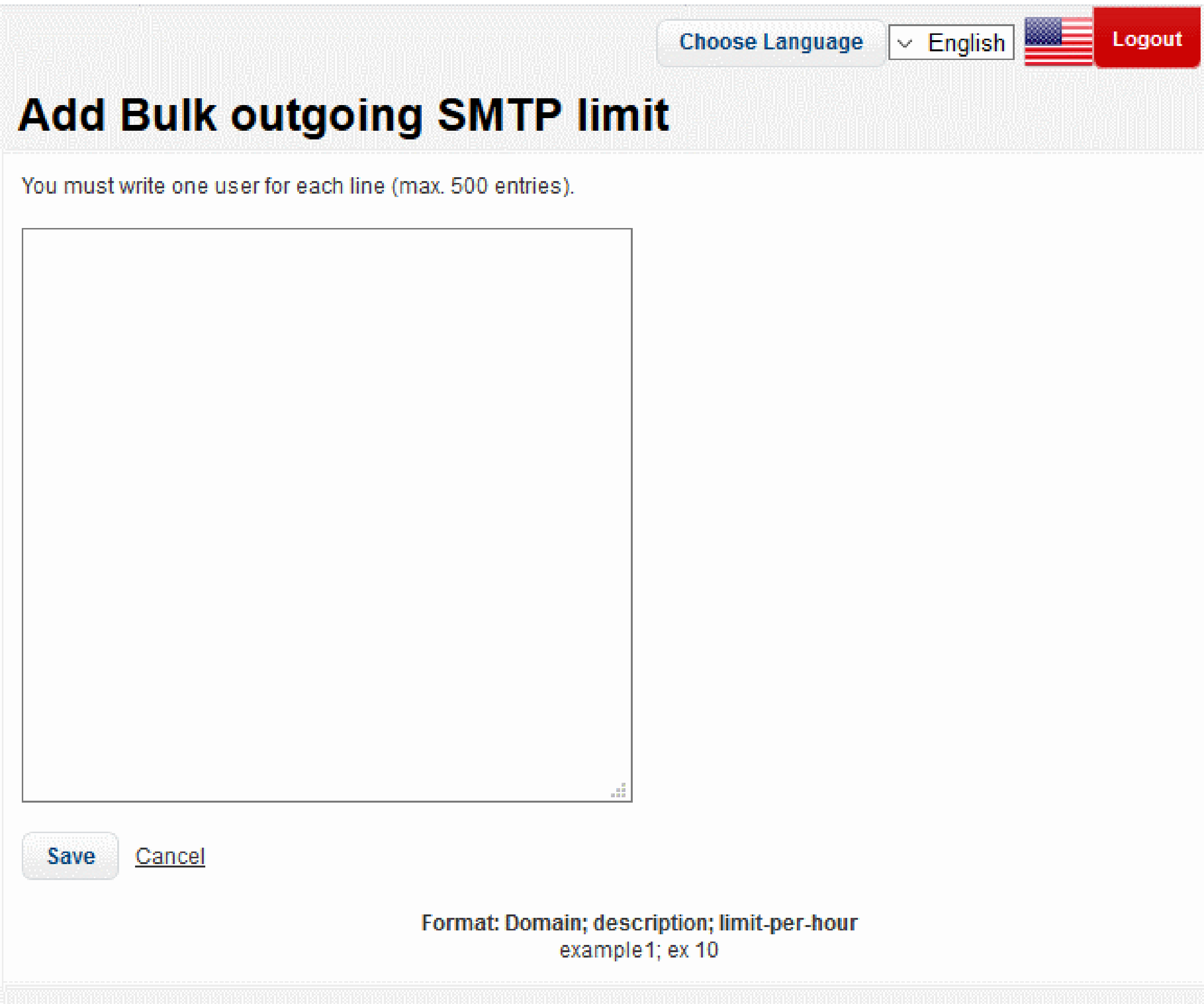
- To set a limitation for multiple user at a time, click the 'Add bulk user limit' link at the top



Outgoing Limits

Limitation type	Limitation object	Description	Limit per-hour	Limit per-day	Action
Domain	comodo.com	co	250	800	
Domain	example.com	ex	100	500	
Username	user1@example.com	user1	100	600	

The 'Add Bulk outgoing SMTP limit' screen will be displayed.



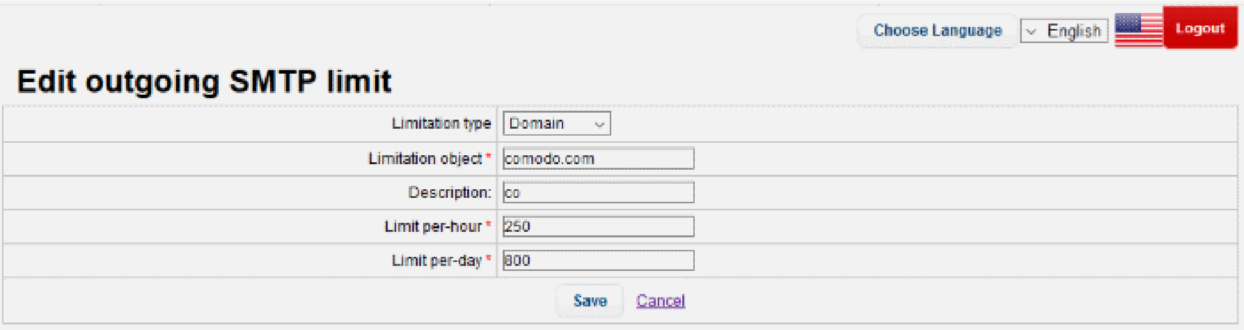
Add Bulk outgoing SMTP limit

You must write one user for each line (max. 500 entries).

Format: Domain; description; limit-per-hour
example1; ex 10

- Enter the limitation for each user per line as per the format shown in the screen.
- Click 'Save' to apply your changes.

The limitations for the added users will be displayed in the 'General' screen.



Edit outgoing SMTP limit

Limitation type	Domain
Limitation object *	comodo.com
Description:	co
Limit per-hour *	250
Limit per-day *	800

- To delete a limitation from the list, click the button in the 'Action' column and confirm it in the confirmation screen.
- To edit a limitation, click the button in the 'Action' column.

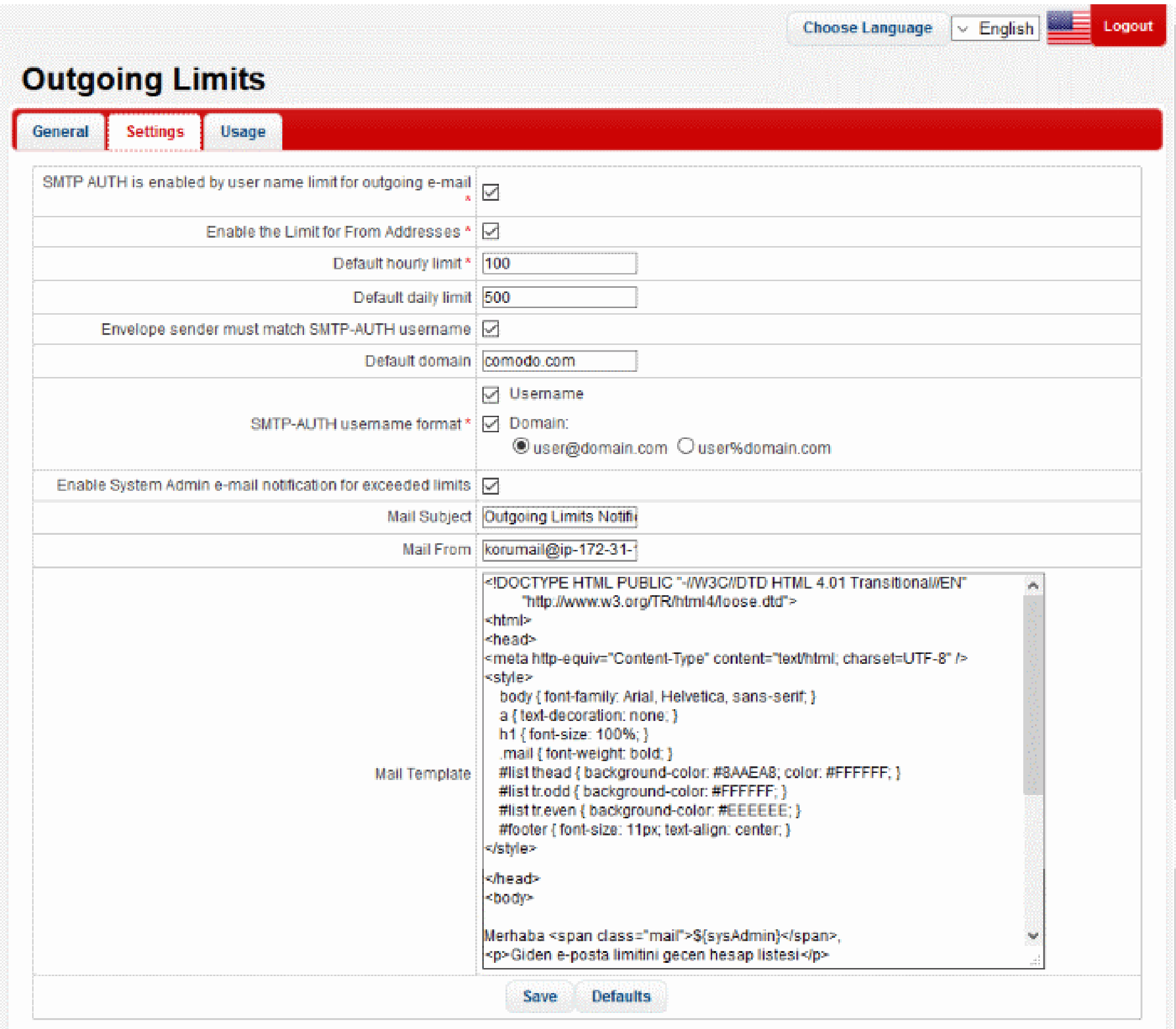
The 'Edit outgoing SMTP limit' screen will be displayed.

The screen is similar to the 'Add outgoing SMTP limit' interface. See '**Configure outgoing limits for domains and users**' for more details.

Configure outgoing limits settings

The 'Settings' tab allows administrators to customize the limitations added in the '**General**' tab.

- To configure outgoing limit settings, click the 'Settings' tab



Outgoing Limits

SMTP AUTH is enabled by user name limit for outgoing e-mail *	☑
Enable the Limit for From Addresses *	☑
Default hourly limit *	100
Default daily limit	500
Envelope sender must match SMTP-AUTH username	☑
Default domain	comodo.com
SMTP-AUTH username format *	☑ Username ☑ Domain: ● user@domain.com ○ user%domain.com
Enable System Admin e-mail notification for exceeded limits	☑
Mail Subject	Outgoing Limits Notifi
Mail From	korumail@ip-172-31-
Mail Template	(see below)

Mail Template

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
        "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<style>
   body { font-family: Arial, Helvetica, sans-serif; }
   a { text-decoration: none; }
   h1 { font-size: 100%; }
   .mail { font-weight: bold; }
   #list thead { background-color: #8AAEA8; color: #FFFFFF; }
   #list tr.odd { background-color: #FFFFFF; }
   #list tr.even { background-color: #EEEEEE; }
   #footer { font-size: 11px; text-align: center; }
</style>

</head>
<body>

Merhaba <span class="mail">${sysAdmin}</span>,
<p>Giden e-posta limitini gecen hesap listesi</p>
```

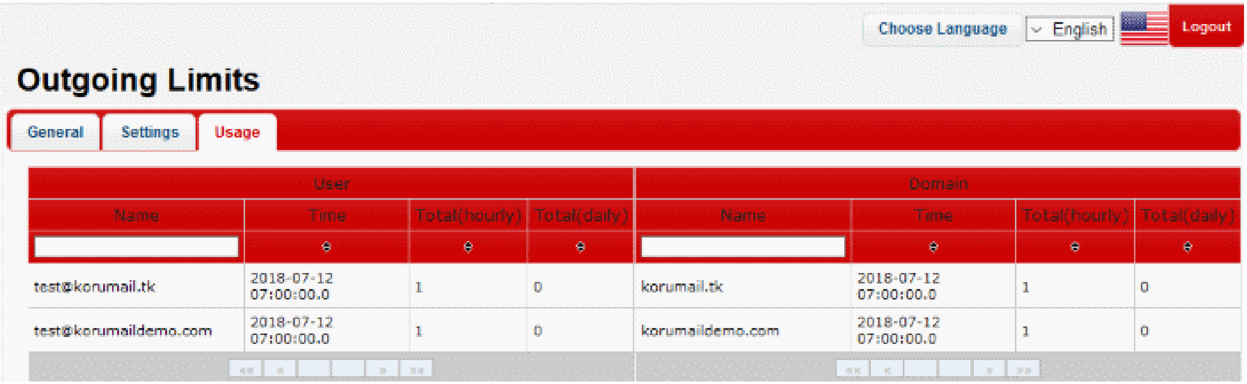
Outgoing Limits: Settings - Table of Parameters	
Parameter	**Description**
SMTP AUTH is enabled by user name limit for outgoing email	If enabled, SMTP AUTH is required for outgoing mails sent by users who are configured in the '**General**' tab to send limited mails.
Enable the Limit for From Addresses	If enabled, the limit configured in the '**General**' tab will apply. Otherwise, the default hourly and daily values below will apply.
Default hourly limit	The maximum number of outgoing mails that can be sent by users per hour
Default daily limit	The maximum number of outgoing mails that can be sent by users per day
Envelope sender must match SMTP-AUTH username	If enabled, the address of the sender must match the SMTP-AUTH username
Default domain	The default domain of the outgoing emails.

SMTP-AUTH username format	Method of authenticating the user. Choose from username or domain methods.
Enable System Admin e-mail notification for exceeded limits	Will send a notification if the number of mails sent by users who are configured in the '**General**' tab exceeds the limit.
Mail subject	Subject of the notification mail mentioned above.
Mail From	The email address from which the notification mail is sent
Mail Template	The template of the notification mail.

- Click 'Save' to apply your changes.

View outgoing mail usage details or domains and users

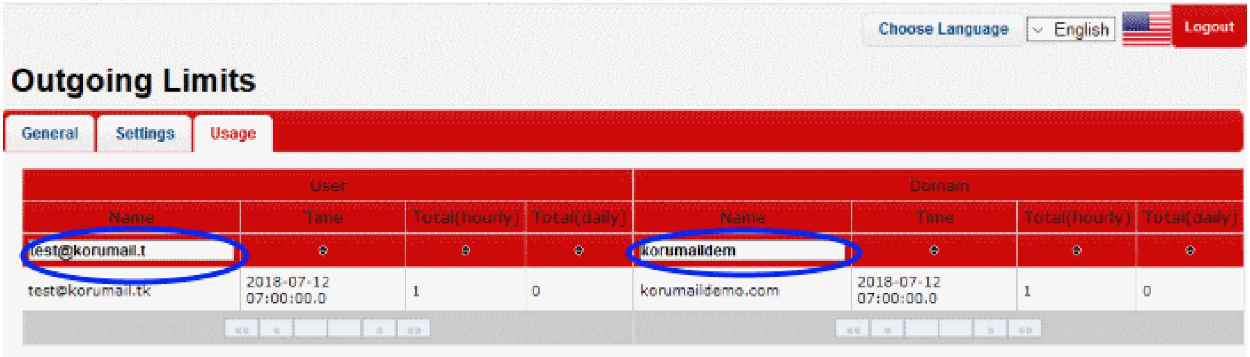
The 'Usage' tab allows administrators to view outgoing mails from users and domains covered by outgoing limits.



User				Domain			
Name	Time	Total(hourly)	Total(daily)	Name	Time	Total(hourly)	Total(daily)
test@korumail.tk	2018-07-12 07:00:00.0	1	0	korumail.tk	2018-07-12 07:00:00.0	1	0
test@korumaildemo.com	2018-07-12 07:00:00.0	1	0	korumaildemo.com	2018-07-12 07:00:00.0	1	0

Outgoing Limits: Usage - Table of Parameters		
Parameter		**Description**
User	Name	Displays the email address of the sender
	Time	The time at which the mail was sent.
	Total (Hourly)	The total number of mails sent in an hour.
	Total (Daily)	The total number of mails sent in a day.
Domain	Name	Displays the email address of the sender on the limited domain
	Time	The time at which the mail was sent.
	Total (Hourly)	The total number of mails sent in an hour.
	Total (Daily)	The total number of mails sent in a day.

To search for a particular recipient, enter the first few letters of the recipient's name in either the 'User' or 'Domain' search field:



Outgoing Limits

User				Domain			
Name	Time	Total(hourly)	Total(daily)	Name	Time	Total(hourly)	Total(daily)
test@korumail.t	⇕	⇕	⇕	korumaildem	⇕	⇕	⇕
test@korumail.tk	2018-07-12 07:00:00.0	1	0	korumaildemo.com	2018-07-12 07:00:00.0	1	0

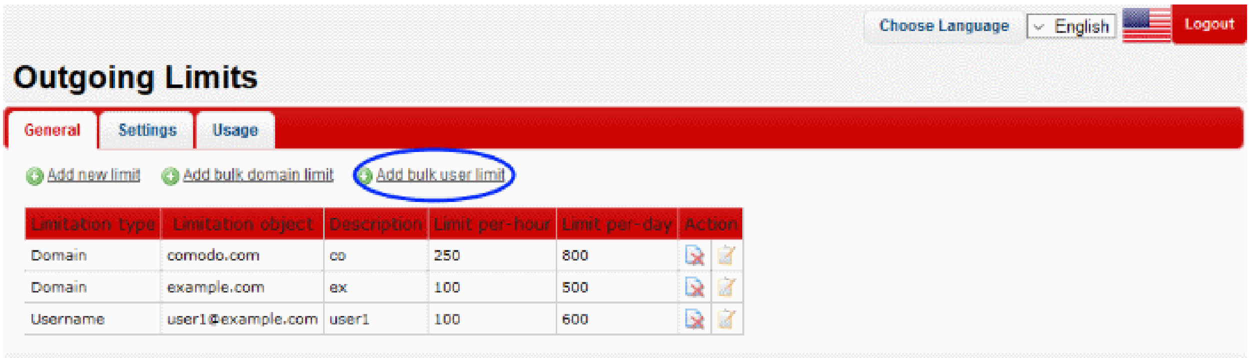
- Clicking the ⇕ button in a column header will sort the table in ascending or descending order of the items in the column.

7.11 Incoming SMTP Limits

- KoruMail allows you to set limits for incoming mails for users and domain names.
- You can configure the system to only allow a certain number of incoming mails per hour and per day.
- The interface lets you add domains or usernames individually or in bulk.

To open the 'Incoming Limits' screen

- Click the 'SMTP' tab on the left menu, then click 'Incoming Limits'.



Outgoing Limits

Limitation type	Limitation object	Description	Limit per-hour	Limit per-day	Action
Domain	comodo.com	co	250	800	
Domain	example.com	ex	100	500	
Username	user1@example.com	user1	100	600	

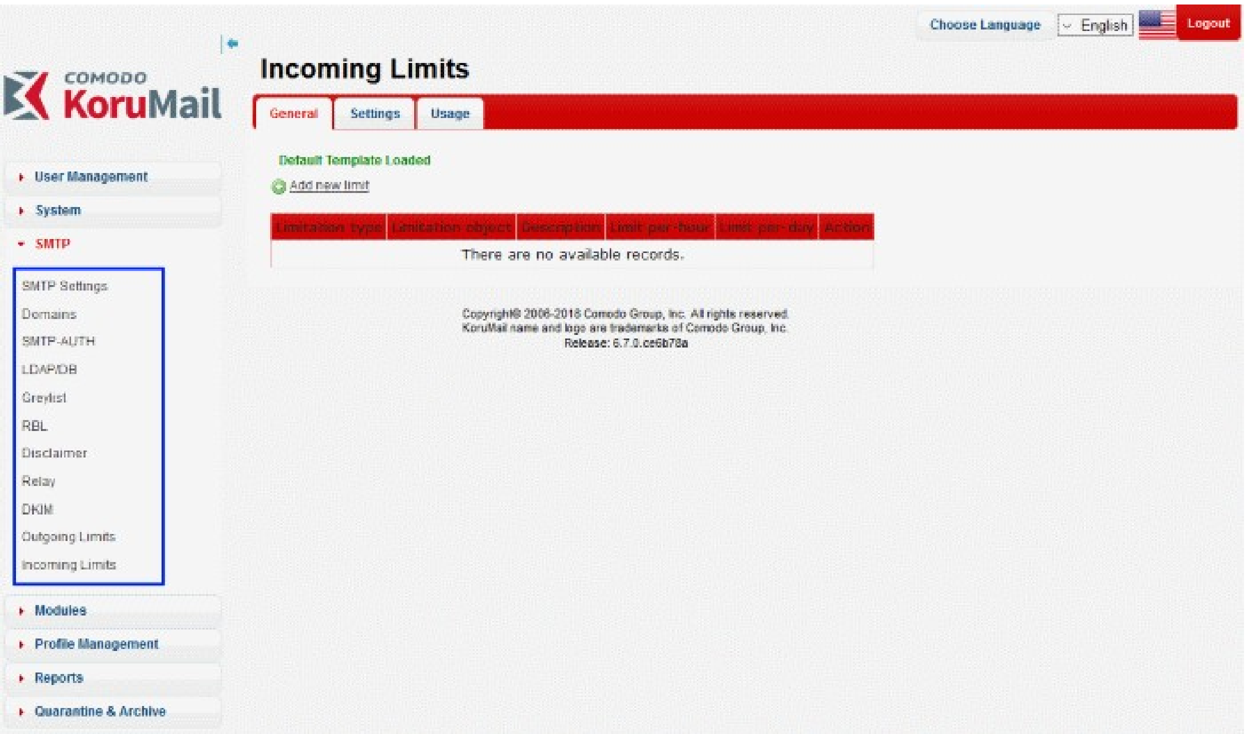
The interface allows administrators to:

- **Configure Incoming limits for domains and users**
- **Configure Incoming limits settings**
- **View Incoming mail usage details for domains and users**

Configure Incoming limits for domains and users

To configure incoming limits for domains and users:

- Click SMTP > Incoming Limits and then click the 'General' tab



Choose Language English Logout

COMODO KoruMail

Incoming Limits

General | Settings | Usage

Default Template Loaded

Add new limit

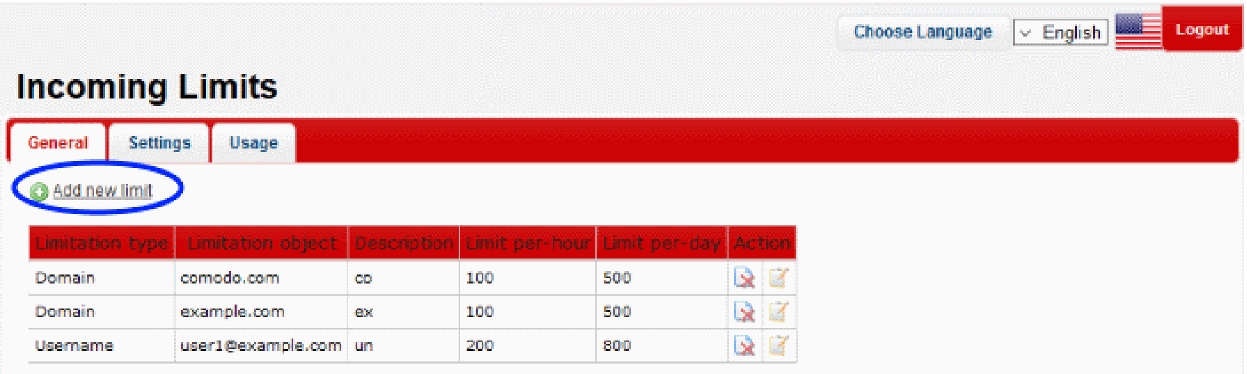
Limitation type	Limitation object	Description	Limit per-hour	Limit per-day	Action
There are no available records.					

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

Incoming Limits: General - Table of Column Descriptions

Column Header	Description	
Limitation Type	Indicates whether the limitation is for a domain or user	
Limitation Object	The details of the domain or the user	
Description	The description for the limitation	
Limit per-hour	Indicates the number of incoming mails allowed per hour	
Limit per-day	Indicates the number of incoming mails allowed per day	
Action	✗	Allows administrators to delete a limitation set for a domain or user
	✎	Allows administrators to edit a limitation set for a domain or user

- To set a limitation for a domain or user individually, click the 'Add new limit' link at the top



Choose Language English Logout

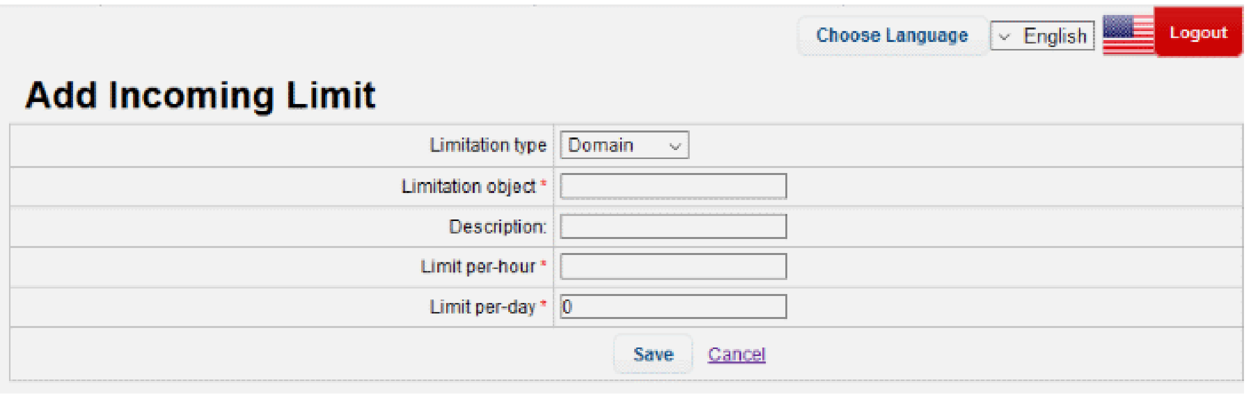
Incoming Limits

General | Settings | Usage

Add new limit

Limitation type	Limitation object	Description	Limit per-hour	Limit per-day	Action
Domain	comodo.com	co	100	500	✗ ✎
Domain	example.com	ex	100	500	✗ ✎
Username	user1@example.com	un	200	800	✗ ✎

The 'Add Incoming Limit' screen will be displayed.



Add Incoming Limit

Limitation type	Domain
Limitation object *	
Description:	
Limit per-hour *	
Limit per-day *	0

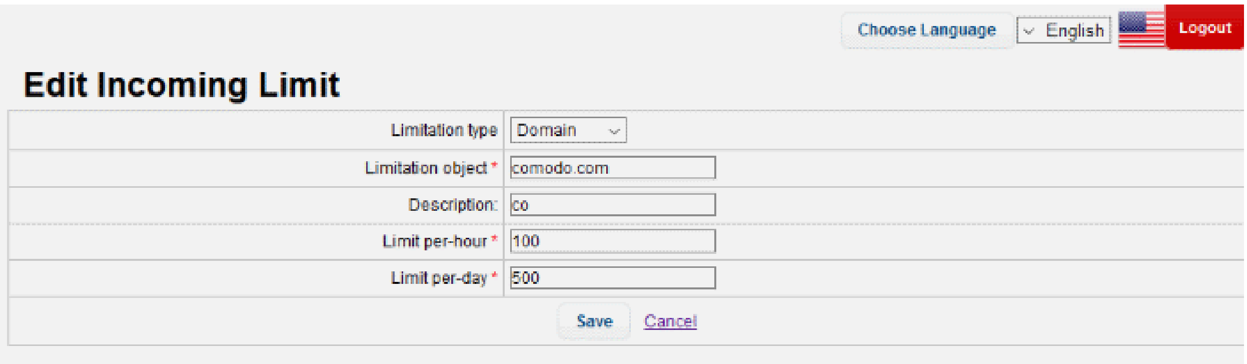
- **Limitation type:** Select whether you want to configure the limit for a domain or user from the drop-down
- **Limitation object:** Enter the name of the domain or username depending on your 'Limitation type' selection
- **Description:** Enter an appropriate description for the limitation
- **Limit per-hour:** Enter the number of outgoing mails allowed per hour for a domain or user
- **Limit per-day:** Enter the number of outgoing mails allowed per day for a domain or user

Click 'Save'. The newly added limitation will be displayed in the list.

The limitations for the added users will be displayed in the 'General' screen.

- To delete a limitation from the list, click the button under the 'Action' column and confirm it in the confirmation screen.
- To edit a limitation, click the button under the 'Action' column.

The 'Edit Incoming Limit' screen will be displayed.



Edit Incoming Limit

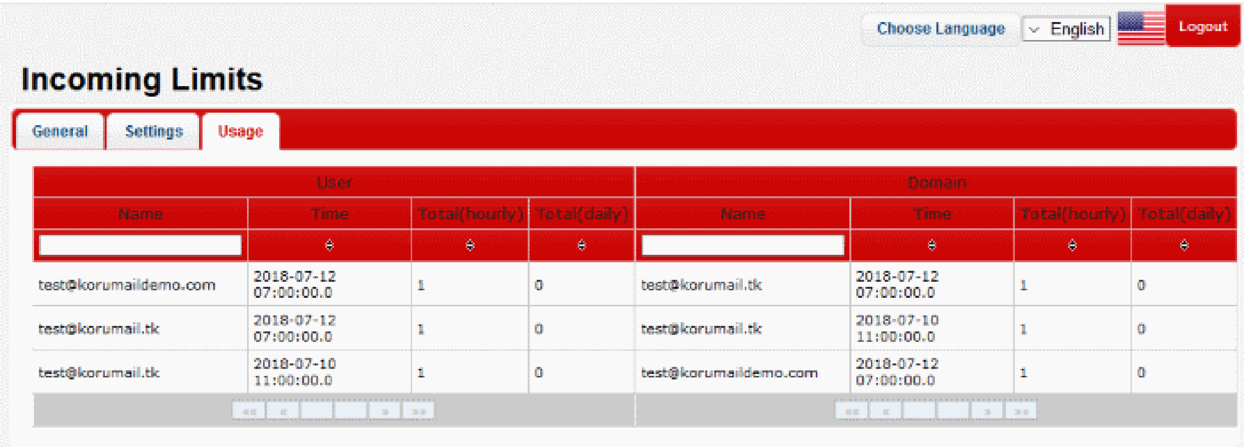
Limitation type	Domain
Limitation object *	comodo.com
Description:	co
Limit per-hour *	100
Limit per-day *	500

The screen is similar to the 'Add Incoming Limit' interface. See '**Configure incoming limits for domains and users**' for more details.

Configure Incoming limits settings

The 'Settings' tab in the 'Incoming Limits' screen allows administrators to configure the settings such that the Korumail server sends an automated email when the incoming limits exceed the set limitations added in the '**General**' tab. Please note that the email content will be available in the Korumail console by default.

- To configure incoming limit settings, click the 'Settings' tab



Incoming Limits

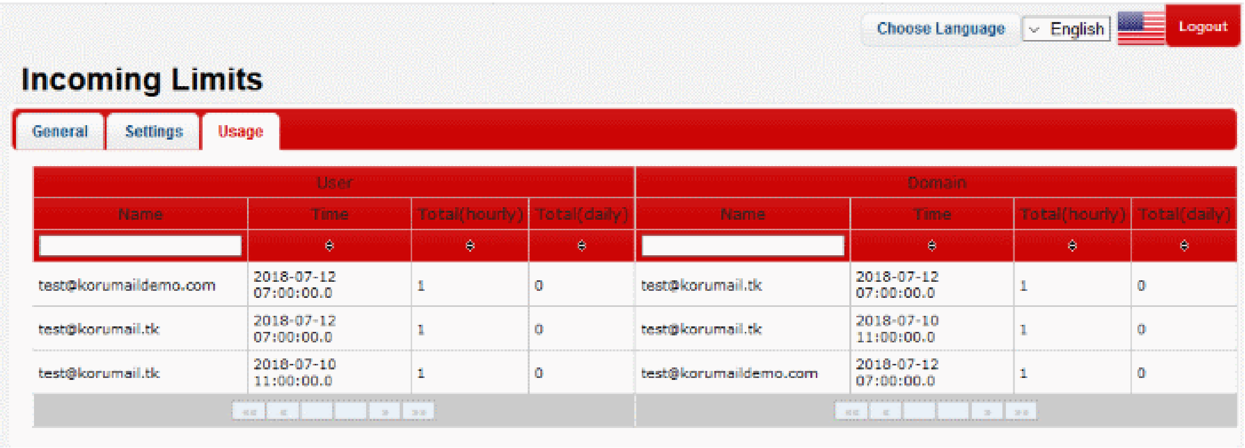
User				Domain			
Name	Time	Total(hourly)	Total(daily)	Name	Time	Total(hourly)	Total(daily)
test@korumaildemo.com	2018-07-12 07:00:00.0	1	0	test@korumail.tk	2018-07-12 07:00:00.0	1	0
test@korumail.tk	2018-07-12 07:00:00.0	1	0	test@korumail.tk	2018-07-10 11:00:00.0	1	0
test@korumail.tk	2018-07-10 11:00:00.0	1	0	test@korumaildemo.com	2018-07-12 07:00:00.0	1	0

Incoming Limits: Settings - Table of Parameters	
Parameter	**Description**
Enable System Admin e-mail notification for exceeded limits	Will send a notification if the number of mails sent by users who are configured in the '**General**' tab exceeds the limit.
Mail subject	Subject of the notification mail mentioned above.
Mail From	The email address from which the notification mail is sent
Mail Template	The template of the notification mail.

- Click 'Save' to apply your changes.

View incoming mail usage details for domains and users

The 'Usage' tab in the 'Incoming Limits' screen allows administrators to view the emails details of the 'Users' and 'Domains'. The parameters that can be viewed via the usage screen for 'Users' and 'Domains' are 'Name'(Name of the recipient), 'Time'(The time and date of the incoming email) and Hourly and daily based count of incoming emails.



Choose Language
English
Logout

Incoming Limits

General
Settings
Usage

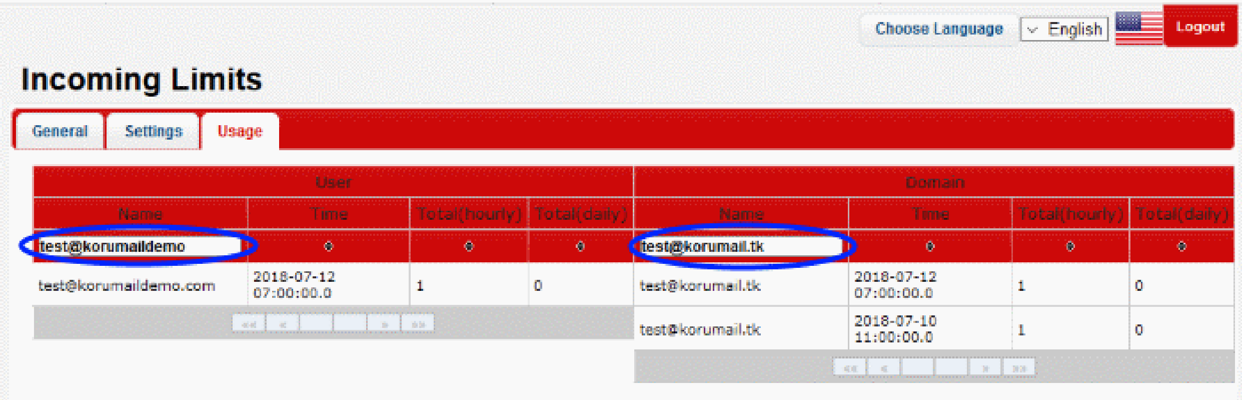
User				Domain			
Name	Time	Total(hourly)	Total(daily)	Name	Time	Total(hourly)	Total(daily)
test@korumaildemo.com	2018-07-12 07:00:00.0	1	0	test@korumail.tk	2018-07-12 07:00:00.0	1	0
test@korumail.tk	2018-07-12 07:00:00.0	1	0	test@korumail.tk	2018-07-10 11:00:00.0	1	0
test@korumail.tk	2018-07-10 11:00:00.0	1	0	test@korumaildemo.com	2018-07-12 07:00:00.0	1	0

Incoming Limits: Usage - Table of Parameters		
Parameter		**Description**
User	Name	Displays the email address of the recipient.
	Time	Time at which the mail is received.
	Total(Hourly)	Total number of emails received in an hour.

	Total(Daily)	Total number of emails received in a day.
Domain	Name	Displays the email address of the recipient on the limited domain.
	Time	Time at which the mail is received.
	Total(Hourly)	Total number of emails received in an hour.
	Total(Daily)	Total number of emails received in a day.

To 'Search' for a particular incoming recipient,

- Enter the first few alphabets of the recipient's name, in the usage details of 'User' and 'Domain'.



Incoming Limits

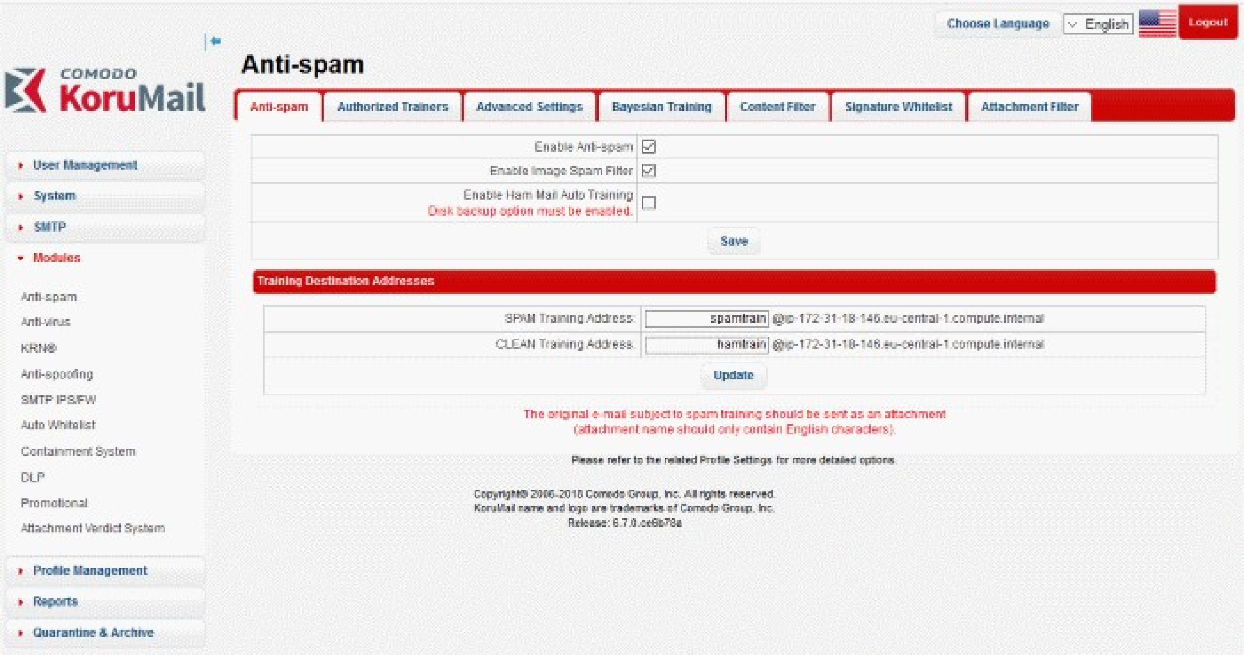
User				Domain			
Name	Time	Total(hourly)	Total(daily)	Name	Time	Total(hourly)	Total(daily)
test@korumaildemo	⬍	⬍	⬍	test@korumail.tk	⬍	⬍	⬍
test@korumaildemo.com	2018-07-12 07:00:00.0	1	0	test@korumail.tk	2018-07-12 07:00:00.0	1	0
				test@korumail.tk	2018-07-10 11:00:00.0	1	0

The intended recipient name will be displayed.

- Clicking the ⬍ button, administrators can view the bottom-most or top-most recipients.

8 Modules

- The 'Modules' area lets you configure the core security components of KoruMail's email defense system.
- The 'Anti-spam' module lets you configure anti-spam settings, containment, auto-whitelists, authorized trainers, content filters and more.
- See the links under the screenshot for more information on each module



Anti-spam

Enable Anti-spam	☑
Enable Image Spam Filter	☑
Enable Ham Mail Auto Training Disk backup option must be enabled.	□

Training Destination Addresses

SPAM Training Address:	spamtrain @ip-172-31-18-146.eu-central-1.compute.internal
CLEAN Training Address:	hamtrain @ip-172-31-18-146.eu-central-1.compute.internal

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

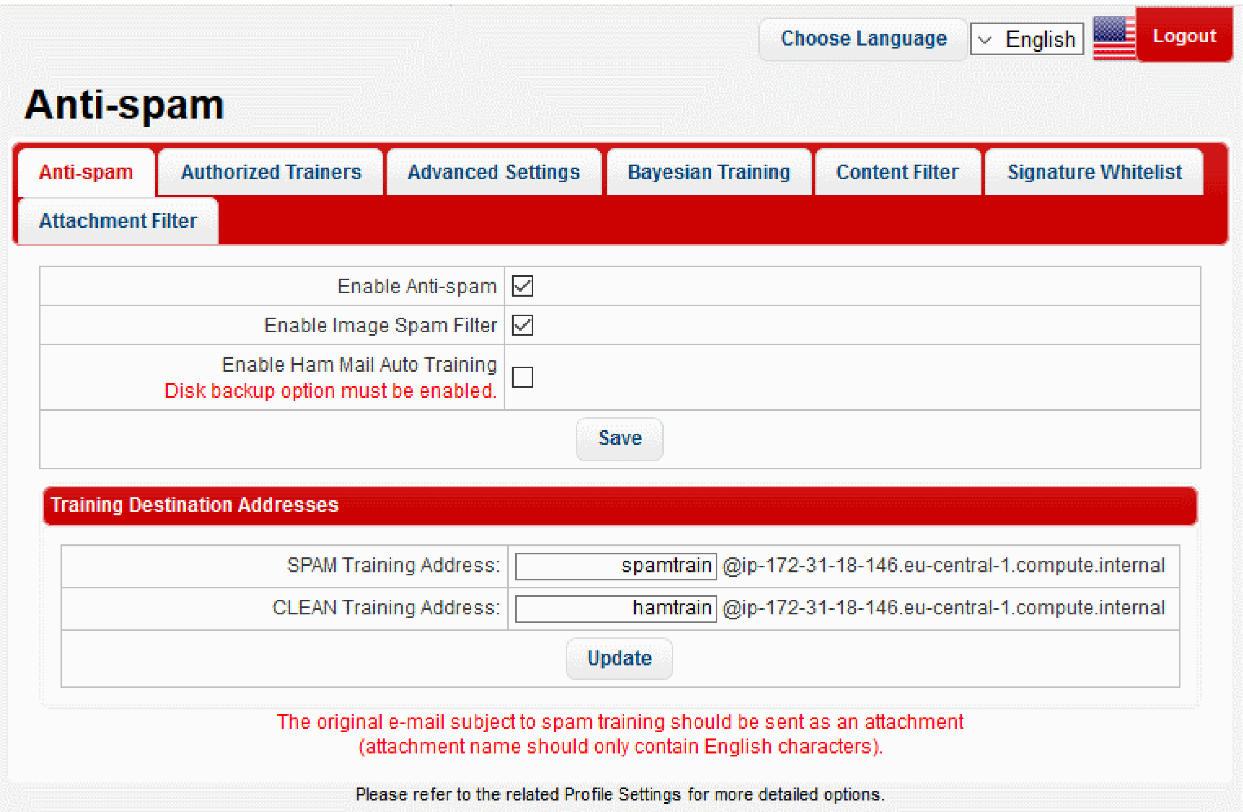
Please refer to the related Profile Settings for more detailed options.

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

- **Anti-spam**
- **Anti-virus**
- **KRN® - KoruMail Reputation Network® Servers**
- **Anti-spoofing**
- **SMTP IPS/FW**
- **Auto Whitelist**
- **Containment System**
- **Data Loss Prevention (DLP)**
- **Attachment Verdict System**

8.1 Anti-spam

- The anti-spam module lets you configure general and advanced settings, define authorized persons who can submit mail for spam training, upload material for Bayesian spam and HAM training, and add content filters.
- KoruMail uses our huge anti-spam database to accurately assign a spam-probability score to each message. Depending on this score, the email is categorized as 'OK' (default = 40 points or below), 'Probable Spam' (default = 40-50 points), 'Spam' (default = 50-100 points) or 'Certainly Spam' (default = 100 points and above).
- The anti-spam module must be enabled in order to activate the parameters in the profile settings. See '**Profile Management**' for more details about profile settings.
- Click 'Modules' > 'Anti-spam' to open the interface.



Anti-spam

Enable Anti-spam	☑
Enable Image Spam Filter	☑
Enable Ham Mail Auto Training Disk backup option must be enabled.	□

Training Destination Addresses

SPAM Training Address:	spamtrain @ip-172-31-18-146.eu-central-1.compute.internal
CLEAN Training Address:	hamtrain @ip-172-31-18-146.eu-central-1.compute.internal

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.

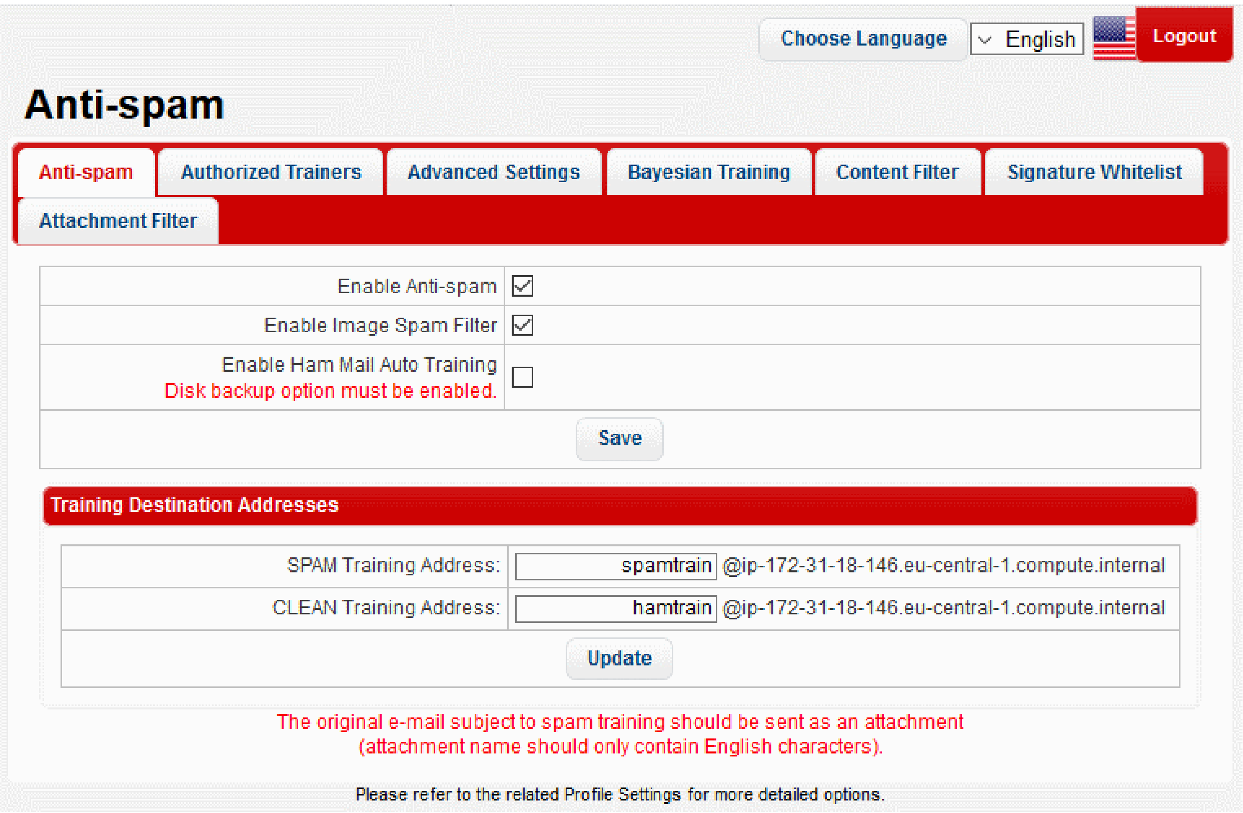
See the following sections for more details:

- **Anti-spam General Settings**
- **Authorized Trainers**
- **Advanced Anti-spam Settings**
- **Bayesian Training**
- **Content Filter**
- **Signature Whitelist**
- **Attachment filter**

8.1.1 Anti-spam General Settings

- The general settings screen lets you enable/disable the spam and image filters, and activate Ham mail training.
- The anti-spam module must be enabled in order to activate the anti-spam parameters specified in profile settings. See '**Profile Management**' for more details about profile settings.

To open the 'Anti-spam' general settings screen



Enable Anti-spam ☑

Enable Image Spam Filter ☑

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

SPAM Training Address: spamtrain @ip-172-31-18-146.eu-central-1.compute.internal

CLEAN Training Address: hamtrain @ip-172-31-18-146.eu-central-1.compute.internal

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.

- Click the 'Anti-spam' tab in the Anti-spam interface.

Anti-spam General Settings - Table of Parameters	
Parameter	**Description**
Enable Anti-spam	• Select this option to activate the anti-spam filtering engine. • The anti-spam parameters specified in the profile settings will be activated only if this setting is enabled here. • See '**Profile Management**' for more details about profile settings.
Enable Image Spam Filter	• Image based spam mails in which textual spam messages are embedded into images are designed to by pass text based spam analysis engine. • KoruMail is capable of filtering image based emails also. • Select this check box to activate the image spam filter.
Enable Ham Mail Auto Training	• Ham is opposite of Spam, meaning mails that are categorized as safe are also known as Ham mails. • KoruMail's spam filtering engine can be trained to identify safe emails to reduce spam identification processing time. • Select this check box to activate the clean email training feature.
Training Destination Addresses	
SPAM Training Address	Displays the domain address to which spam emails can be sent for training purposes. Enter the username part of the address to whom the spam mails can be sent.
CLEAN Training Address	Displays the domain address to which safe emails can be sent for training purposes. Enter the username part of the address to whom the safe mails can be sent.

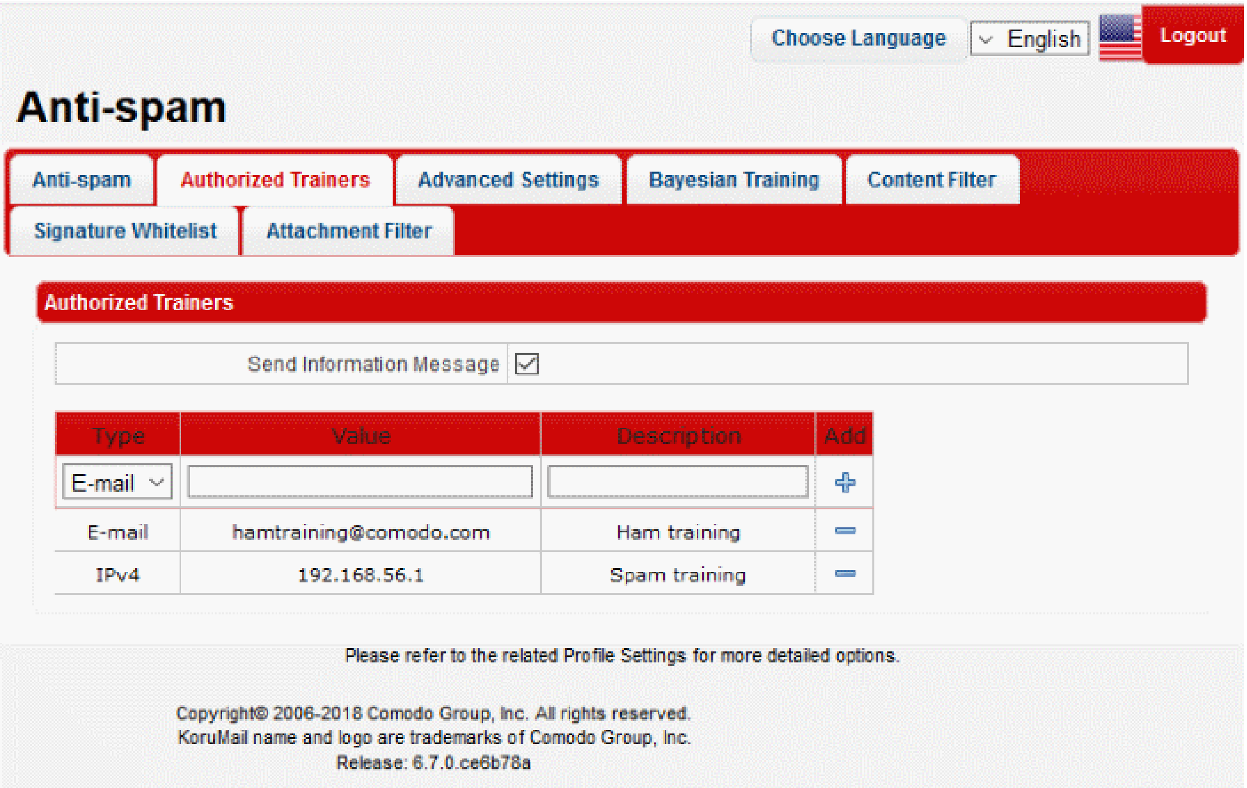
- Click the 'Save' and 'Update' buttons to apply your changes.

8.1.2 Authorized Trainers

- Allows you to define the sources from which spam training emails can be sent.
- Submitting sample junk mail to KoruMail allows the system to learn, adapt and protect against new spam types.
- Training content will only be accepted from the sources you specify here.

To open the 'Authorized Trainers' screen,

- Click the 'Authorized Trainers' tab in the Anti-spam interface.



Send Information Message ☑

Type	Value	Description	Add
E-mail			+
E-mail	hamtraining@comodo.com	Ham training	−
IPv4	192.168.56.1	Spam training	−

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: 6.7.0.ce6b78a

Authorized Trainers - Table of Column Descriptions		
Column Header	**Description**	
Type	Indicates the type of source of authorized trainers. The options available are Email, IPv4 and IPv6.	
Value	The details of the source ID	
Description	The description for the authorized trainer	
Add	+	Add a source ID after filling the fields in the row
	−	Delete an authorized trainer from the list

- **Send Information Message**: If enabled, will send a notification to the new trainer to inform them they have been added as a trainer.(***Default - Disabled***)

To add an authorized trainer

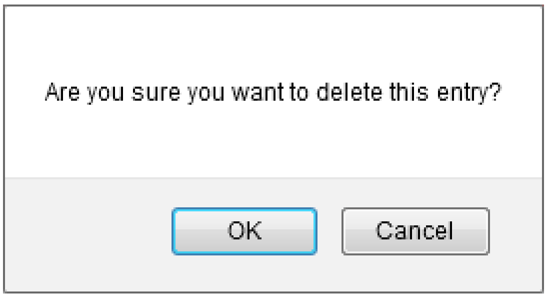
- Select the type of source from the options - Email, IPv4 or IPv6.

- Enter the source ID in the 'Value' field. This depends on the 'Type' selected.
- Provide an appropriate description for the authorized trainer in the 'Description' field.
- Click the ✚ button.

The authorized trainer will be added and listed in the table.

To remove an authorized trainer

- Click the ➖ button beside an entry that you want to remove.



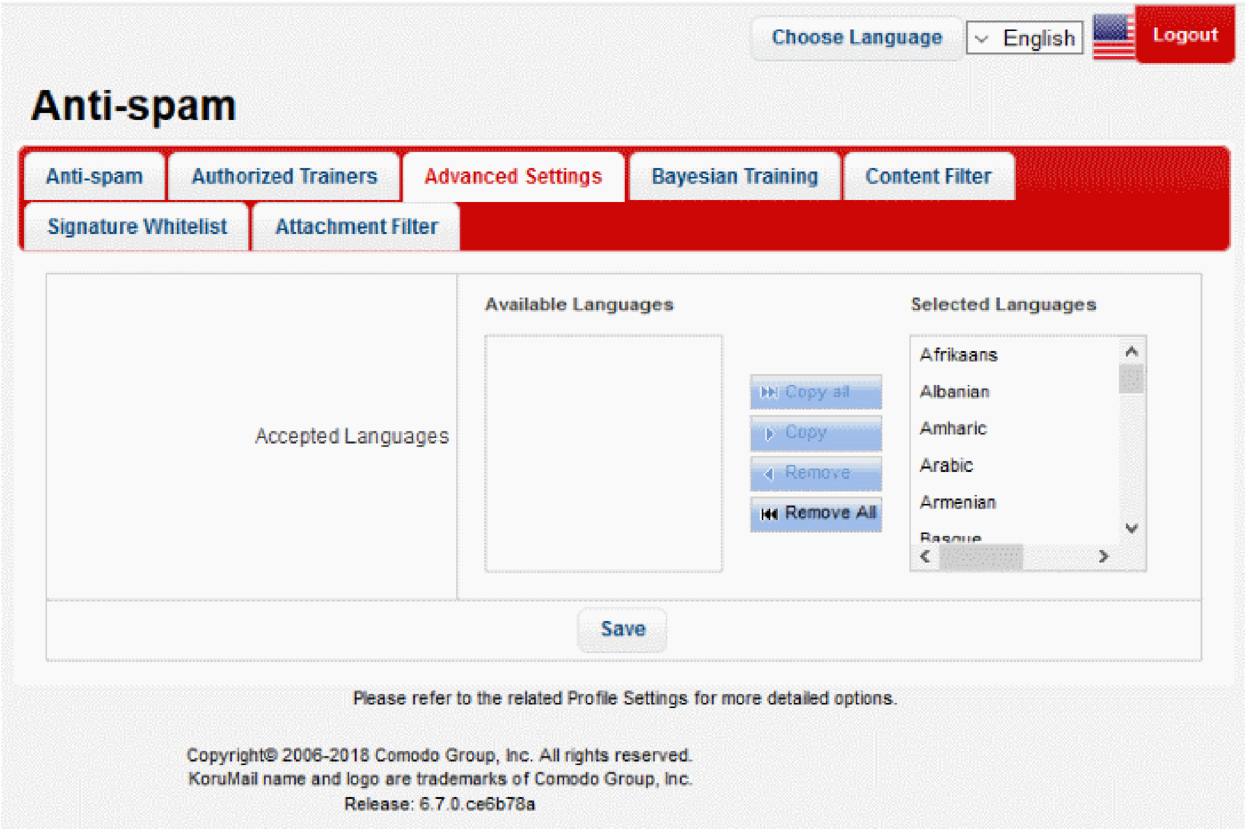
Are you sure you want to delete this entry?

- Click 'OK' to confirm the removal of an authorized trainer.

8.1.3 Advanced Anti-spam Settings

The 'Advanced Settings' screen lets you configure language settings. Languages you select here will be analyzed for spam using the Bayesian spam classifier.

- Click 'Anti-spam' > 'Advanced Settings' to open this interface.



Selected Languages: Afrikaans, Albanian, Amharic, Arabic, Armenian, Basque

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: 6.7.0.ce6b78a

- **Selected Languages:** The languages which will be analyzed by the Bayesian spam engine. A set of languages is provided by default. Use the 'Copy' and 'Remove' buttons to enable or disable languages.

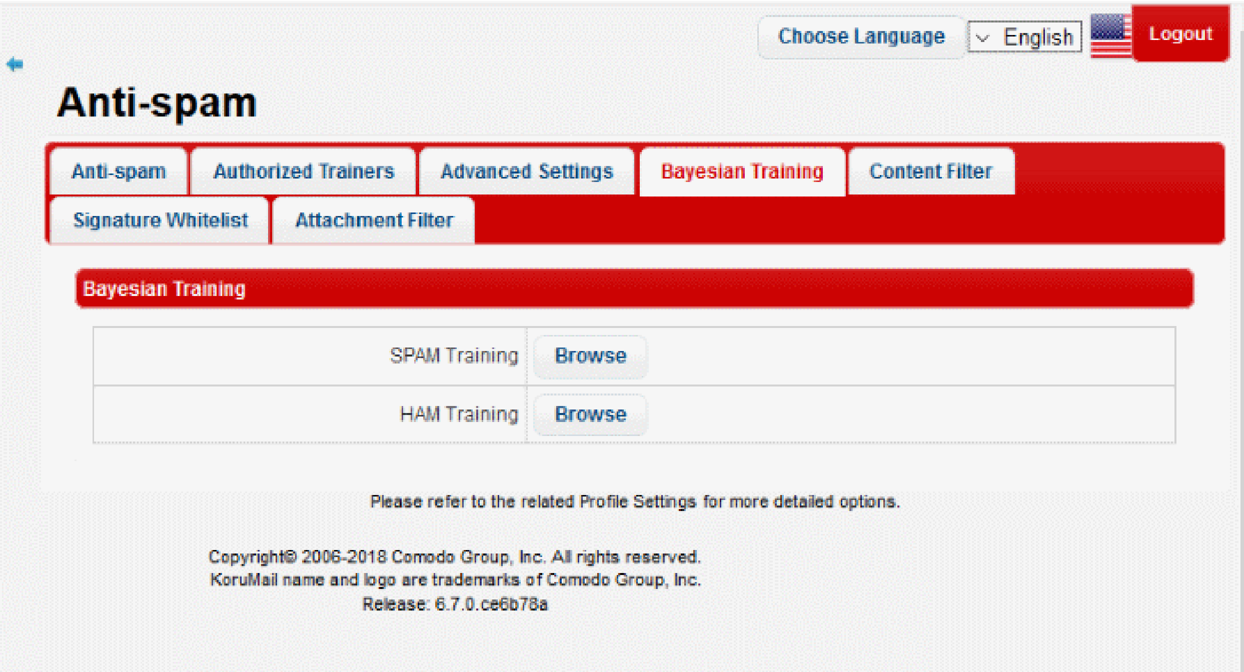
Click 'Save' to apply your changes.

8.1.4 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.

To open the 'Bayesian Training' screen,

- Click the 'Bayesian Training' tab in the 'Anti-spam' interface.



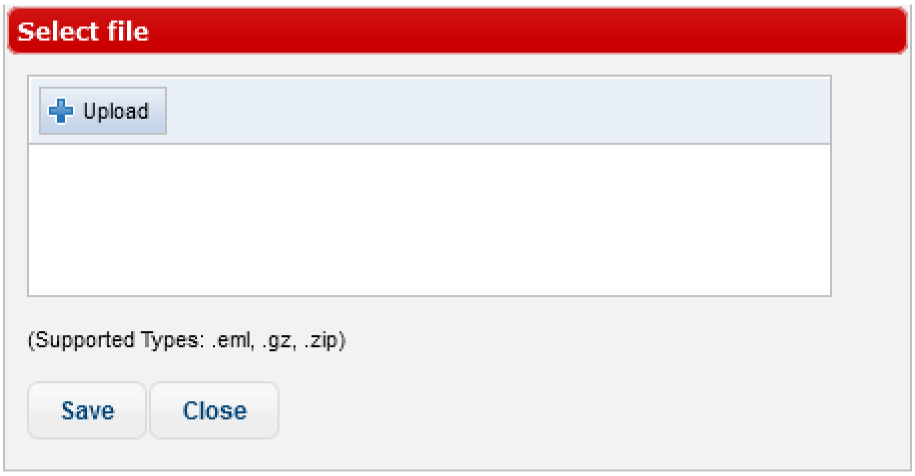
Please refer to the related Profile Settings for more detailed options.

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

- **SPAM Training:** Allows to upload spam content to train the Bayesian spam engine
- **HAM Training:** Allows to upload safe content to train the Bayesian spam engine

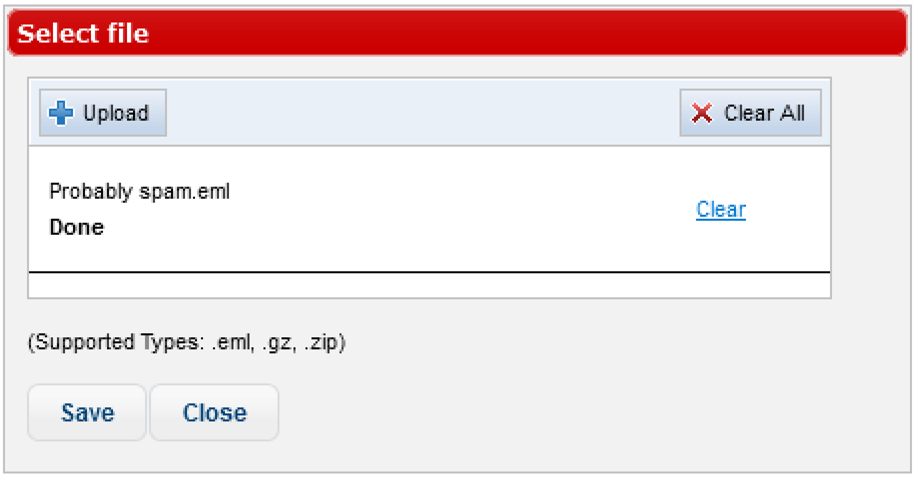
To upload content

- Click the 'Browse' button



(Supported Types: .eml, .gz, .zip)

- Click the 'Upload' button, navigate to the location where the content is saved and click 'Open'. (Note: Only .eml, .gz and .zip file formats are supported)



Probably spam.eml
Done

(Supported Types: .eml, .gz, .zip)

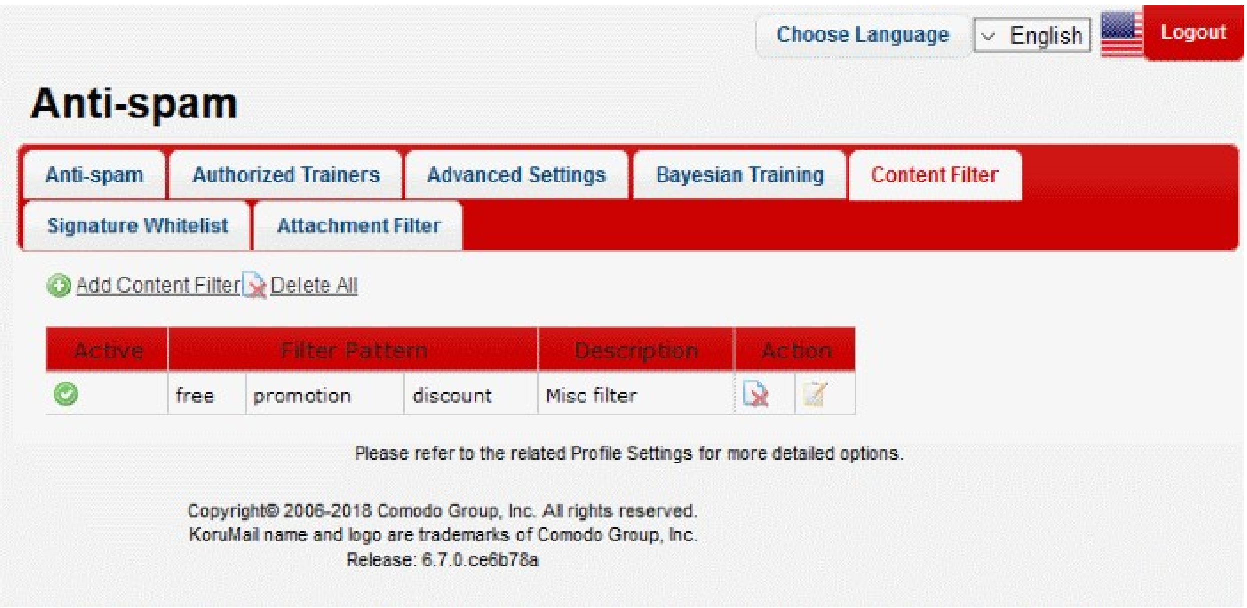
- Repeat the process to add more files
- To remove a file from the list, click the 'Clear' link beside it
- To remove all the files from the list, click the 'Clear All' button at the top
- To upload the files, click the 'Save' button

8.1.5 Content Filter

KoruMail's content filter can detect words or patterns of words in the body of emails then mark those messages as spam.

To open the 'Content Filter' screen,

- Click 'Anti-spam' > 'Content Filter':



Active	Filter Pattern			Description	Action
✓	free	promotion	discount	Misc filter	

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: 6.7.0.ce6b78a

Content Filter - Table of Column Descriptions	
Column Header	**Description**
Active	Whether the content filter is enabled or disabled
Filter Pattern	Displays the details of the filter pattern.
Description	The description for the added 'Content Filter'

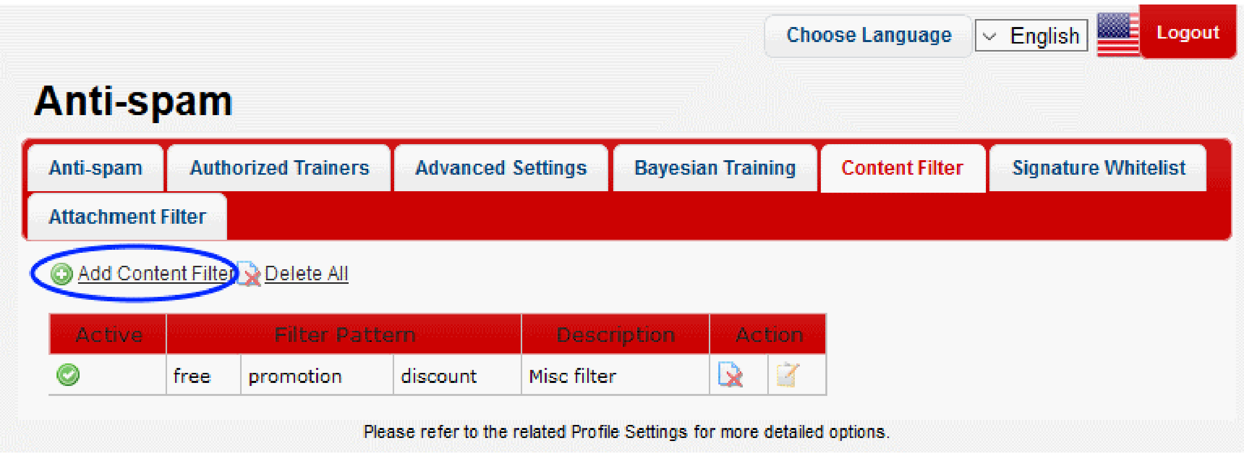
Action	✗	Allows administrators to delete a filter
	✎	Allows administrators to edit a filter

The interface allows administrators to:

- Add a new content filter
- Edit a content filter
- Delete a content filter

To add a new content filter

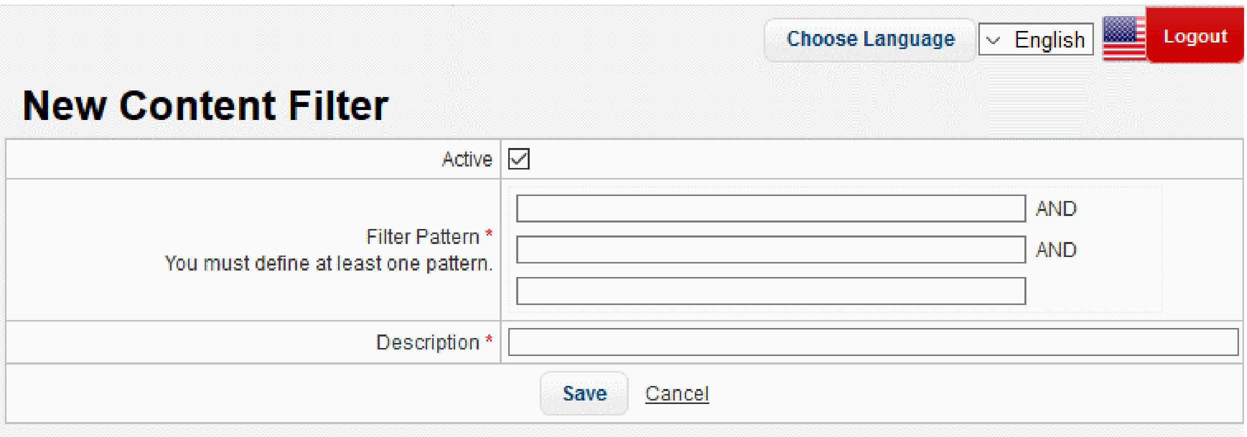
- Click the 'Add Content Filter' link at the top.



Active	Filter Pattern			Description	Action	
✓	free	promotion	discount	Misc filter	✗	✎

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

The 'New Content Filter' screen will be displayed.



Active	☑
Filter Pattern * You must define at least one pattern.	AND AND
Description *	

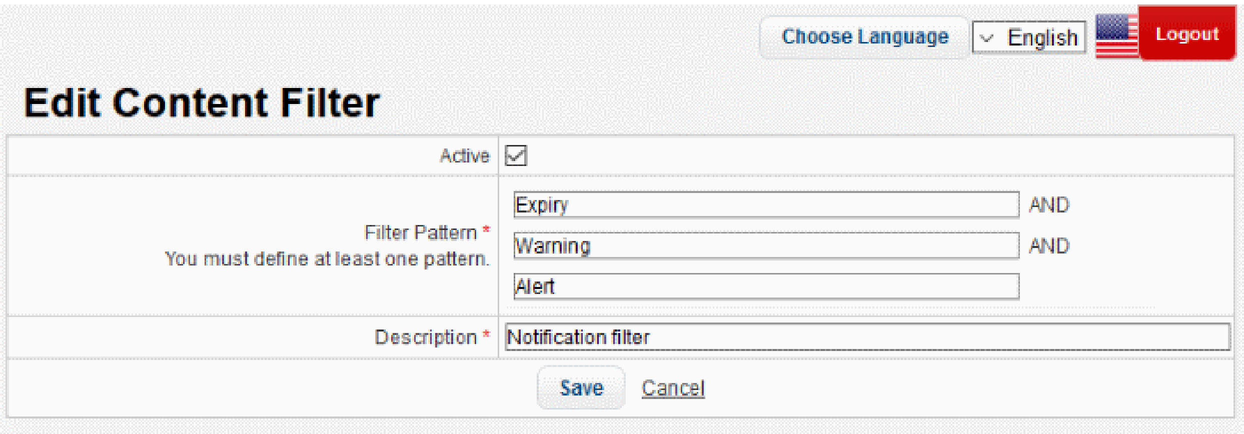
- **Active:** Select the check box to activate the content filter
- **Filter Pattern:** Enter the words or combination of words that should be checked and mark the email as spam.
- **Description:** Enter an appropriate name for the content filter

Click the 'Save' button. The newly added filter will be listed in the screen.

To edit a content filter

- Click the ✎ button beside a filter that you want to edit.

The 'Edit Content Filter' screen will be displayed.



Edit Content Filter

Active ☑

Filter Pattern *
You must define at least one pattern.

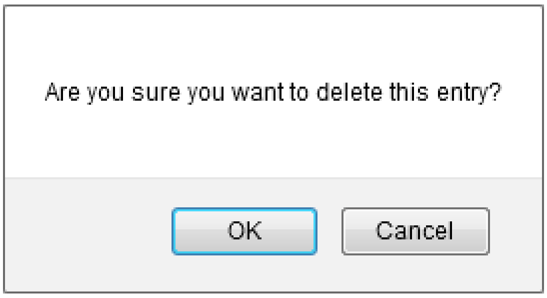
Expiry AND
Warning AND
Alert

Description * Notification filter

- Edit the content filter as required and click the 'Save' button

To delete a content filter

- Click the button beside a filter that you want to remove

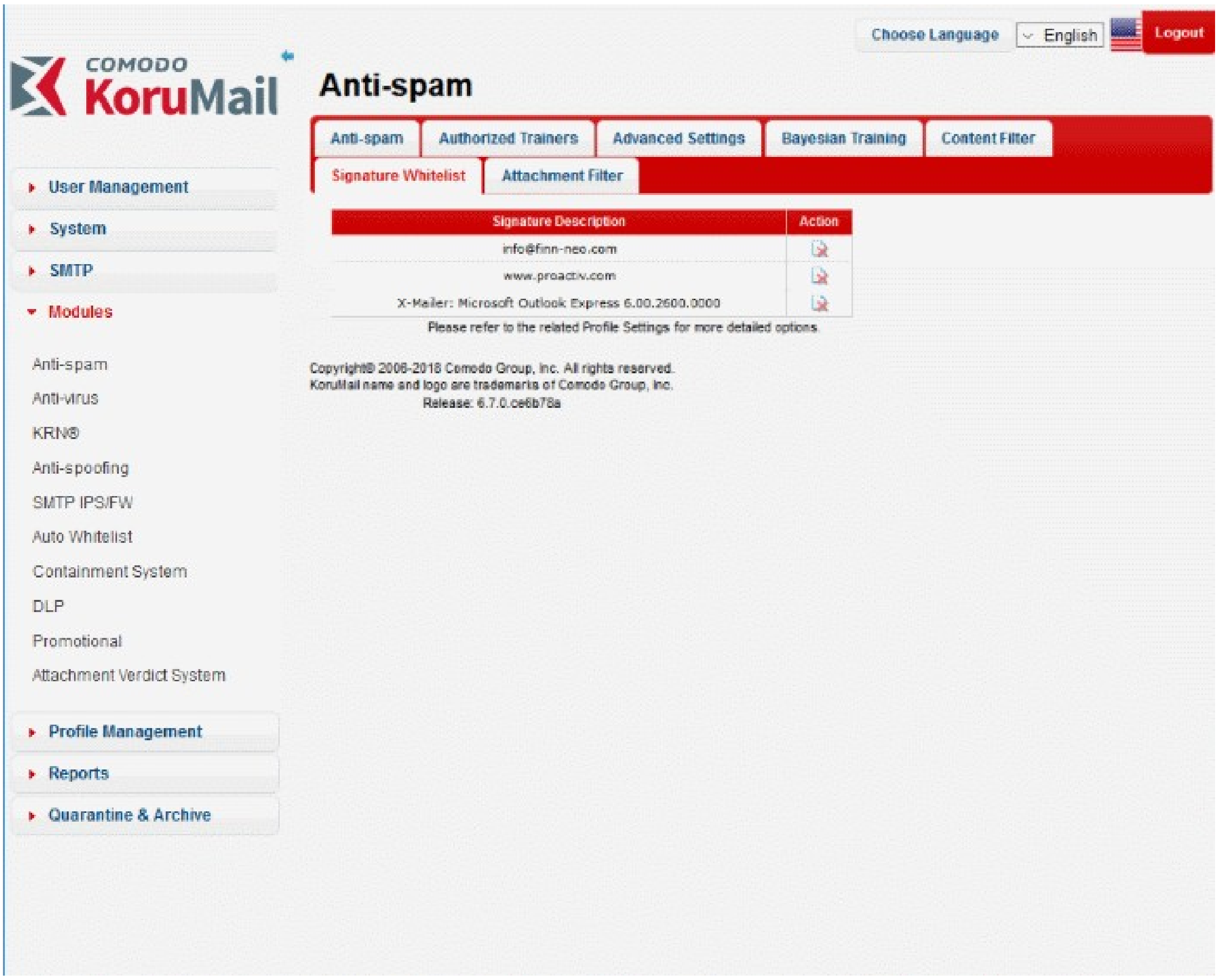


Are you sure you want to delete this entry?

- Click 'OK' to confirm the deletion of the filter

8.1.6 Signature Whitelist

This is a list of digital signatures that came attached to white-listed emails. Administrators can manually whitelist mails from the 'Mail logs' interface. You can white-list email addresses or entire domains.



Anti-spam

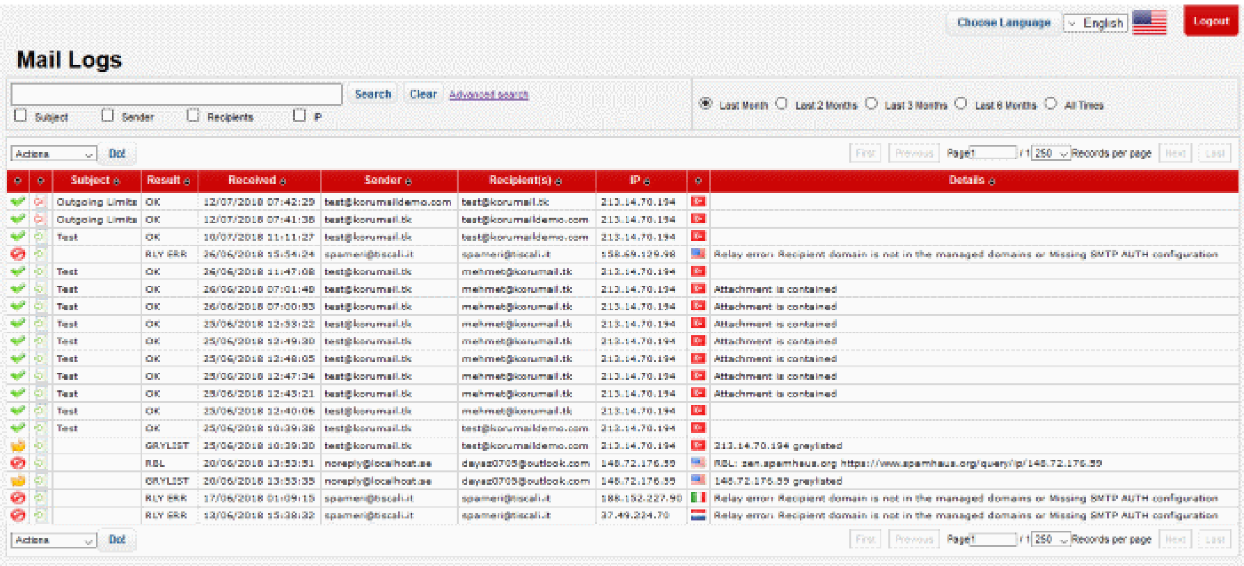
Signature Description	Action
info@finn-neo.com	
www.proactiv.com	
X-Mailer: Microsoft Outlook Express 6.00.2600.0000	

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: 6.7.0.ce6b78a

To whitelist emails in 'Mail Logs'

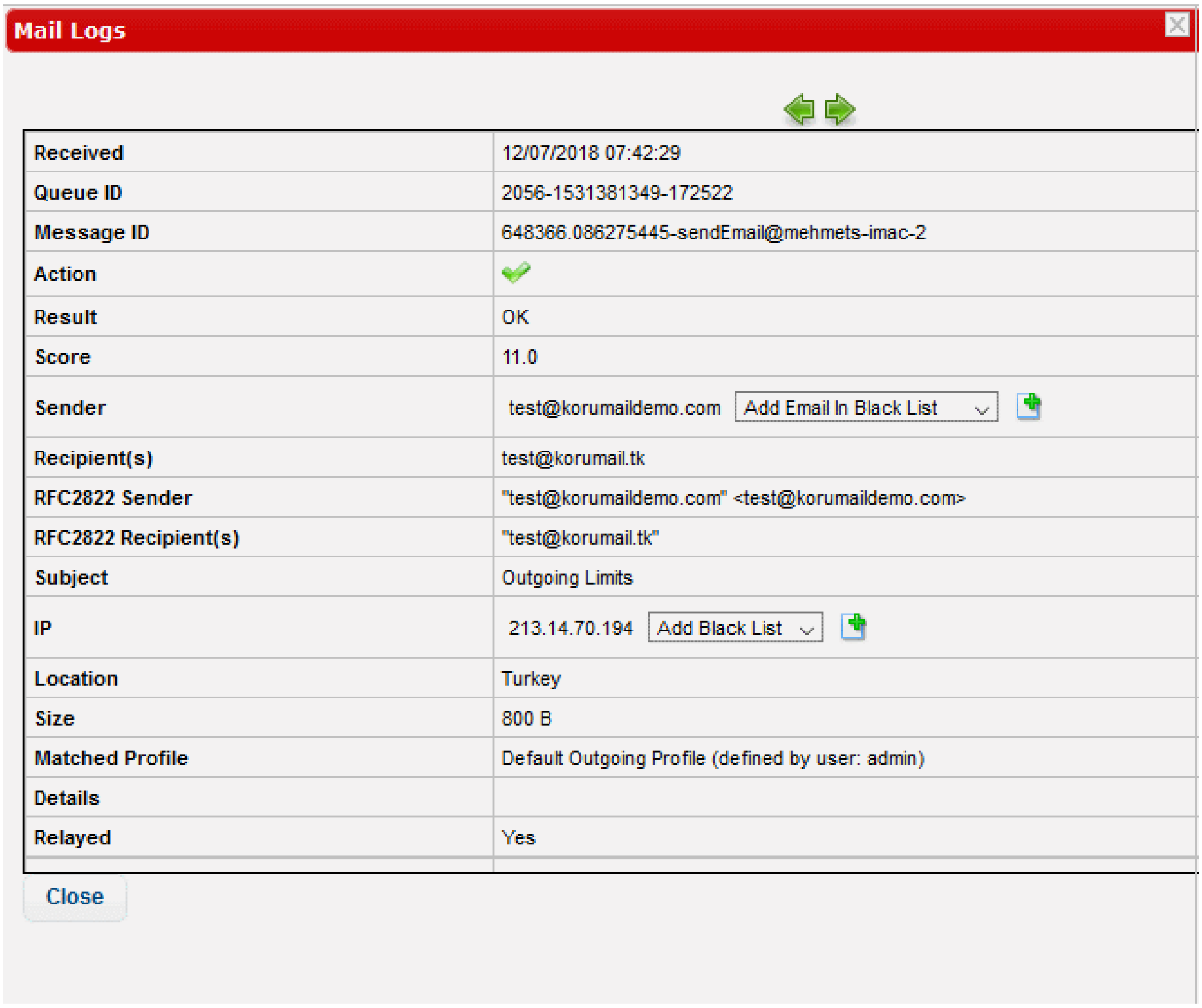
- Click 'Mail Logs' from reports menu.



Mail Logs

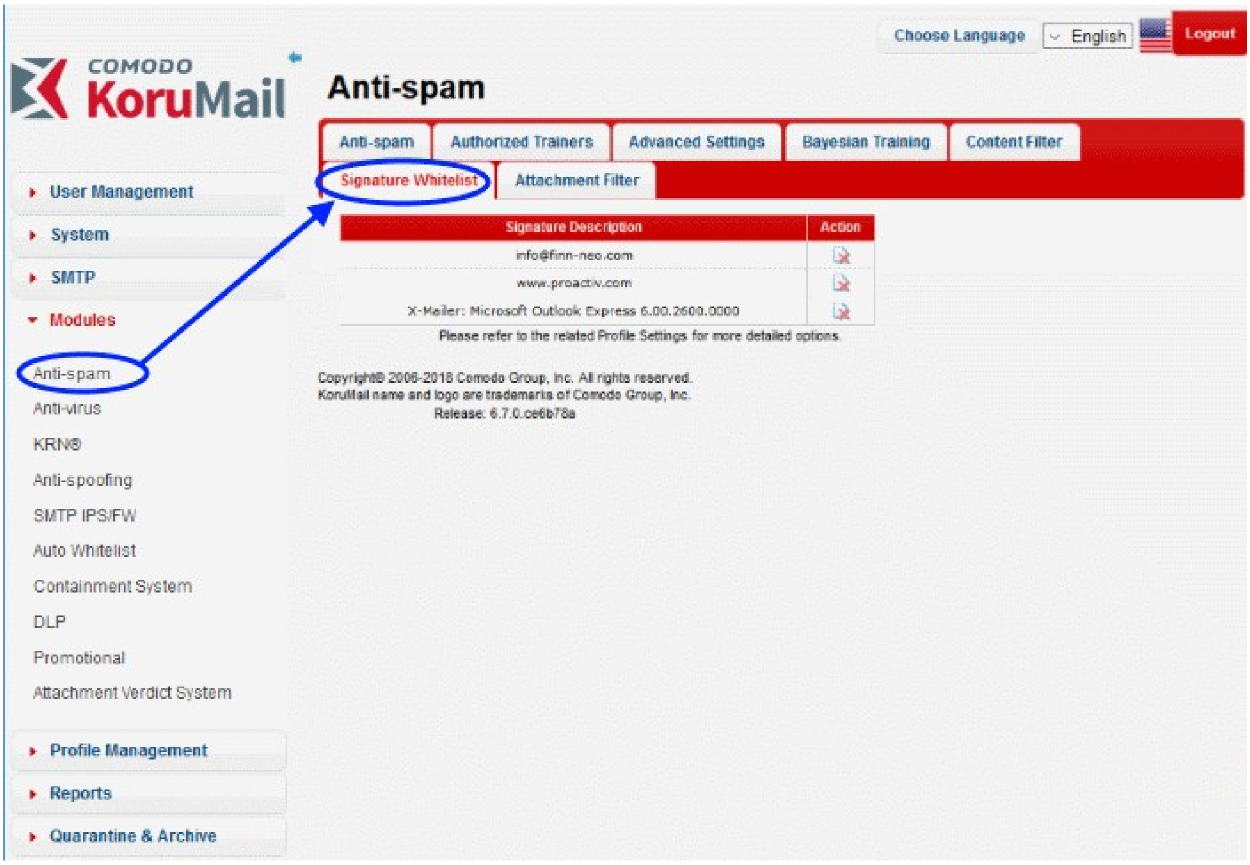
		Subject	Result	Received	Sender	Recipient(s)	IP		Details
✓		Outgoing Limits	OK	12/07/2018 07:42:29	test@korumaildemo.com	test@korumail.tk	213.14.70.194		
✓		Outgoing Limits	OK	12/07/2018 07:41:38	test@korumail.tk	test@korumaildemo.com	213.14.70.194		
✓		Test	OK	10/07/2018 11:11:27	test@korumail.tk	test@korumaildemo.com	213.14.70.194		
⊘			RLY ERR	26/06/2018 15:54:24	spamer@tiscali.it	spamer@tiscali.it	158.69.129.98		Relay error: Recipient domain is not in the managed domains or Missing SMTP AUTH configuration
✓		Test	OK	26/06/2018 11:47:08	test@korumail.tk	mehmet@korumail.tk	213.14.70.194		
✓		Test	OK	26/06/2018 07:01:40	test@korumail.tk	mehmet@korumail.tk	213.14.70.194		Attachment is contained
✓		Test	OK	26/06/2018 07:00:53	test@korumail.tk	mehmet@korumail.tk	213.14.70.194		Attachment is contained
✓		Test	OK	25/06/2018 12:53:22	test@korumail.tk	mehmet@korumail.tk	213.14.70.194		Attachment is contained
✓		Test	OK	25/06/2018 12:49:30	test@korumail.tk	mehmet@korumail.tk	213.14.70.194		Attachment is contained
✓		Test	OK	25/06/2018 12:48:05	test@korumail.tk	mehmet@korumail.tk	213.14.70.194		Attachment is contained
✓		Test	OK	25/06/2018 12:47:34	test@korumail.tk	mehmet@korumail.tk	213.14.70.194		Attachment is contained
✓		Test	OK	25/06/2018 12:43:21	test@korumail.tk	mehmet@korumail.tk	213.14.70.194		Attachment is contained
✓		Test	OK	25/06/2018 12:40:06	test@korumail.tk	mehmet@korumail.tk	213.14.70.194		
✓		Test	OK	25/06/2018 10:39:38	test@korumail.tk	test@korumaildemo.com	213.14.70.194		
			GRYLIST	25/06/2018 10:39:30	test@korumail.tk	test@korumaildemo.com	213.14.70.194		213.14.70.194 greylisted
⊘			RBL	20/06/2018 13:53:51	noreply@localhost.ae	dayaz0705@outlook.com	148.72.176.59		RBL: zen.spamhaus.org https://www.spamhaus.org/query/ip/148.72.176.59
			GRYLIST	20/06/2018 13:53:35	noreply@localhost.ae	dayaz0705@outlook.com	148.72.176.59		148.72.176.59 greylisted
⊘			RLY ERR	17/06/2018 01:09:15	spamer@tiscali.it	spamer@tiscali.it	188.152.227.90		Relay error: Recipient domain is not in the managed domains or Missing SMTP AUTH configuration
⊘			RLY ERR	13/06/2018 15:38:32	spamer@tiscali.it	spamer@tiscali.it	37.49.224.70		Relay error: Recipient domain is not in the managed domains or Missing SMTP AUTH configuration

- Click the 'Advanced search' link.
- Select 'Result' from the first drop down.
- Select 'EQUALS' from the second drop down and then choose 'CERTAINLY SPAM'.



Received	12/07/2018 07:42:29
Queue ID	2056-1531381349-172522
Message ID	648366.086275445-sendEmail@mehmets-imac-2
Action	✓
Result	OK
Score	11.0
Sender	test@korumaildemo.com Add Email In Black List
Recipient(s)	test@korumail.tk
RFC2822 Sender	"test@korumaildemo.com" <test@korumaildemo.com>
RFC2822 Recipient(s)	"test@korumail.tk"
Subject	Outgoing Limits
IP	213.14.70.194 Add Black List
Location	Turkey
Size	800 B
Matched Profile	Default Outgoing Profile (defined by user: admin)
Details	
Relayed	Yes

- Select 'Add email to Whitelist' in sender field and 'Add Whitelist' in IP field in the dialog and then choose the email that you need to whitelist and click the 'Add White Signature Lists' link.



Signature Description	Action
info@finn-neo.com	
www.proactiv.com	
X-Mailer: Microsoft Outlook Express 6.00.2600.0000	

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

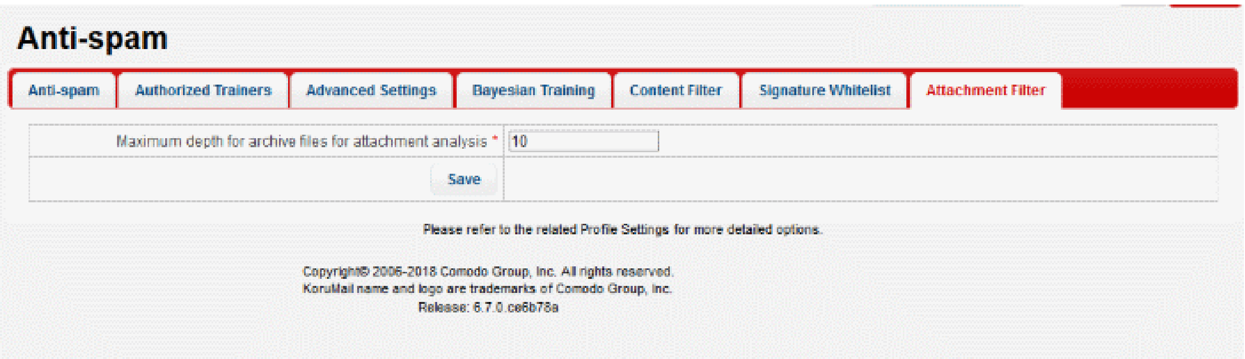
Copyright© 2006-2018 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 6.7.0.ce6b78a

The email will automatically populate in the 'Signature Whitelist' tab in Anti-spam' module.

8.1.7 Attachment Filter

This area lets you 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. However, if the 2nd zip contained another zip inside it, then KoruMail will not scan it.

- Click 'Modules' > 'Antispam' > 'Attachment Filter' tab.



Maximum depth for archive files for attachment analysis * 10

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: 6.7.0.ce6b78a

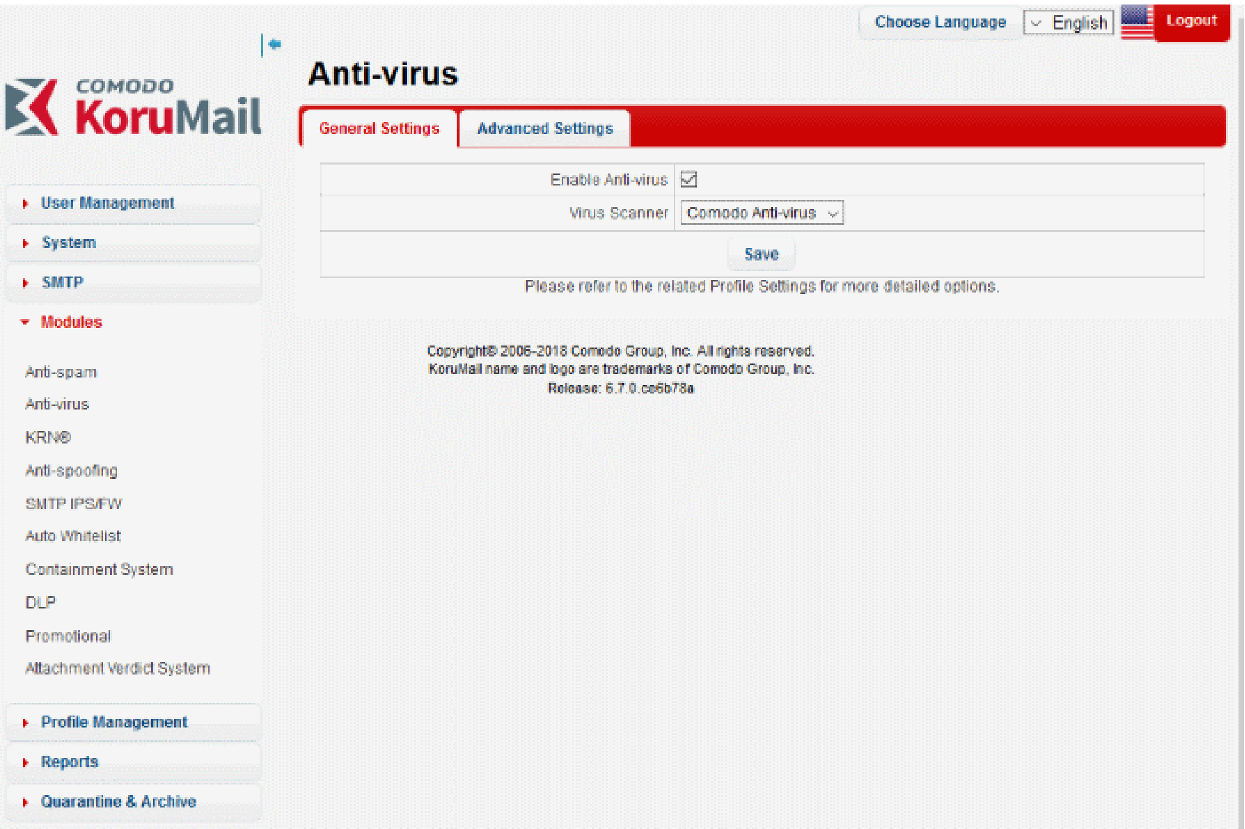
- **Maximum depth for archive files for attachment analysis:** Max. archive levels that will be analyzed. Enter the maximum number of nested archives which should be opened and examined for data-leak infringements. If an archive contains more sub-archives than this threshold then the entire attachment will be blocked.
- Click 'Save' to apply your choice.

8.2 Anti-Virus

- KoruMail is capable of virus scanning all emails that pass through its engine.
- KuruMail includes built-in Comodo AntiVirus program and you have the option to select Comodo's AV program.
- The anti-virus module must be enabled in order to activate the anti-virus parameters specified in profile settings. See 'Profile Management' for more details about profile settings.

To open the 'Anti-virus' interface

- Click the 'Modules' tab on the left, then click 'Anti-virus'.



Enable Anti-virus ☑

Virus Scanner: Comodo Anti-virus

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

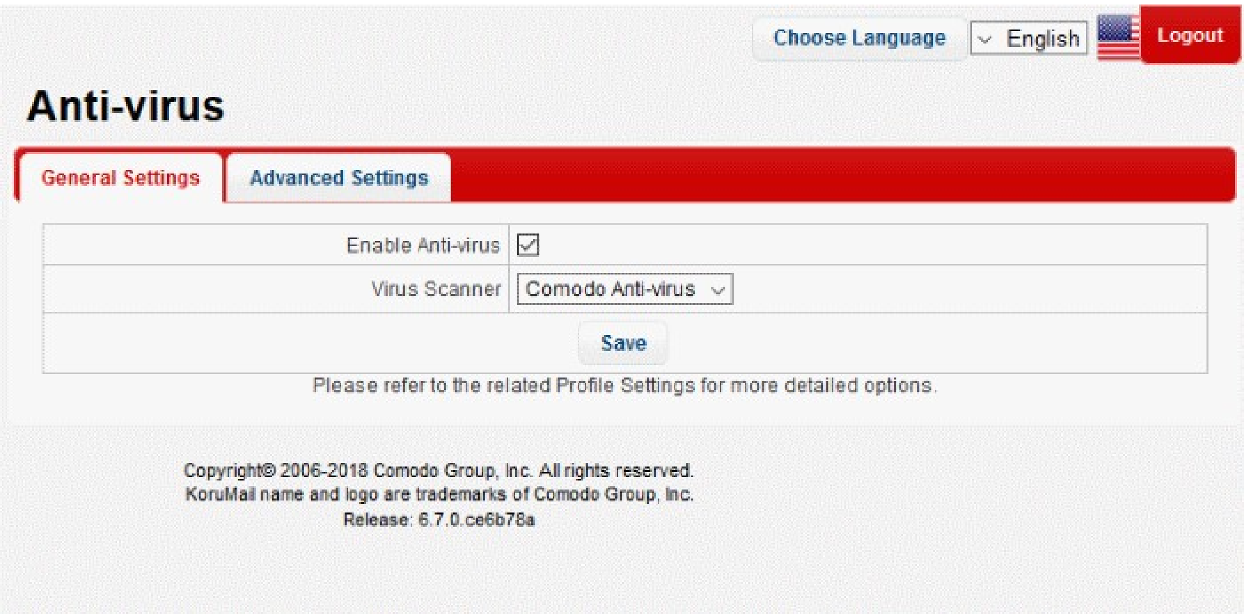
Copyright© 2006-2018 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 6.7.0.ce6b78a

See the following sections for more details:

- **Anti-Virus General Settings**
- **Advanced Anti-Virus Settings**

8.2.1 Anti-Virus General Settings

- The antivirus settings screen lets you enable/disable the AV module and select which AV engine you wish to use.
- The antivirus module must be enabled to activate the AV parameters in profile settings. See '**Profile Management**' for more details about profile settings.
- Click 'Antivirus' > 'General Settings' to open this interface.



Enable Anti-virus ☑

Virus Scanner: Comodo Anti-virus

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: 6.7.0.ce6b78a

Anti-virus General Settings - Table of Parameters	
Parameter	**Description**
Enable Anti-virus	• Select this to active the anti-virus scanning engine. • The anti-virus parameters specified in the profile settings will be activated only if this setting is enabled here. • See '**Profile Management**' for more details about profile settings.
Virus Scanner	Select the AV program from the drop-down that should be used for scanning the emails. The AV programs available for selection is Comodo AV.

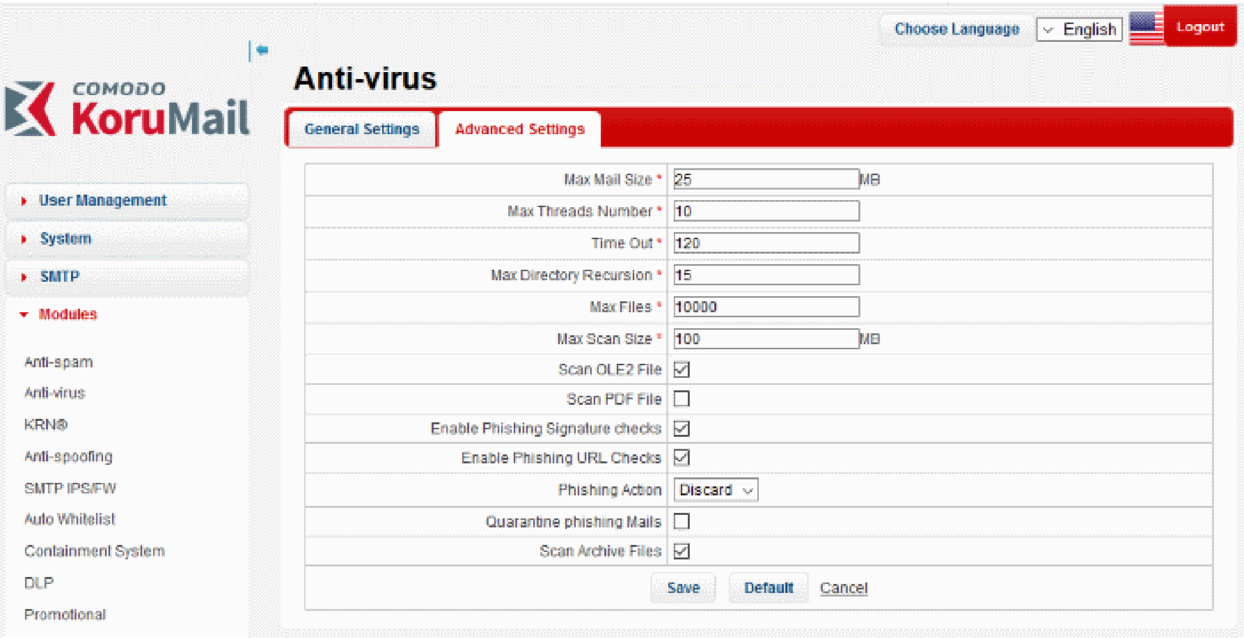
- Click 'Save' to apply your changes.

8.2.2 Advanced Anti-Virus Settings

- The 'Advanced Settings' screen allows administrators to set the maximum size of email that should be scanned, the number of mail threads, the maximum number of files and more.
- Please note that if the maximum size is surpassed then the antivirus filter for the particular email will not be applied.

To open the 'Advanced Settings' screen

- Click the 'Advanced Settings' tab in the 'Anti-virus' interface.



Max Mail Size * 25 MB

Max Threads Number * 10

Time Out * 120

Max Directory Recursion * 15

Max Files * 10000

Max Scan Size * 100 MB

Scan OLE2 File ☑

Scan PDF File □

Enable Phishing Signature checks ☑

Enable Phishing URL Checks ☑

Phishing Action Discard

Quarantine phishing Mails □

Scan Archive Files ☑

Anti-virus Advanced Settings - Table of Parameters	
Parameter	**Description**
Max Mail Size	The maximum size of email that should be scanned.
Max Threads Number	The maximum number of email threads in a email that should be scanned.
Time Out	The AV scanning time in seconds for an email.
Max Directory Recursion	Maximum number of sub-directories or nested archives that will be scanned. If an archive contains more than this threshold then the attachment will be blocked.
Max Files	Maximum number of files that can be scanned within an archive or email.
Max Scan Size	Maximum amount of data (specified value set) scanned for each input file. Archived files are scanned till the Antivirus scanner reaches the set value.
Scan OLE2 File	If enabled, AV scan is run for OLE2 file formats.
Scan PDF File	If enabled, AV scan is run for PDF file formats.
Enable Phishing Signature checks	If enabled, AV scanner checks for phishing emails
Enable Phishing URL checks	If enabled, AV scanner checks for emails that originated from phishing URLs
Scan Archive Files	If enabled, archived mails will also be scanned. The type of mails that should be archived and its related settings are configured in profile settings. See '**Profile Management**' for more details about profile settings.

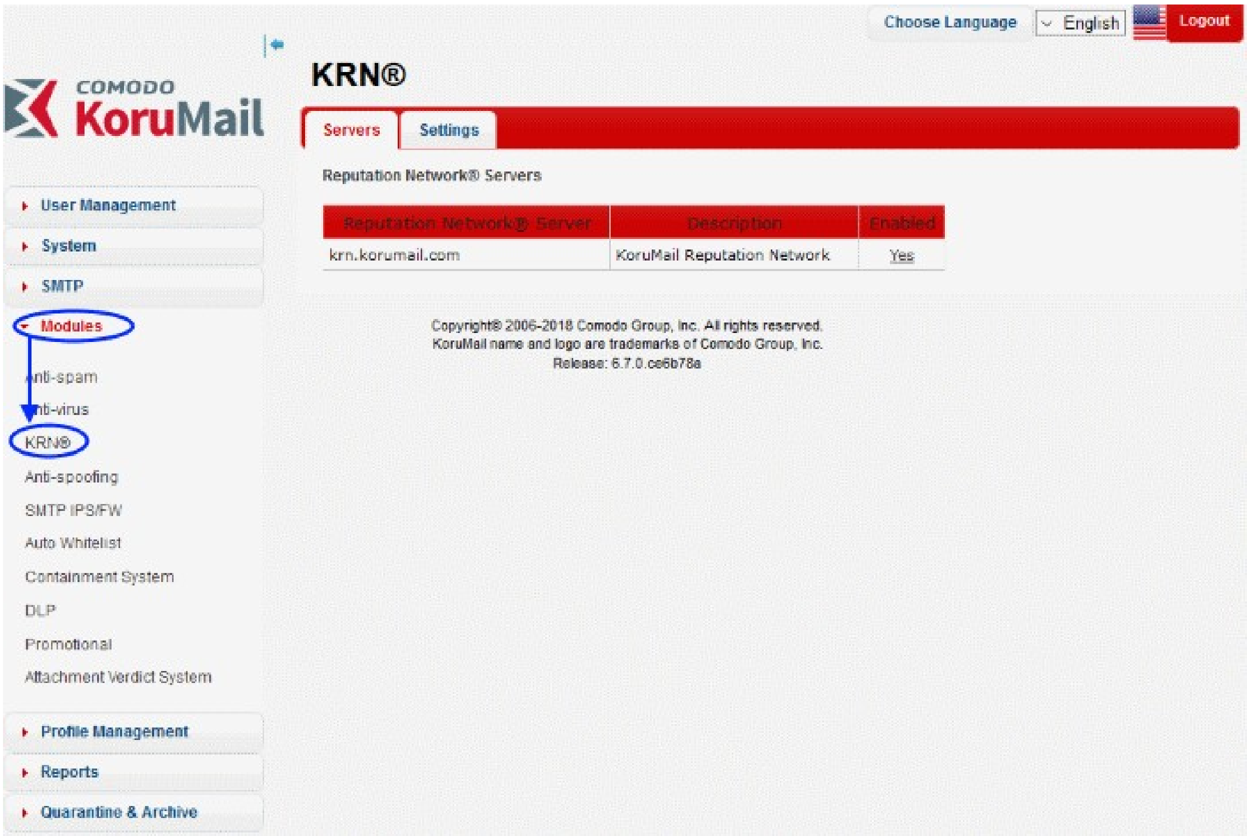
- Click 'Save' to apply your changes.
- To restore the default 'Anti-viurs Advanced Settings' value, click the 'Default' button.

8.3 KoruMail Reputation Network (KRN)

- KoruMail Reputation Network is an IP reputation scoring system developed by Comodo.
- It not only includes traditional features such as real-time IP blacklists (RBL) but also has ‘whitelist’ and ‘greylisting ignore’ features.
- The whitelisting feature means emails that come from trusted sources will be permitted, which helps to reduce false-positive rates.

To open the 'KRN®' interface

- Click the 'Modules' tab on the left, then click 'KRN®'



Reputation Network® Servers

Reputation Network® Server	Description	Enabled
krn.korumail.com	KoruMail Reputation Network	Yes

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

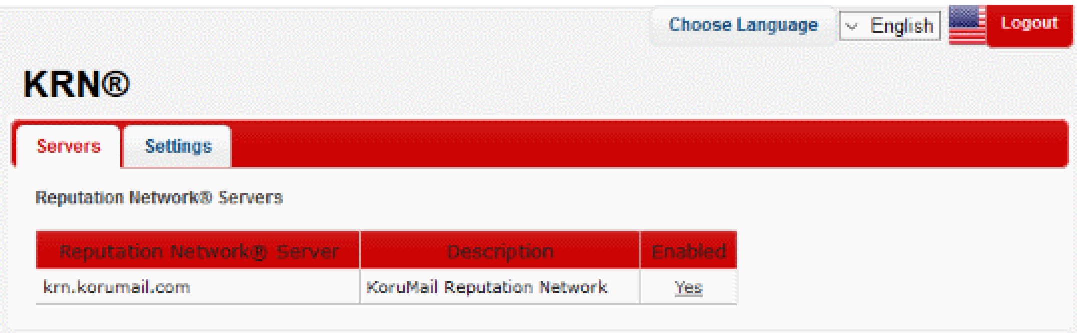
The interfce allows administrators to:

- Enable / disable a KRN server
- Configure KRN settings

To enable / disable a KRN server

A newly added KRN server will be in enabled status by default.

- To switch a KRN server between enabled and disabled statuses, click the 'Yes' or 'No' link under the 'Enabled' column.



Reputation Network® Servers

Reputation Network® Server	Description	Enabled
krn.korumail.com	KoruMail Reputation Network	Yes

KRN Settings

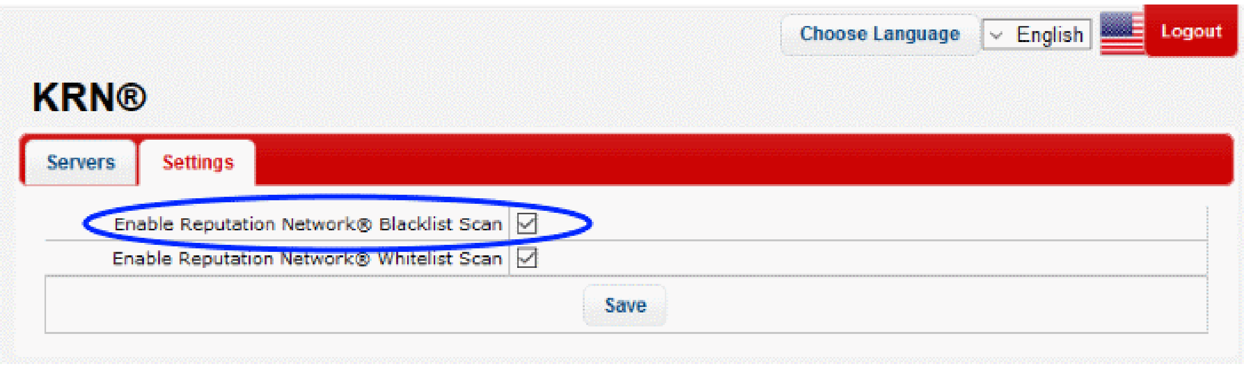
- The KRN settings interface allows administrators to enable / disable KRN Blacklist and Whitelist scan.
- The KRN Blacklist and Whitelist scan in the KRN module must be enabled in order to activate the KRN scan parameters specified in profile settings.
- See '**Profile Management**' for more details about profile settings.

The 'Settings' tab in KRN module allows administrators to:

- **Enable / disable KRN blacklist scan**
- **Enable / disable KRN whitelist scan**

To enable / disable KRN blacklist scan

- Click the 'Settings' tab in the KRN® ' interface

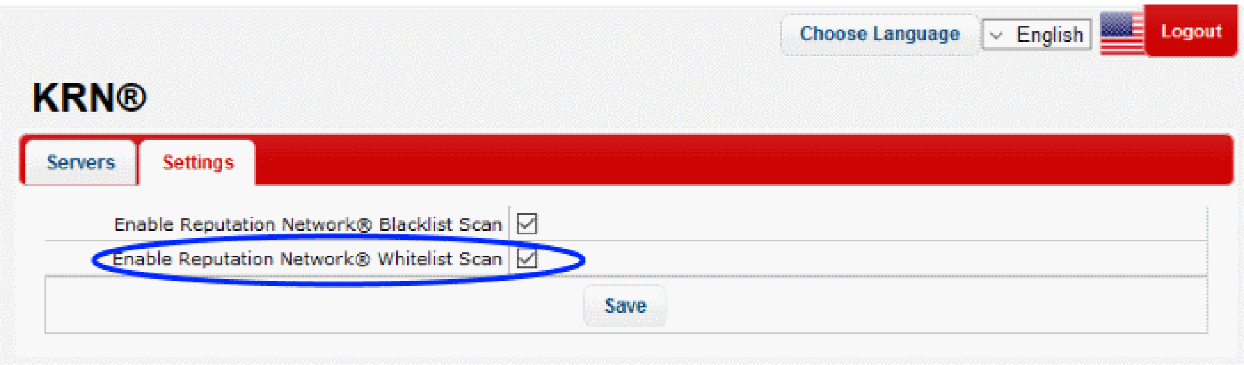


Enable Reputation Network® Blacklist Scan ☑
Enable Reputation Network® Whitelist Scan ☑

- Select / deselect the 'Enable KoruMail Reputation Network® Blacklist Scan' check box to activate or deactivate the KRN blacklist scan
- Click 'Save' to apply your changes.

To enable / disable KRM whitelist scan

- Click the 'Settings' tab in the KRN® ' interface



Enable Reputation Network® Blacklist Scan ☑
Enable Reputation Network® Whitelist Scan ☑

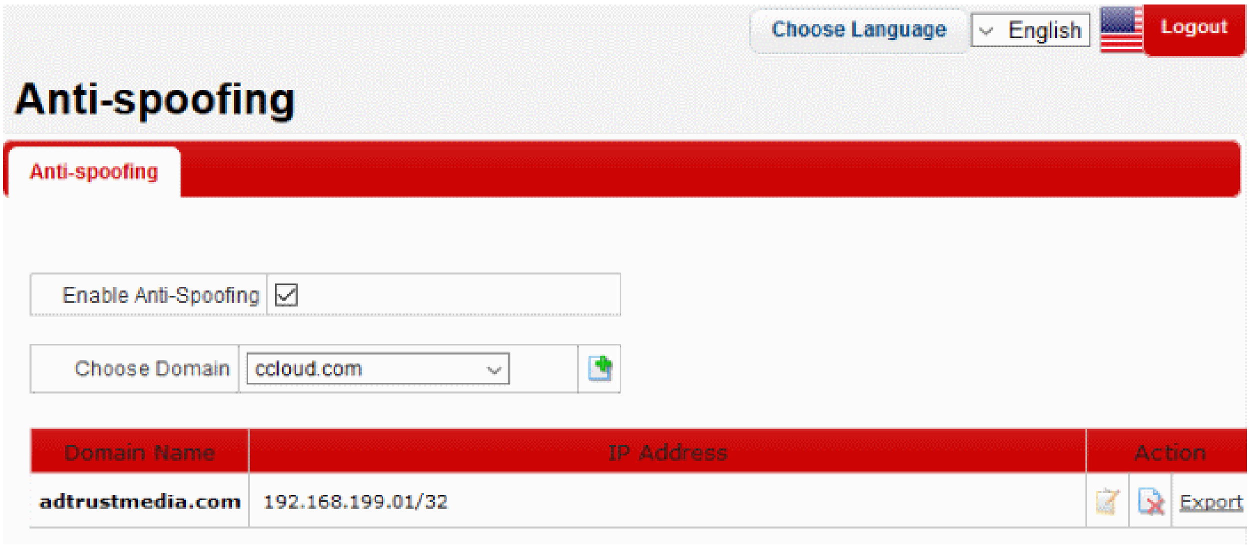
- Select / deselect the 'Enable KoruMail Reputation Network® Whitelist Scan' check box to activate or deactivate the KRN whitelist scan
- Click 'Save' to apply your changes.

8.4 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.
- Email spoofing is possible because SMTP (Simple Mail Transfer Protocol) being the main protocol used in sending emails, does not include an authentication mechanism.
- The 'Anti-Spoofing' feature in KoruMail prevents spammers from sending messages with falsified 'From' addresses from your protected domains.
  - It uses SPF records, which is a type of DNS record that identifies which servers are permitted to send emails on behalf of the protected domains.
- KoruMail allows you to add a range of IP addresses for a protected domain, which an MTA (Mail Transfer Agent) can look up to confirm whether an email is being sent from an authorized server.

To open the 'Anti-spoofing' interface

- Click the 'Modules' tab on the left, then click 'Anti-spoofing'.



Enable Anti-Spoofing ☑

Choose Domain ccloud.com

Domain Name	IP Address	Action
adtrustmedia.com	192.168.199.01/32	✎ ☒ Export

- Select the 'Enable Anti-Spoofing' check box to add IP addresses for your domains.

Anti-Spoofing - Table of Column Descriptions

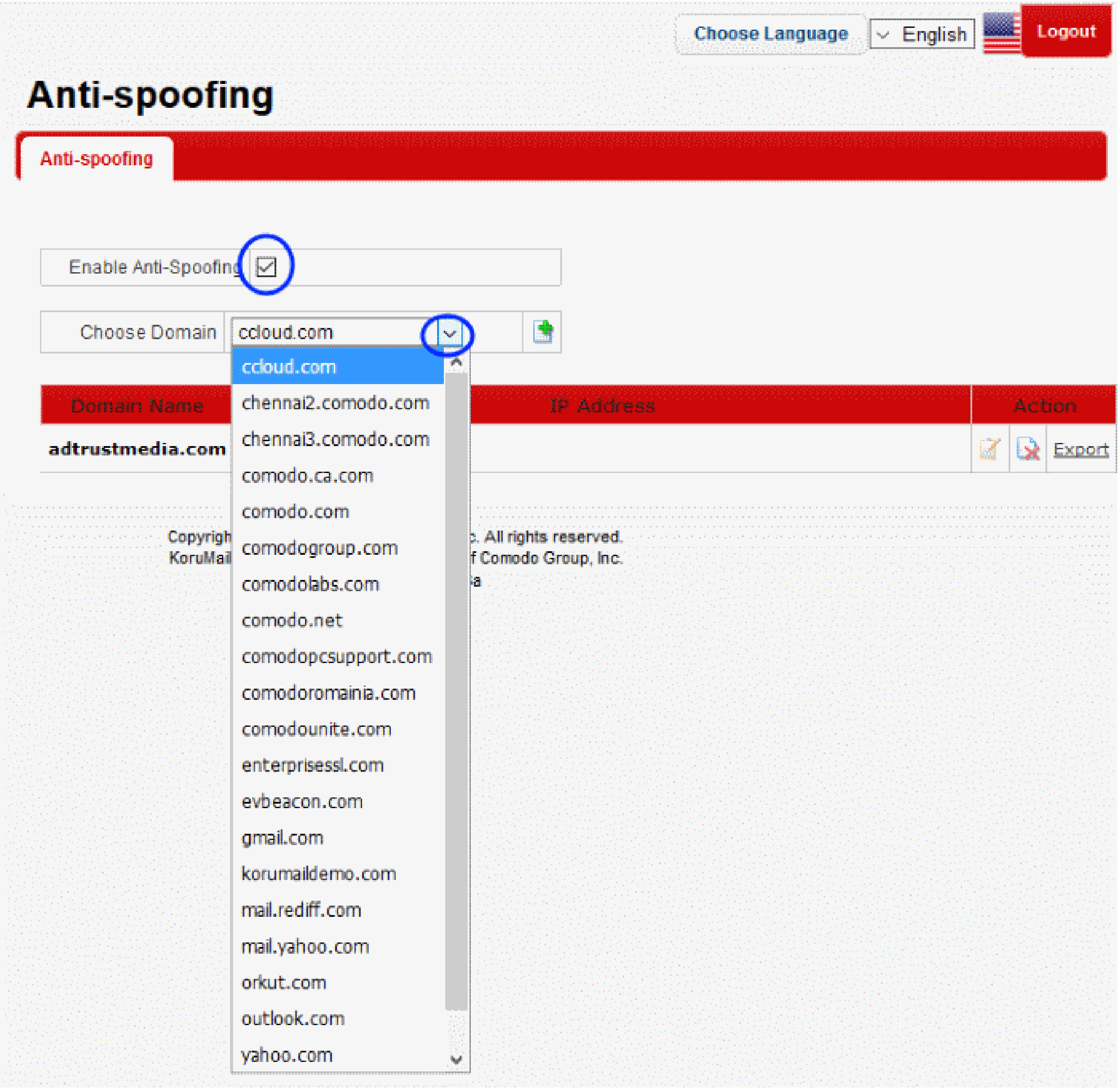
Column Header	Description	
Domain Name	Displays the name of the protected domain	
IP Address	Displays IP range added for the domain	
Action	☒	Allows administrators to delete a domain name
	✎	Allows administrators to edit the 'IP address' for a domain
	Export	Allows to export the IP address for a domain

The interface allows administrators to:

- **Add IP range for a domain**
- **Edit IP range for a domain**
- **Delete a domain name from the list**
- **Export the list of IP addresses**

To add an IP range for a domain

- Select the 'Enable Anti-Spoofing' check box
- Select the domain for which you want to add the IP range



Anti-spoofing

Enable Anti-Spoofing ☑

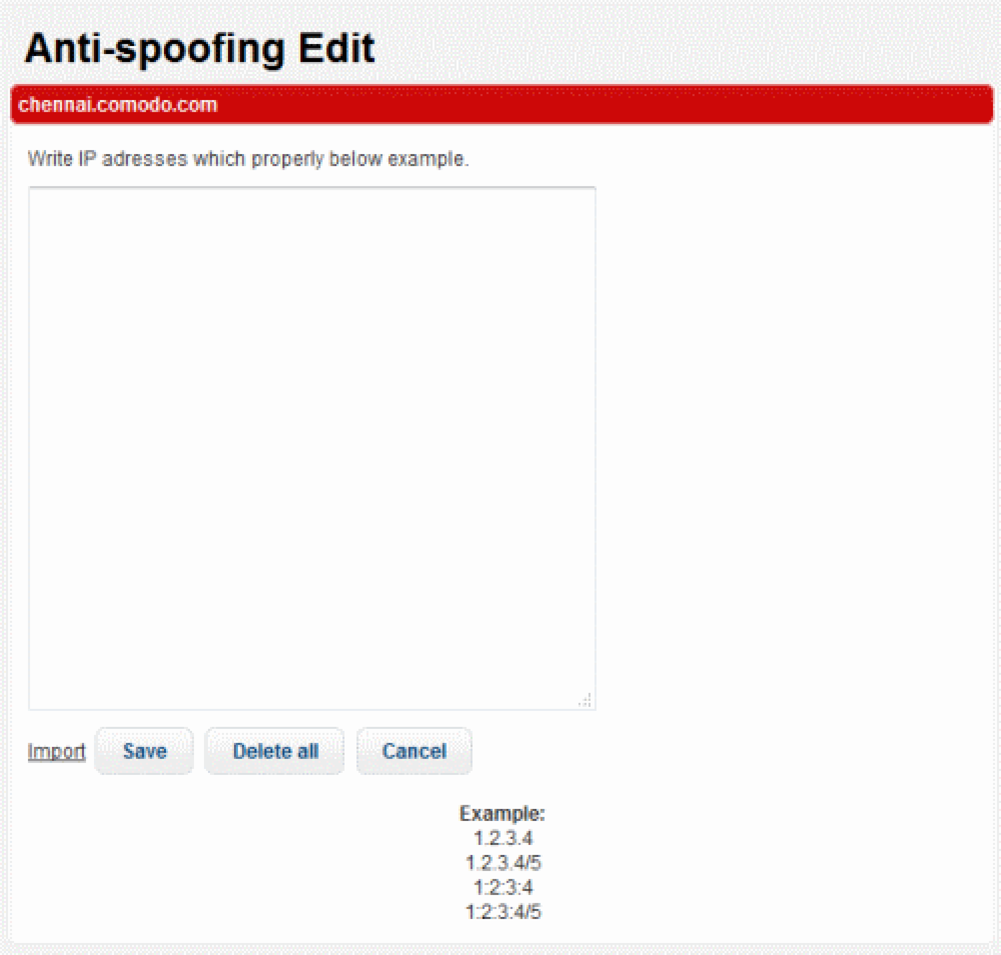
Choose Domain: ccloud.com

Domain Name	IP Address	Action
adtrustmedia.com		Export

Copyrigh... c. All rights reserved.
KoruMail ... f Comodo Group, Inc.
...a

- Click the ✚ button

The 'Anti-spoofing Edit' screen will be displayed.



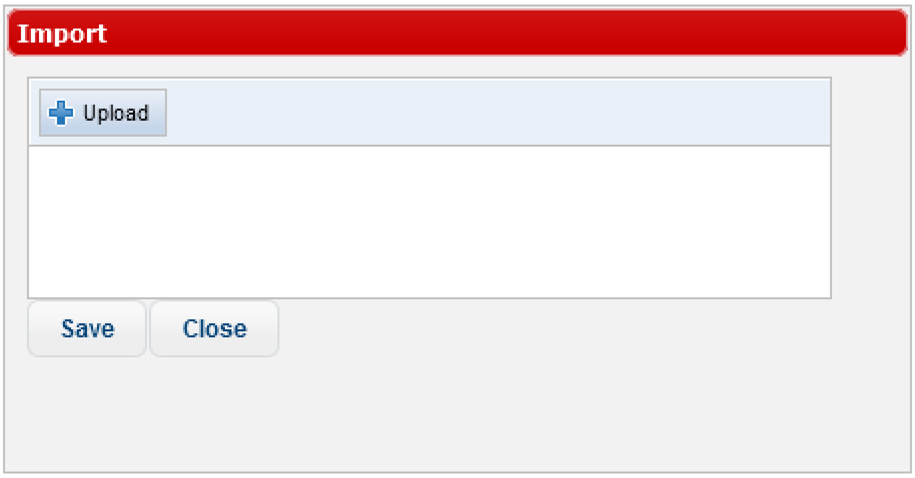
Anti-spoofing Edit

chennai.comodo.com

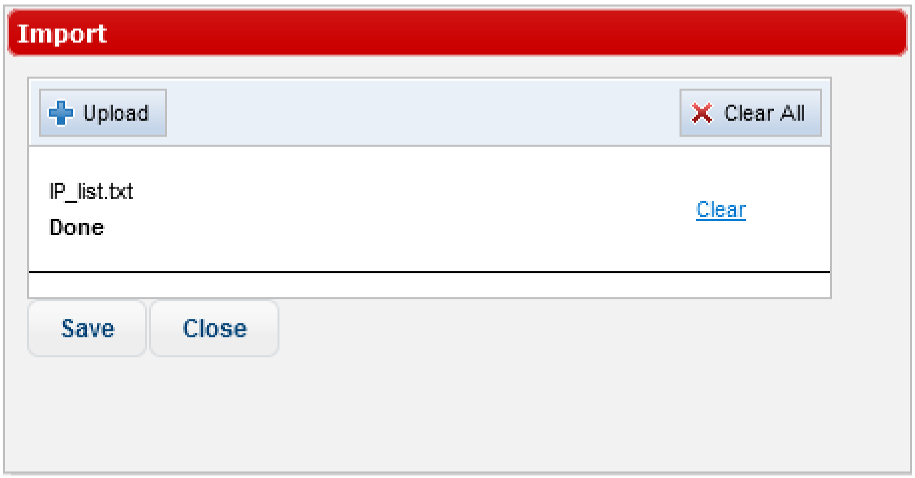
Write IP adresses which properly below example.

Example:
1.2.3.4
1.2.3.4/5
1:2:3:4
1:2:3:4/5

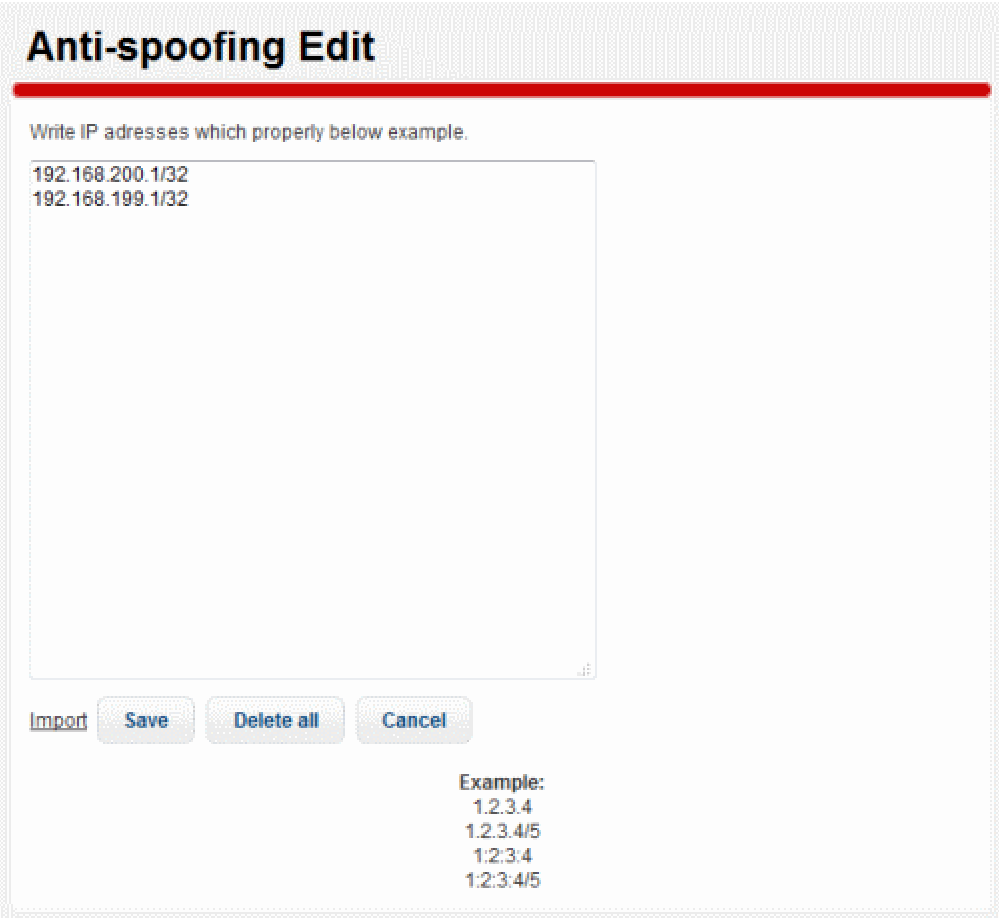
- To add the IP range manually, enter the address each per line in the field and click the 'Save' button.
- To import from a saved file, click the 'Import' link



- Click the 'Upload' button, navigate to the location where the file is saved and click 'Open'



- Repeat the process to add more files to the list.
- To remove a file from the list, click 'Clear' beside it.
- To remove all the files, click 'Clear All' at the top.
- Click 'Save'.



192.168.200.1/32
192.168.199.1/32

- Click 'Delete all' to remove all the addresses and click 'OK' in the confirmation screen.
- Click 'Save' to add the IP addresses for the domain.

To edit IP range for a domain

- Click the button under the 'Action' column beside a domain name that you want to edit the IP addresses.

The 'Anti-spoofing Edit' screen will be displayed.

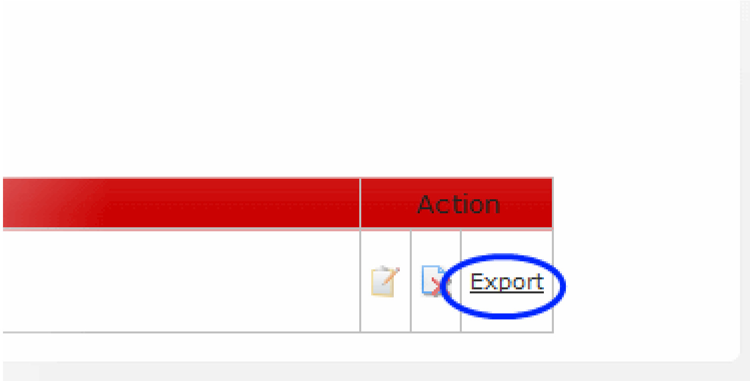
- Edit the address as required and click the 'Save' button.

To delete a domain from the list

- To delete a domain name from the list, click the ☒ button under the 'Action' column and confirm it in the confirmation screen.

To export the list of IP addresses for a domain

- Click the 'Export' link under the 'Action' column



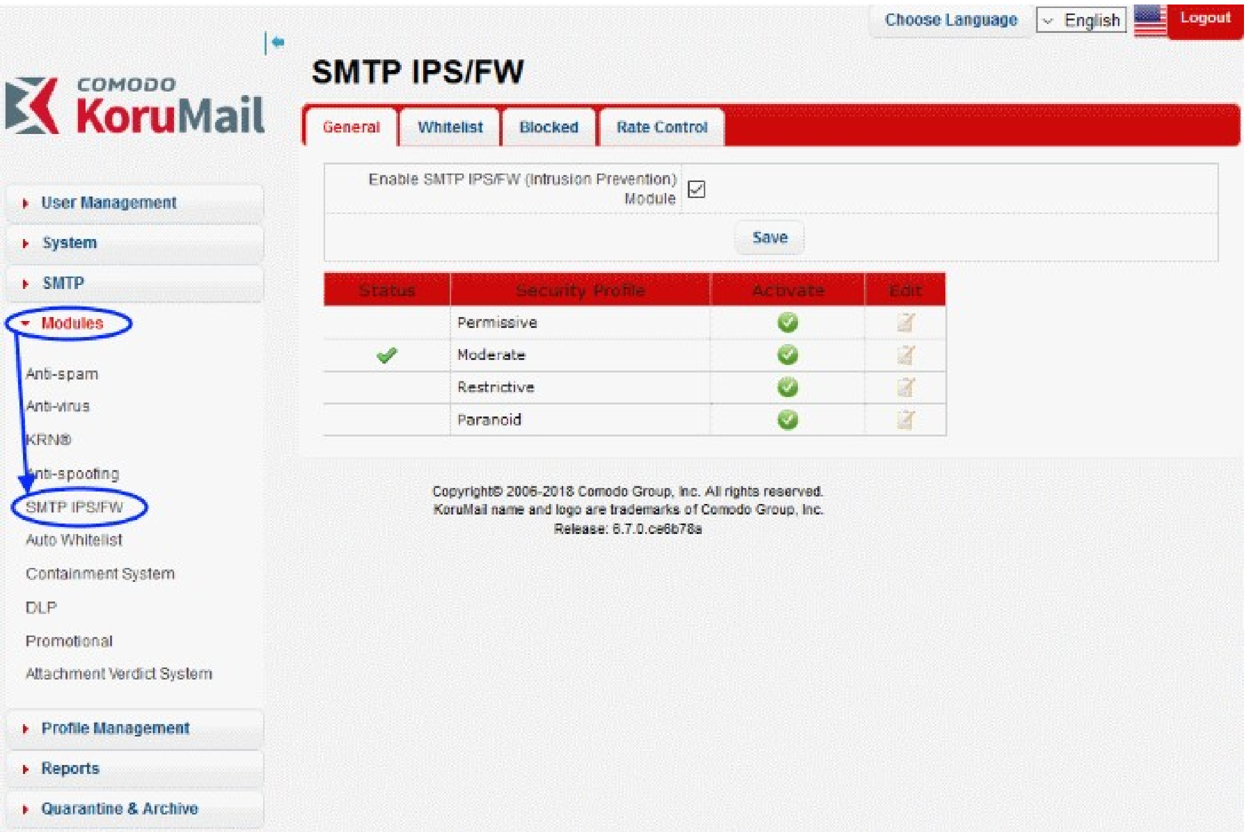
- Download and save the SPF IP list as a text file to your system.

8.5 SMTP IPS/FW

- KourMail's SMTP Intrusion Prevention System (IPS) and Firewall (FW) module provide protection against Denial of Service (DoS) and SYN attacks.
- SYN attacks are dealt with using SYN Cookies and SYN Cache features.
- DoS attacks are blocked by deploying various usage limitations.
    - For example, KoruMail can limit the number of connections it accepts in a certain time-period. The IPS/FW module will block IPs that want make more connections more than the limit. You can specify the limit in a security profile.
- The module also lets you create whitelist and block rules to better control spam. The rate control feature, a subset of the DoS protection system, allows you to control how many connections are allowed within the specified time from the same IP address.

To open the 'SMTP IPS/FW' interface

- Click the 'Modules' tab on the left, then click 'SMTP IPS/FW'.



SMTP IPS/FW

Enable SMTP IPS/FW (Intrusion Prevention) Module ☑

Status	Security Profile	Activate	Edit
	Permissive	✓	✎
✓	Moderate	✓	✎
	Restrictive	✓	✎
	Paranoid	✓	✎

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

See the following sections for more details.

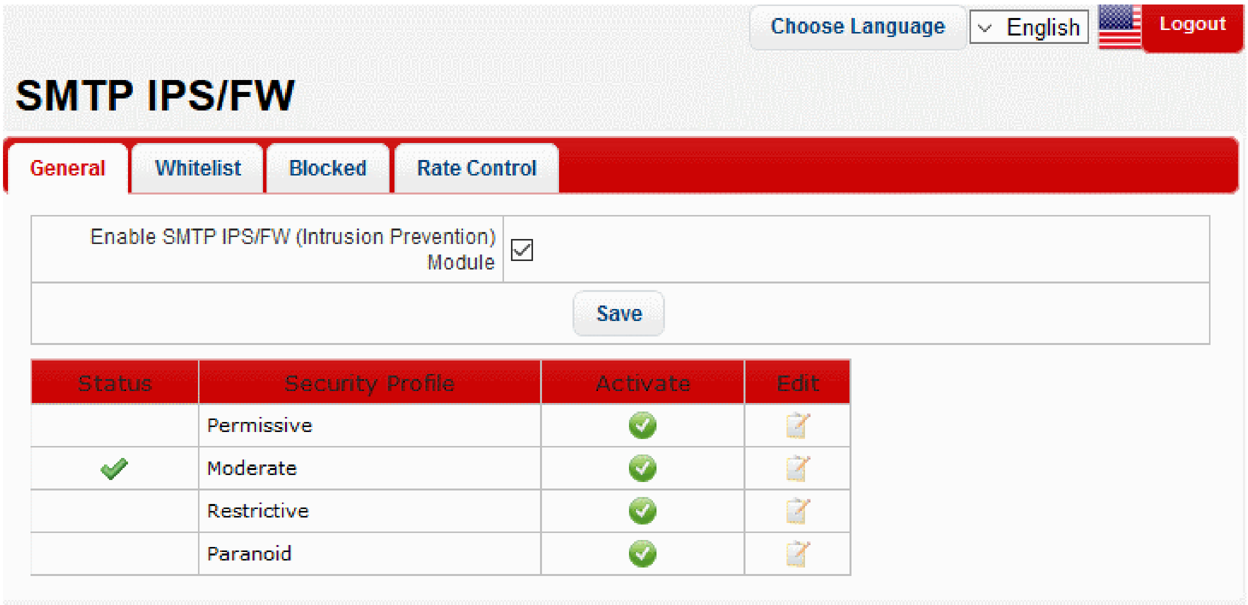
- **SMTP IPS General Settings**
- **Whitelist IP Addresses**
- **Blocked IP Addresses**
- **Rate Control**

8.5.1 SMTP IPS General Settings

- Enable/disable the intrusion prevention system (IPS) and configure a security profile for KoruMail.
- The IPS allows KoruMail to control the number of SMTP connections from any single IP address.
- This helps to detect and block spam/denial-of-service attacks and aids traffic management.

To open the 'IPS General Settings' interface

- Click the 'General' tab in the 'SMTP IPS/FW' screen.



SMTP IPS/FW

Enable SMTP IPS/FW (Intrusion Prevention) Module ☑

Status	Security Profile	Activate	Edit
	Permissive	✓	✎
✓	Moderate	✓	✎
	Restrictive	✓	✎
	Paranoid	✓	✎

- SMTP IPS/FW (Intrusion Prevention) Module: Activate the module. The relevant settings specified in the security profile will now be applied.

The module has a set of predefined security profiles with different . You can edit a profile if required.

IPS General Settings - Table of Column Descriptions		
Column Header	**Description**	
Status	Indicates whether the security profile is active.	
Security Profile	• The profile determines how strict KoruMail should be regarding simultaneous connections from the same IP address. • Click the 'Edit' button to see the specific details of each profile. You are free to edit a profile as you wish.	
Activate	Enable the profile. Please note that only one security profile can be active at a time.	
Edit	✎	Modify the settings of the profile.

The interface allows administrators to:

- Activate a security profile
- Edit the parameters of a security profile

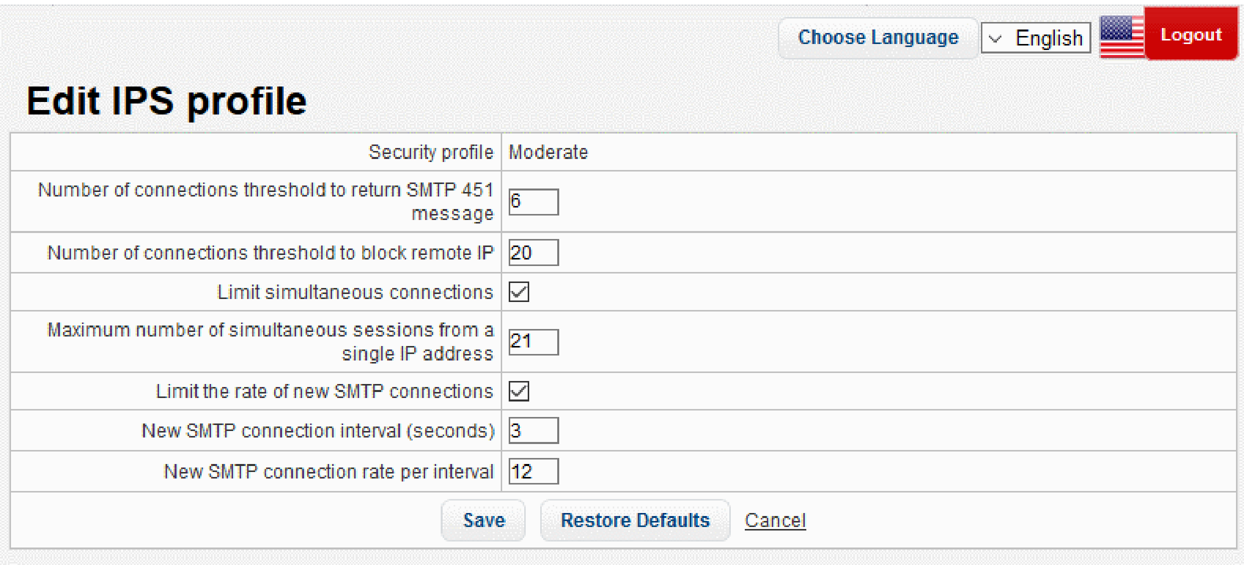
To activate a security profile

- Click the ✓ button under the 'Activate' column in a security profile row that you want to enable. Please note that only one security profile can be active at a time.

The 'Settings saved successfully' message will be displayed at the top.

To edit the parameters of a security profile

- Click the ✎ button under the 'Edit' column in a security profile row that you want to edit.



Edit IPS profile

Security profile	Moderate
Number of connections threshold to return SMTP 451 message	6
Number of connections threshold to block remote IP	20
Limit simultaneous connections	☑
Maximum number of simultaneous sessions from a single IP address	21
Limit the rate of new SMTP connections	☑
New SMTP connection interval (seconds)	3
New SMTP connection rate per interval	12

The 'Edit IPS profile' screen will be displayed.

IPS Profile - Table of Parameters	
Parameter	**Description**
Security profile	The name of the predefined profile.
Number of connections threshold to return SMTP 451 message	• Max. connections before KoruMail will refuse further connections and send 451 errors messages to the sender. Change line to: If you wish to unblock this sender, please use the form at https://tools.korumail.com/contact to request Comodo whitelist or unblock the IP.
Number of connections threshold to block remote IP	Max. connections before KoruMail firewall blocks the source IP address.
Limit simultaneous connections	Enable controls on the number of simultaneous connections. See settings below.
Maximum number of simultaneous sessions from a single IP address	Maximum number of sessions that can be opened by a single IP address after limiting instant SMTP connections.
Limit the rate of new SMTP connections	If enabled, the parameters 'New SMTP connection interval' and 'New SMTP connection rate' can be specified to set limitations on new SMTP connections.
New SMTP connection interval (seconds)	The time between a new connection and the previous connection.
New SMTP connection rate	Maximum number of new SMTP connections in specified interval.

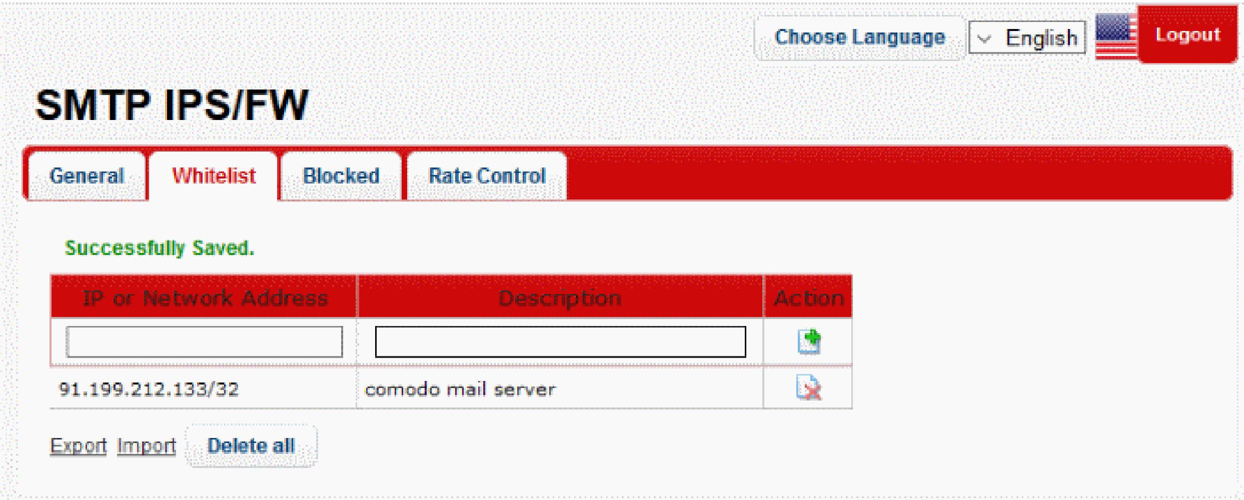
- Click 'Save' apply your changes.
- Click 'Restore Defaults' to restore the parameters to factory setting.

8.5.2 Whitelist IP Addresses

Whitelisted IP addresses will not be filtered by the SMTP IPS module.

To open the 'Whitelist' interface,

- Click the 'Whitelist' tab in the SMTP IPS/FW module.



Successfully Saved.

IP or Network Address	Description	Action
		✚
91.199.212.133/32	comodo mail server	✗

Whitelist Settings - Table of Column Descriptions		
Column Header	**Description**	
IP or Network Address	The details of IP or networked addresses that are whitelisted.	
Description	The description provided for the IP/Network address.	
Action	✚	Allows administrators to add a Network or IP address after entering the details in the row.
	✗	Allows administrators to delete a whitelisted Network or IP address from the list.

The interface allows administrators to:

- Add a network or IP address to whitelist
- Delete a whitelisted network or IP address from the list
- Export the whitelisted network or IP address details
- Import lists of whitelisted network or IP addresses from files

To add a network or IP address to whitelist

- Enter the IP or Network address details in the first field
- Enter an appropriate description for the address in the field under 'Description'.
- Click the ✚ button.

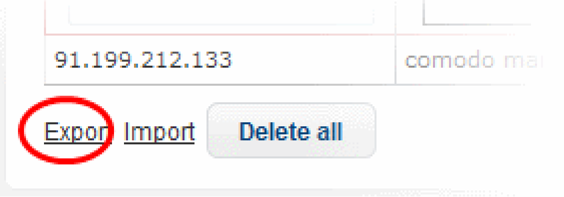
The address will be added and listed as whitelisted.

To delete a whitelisted network or IP address from the list

- Click the ☒ button beside an address that you want to delete and click 'OK' in the confirmation screen
- Click the 'Delete all' button below to remove all the whitelisted addresses from the list and click 'OK' in the confirmation screen.

To export the whitelisted network or IP address details

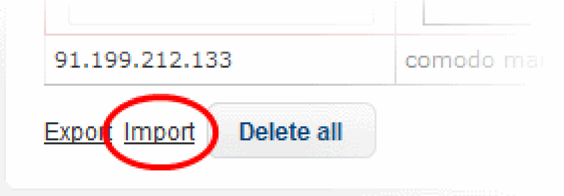
- Click the 'Export' link at the bottom of the screen



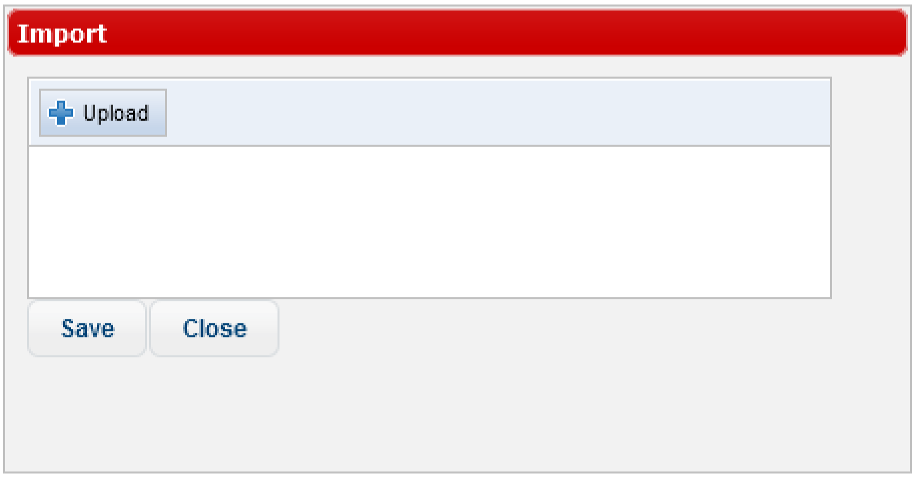
- Download and save the list as a text file to your system.

To import lists of whitelisted network or IP addresses from files

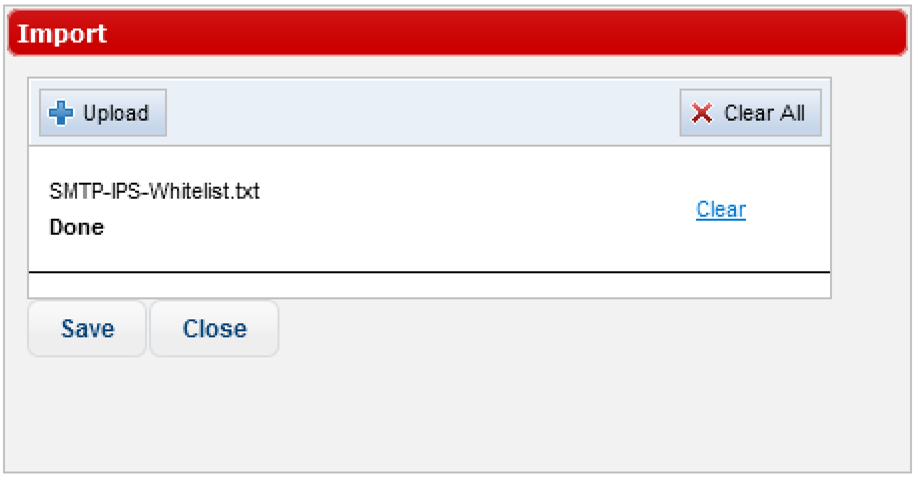
- Click the 'Import' link at the bottom of the screen



- Click the 'Upload' button, navigate to the location where the file is saved and click 'Open'



- Repeat the process to add more files to the list.



Import

SMTP-IPS-Whitelist.txt
Done

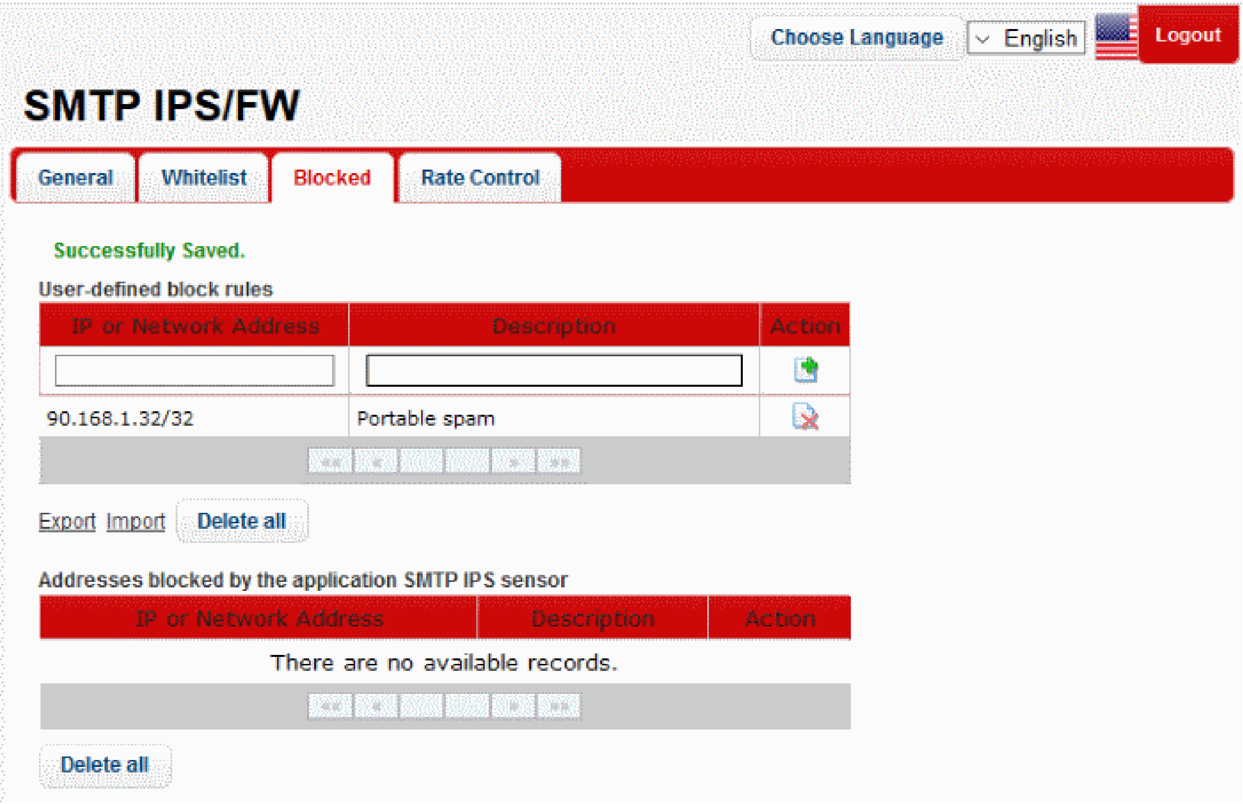
- To remove a file from the list, click the 'Clear' link beside it.
- To remove all the files, click the 'Clear All' button at the top.
- Click the 'Save' button.

8.5.3 Blocked IP Addresses

- Add IP addresses to the blacklist so that mails from these sources never reach the SMTP level for processing.
- This page lists blocked by policy rules and IPs blocked by the intrusion prevention module.
- Admins can unblock IP addresses by simply deleting the row from the table.

To open the 'Blocked' interface

- Click the 'Blocked' tab in the SMTP IPS/FW module.



SMTP IPS/FW

Successfully Saved.

User-defined block rules

IP or Network Address	Description	Action
90.168.1.32/32	Portable spam	

Addresses blocked by the application SMTP IPS sensor

IP or Network Address	Description	Action
There are no available records.		

The interface allows you to:

- Add a network or IP address to be blocked
- Delete a blocked network or IP address from the list
- Export the blocked network or IP address details
- Import lists of network or IP addresses from files to be blocked
- Delete an automatically blocked network or IP address by SMTP IPS sensor from the list

To add a network or IP address to be blocked

- Enter the IP or Network address details in the first field
- Enter an appropriate description for the address in the field under 'Description'.
- Click the ➕ button.

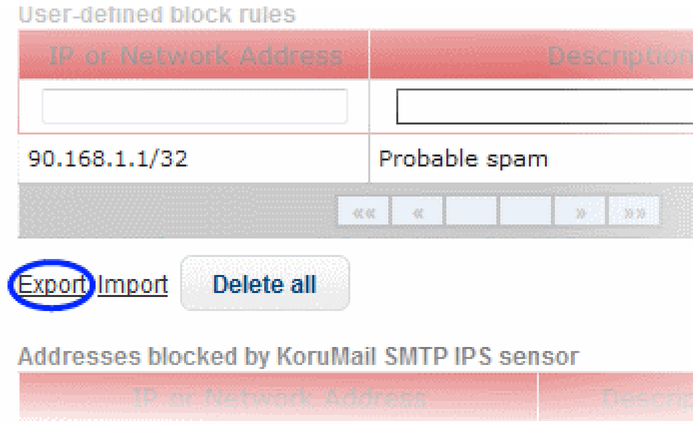
The address will be added and listed.

To delete a blocked network or IP address from the list

- Click the ✗ button beside an address that you want to delete and click 'OK' in the confirmation screen
- Click the 'Delete all' button below to remove all the blocked addresses from the list and click 'OK' in the confirmation screen.

To export the blocked network or IP address details

- Click the 'Export' link at the bottom of the screen


User-defined block rules

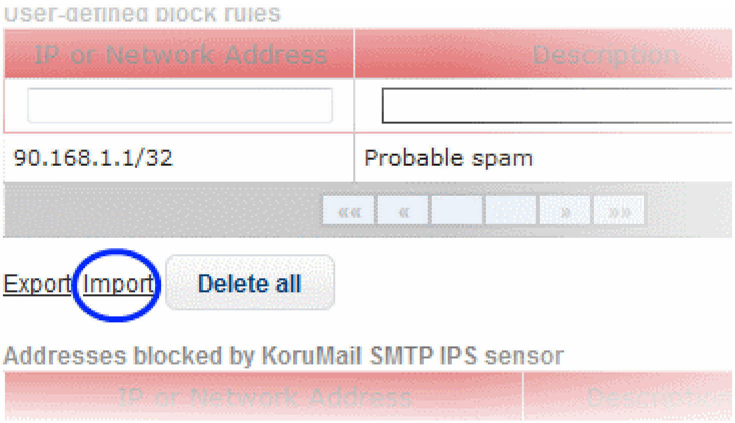
IP or Network Address	Description
90.168.1.1/32	Probable spam

Addresses blocked by KoruMail SMTP IPS sensor

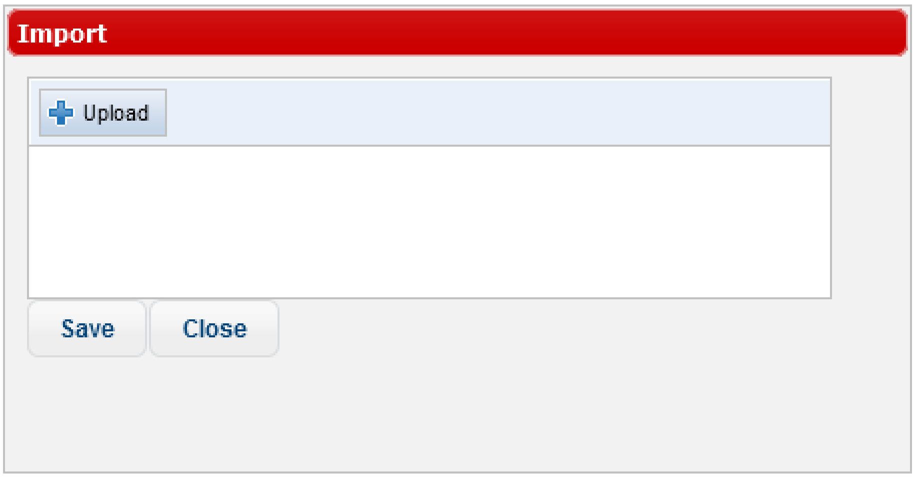
- Download and save the list as a text file to your system.

To import lists of network or IP addresses from files to be blocked

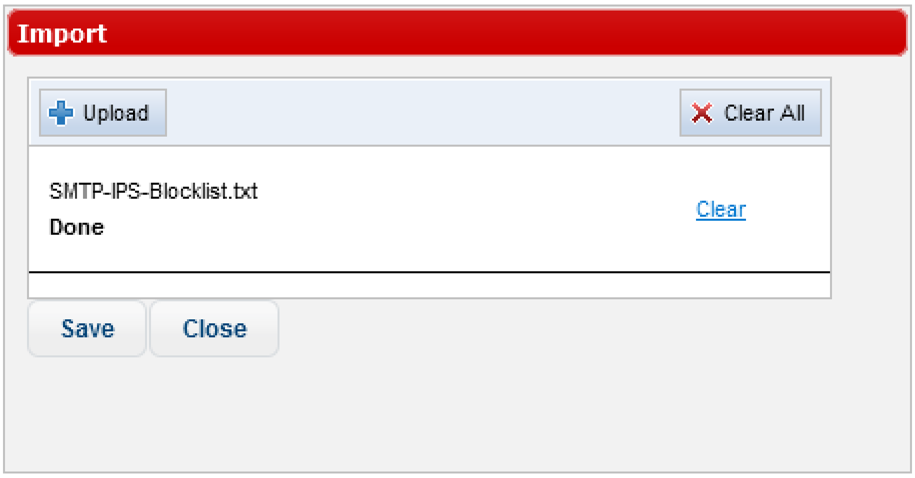
- Click the 'Import' link at the bottom of the screen



- Click the 'Upload' button, navigate to the location where the file is saved and click 'Open'



- Repeat the process to add more files to the list.

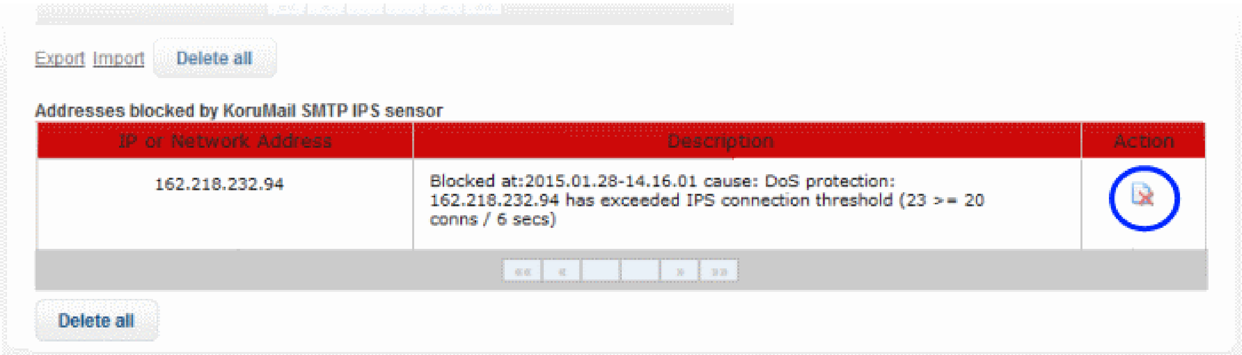


- To remove a file from the list, click the 'Clear' link beside it.
- To remove all the files, click the 'Clear All' button at the top.
- Click 'Save'

To delete an automatically blocked network or IP address by SMTP IPS sensor from the list

If you know the IP addresses blocked by the SMTP IPS sensor is a trusted source, then you can delete it from the list.

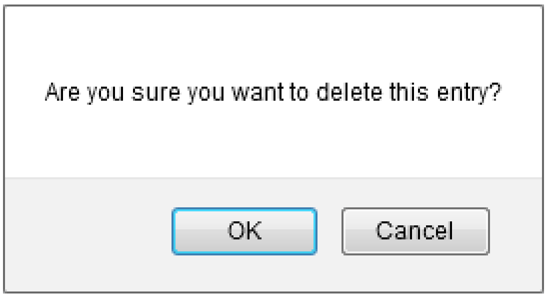
- In the 'Addresses blocked by KoruMail SMTP IPS sensor' table, click the button beside an address that you want to delete.



Addresses blocked by KoruMail SMTP IPS sensor

IP or Network Address	Description	Action
162.218.232.94	Blocked at:2015.01.28-14.16.01 cause: DoS protection: 162.218.232.94 has exceeded IPS connection threshold (23 >= 20 conns / 6 secs)	

- Click 'OK' in the confirmation screen

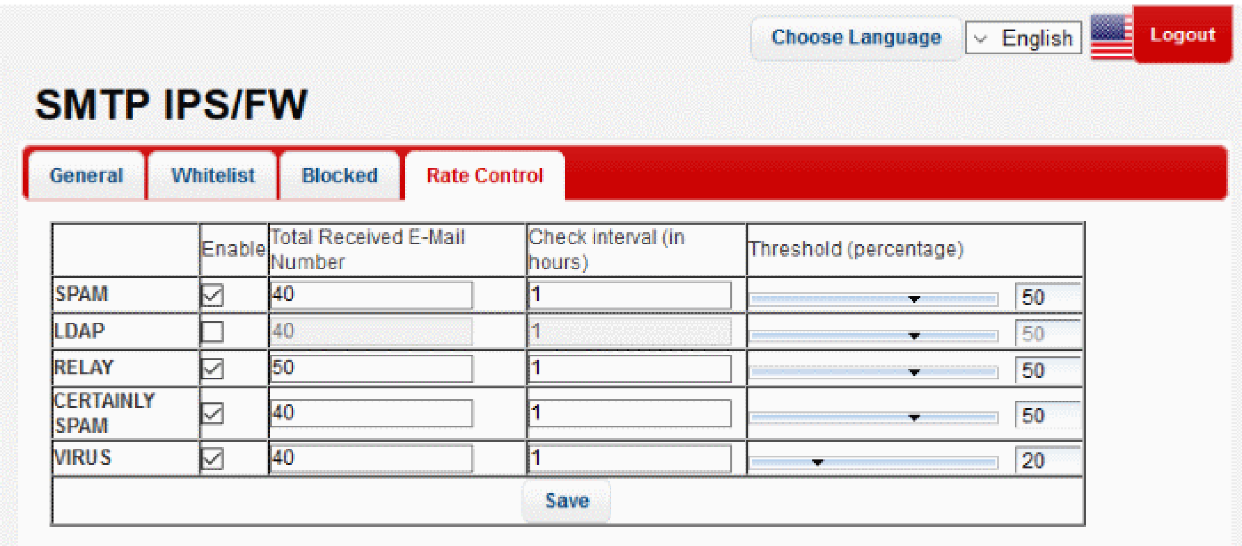

Are you sure you want to delete this entry?

8.5.4 Rate Control

- The 'Rate Control' feature protects an organization from spammers that send huge amounts of mail to your mail server.
- It counts the number of suspicious mails sent by a source in a set period of time. If the value exceeds the specified threshold then the sender IP is added to the blacklist.

To open the 'Rate Control' interface

- Click the 'Rate Control' tab in the SMTP IPS/FW module.



	Enable	Total Received E-Mail Number	Check interval (in hours)	Threshold (percentage)
SPAM	☑	40	1	50
LDAP	□	40	1	50
RELAY	☑	50	1	50
CERTAINLY SPAM	☑	40	1	50
VIRUS	☑	40	1	20

Rate Control Settings - Table of Column Descriptions	
Column Header	**Description**
Category	SPAM - Mails that are categorized as spam

	LDAP - Verification of LDAP users. When incoming mails are for users that are not in LDAP, the originating IP address will be blacklisted. For example, if the number of mails is set as 50, and the threshold percentage as 50%, then if from a source if the number of mails for non LDAP users exceeds 25 within the check interval, then the source will be blacklisted RELAY - IPs from which mails can be sent by users who are not available on the mail server. CERTAINLY SPAM - Mails that are categorized as definite spam. VIRUS - Mails that are categorized as with virus
Enable	Activate or disable the Rate Control for a mail category
Total Received Mails	The number of mails that need to be received in the specified interval before Korumail will activate threshold checks. If Korumail receives this number of mails from a source within the 'check interval' time, it will check what % of those mails are spam/relay/etc. If this exceeds the figure specified as the threshold then it will blacklist the sender.
Check interval (in hours)	Enter the time in hours for the specified number of mails to be checked for a category.
Threshold (percentage)	Percentage of mail in the category. For example, if the number of email is set as 60 for a category, then a 50% threshold means that when the number exceeds 30, then the originating IP address will be blocked.

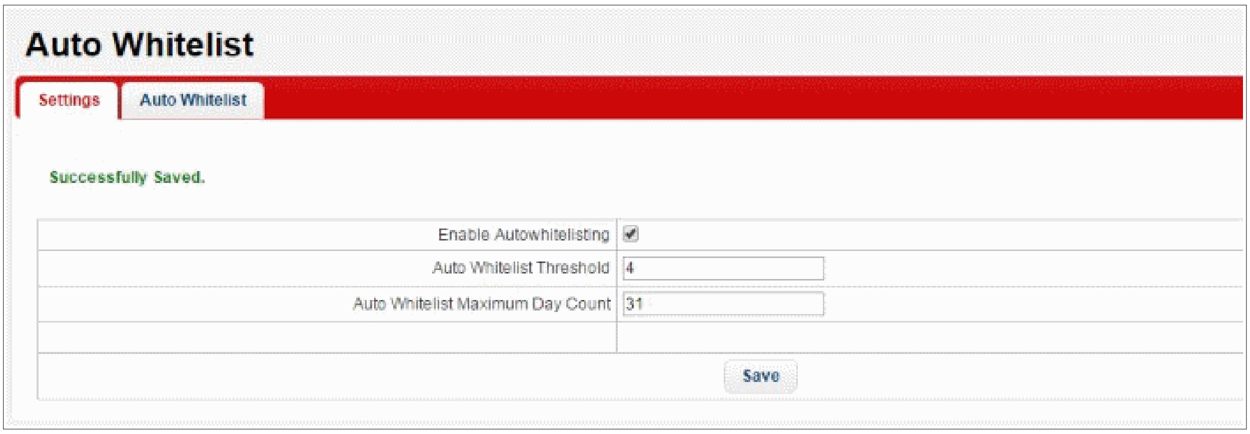
- Click 'Save' to apply your changes.

8.6 Auto Whitelist

Korumail allows administrators to automatically whitelist incoming and outgoing mails to and from specific email addresses. The 'Auto Whitelist' module must be enabled to activate the whitelisting of addresses specified in profile settings. See '**Profile Management**' or more details about profile settings.

Auto Whitelist Settings:

- Click 'Modules' > 'Auto Whitelist'.



Auto Whitelist

Successfully Saved.

Enable Autowhitelisting ☑

Auto Whitelist Threshold 4

Auto Whitelist Maximum Day Count 31

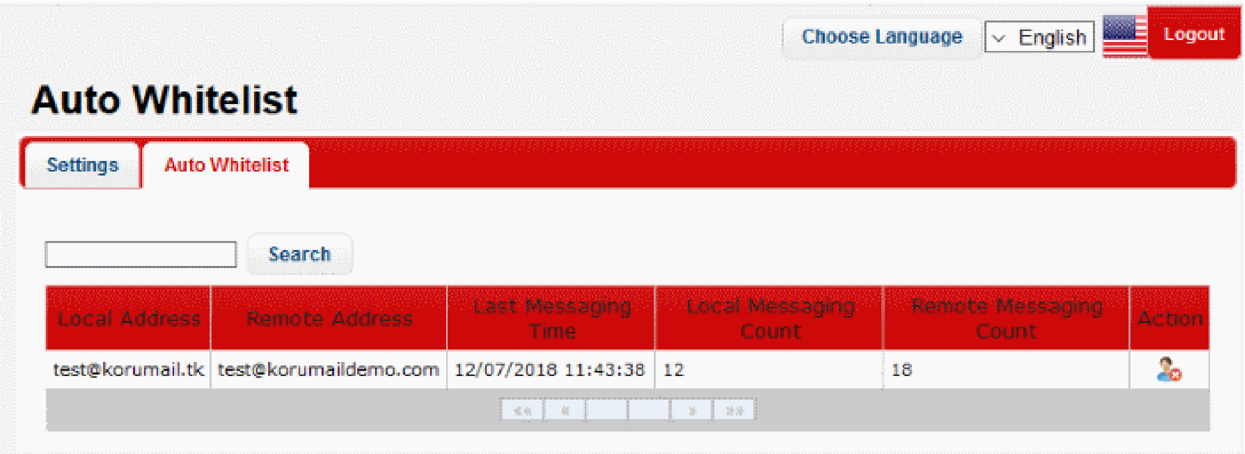
- **Enable Autowhitelisting:** Activate automatic whitelist checks on incoming and outgoing emails
- **Auto Whitelist Threshold:** How many emails must be exchanged before the remote sender is added to the whitelist. Note - The threshold should be reached within the number of days specified in the 'Auto Whitelist Maximum Day Count' field.

- **Auto Whitelist Maximum Day Count:** To activate auto-whitelisting, Korumail must receive the amount of mails in the threshold field within the number of days specified here.

- Click 'Save' to apply your changes.

Please note that you can manually whitelist emails from the 'Mail logs' interface.

Auto Whitelist details



Local Address	Remote Address	Last Messaging Time	Local Messaging Count	Remote Messaging Count	Action
test@korumail.tk	test@korumaildemo.com	12/07/2018 11:43:38	12	18	

The Auto Whitelist tab displays emails which have been whitelisted by currently active profiles.

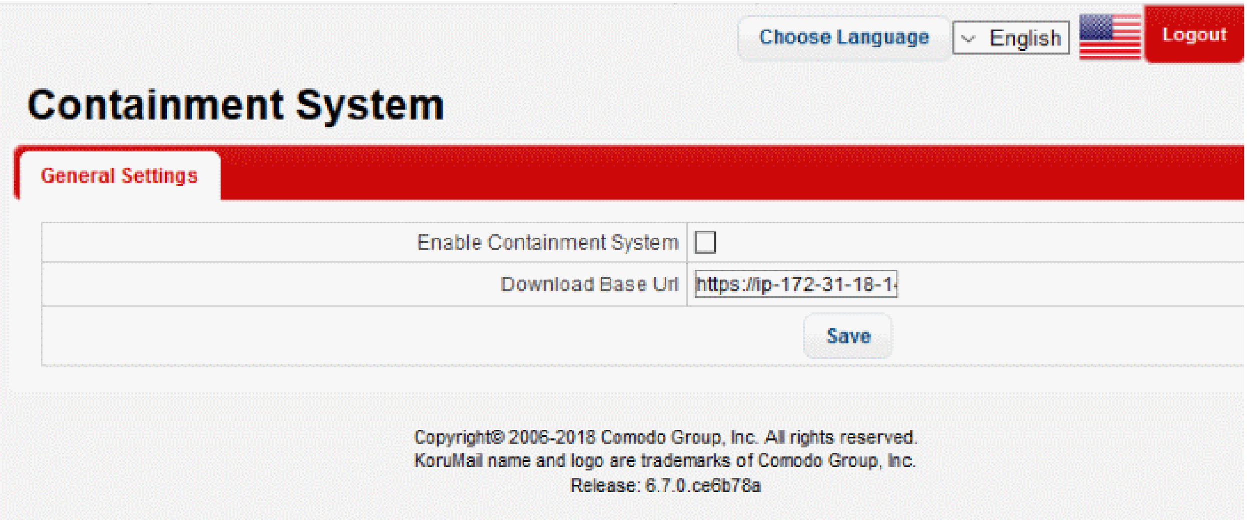
Auto Whitelist - Table of Column Headers	
Column Header	**Description**
Local Address	The recipient's email address
Remote Address	The sender's email address
Last Messaging Time	The time of the most recent sent or received mail
Local Messaging Count	The number of mails received
Remote Messaging Count	The number of messages sent
Action	Deletes auto-whitelisted items

8.7 Containment System

- Containment protects users from zero-day malware by opening any untrusted attachments in a secure, virtual environment. This environment is 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. This isolation means the attachment cannot damage the host machine nor steal confidential information.
- Process in brief:
  - 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

To configure containment system,

- Click the 'Modules' tab on the left, then click 'Containment System'.



Containment System

General Settings

Enable Containment System	□
Download Base Url	https://ip-172-31-18-1

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

  - **Enable Containment System**: When enabled, files that have an 'Unknown' trust rating are contained.
  - **Download Base Url**: The URL from which users will download the wrapped version of the file.
- Click 'Save' to apply your changes.

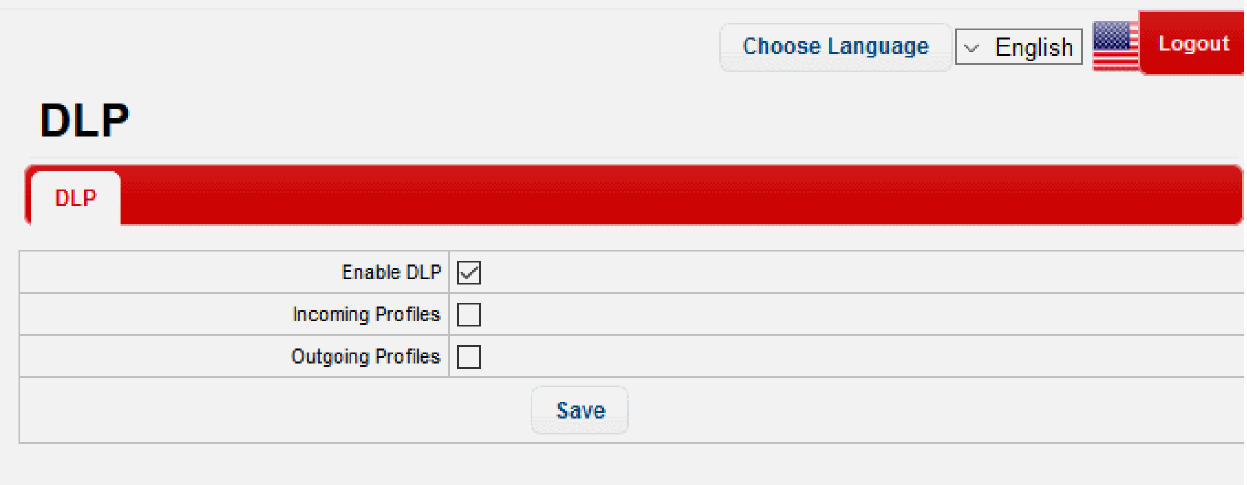
See **Attachment Verdict System** if you need more information on file ratings.

8.8 Data Leak Prevention (DLP)

- KoruMail is integrated with a DLP (Data Leak Prevention) engine that prevents data theft via emails.
- The engine searches for configured words in incoming and outgoing mails and applies actions as per the settings in the profile. Actions include quarantining the mail and / or notifying the administrator.
- The DLP module must be enabled in order to activate the DLP parameters specified in the profile settings.
- See '**Profile Management**' for more details about profile settings.

To open the 'DLP' interface

- Click the 'Modules' tab on the left, then click 'DLP'.



DLP

DLP

Enable DLP	☑
Incoming Profiles	□
Outgoing Profiles	□

- **Enable DLP:** Select the check box to display the 'Incoming Profiles' and 'Outgoing Profiles' check boxes.
- **Incoming Profiles:** Select the check box to apply the DLP profile parameters to incoming mails
- **Outgoing Profile:** Select the check box to apply the DLP profile parameters for outgoing mails

See '**Profile Management**' for more details about profile settings.

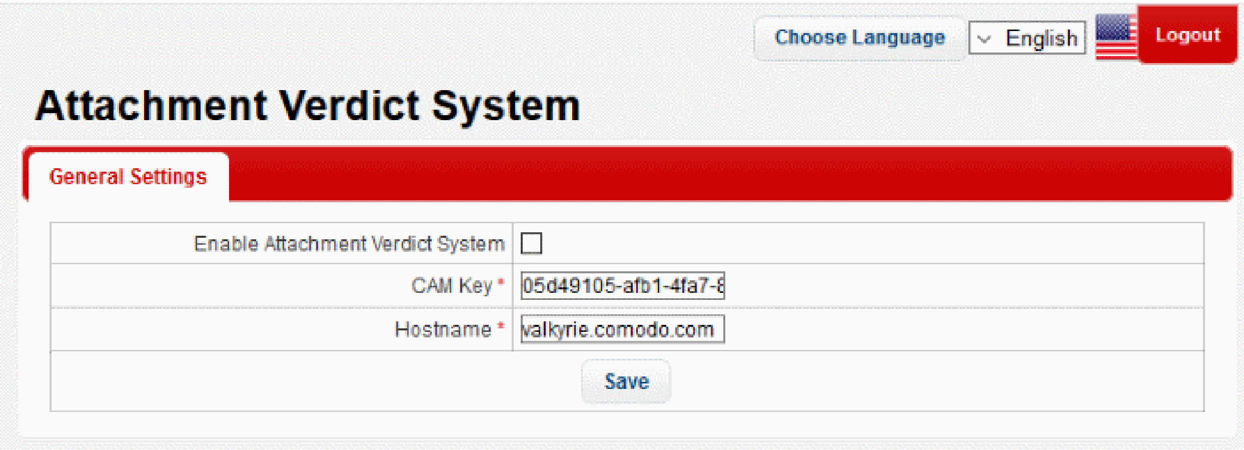
- Click 'Save' to apply your changes.

8.9 Attachment Verdict System

- The 'Attachment Verdict System' settings area enables administrators to configure settings related to the analysis of email attachments.
- If enabled, verdicting system will automatically submit email attachments (windows executable files and pdf files) with an 'unknown' trust rating to Comodo Valkyrie for analysis.
- Valkyrie will run a series of behavioral tests to find out whether or not the attachment is malicious.

To open the attachment verdict settings area

- Click Modules > Attachment Verdict System



Attachment Verdict System

General Settings

Enable Attachment Verdict System	□
CAM Key *	05d49105-afb1-4fa7-8
Hostname *	valkyrie.comodo.com

Attachment Verdict System - Table of Column Headers	
Column Header	**Description**
Enable Attachment Verdict System	• If enabled, Korumail will automatically check the trust rating of Windows executables and pdf files in Comodo's file look up server (FLS). • The verdict from the FLS can be 'Clean', 'Malware' or 'Unknown'. • Clean attachments will be allowed to proceed while malware attachments will be automatically quarantined (providing 'Quarantine mails containing viruses' is enabled in the antivirus section of the profile). • 'Unknown' files will be submitted to Comodo's real-time file analysis system, Valkyrie, for behavior testing. • Valkyrie's tests will determine whether the unknown file is clean or malware and apply the appropriate action as mentioned above.
CAM Key	Comodo Accounts Manager License key. The customers must sign up with Comodo Accounts Manager and order the Korumail product to avail a license key.
Hostname	Hostname of the file attachment verdict system. This is set to the Comodo Valkyrie server by default. Only change this if you have established a different server with Comodo support.

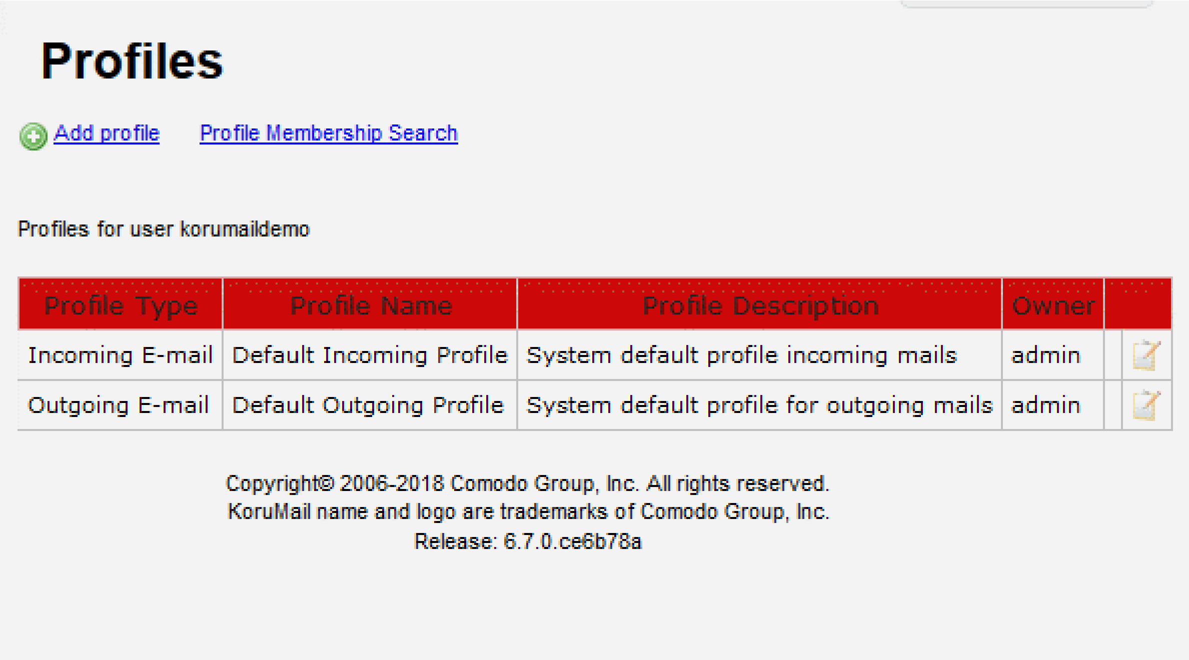
Please note that, if the 'Enable Attachment Verdict System is enabled' and the 'Send files that not found in File Verdict System' is disabled, then the unknown files are not uploaded to Valkyrie for analysis. See **Attachment Verdict Reports**, to view reports of attachment verdict system.

9 Profile Management

- Profiles are a collection of settings for KoruMail features such as 'Anti-virus', 'Anti-spam', 'Black List' and White List'. Profile can be applied to domains and/or users.
- There are two kinds of profiles that can be created in KoruMail - 'Incoming E-mail' and 'Outgoing E-mail'. Admins can apply different profiles for incoming mails and outgoing mails.
- KoruMail ships with a set of default incoming and outgoing profiles that can be edited but not deleted.

To open the 'Profiles' interface

- Click the 'Profile Management' tab on the left, then click 'Profiles'



Profiles

Profiles for user korumaildemo

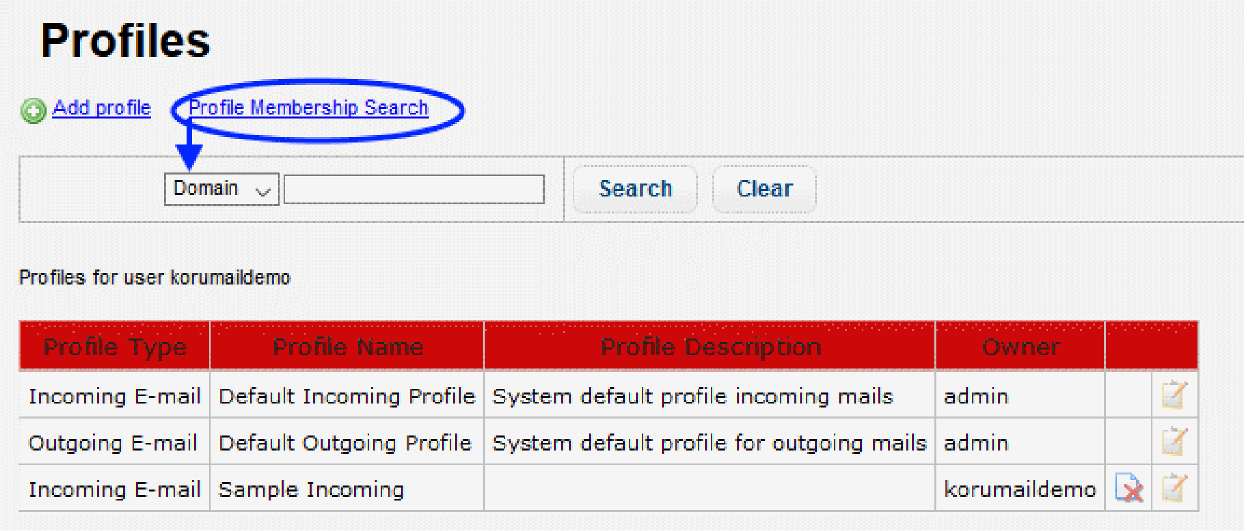
Profile Type	Profile Name	Profile Description	Owner	
Incoming E-mail	Default Incoming Profile	System default profile incoming mails	admin	
Outgoing E-mail	Default Outgoing Profile	System default profile for outgoing mails	admin	

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

Profiles - Table of Column Headers		
Column Header	**Description**	
Profile Type	The type of profile whether incoming or outgoing	
Profile Name	The name of the profile. The name of default profiles will be auto filled.	
Profile Description	The description provided for the profile	
Owner	The name of the group to which the profile creator belongs	
Action		Allows administrators to delete a profile. The default incoming or outgoing profile wil apply to the domains and / or users beloning to a profile when it is deleted.
		Allows administrators to edit the settings in a profile.

Search Option

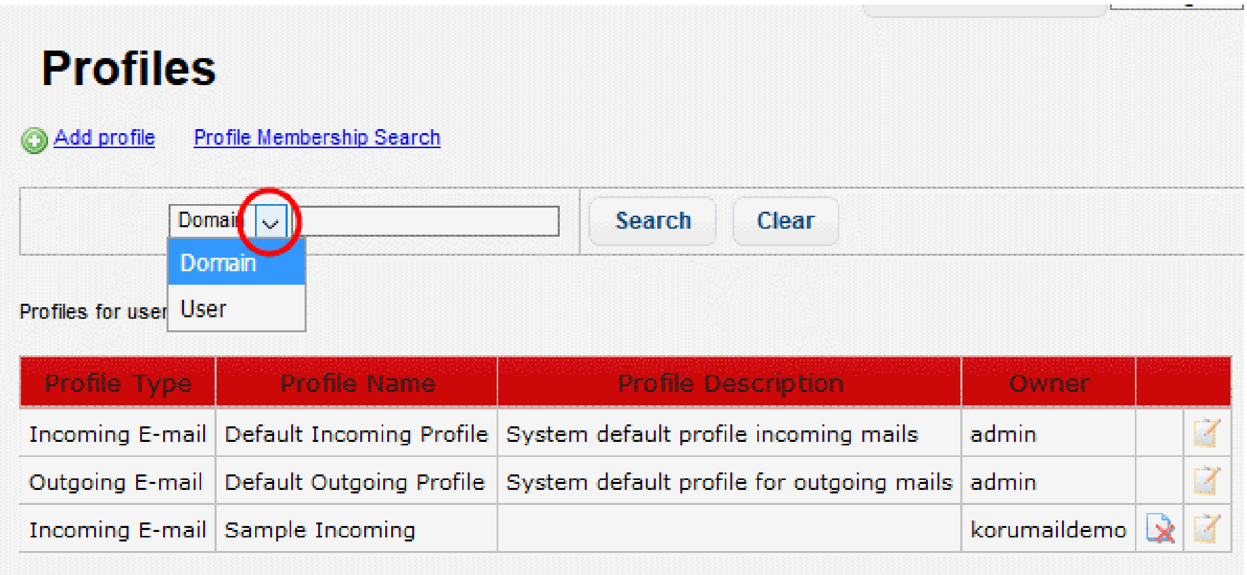
Click the 'Profile Membership Search' link at the top to search for a profile that is applied to domain and / or users.



Profiles for user korumaildemo

Profile Type	Profile Name	Profile Description	Owner	
Incoming E-mail	Default Incoming Profile	System default profile incoming mails	admin	
Outgoing E-mail	Default Outgoing Profile	System default profile for outgoing mails	admin	
Incoming E-mail	Sample Incoming		korumaildemo	

- Select 'Domain' or 'User' from the drop-down for which you want to search the profile

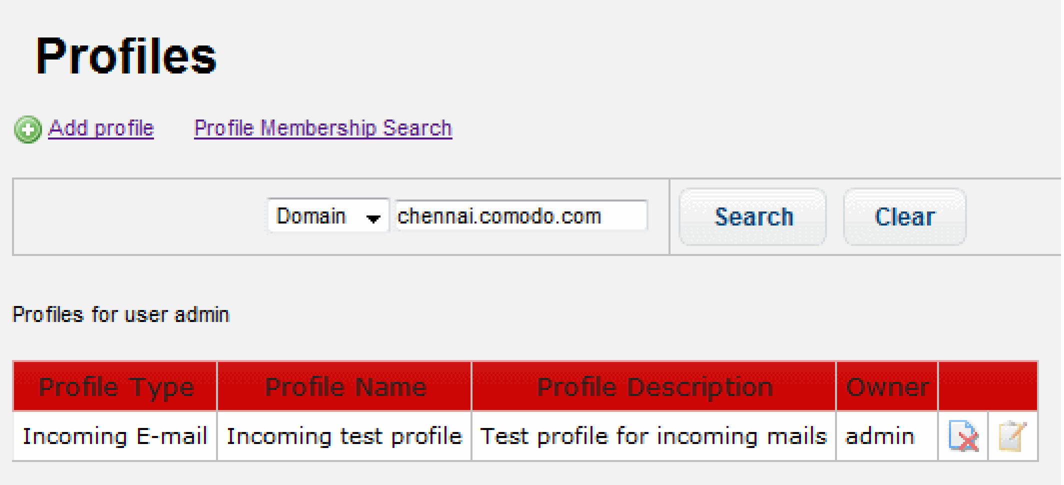


Profiles for user

Profile Type	Profile Name	Profile Description	Owner	
Incoming E-mail	Default Incoming Profile	System default profile incoming mails	admin	
Outgoing E-mail	Default Outgoing Profile	System default profile for outgoing mails	admin	
Incoming E-mail	Sample Incoming		korumaildemo	

- Enter the domain or user details and click the the 'Search' button.

The profile applied for the entered details will be displayed.



Domain: chennai.comodo.com

Profiles for user admin

Profile Type	Profile Name	Profile Description	Owner	
Incoming E-mail	Incoming test profile	Test profile for incoming mails	admin	

- To remove the details in the search field, click the 'Clear' button.
- To remove the search field, click the 'Profile Membership Search' link again.

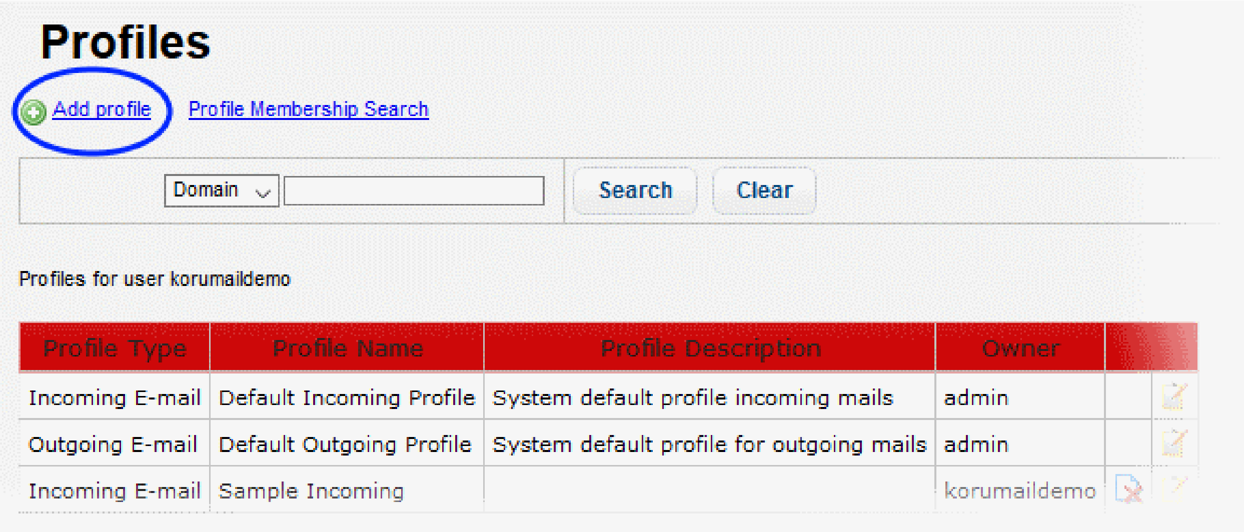
The 'Profiles' interface allows administrators to:

- **Add and Confgure a New Profile**
- **Edit a Profile**
- **Delete a Profile**

9.1 Add and Configure a New Profile

Profiles let you configure how Korumail's scanners and filters should handle mail on your protected domains. The items that can be set in a profile include Anti-virus, Anti-spam, SMTP, Attachment Filter, Black List, White List, Header Filter, Archive and Quarantine, Data Leak Prevention (DLP) and Realtime Blackhole List (RBL).

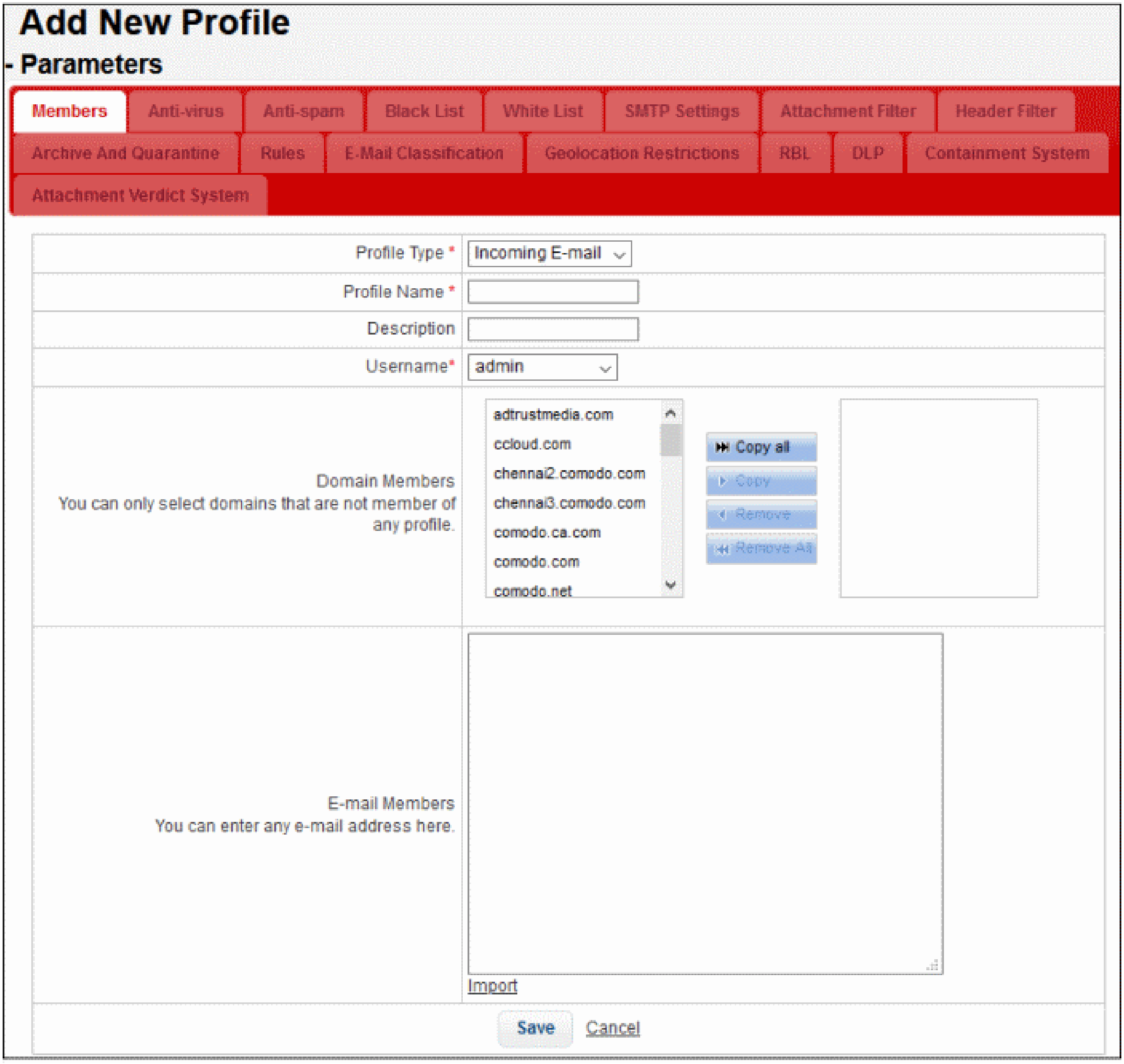
- Click 'Profiles' > 'Add profile'



Profiles for user korumaildemo

Profile Type	Profile Name	Profile Description	Owner		
Incoming E-mail	Default Incoming Profile	System default profile incoming mails	admin		
Outgoing E-mail	Default Outgoing Profile	System default profile for outgoing mails	admin		
Incoming E-mail	Sample Incoming		korumaildemo		

The 'Add New Profile' screen will be displayed:



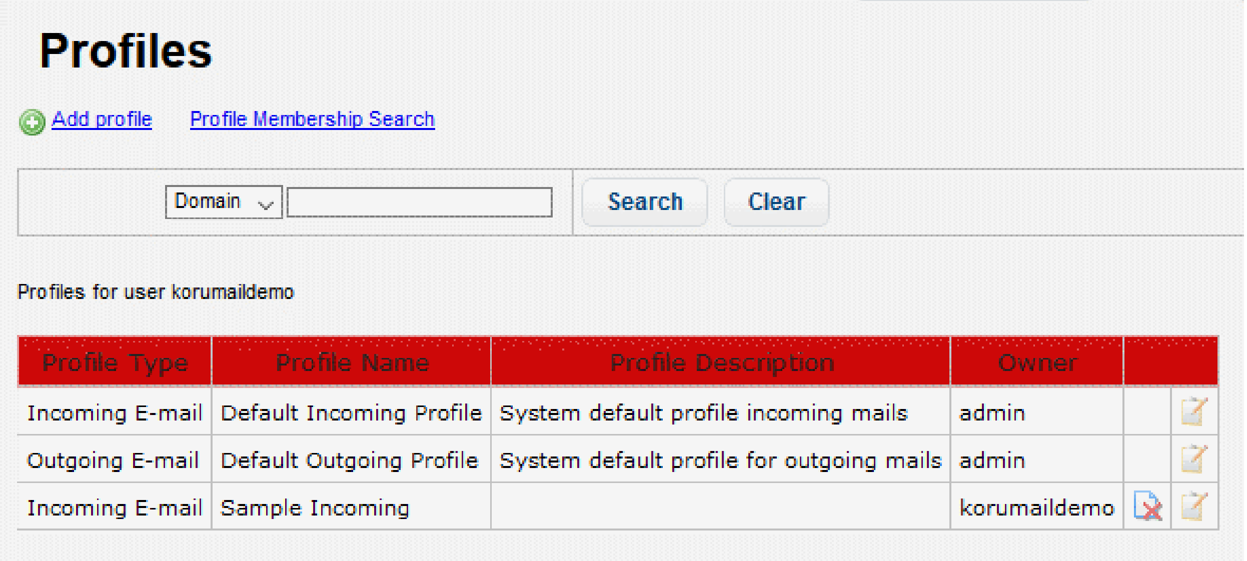
Profile Type *	Incoming E-mail
Profile Name *	
Description	
Username*	admin
Domain Members You can only select domains that are not member of any profile.	adtrustmedia.com ccloud.com chennai2.comodo.com chennai3.comodo.com comodo.ca.com comodo.com comodo.net
E-mail Members You can enter any e-mail address here.	

Profiles - Table of Parameters	
Parameter	**Description**
Profile Type	Select whether you want the profile to apply to incoming mails or outgoing mails
Profile Name	Enter a name for the profile
Description	Provide an appropriate description for the profile
Username	Select the username of the person who is adding the profile. Only users with appropriate privileges will be listed.
Domain Members	Allows administrators with appropriate privileges to add domains for the profile. The box in the left side displays the domains that were added in the '**Managed Domains**' section. Any domain that is already added to a profile will not be listed. Domains can be added by selecting and clicking the appropriate button (Copy all, Copy, Remove, Remove all) in the middle. All the users in a domain added here will be applied the profile.
Email Members	Allows administrators with appropriate privileges to add users for the profile who may

	belong to other domains that are not added for a profile. Please note that for an incoming profile only users belonging to domains added in the '**Managed Domains**' section can be added here. For an outgoing profile, you can also add users belonging to domains that are not added in the '**Managed Domains**' section.
Import	Allows administrators to add users for the profile by importing them from a saved file. For importing users for an incoming profile the same limitations mentioned in the above row will apply.

- Click 'Save' to apply your changes

The profile will be saved and the tabs for configuring other parameters will be displayed.



Profiles for user korumaildemo

Profile Type	Profile Name	Profile Description	Owner	
Incoming E-mail	Default Incoming Profile	System default profile incoming mails	admin	
Outgoing E-mail	Default Outgoing Profile	System default profile for outgoing mails	admin	
Incoming E-mail	Sample Incoming		korumaildemo	

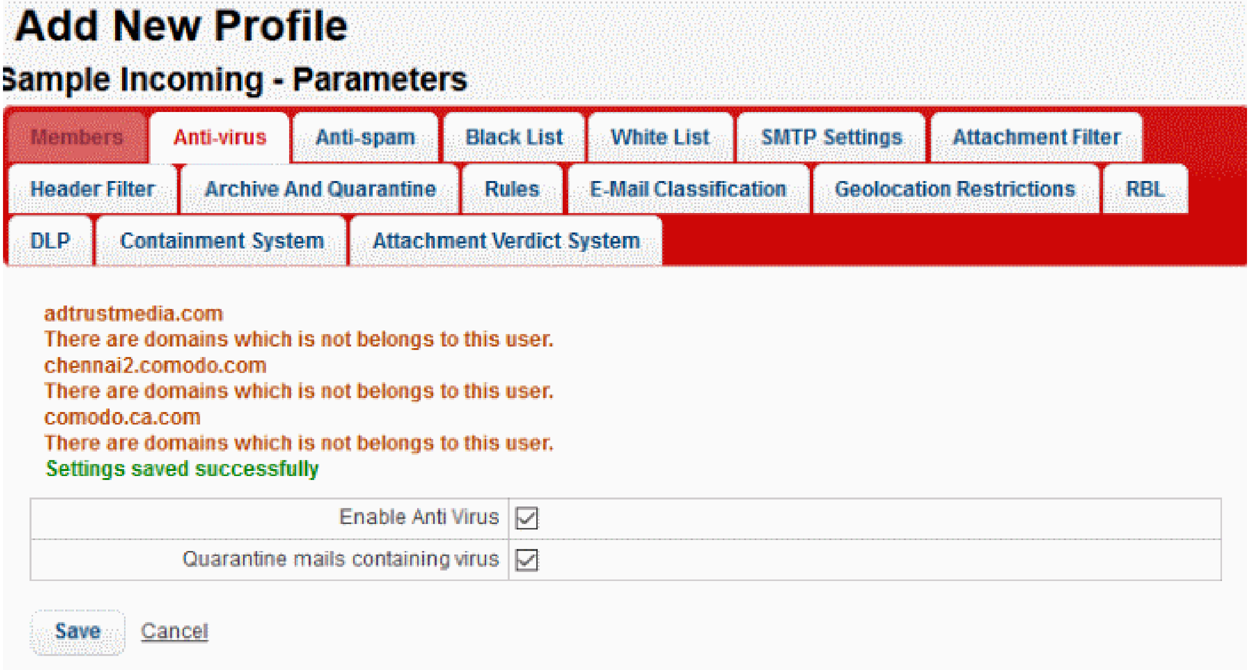
The interface allows administrators to configure profile parameters for:

- **Anti-virus**
- **Anti-spam**
- **Black List**
- **White List**
- **SMTP Settings**
- **Attachment Filter**
- **Header Filter**
- **Archive and Quarantine**
- **Rules**
- **Email Classification**
- **Geolocation Restrictions**
- **Realtime Blackhole List (RBL)**
- **Data Leak Prevention (DLP)**
- **Containment System**
- **Attachment Verdict System**

Note: All tabs are disabled until you complete and save the details of the domain members.

Anti-virus

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Anti-virus' tab



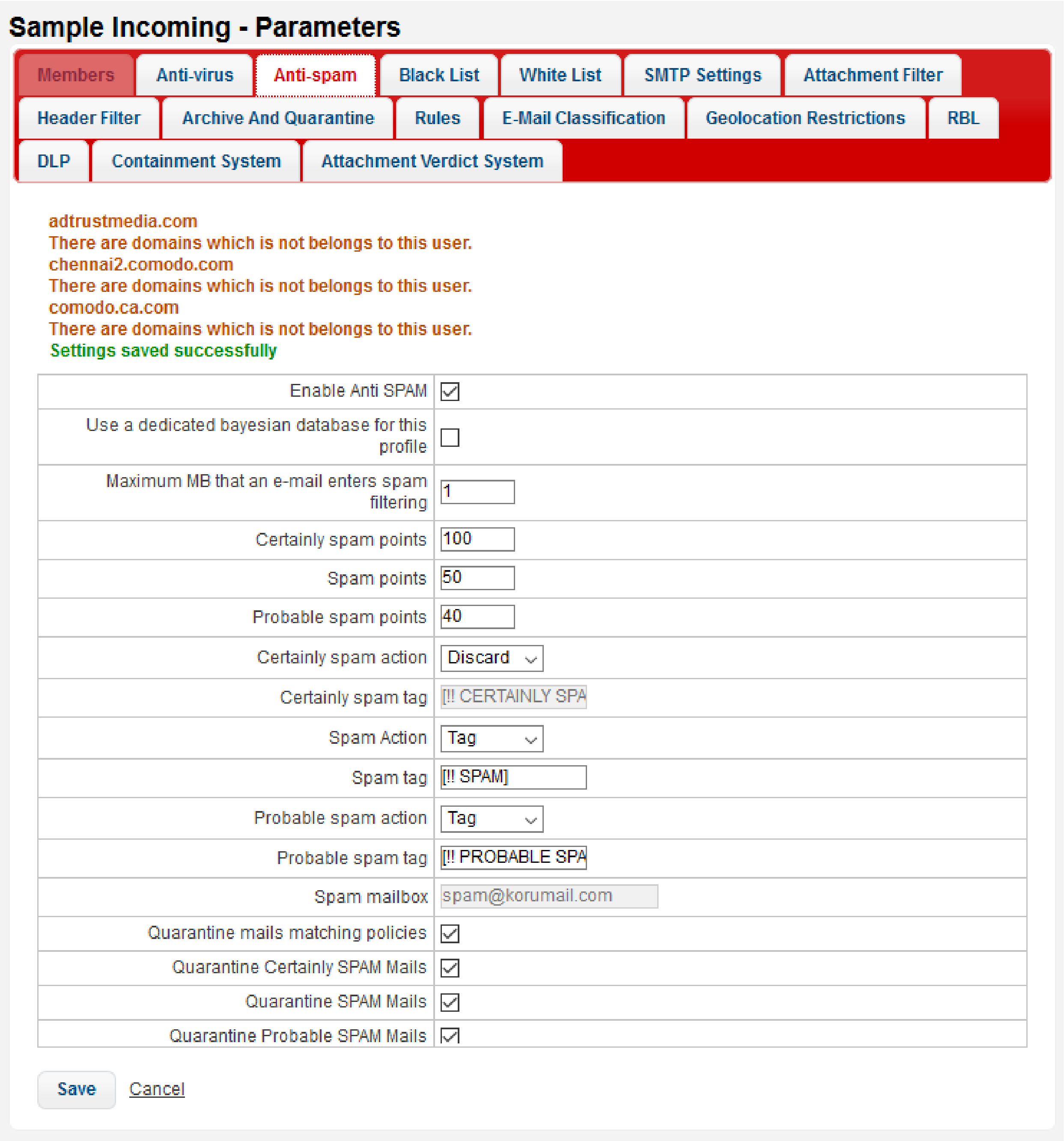
adtrustmedia.com
There are domains which is not belongs to this user.
chennai2.comodo.com
There are domains which is not belongs to this user.
comodo.ca.com
There are domains which is not belongs to this user.
Settings saved successfully

Enable Anti Virus	☑
Quarantine mails containing virus	☑

  - **Enable Anti Virus:** Select the check box to enable the anti-virus engine for this profile. Please note the '**Anti-virus**' module should be enabled for this parameter to become active.
  - **Quarantine mails containing virus:** Mails detected with viruses will be quarantined. Users can log into the 'Quarantine Webmail' interface to view his/her mails that are quarantined.
- Click 'Save' to apply your changes.

Anti-spam

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Anti-spam' tab



Sample Incoming - Parameters

adtrustmedia.com
There are domains which is not belongs to this user.
chennai2.comodo.com
There are domains which is not belongs to this user.
comodo.ca.com
There are domains which is not belongs to this user.
Settings saved successfully

Enable Anti SPAM	☑
Use a dedicated bayesian database for this profile	□
Maximum MB that an e-mail enters spam filtering	1
Certainly spam points	100
Spam points	50
Probable spam points	40
Certainly spam action	Discard
Certainly spam tag	[!! CERTAINLY SPA
Spam Action	Tag
Spam tag	[!! SPAM]
Probable spam action	Tag
Probable spam tag	[!! PROBABLE SPA
Spam mailbox	spam@korumail.com
Quarantine mails matching policies	☑
Quarantine Certainly SPAM Mails	☑
Quarantine SPAM Mails	☑
Quarantine Probable SPAM Mails	☑

Profiles: Anti-spam Settings - Table of Parameters	
Parameter	**Description**
Enable Anti SPAM	Select the check box to enable the anti-spam engine for this profile. Please note the '**Anti-spam**' module should be enabled for this parameter to become active.
Use a dedicated bayesian database for this profile	Select the check box to enable the anti-spam engine to use Bayesian database also for detecting spam mails. Please note the 'Bayes Spam engine' in the '**Advanced Settings**' section of '**Anti-spam**' module should be enabled for this parameter to become active.
Maximum MB that an e-mail enters spam filtering	Enter the maximum size of emails for which spam filtering will be enabled. If the size of an email exceeds the entered value, then the email will not be scanned and placed in queue for delivery to the recipient.
Certainly spam points	Enter a value between 1 and 100 that will classify an email as definitely spam.

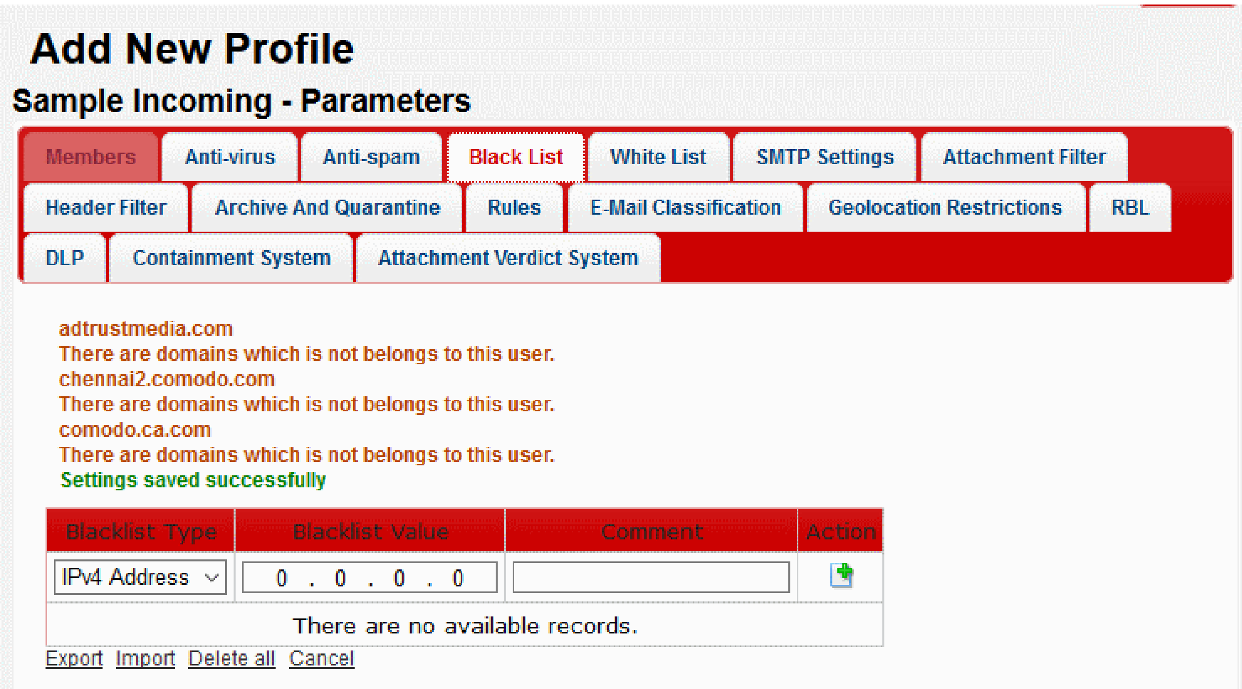
	Suggested values are between 90 - 100 points.
Spam points	Enter a value between 1 and 100 that will classify an email as spam. Suggested values are between 51 - 89 points.
Probable spam points	Enter a value between 1 and 100 that will classify an email as probable spam. Suggested values are between 40 - 50 points.
Certainly spam action	Select the action that has to be taken for emails that are categorized as definitely spam. The options available are: • **Tag** - The email will be sent to the recipient with a tag as entered in the next field 'Certainly spam tag' • **Forward** - The mail will be forwarded to a mail box defined in the 'Spam mailbox' field • **CC** - The mail will be sent to the recipient and a copy will be sent to a mail box defined in the 'Spam mailbox' field • **Discard** - The mail will be quarantined. Daily notifications will be sent to user with details of quarantined emails. The user can view the email using the 'Quarantined Email' web interface. • **Reject** - The mail will be rejected and a reject command will be sent to the sender mail server.
Certainly spam tag	Enter the tag text for emails that are categorized as definitely spam
Spam Action	Select the action that has to be taken for emails that are categorized as spam. The options available are: • **Tag** - The email will be sent to the recipient with a tag as entered in the next field 'Spam tag' • **Forward** - The mail will be forwarded to a mail box defined in the 'Spam mailbox' field • **CC** - The mail will be sent to the recipient and a copy will be sent to a mail box defined in the 'Spam mailbox' field • **Discard** - The mail will be quarantined. Daily notifications will be sent to user with details of quarantined emails. The user can view the email using the 'Quarantined Email' web interface. • **Reject** - The mail will be rejected and a reject command will be sent to the sender mail server.
Spam tag	Enter the tag text for emails that are categorized as spam
Probable spam action	Select the action that has to be taken for emails that are categorized as probable spam. The options available are: • **Tag** - The email will be sent to the recipient with a tag as entered in the next field 'Probable spam tag' • **Forward** - The mail will be forwarded to a mail box defined in the 'Spam mailbox' field • **CC** - The mail will be sent to the recipient and a copy will be sent to a mail box defined in the 'Spam mailbox' field • **Discard** - The mail will be quarantined. Daily notifications will be sent to user with details of quarantined emails. The user can view the email using the 'Quarantined Email' web interface. • **Reject** - The mail will be rejected and a reject command will be sent to the sender mail server.
Probable spam tag	Enter the tag text for emails that are categorized as probable spam

Spam mailbox	Enter the email address to which the forwarded and CCed spam emails configured in the 'Spam action' drop-down will be sent.
Quarantine mails matching policies	If enabled, emails that are matching the configured profile will be quarantined.
Quarantine Certainly SPAM Mails	If enabled, emails that are categorized as definitely spam will be quarantined.
Quarantine SPAM Mails	If enabled, emails that are categorized as spam will be quarantined.
Quarantine Probable SPAM Mails	If enabled, emails that are categorized as probable spam will be quarantined.

- Click 'Save' to apply your changes.

Black List

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Black List' tab



Add New Profile

Sample Incoming - Parameters

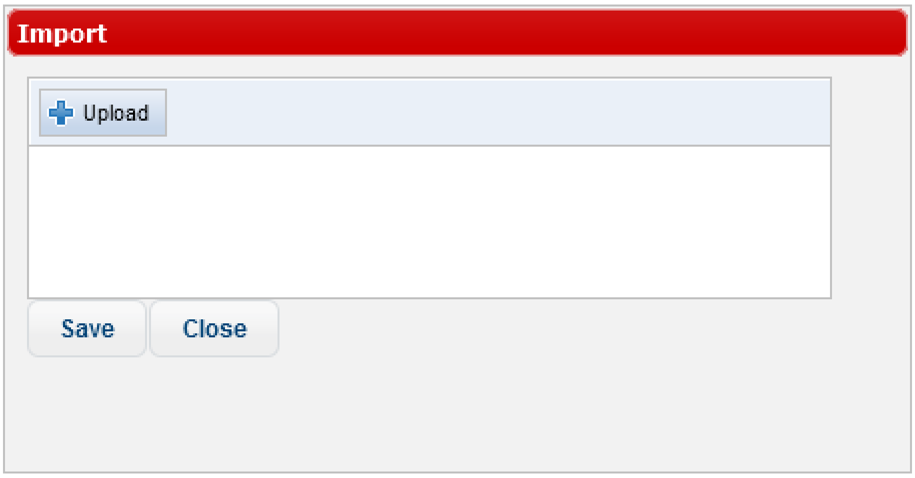
adtrustmedia.com
There are domains which is not belongs to this user.
chennai2.comodo.com
There are domains which is not belongs to this user.
comodo.ca.com
There are domains which is not belongs to this user.
Settings saved successfully

Blacklist Type	Blacklist Value	Comment	Action
IPv4 Address	0 . 0 . 0 . 0		➕
There are no available records.			

Profiles: Black List Settings - Table of Column Descriptions	
Column Header	**Description**
Blacklist Type	Select the type of source that has to be blacklisted. The options available are: • IPv4 Address • IPv6 Address • E-mail • Domain • IPv4 Network

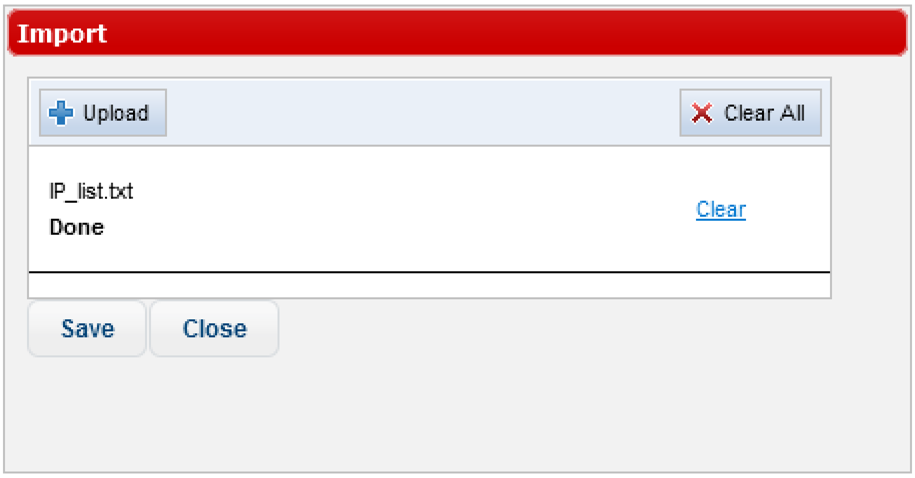
	- IPv6 Network	
Blacklist Value	Enter the details for the type of blacklist selected in the first column.	
Comment	Provide an appropriate description for the blacklisted source	
Action	✚	Allows administrators to add a blacklist type after filling the fields in the row
	✖	Allows administrators to delete a blacklist type from the list

- To save the list of blacklisted sources, click the 'Export' link and save it to your system.
- To import a list of sources to be blacklisted, click the 'Import' link



- Click the 'Upload' button, browse to the location where the file is saved and click 'Open'.

The file will be added.



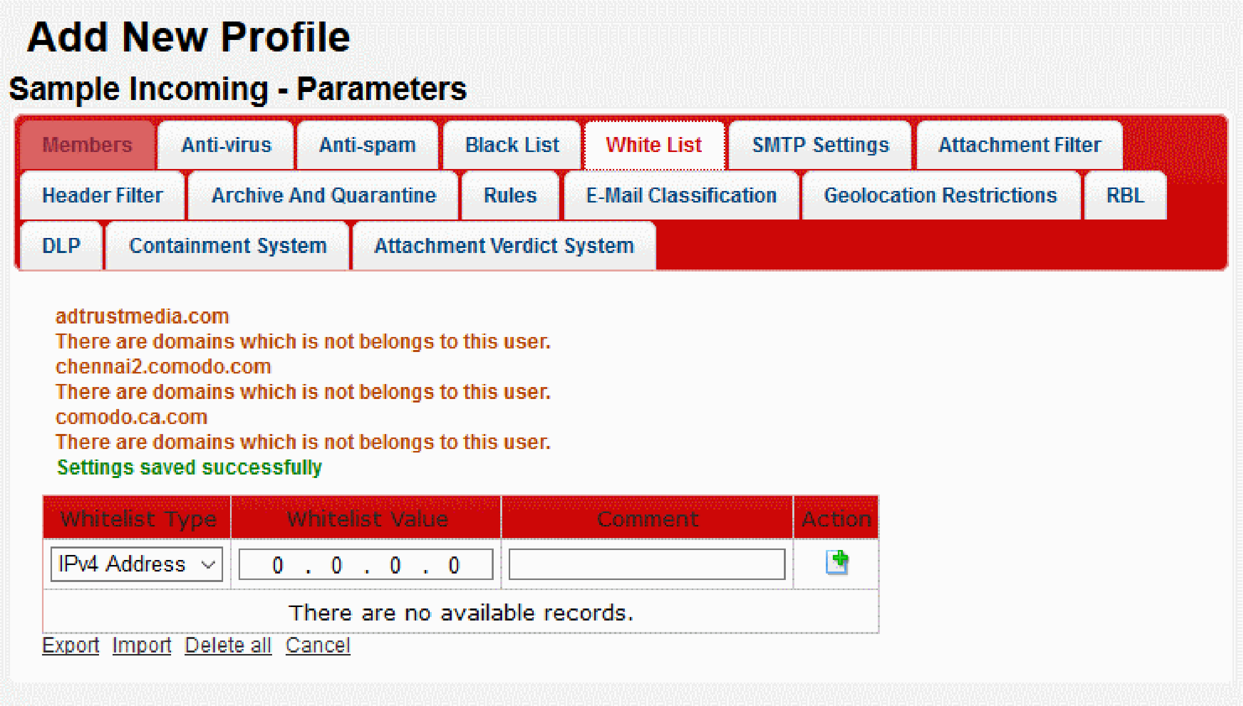
IP_list.txt
Done

- Repeat the process to add more files.
- To remove a file, click the 'Clear' link beside it.
- To remove all the added files, click the 'Clear All' button at the top right.
- To import the list from the files, click 'Save'.

- To delete a blacklist type from the list, click ✗ under the 'Action' column header and click 'OK' in the confirmation screen.
- To remove all the blacklisted sources, click the 'Delete all' link and click 'OK' in the confirmation screen.

White List

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'White List' tab



Add New Profile

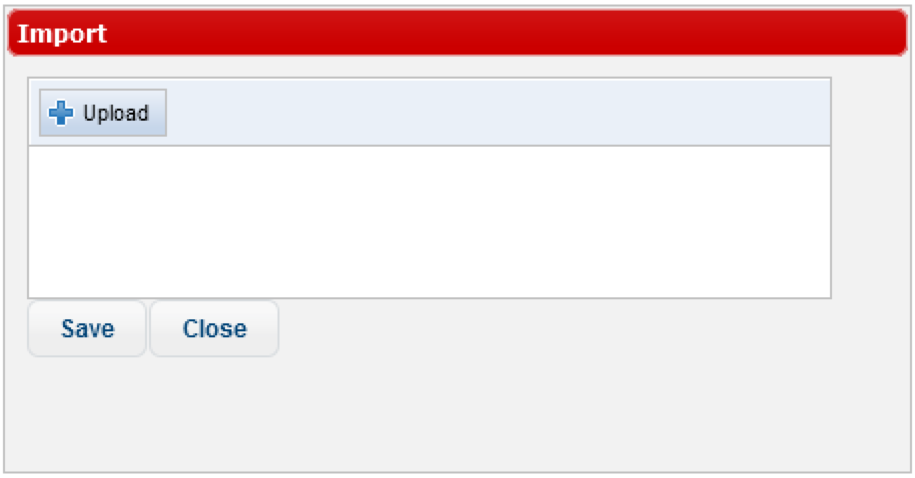
Sample Incoming - Parameters

adtrustmedia.com
There are domains which is not belongs to this user.
chennai2.comodo.com
There are domains which is not belongs to this user.
comodo.ca.com
There are domains which is not belongs to this user.
Settings saved successfully

Whitelist Type	Whitelist Value	Comment	Action
IPv4 Address	0 . 0 . 0 . 0		✚
There are no available records.			

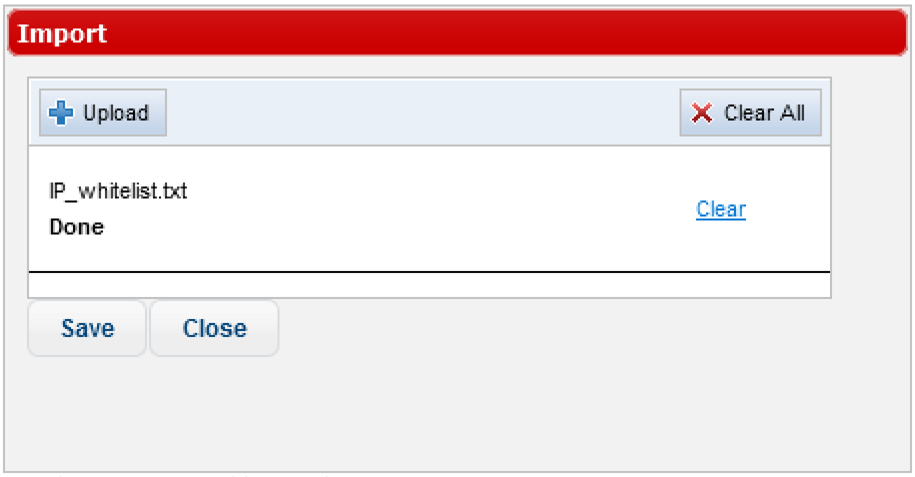
Profiles: White List Settings - Table of Column Descriptions		
Column Header	**Description**	
Whitelist Type	Select the type of source that has to be whitelisted. The options available are: • IPv4 Address • IPv6 Address • E-mail • Domain • IPv4 Network • IPv6 Network	
Whitelist Value	Enter the details for the type of whitelist selected in the first column.	
Comment	Provide an appropriate description for the blacklisted source.	
Action	✚	Allows administrators to add a whitelist type after filling the fields in the row.
	✗	Allows administrators to delete a whitelist type from the list.

- To save the list of whitelisted sources, click the 'Export' link and save it to your system.
- To import a list of sources to be whitelisted, click the 'Import' link



- Click the 'Upload' button, browse to the location where the file is saved and click 'Open'.

The file will be added.

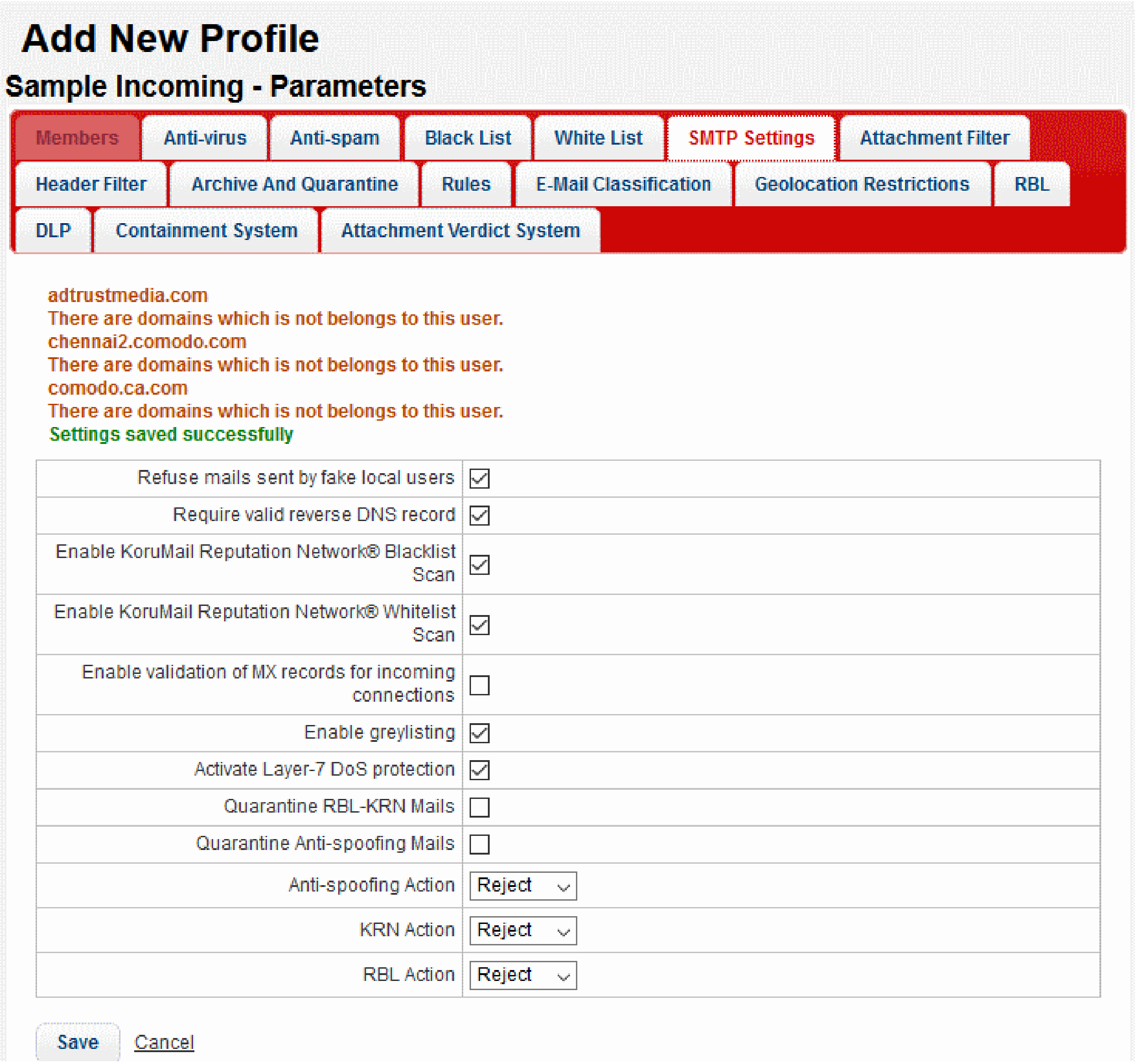


- Repeat the process to add more files.
- To remove a file, click the 'Clear' link beside it.
- To remove all the added files, click 'Clear All' at the top right.
- To import the list from the files, click 'Save' .

- To delete a whitelist type from the list, click ☒ under the 'Action' column header and click 'OK' in the confirmation screen.
- To remove all the whitelisted sources, click the 'Delete all' link and click 'OK' in the confirmation screen.

SMTP Settings

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'SMTP Settings' tab



Add New Profile

Sample Incoming - Parameters

adtrustmedia.com
There are domains which is not belongs to this user.
chennai2.comodo.com
There are domains which is not belongs to this user.
comodo.ca.com
There are domains which is not belongs to this user.
Settings saved successfully

Refuse mails sent by fake local users	☑
Require valid reverse DNS record	☑
Enable KoruMail Reputation Network® Blacklist Scan	☑
Enable KoruMail Reputation Network® Whitelist Scan	☑
Enable validation of MX records for incoming connections	□
Enable greylisting	☑
Activate Layer-7 DoS protection	☑
Quarantine RBL-KRN Mails	□
Quarantine Anti-spoofing Mails	□
Anti-spoofing Action	Reject
KRN Action	Reject
RBL Action	Reject

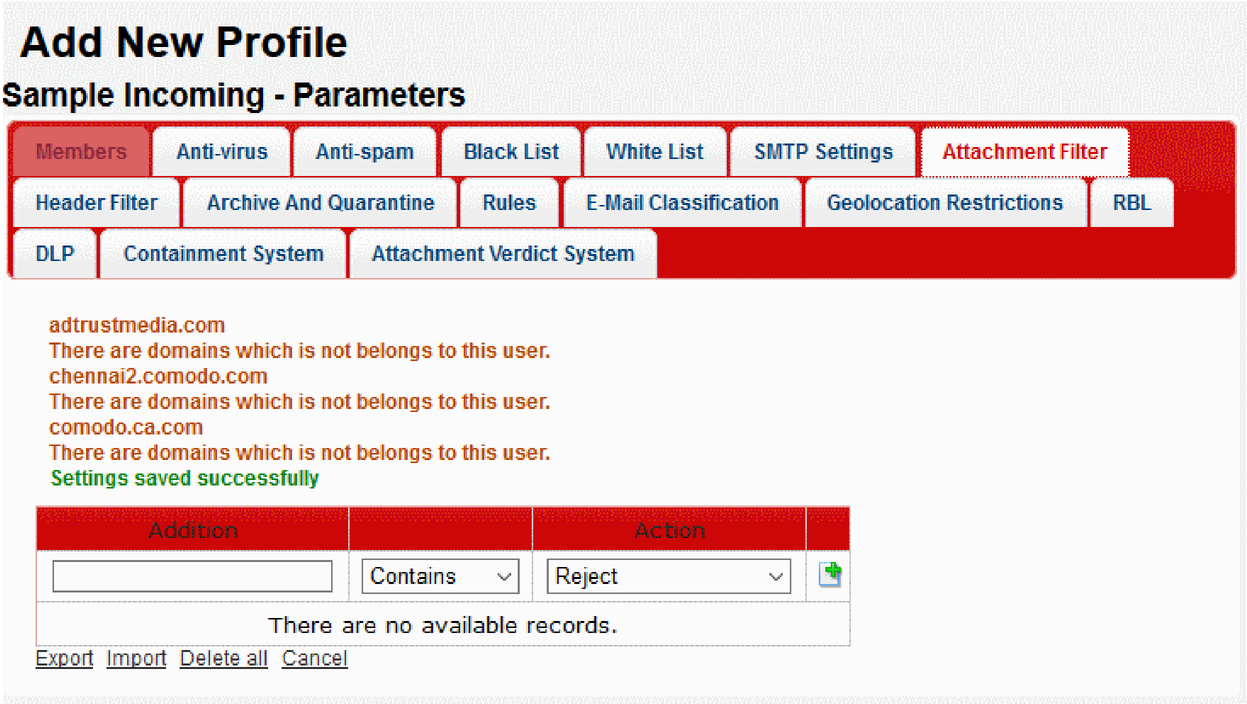
Profiles: SMTP Settings - Table of Parameters	
Parameter	**Description**
Refuse mails sent by fake local users	If enabled, KoruMail checks the 'From' details of an outgoing message with that of the added users and rejects if the users' details are not available.
Require valid reverse DNS record	If enabled, the added domains should have a valid reverse DNS record for the mails to be processed and delivered
Enable KoruMail Reputation Network® Blacklist Scan	If enabled, mails are scanned for blacklist sources listed in the KoruMail Reputation Network® (KRN) servers. Please note the KRN server setting should be **enabled** in the **KRN** module.
Enable KoruMail Reputation Network® whitelist Scan	If enabled, mails are scanned for whitelist sources listed in the KoruMail Reputation Network® (KRN) servers. Please note the KRN server setting should be **enabled** in the **KRN** module.
Enable validation of MX records for incoming connections	MX records maintain the entries of email server details to which the received emails for the protected domains are sent. If this check box is enabled, MX records for the protected will be checked and validated.

Enable greylisting	If enabled, KoruMail creates a Greylist of source IP address/domains from where emails are sent to recipients protected by its filtering engine. Mails received from a source for the first time is rejected by KoruMail and sends a command to the source to resend the email. Generally, spammers do not resend emails. If the email is sent again from the source again, KoruMail accepts the mail and initiates the filtering process.
Activate Layer-7 DoS protection	If enabled, KoruMail will activate the Layer 7 Denial of Service protection feature.
Quarantine RBL-KRN Mails	If enabled, both RBL and KRN mails mails will be Quarantined.
Quarantine Antispoofing Mails	If enabled, the spoofing mails will be Quarantined.
Anti-spoofing Action	Select the action to be performed when the condition is met for a mail. The options available are: Reject - The mail will be rejected and a reject response will be sent to the sender's mail server Discard – The mail will be rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface.
KRN Action	Select the action to be performed when the condition is met for a mail. The options available are: Reject - The mail will be rejected and a reject response will be sent to the sender's mail server Discard – The mail will be rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface.
RBL Action	Select the action to be performed when the condition is met for a mail. The options available are: Reject - The mail will be rejected and a reject response will be sent to the sender's mail server Discard – The mail will be rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface.

- Click 'Save' to apply your changes.

Attachment Filter

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Attachment Filter' tab

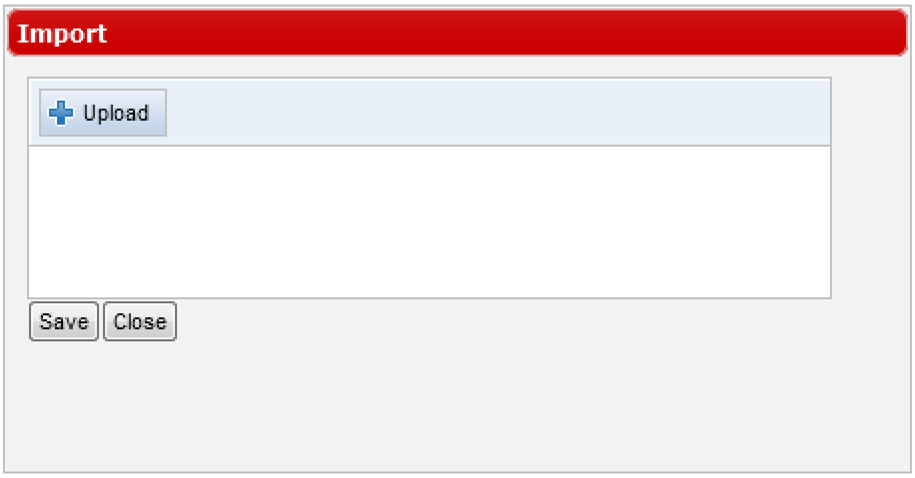


adtrustmedia.com
There are domains which is not belongs to this user.
chennai2.comodo.com
There are domains which is not belongs to this user.
comodo.ca.com
There are domains which is not belongs to this user.
Settings saved successfully

Addition		Action	
	Contains	Reject	
There are no available records.			

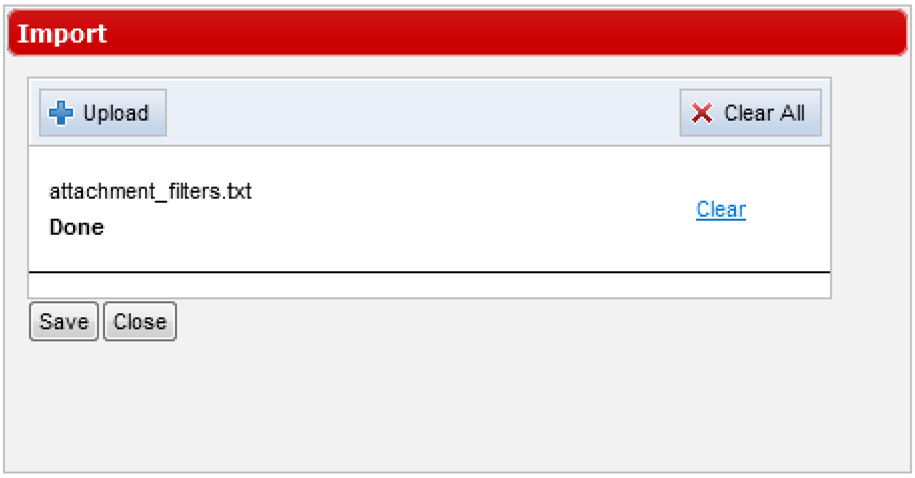
Profiles: Attachment Filter Settings - Table of Column Descriptions		
Column Header	**Description**	
Addition	Enter the keyword that should be scanned for the attachments	
Condition	Select the condition from the drop-down. The options available are: • Contains • Equals to • Starts with • Ends with	
Action	Select the action to be performed when the condition is met for an attachment in a mail. The options available are: • Reject - The mail will be rejected and a reject response will be sent to the sender's mail server • Remove attachment - The mail will be delivered to the recipient without the attachment.	
	➕	Allows administrators to add an attachment filter rule after filling the fields in the row
	✗	Allows administrators to delete attachment filter rule from the list

- To save the list of 'Attachment Filter' rules, click the 'Export' link and save it to your system
- To import a list of 'Attachment Filter' rules from a saved file, click the 'Import' link



- Click the 'Upload' button, browse to the location where the file is saved and click 'Open'.

The file will be added.



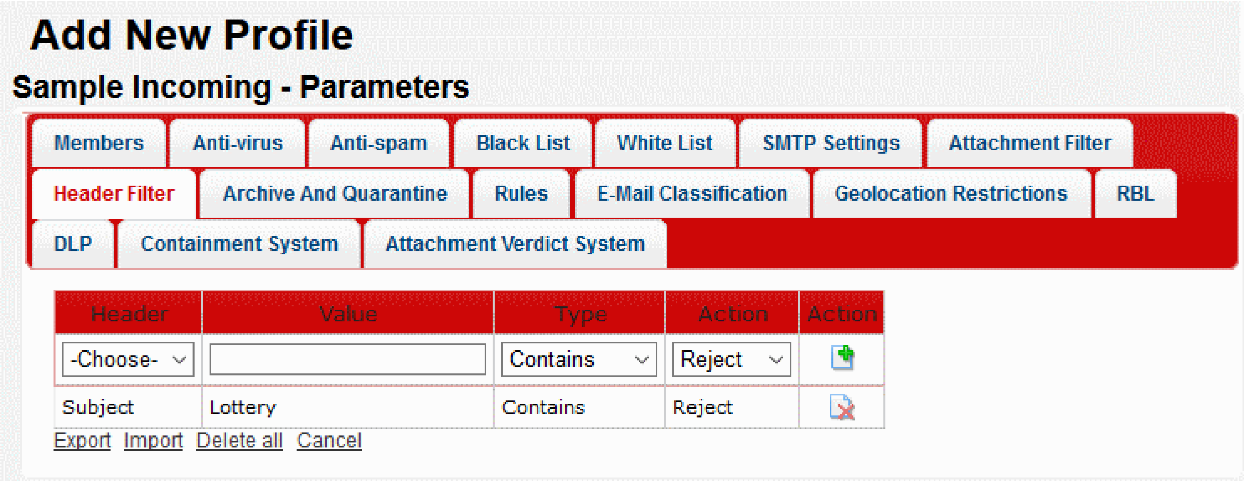
attachment_filters.txt
Done

- Repeat the process to add more files.
- To remove a file, click the 'Clear' link beside it.
- To remove all the added files, click 'Clear All' at the top right.
- To import the list from the files, click 'Save'.

- To delete an 'Attachment Filter' rule from the list, click the ☒ button under the last column and click 'OK' in the confirmation screen.
- To remove all the 'Attachment Filter' rules, click the 'Delete all' link and click 'OK' in the confirmation screen.

Header Filter

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Header Filter' tab



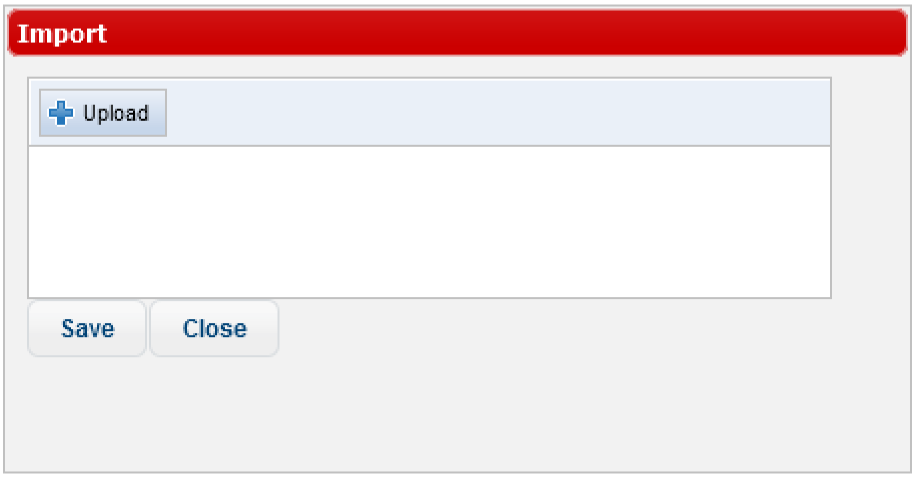
Add New Profile

Sample Incoming - Parameters

Header	Value	Type	Action	Action
-Choose-		Contains	Reject	➕
Subject	Lottery	Contains	Reject	✖

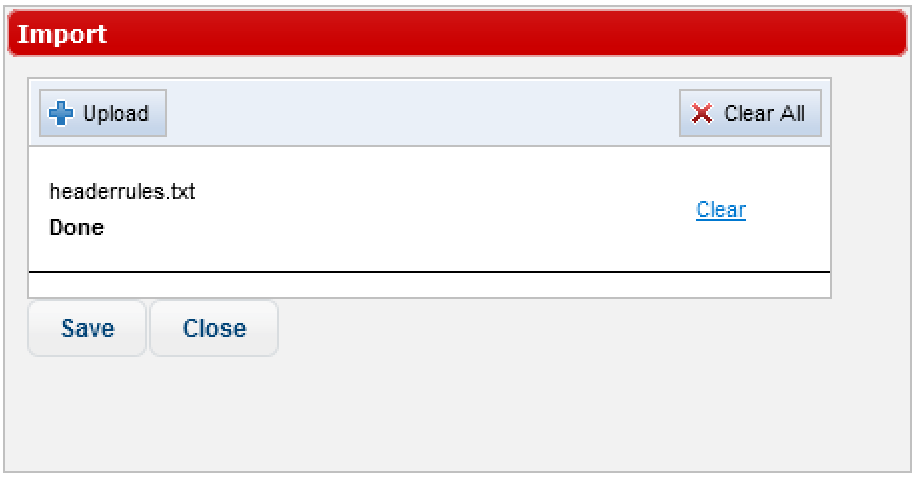
Profiles: Header Filter Settings - Table of Column Descriptions		
Column Header	**Description**	
Header	Select the header type that you want to add a 'Header Filter' rule for. The choices available are: • Subject • Received • To • From	
Value	Enter the keyword that should be scanned for the selected header type.	
Type	Select the condition from the drop-down. The options available are: • Contains • Equals to • Starts with • Ends with	
Action	Select the action to be performed when the condition is met for a 'Header Filter' rule in a mail. The options available are: • Reject - The mail will be rejected and a reject response will be sent to the sender's mail server • Discard – The mail will be rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface.	
Action	➕	Allows administrators to add a 'Header Filter' rule after filling the fields in the row.
	✖	Allows administrators to delete a 'Header Filter' rule from the list.

- To save the list of 'Header Filter' rules, click the 'Export' link and save it to your system
- To import a list of 'Header Filter' rules from a saved file, click the 'Import' link



- Click the 'Upload' button, browse to the location where the file is saved and click 'Open'.

The file will be added.



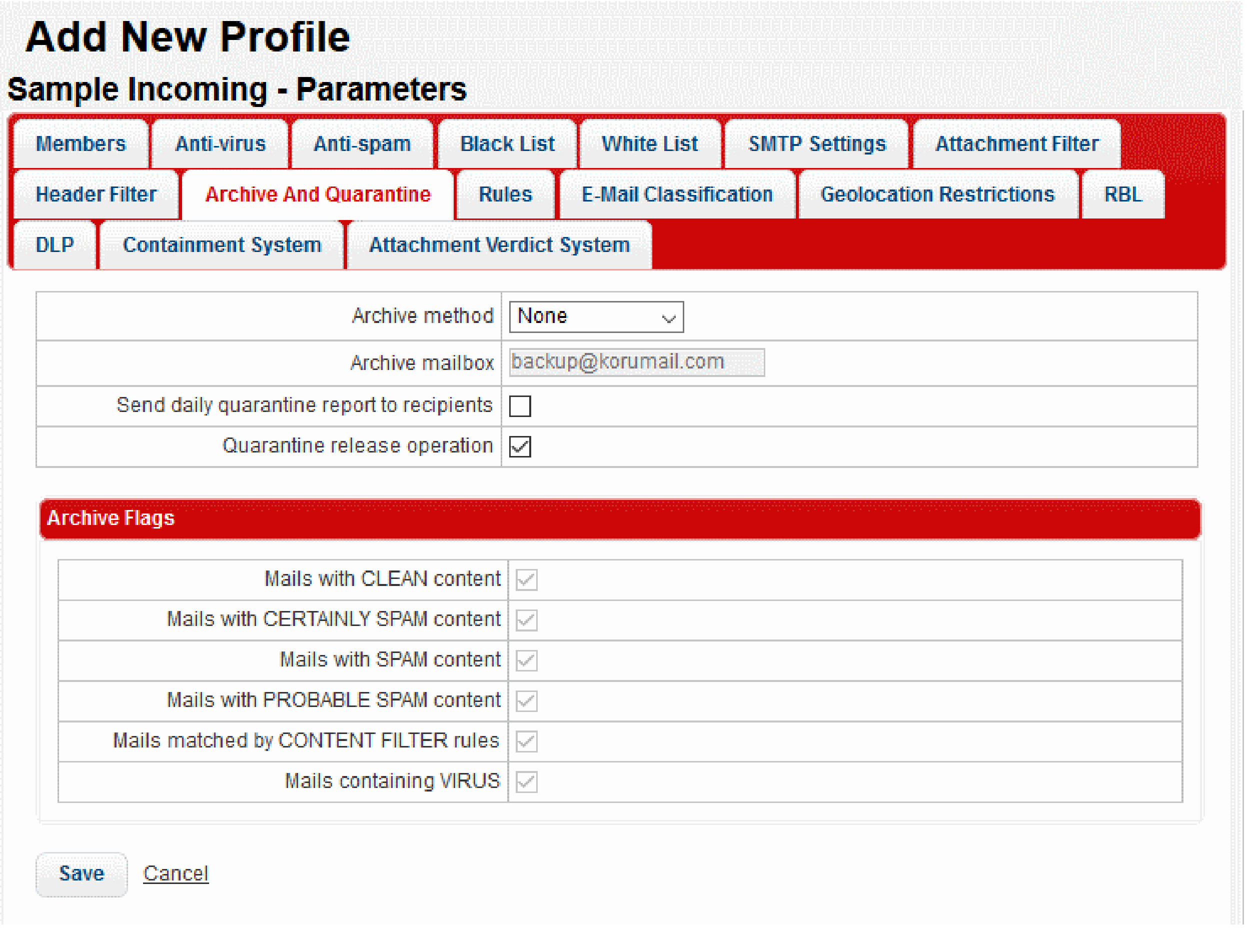
headerrules.txt
Done

- Repeat the process to add more files.
- To remove a file, click the 'Clear' link beside it.
- To remove all the added files, click 'Clear All' at the top right.
- To import the list from the files, click 'Save'.

- To delete a 'Header Filter' rule from the list, click the ☒ button under the last column and click 'OK' in the confirmation screen.
- To remove all the 'Header Filter' rules, click the 'Delete all' link and click 'OK' in the confirmation screen.

Archive and Quarantine

- Click the 'Archive and Quarantine' tab



Add New Profile

Sample Incoming - Parameters

Archive method	None
Archive mailbox	backup@korumail.com
Send daily quarantine report to recipients	□
Quarantine release operation	☑

Archive Flags

Mails with CLEAN content	☑
Mails with CERTAINLY SPAM content	☑
Mails with SPAM content	☑
Mails with PROBABLE SPAM content	☑
Mails matched by CONTENT FILTER rules	☑
Mails containing VIRUS	☑

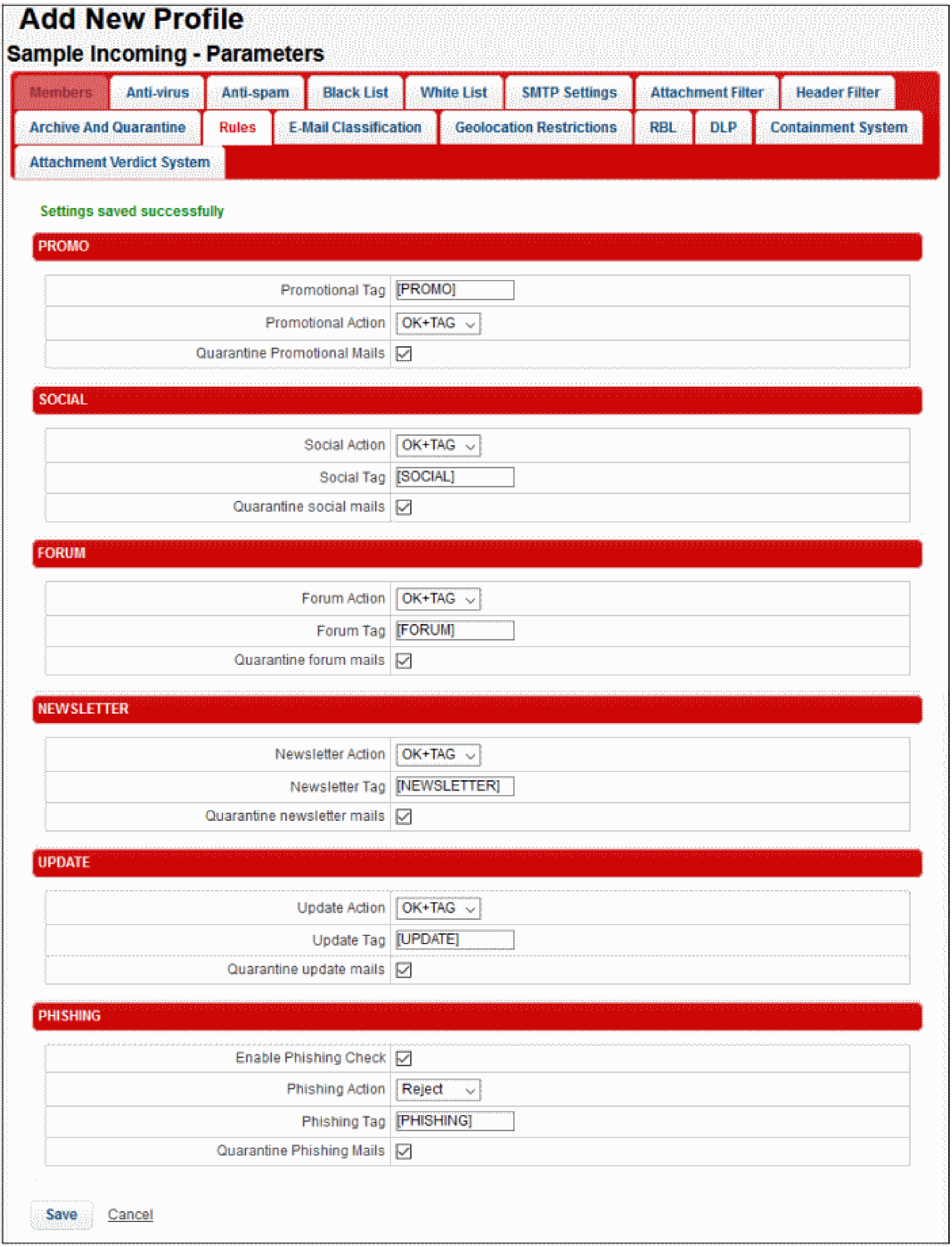
Profiles: Archive and Quarantine Settings - Table of Parameters	
Parameter	**Description**
Archive method	Select how the mails should be archived from the drop-down. The options available are: • None - The mails are not archived • Forward - The mails are forwarded to the mail address entered in the next row 'Archive mailbox' • Disk - The mails are stored in local disk • Disk + Forward - The mails are stored in local disk and a copy is forwarded to the mail address entered in the next row 'Archive mailbox' Please note the archived and quarantined mails are removed from the disk as per the configuration done in the '**Quarantine & Archive Settings**' interface.
Archive mailbox	This field becomes active only when an archive method is selected in the first row. Enter the mail address to which the archived and quarantined mails will be sent.
Send daily quarantine report to recipients	If enabled, the users will receive daily reports of their quarantined mails. Users can view their quarantined mails in the 'KoruMail Quarantine Webmail' interface by clicking the 'Quarantine Webmail' link in the 'Login' screen.
Quarantine Release Operation	Allows users to release their mails from quarantine
Archive Flags	
Mails with CLEAN content	If enabled, mails that are categorized as safe will be archived as per the 'Archive

	method' setting done in the first row.
Mails with CERTAINLY SPAM content	If enabled, mails that are categorized as 'Certainly Spam' will be archived as per the 'Archive method' setting done in the first row.
Mails with SPAM content	If enabled, mails that are categorized as 'Spam' will be archived as per the 'Archive method' setting done in the first row.
Mails with PROBABLE SPAM content	If enabled, mails that are categorized as 'Probable Spam' will be archived as per the 'Archive method' setting done in the first row.
Mails matched by CONTENT FILTER rules	If enabled, mails that are filtered for content per the settings done in '**Content Filter**' in the '**Anti-spam**' module will be archived as per the 'Archive method' setting done in the first row.
Mails containing VIRUS	If enabled, mails that are categorized are with virus will be archived as per the 'Archive method' setting done in the first row.

- Click 'Save' to apply your changes.

Rules

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Rules' tab



Add New Profile

Sample Incoming - Parameters

Settings saved successfully

PROMO

Promotional Tag	[PROMO]
Promotional Action	OK+TAG
Quarantine Promotional Mails	☑

SOCIAL

Social Action	OK+TAG
Social Tag	[SOCIAL]
Quarantine social mails	☑

FORUM

Forum Action	OK+TAG
Forum Tag	[FORUM]
Quarantine forum mails	☑

NEWSLETTER

Newsletter Action	OK+TAG
Newsletter Tag	[NEWSLETTER]
Quarantine newsletter mails	☑

UPDATE

Update Action	OK+TAG
Update Tag	[UPDATE]
Quarantine update mails	☑

PHISHING

Enable Phishing Check	☑
Phishing Action	Reject
Phishing Tag	[PHISHING]
Quarantine Phishing Mails	☑

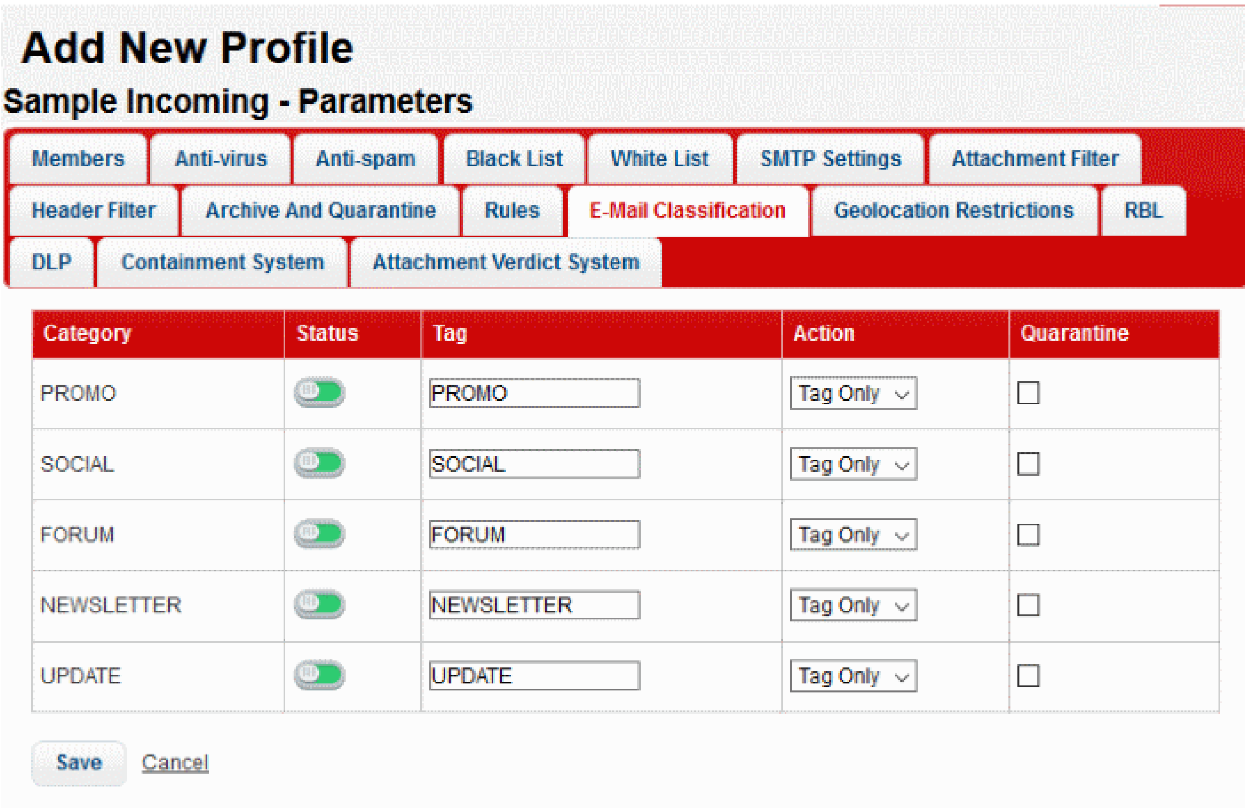
Rules Settings - Table of Parameters	
Parameter	**Description**
PROMO	
Promotion Tag	Promotional emails are sent to the recipient with the tag as entered in this field.
Promotional Action	Select the action when the condition is met for a 'Rules' setting in a promotional mail. The options available are: • OK + TAG - The tagged mail is sent to the recipient. • OK – The mail is sent to the recipient without tag • Reject - The mail is rejected and a reject response us sent to the sender mail server. • Discard - The mail is rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface.
Quarantine Promotional Mails	If enabled, promotional mails are quarantined.
SOCIAL	
Social Action	Select the action when the condition is met for a 'Rules' setting in a social mail. The options available are: • OK + TAG - The tagged mail is sent to the recipient. • OK – The mail is sent to the recipient without tag • Reject - The mail is rejected and a reject response is sent to the sender mail server. • Discard - The mail is rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface.
Social Tag	Social emails are sent to the recipient with the a tag as entered in this field.
Quarantine social mails	If enabled, social mails are quarantined
FORUM	
Forum Action	Select the action when the condition is met for a 'Rules' setting in a forum mail. The options available are: • OK + TAG - The tagged mail is sent to the recipient. • OK – The mail is sent to the recipient without tag • Reject - The mail is rejected and a reject response is sent to the sender mail server. • Discard - The mail is rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface.
Forum Tag	Forum based emails are sent to the recipient with the tag as entered in this field.
Quarantine forum mails	If enabled, forum mails are quarantined
NEWSLETTER	
Newsletter Action	Select the action when the condition is met for a 'Rules' setting in a newsletter mail.

	The options available are: • OK + TAG - The tagged mail is sent to the recipient. • OK – The mail is sent to the recipient without tag • Reject - The mail is rejected and a reject response is sent to the sender mail server. • Discard - The mail is rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface.
Newsletter Tag	Newsletter emails are sent to the recipient with the tag as entered in this field.
Quarantine newsletter mails	If enabled, newsletter mails are quarantined
UPDATE	
Update Action	Select the action when the condition is met for a 'Rules' setting in a update mail. The options available are: • OK + TAG - The tagged mail is sent to the recipient. • OK – The mail is sent to the recipient without tag • Reject - The mail is rejected and a reject response is sent to the sender mail server. • Discard - The mail is rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface.
Update Tag	Update emails are sent to the recipient with the tag as entered in this field.
Quarantine update mails	If enabled, update mails are quarantined
PHISHING	
Enable Phishing Check	If enabled, checks for phishing emails.
Phishing Action	Select the action when the condition is met for a 'Rules' setting in a phishing mail. The options available are: • OK + TAG - The tagged mail is sent to the recipient. • OK – The mail is sent to the recipient without tag • Reject - The mail is rejected and a reject response is sent to the sender mail server. • Discard - The mail is rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface.
Phishing Tag	Phishing emails are sent to the recipient with the a tag as entered in this field.
Quarantine Phishing Mails	If enabled, phishing mails are quarantined.

- Click 'Save' to apply your changes.

Email Classification

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Email Classification' tab



Add New Profile

Sample Incoming - Parameters

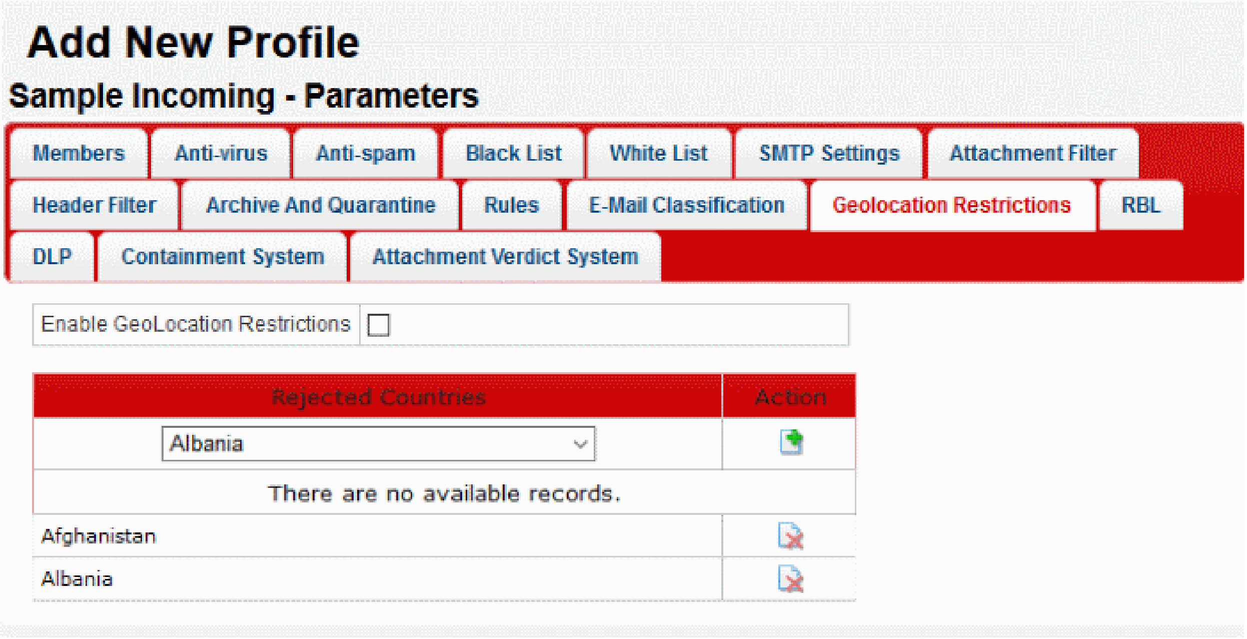
Category	Status	Tag	Action	Quarantine
PROMO	●	PROMO	Tag Only	□
SOCIAL	●	SOCIAL	Tag Only	□
FORUM	●	FORUM	Tag Only	□
NEWSLETTER	●	NEWSLETTER	Tag Only	□
UPDATE	●	UPDATE	Tag Only	□

Category	The type of mail received.
Status	Whether the rule is enabled or not.
Tag	The name prefixed to the email to show the email classification. For example, promotional email subjects are prefixed with [PROMO].
Action	Select the action to be performed when the condition is met for a 'Rules' setting in a forum mail. The options available are: • Discard - The mail will be rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface. • TAG Only - The tagged mail will be sent to the recipient. • Reject - The mail will be rejected and a reject response will be sent to the sender mail server. • OK - The mail will be sent to the recipient without tag.
Quarantine	If enabled, the corresponding category of mails will be quarantined

- Click 'Save' to apply your changes.

Geolocation Restrictions

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Geolocation Restrictions' tab



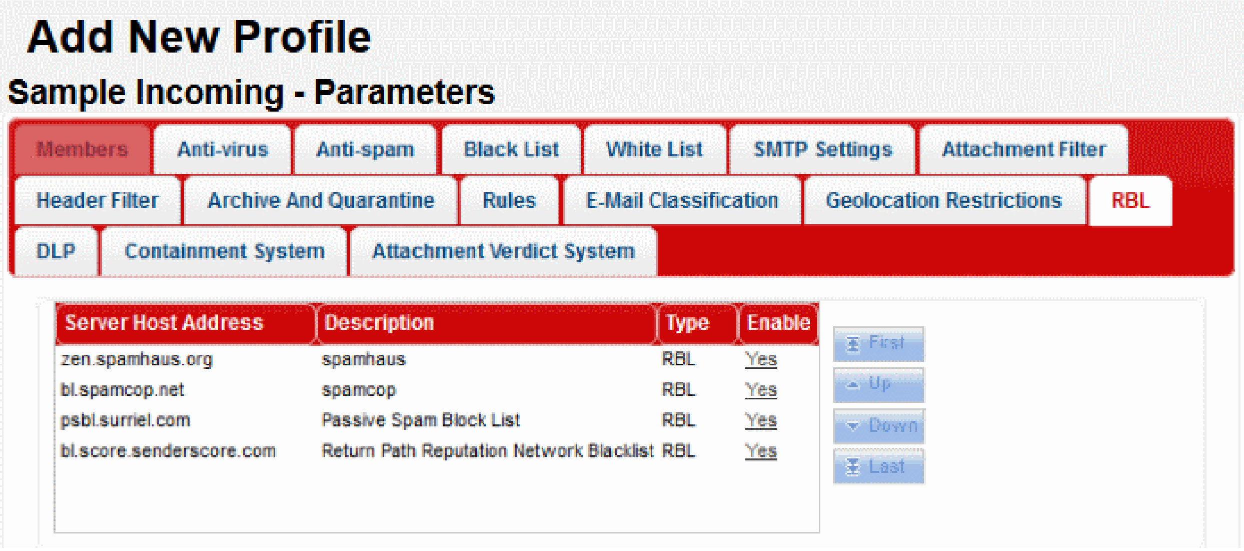
Enable GeoLocation Restrictions □

Rejected Countries	Action
Albania	
There are no available records.	
Afghanistan	
Albania	

Profiles: Geolocation Restrictions Settings - Table of Column Descriptions		
Column Header	**Description**	
Rejected Countries	Select the country you want Korumail to reject. Please note that you have to enable SMTP > General settings.	
Action		Allows administrators to add a country after selecting it in the row.
		Allows administrators to delete the country from the list.

Realtime Blackhole List (RBL)

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'RBL' tab

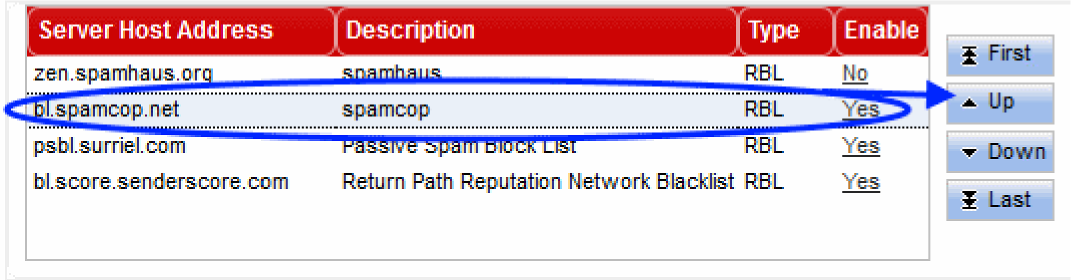


Server Host Address	Description	Type	Enable
zen.spamhaus.org	spamhaus	RBL	Yes
bl.spamcop.net	spamcop	RBL	Yes
psbl.surriel.com	Passive Spam Block List	RBL	Yes
bl.score.senderscore.com	Return Path Reputation Network Blacklist	RBL	Yes

The screen displays the RBL servers that are available by default and added manually. See '**Manage RBL Servers**' for more details.

RBL Servers - Table of Column Descriptions	
Column Header	**Description**
Server Host Address	The address of the RBL server.
Description	The description provided at the time of adding the RBL server.
Type	The type of block list selected.
Enable	Allows administrators to activate or deactivate a RBL server in the list. If a server is disabled, KoruMail skips it and refers to the next server in the line.

The control buttons next to the table allows to reorder the RBL server list for checking the blacklisted IP addresses available in the servers. The enabled RBL server listed first will be checked first and move down the order. Use the control buttons to move a server up or down the order.

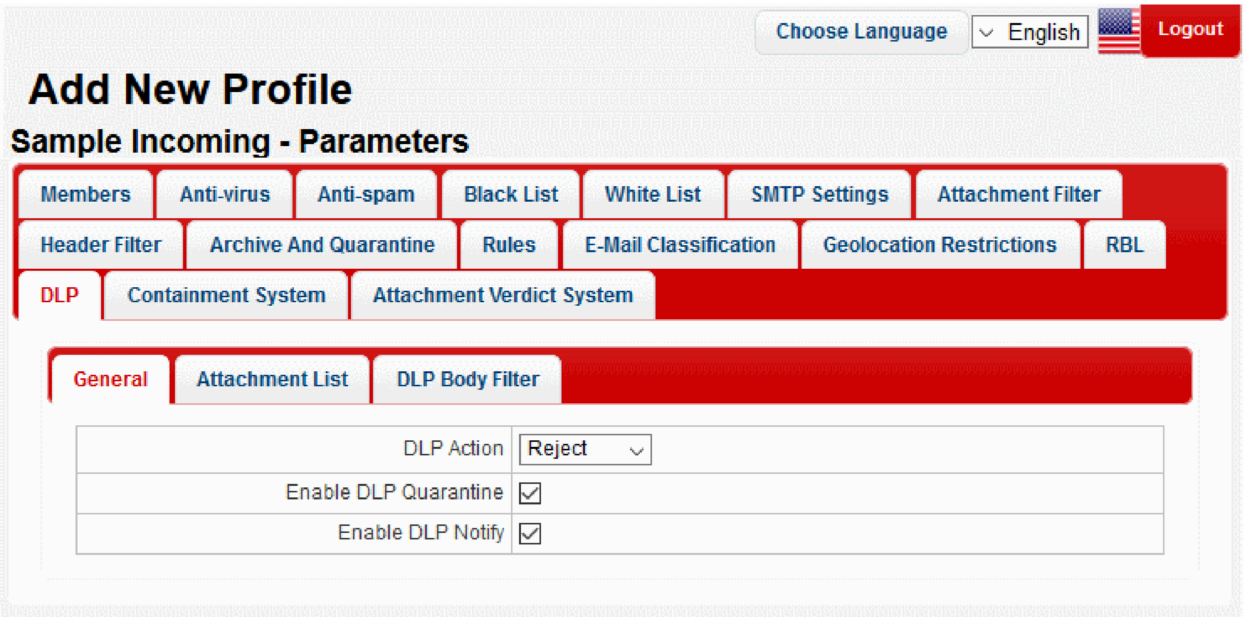


Server Host Address	Description	Type	Enable
zen.spamhaus.org	spamhaus	RBL	No
bl.spamcop.net	spamcop	RBL	Yes
psbl.surriel.com	Passive Spam Block List	RBL	Yes
bl.score.senderscore.com	Return Path Reputation Network Blacklist	RBL	Yes

Data Leak Prevention (DLP)

The DLP feature is capable of scanning mails for important key words such as credit card, social security numbers, attachments and takes action as per the settings. Please note that the DLP module should be enabled for the settings configured here to take effect. See '**Data Leak Prevention**' for more details.

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'DLP' tab

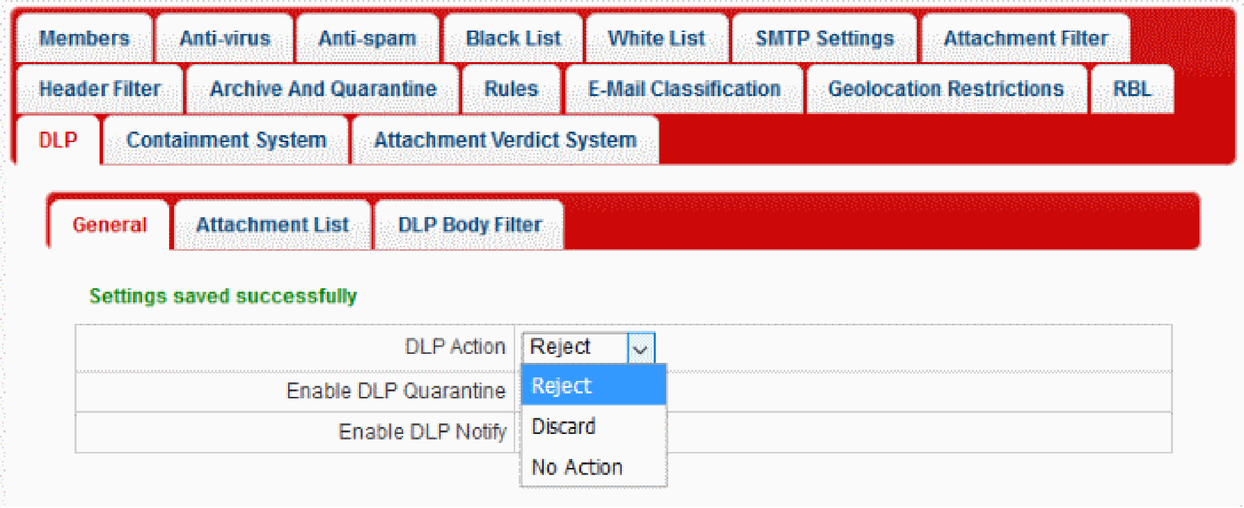


Add New Profile

Sample Incoming - Parameters

DLP Action	Reject
Enable DLP Quarantine	☑
Enable DLP Notify	☑

DLP General Settings



Settings saved successfully

DLP Action	Reject
Enable DLP Quarantine	
Enable DLP Notify	

- **DLP Action** - These settings determine what action should be taken if KoruMail detects a message that could present a data leak.

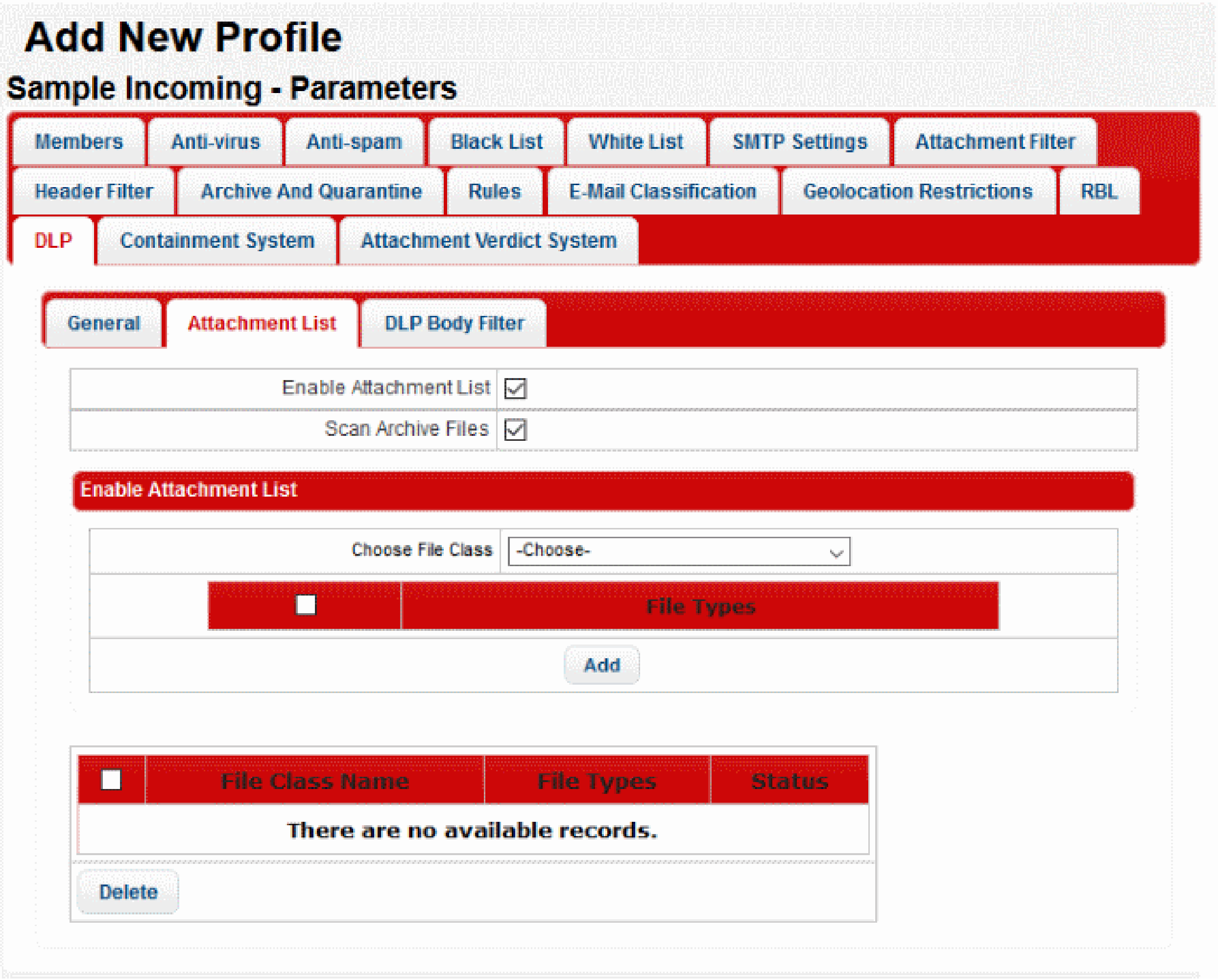
The options available are:

  - **No Action** - The mail will be allowed and the system admin will be notified if 'DLP Notify' is enabled.
  - **Reject** - The mail will be rejected and a reject warning will be sent to the sender's email address.
  - **Discard** - The mail will be deleted and if 'DLP Quarantine' is enabled, it will be quarantined and the system admin will be notified.

- **Enable DLP Quarantine** – If selected, KoruMail quarantines mails with data leak. Please note the setting in 'DLP Action' should be 'Discard' for mails to be quarantined.
- **Enable DLP Notify** – If selected, KoruMail alerts the system admin about DLP breaches.

Attachment List

- Click the 'Attachment List' tab



Add New Profile

Sample Incoming - Parameters

Enable Attachment List	☑
Scan Archive Files	☑

Enable Attachment List

Choose File Class: -Choose-

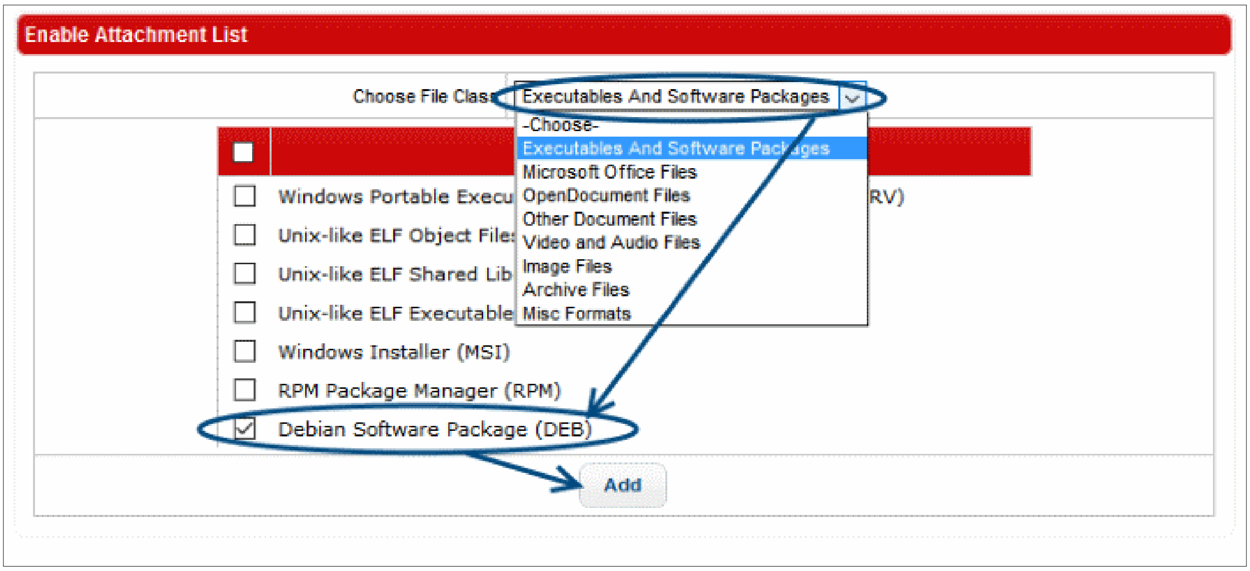
□	File Types

□	File Class Name	File Types	Status
There are no available records.			

- **Enable Attachment List** - Select the check box to block emails with attachment file class defined below in the table.
- **Scan Archive Files** - Select the check box to scan the attached zip files and block emails with attachment file class defined below in the table.

To add a file class

- Select the file class from the 'Choose File Class' drop-down



Enable Attachment List

Choose File Class: Executables And Software Packages

□ Windows Portable Execu… RV)

□ Unix-like ELF Object File…

□ Unix-like ELF Shared Lib…

□ Unix-like ELF Executable…

□ Windows Installer (MSI)

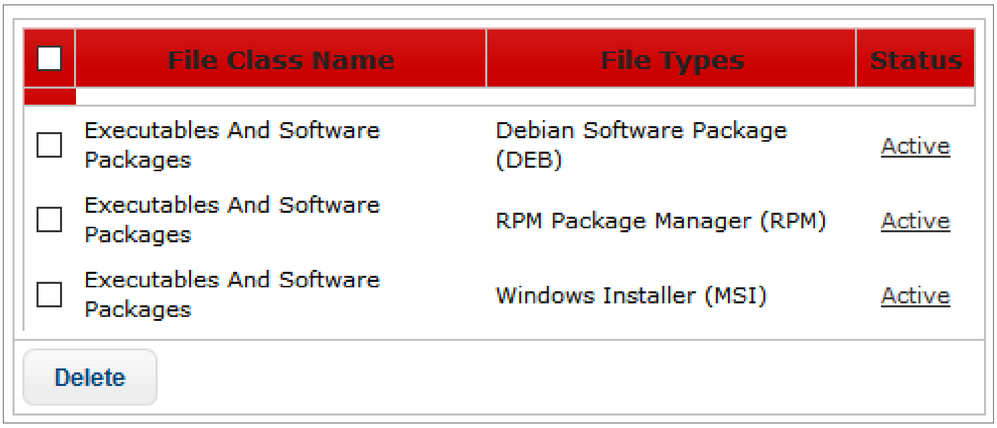
□ RPM Package Manager (RPM)

☑ Debian Software Package (DEB)

The file types for the selected file class will be displayed on the right side table.

- Select the file type or the check box above to select all the file types and click the 'Add' button beside it.

The added file types for the selected file class will be displayed in the table below the first table.



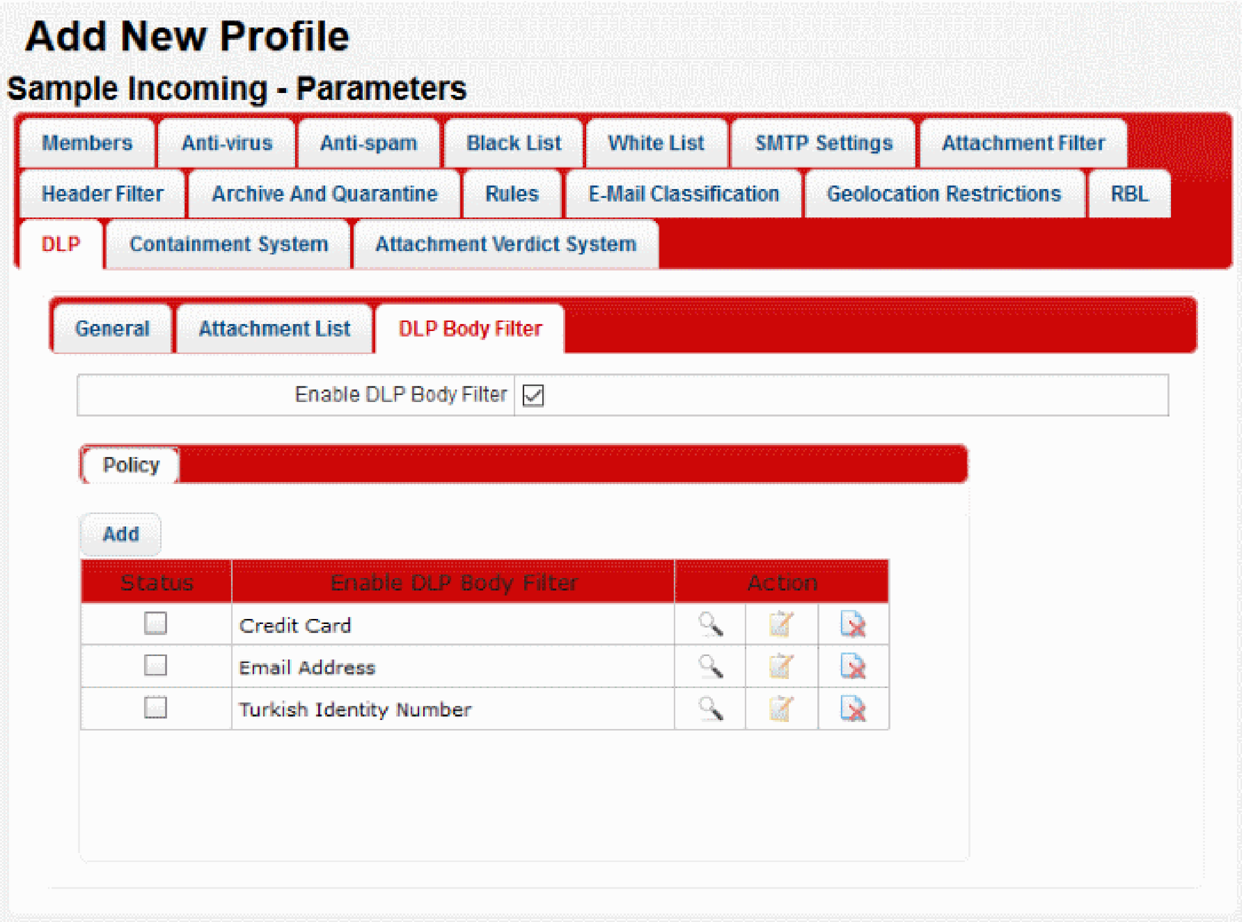
□	File Class Name	File Types	Status
□	Executables And Software Packages	Debian Software Package (DEB)	Active
□	Executables And Software Packages	RPM Package Manager (RPM)	Active
□	Executables And Software Packages	Windows Installer (MSI)	Active

- Clicking the link beside a file type under the 'Status' column header toggles the status between 'Active' and 'Passive'. 'Active' status indicates emails with attached file type will be blocked.
- To delete a file type from the list, select it and click the 'Delete' button. To delete all file types, select the check box beside 'File Class Name' column header and click the 'Delete button.

DLP Body Filter

The 'DLP Body Filter' feature searches the content of an email for sensitive information such as credit card details, email address and so on and take action as per the settings done in 'DLP Action'. KoruMail comes with three predefined DLP Body Filters and allows the administrators to add more filters as required.

- **Enable DLP Body Filter**: Select the check box to apply the configured body filters



Add New Profile

Sample Incoming - Parameters

Enable DLP Body Filter ☑

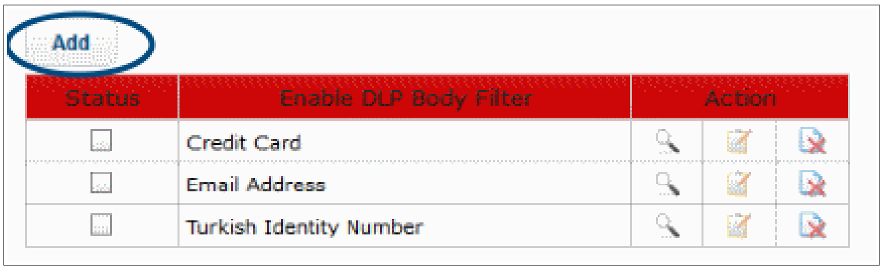
Status	Enable DLP Body Filter	Action		
□	Credit Card	🔍	📝	❌
□	Email Address	🔍	📝	❌
□	Turkish Identity Number	🔍	📝	❌

Profiles: DLP Body Filter Settings - Table of Column Descriptions

Column Header	Description	
Status	Select the check box to enable the filter.	
Enable DLP Body Filter	The name of the filter.	
Action	🔍	Allows to view the details of the body filter.
	📝	Allows to edit a body filter.
	❌	Allows to delete a body filter.

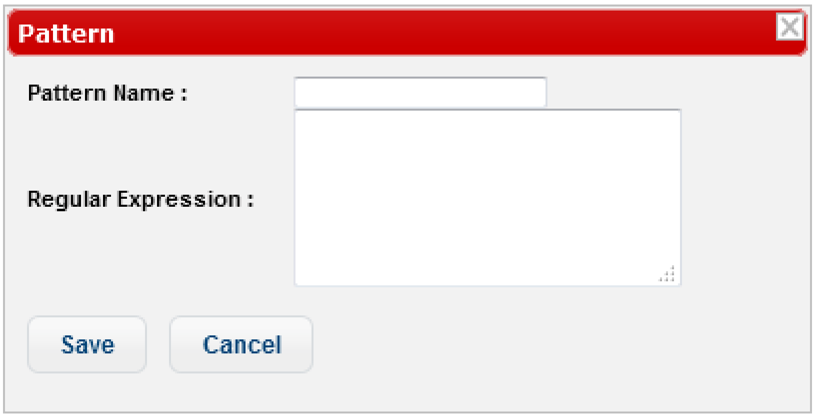
To add a new DLP body filter

- Click the 'Add' button at the top of the table



Status	Enable DLP Body Filter	Action		
□	Credit Card			
□	Email Address			
□	Turkish Identity Number			

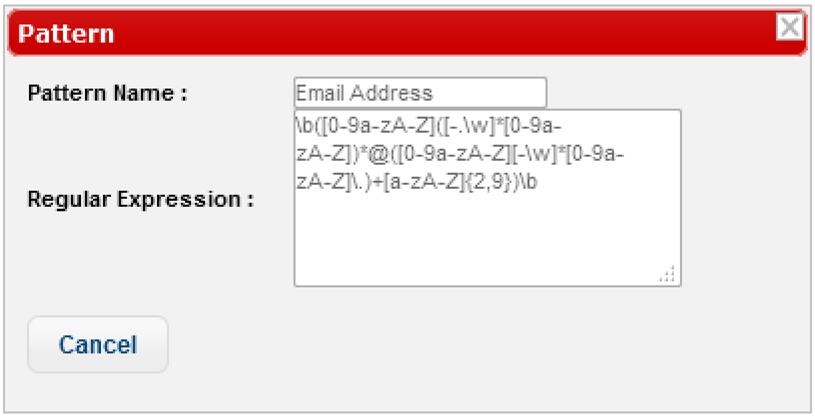
The filter 'Pattern' screen will be displayed.



- **Pattern Name**: Enter the name of the filter pattern
- **Regular Expression**: Enter the regular expression to define the search pattern. To know more about Regular Expression, see Wikipedia at **http://en.wikipedia.org/wiki/Regular_expression**. You can also enter keywords in the field to search and block the email containing it.

To view the details of a pattern

- Click the 🔍 icon beside a body filter that you want to view the details



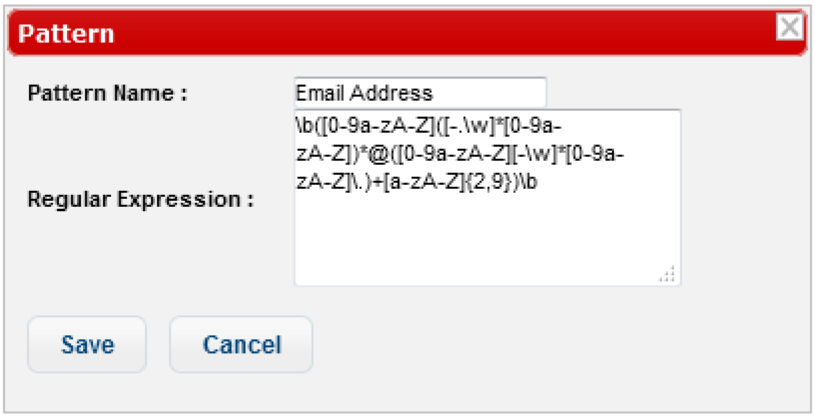
Pattern Name : Email Address

Regular Expression : \b([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])*@([0-9a-zA-Z][-\w]*[0-9a-zA-Z]\.)+[a-zA-Z]{2,9})\b

- Click the 'Cancel' button or close the dialog to return to main screen.

To edit a body filter

- Click the 📝 icon beside a body filter that you want to edit the details



Pattern Name : Email Address

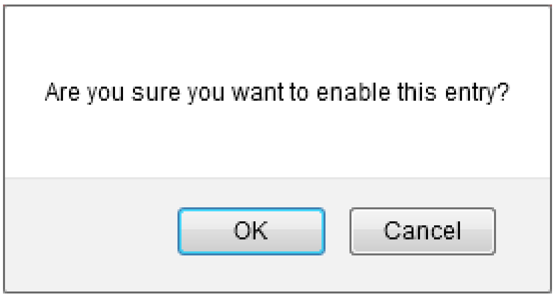
Regular Expression :

```
\b([0-9a-zA-Z]([-.\w]*[0-9a-
zA-Z])*@([0-9a-zA-Z][-\w]*[0-9a-
zA-Z]\.)+[a-zA-Z]{2,9})\b
```

- Edit the details as required and click the 'Save' button

To delete a body filter

- Click the ❌ icon beside a body filter that you want to delete

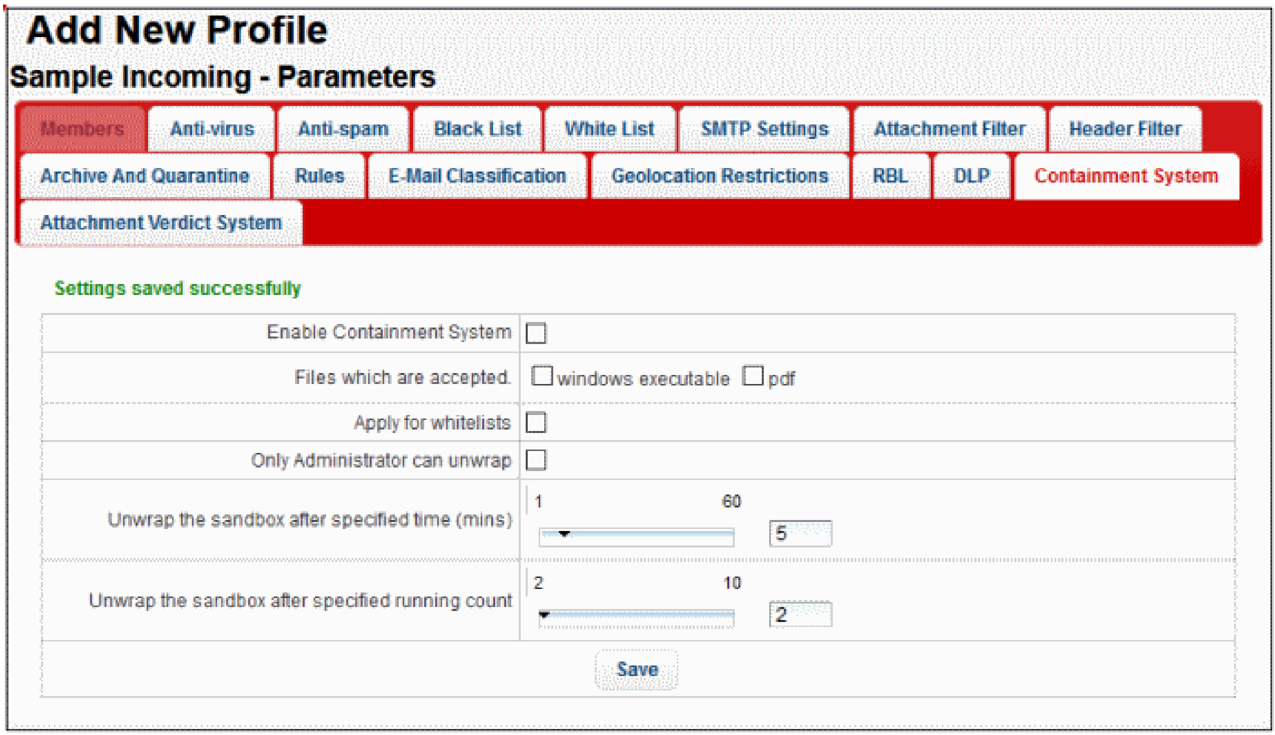


Are you sure you want to enable this entry?

- Click 'OK' to confirm the deletion.

Containment System

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Containment System' tab



Add New Profile

Sample Incoming - Parameters

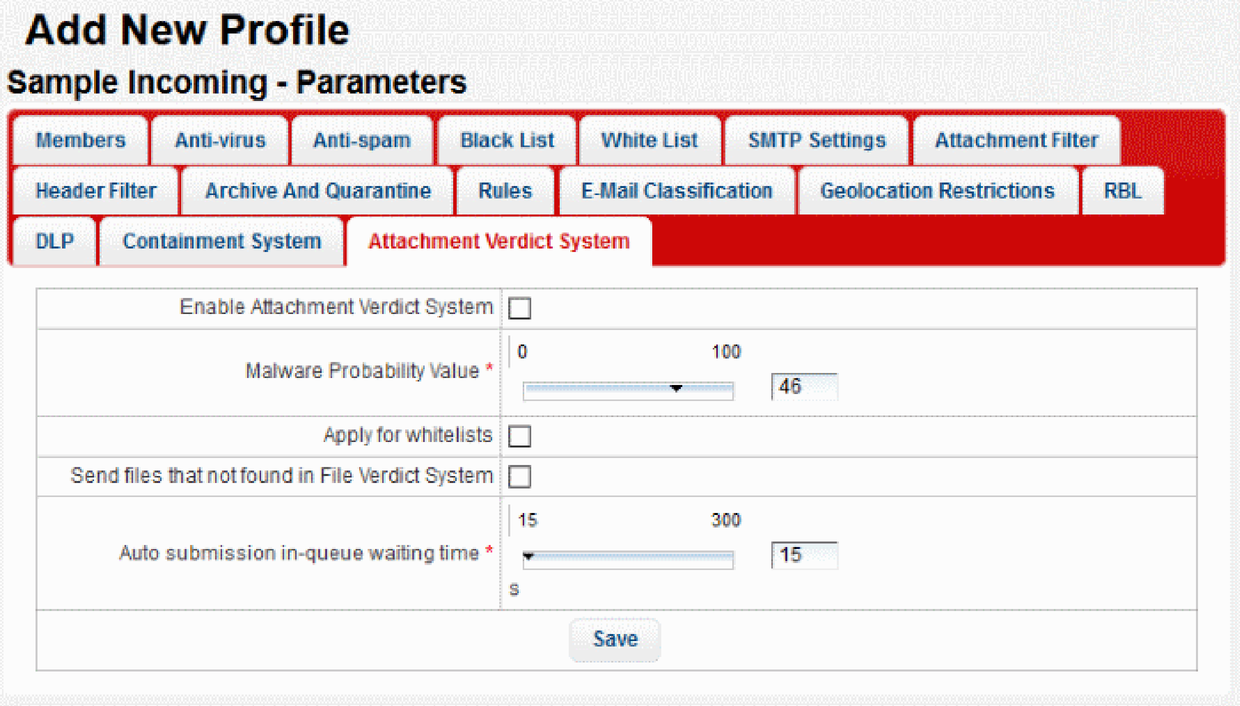
Settings saved successfully

Enable Containment System	□
Files which are accepted.	□ windows executable □ pdf
Apply for whitelists	□
Only Administrator can unwrap	□
Unwrap the sandbox after specified time (mins)	1 – 60: 5
Unwrap the sandbox after specified running count	2 – 10: 2

Containment System - Table of Column Headers	
Column Header	**Description**
Enable Containment System	If enabled, email attachments (pdfs and windows executables) will be 'wrapped' with containment code before delivery. This means they will open in an isolated, virtual environment known as the container, instead of directly on the endpoint. The attachment will open as normal from the end-user's point-of-view, but it will not be allowed to access important system files, user data or to cause damage to the host system.
Files which are accepted	If enabled, will deliver files in the chosen format
Apply for whitelists	If enabled, KoruMail will also analyze white-listed sources.
Only Administrator can unwrap	Safe files in the containment when run are unwrapped immediately for both users and admins. Malicious files are blocked. Contained files for which results are unsure (not safe nor malicious) are unwrapped if specified time or count (mentioned in rows below) is reached. If this setting is: • Enabled - Only admins can unwrap contained files for which results are unsure (not safe nor malicious) • Disabled – Both admins and users can unwrap contained files for which results are unsure (not safe nor malicious)
Unwrap the sandbox after specified time (mins)	Unsure files (not safe nor malicious) when run are moved out of containment after the specified time. Move the slider to set the time.
Unwrap the sandbox after specified running count	Unsure files (not safe nor malicious) when opened 'X' times as specified here are moved out of containment. Move the slider to set the count.

Attachment Verdict System

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Attachment Verdict System' tab



Add New Profile

Sample Incoming - Parameters

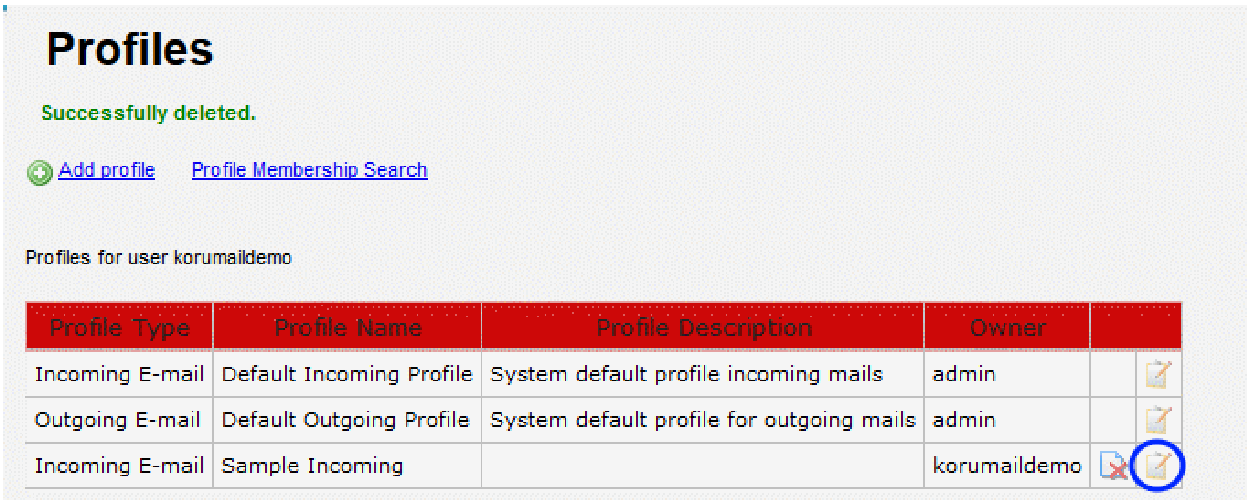
Enable Attachment Verdict System	□
Malware Probability Value *	0 100 46
Apply for whitelists	□
Send files that not found in File Verdict System	□
Auto submission in-queue waiting time *	15 300 15 s

Profiile: Attachment Verdict System - Table of Column Headers	
Column Header	**Description**
Enable Attachment Verdict System	• If enabled, Korumail will automatically check the trust rating of Windows executables and pdf files in Comodo's file look up server (FLS). • The verdict from the FLS can be ‘Clean’, ‘Malware’ or ‘Unknown’. • Clean attachments will be allowed to proceed while malware attachments will be automatically quarantined (providing ‘Quarantine mails containing viruses’ is enabled in the antivirus section of the profile). • ‘Unknown’ files will be submitted to Comodo’s real-time file analysis system, Valkyrie, for behavior testing. • Valkyrie’s tests will determine whether the unknown file is clean or malware and apply the appropriate action as mentioned above.
Malware Probability Value	• The threshold at which Korumail will designate an unknown file as 'malware' based on Valkyrie results. • Comodo recommend that administrators leave this setting at the default and only move it after consultation with Comodo support. • Valkyrie examines the behavior of unknown files and assigns a score indicating how likely it is that the file is malware. • Under the default settings, a score of 46+ is classed as malware. • Raising the value in this slider means KoruMail is more tolerant/less likely to class attachments as malware.
Apply for whitelists	When enabled, Korumail sandboxes clean mails as well
Send files that not found in	If enabled, Korumail will upload files rated 'Unknown', to the attachment verdict system

File Verdict System	for detailed behavior analysis
Auto-submission in queue waiting time	Define in seconds how long Korumail should wait before the submission times-out.

9.1.1 Edit a Profile

- Click 'Profile Management' > 'Profiles'
- Click the 📝 icon beside a profile in the 'Profiles' screen that you want to edit the details



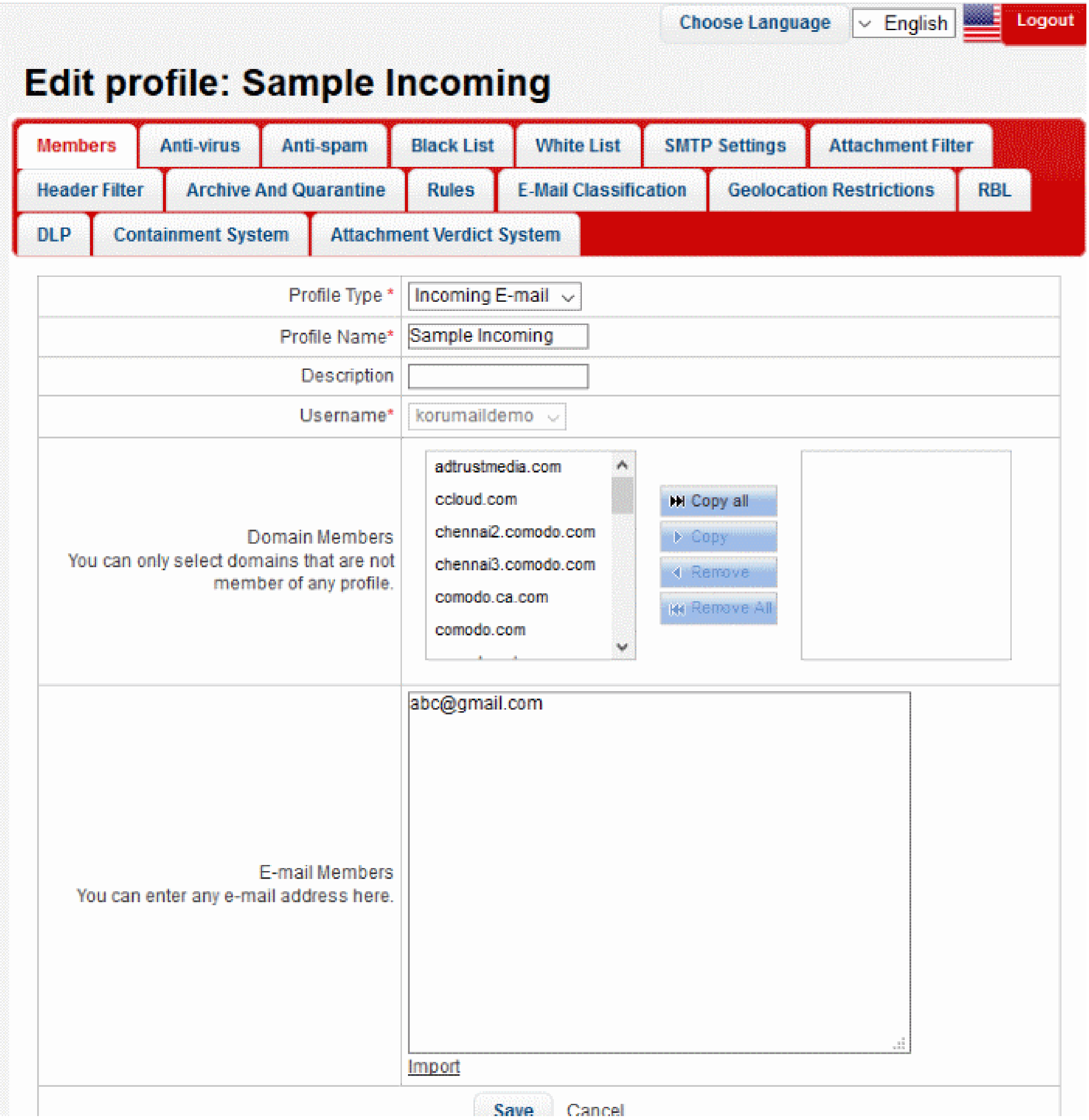
Profiles

Successfully deleted.

Profiles for user korumaildemo

Profile Type	Profile Name	Profile Description	Owner	
Incoming E-mail	Default Incoming Profile	System default profile incoming mails	admin	📝
Outgoing E-mail	Default Outgoing Profile	System default profile for outgoing mails	admin	📝
Incoming E-mail	Sample Incoming		korumaildemo	✕ 📝

The 'Edit Profile' screen will open



Edit profile: Sample Incoming

Profile Type * : Incoming E-mail

Profile Name* : Sample Incoming

Description :

Username* : korumaildemo

Domain Members
You can only select domains that are not member of any profile.

adtrustmedia.com
ccloud.com
chennai2.comodo.com
chennai3.comodo.com
comodo.ca.com
comodo.com

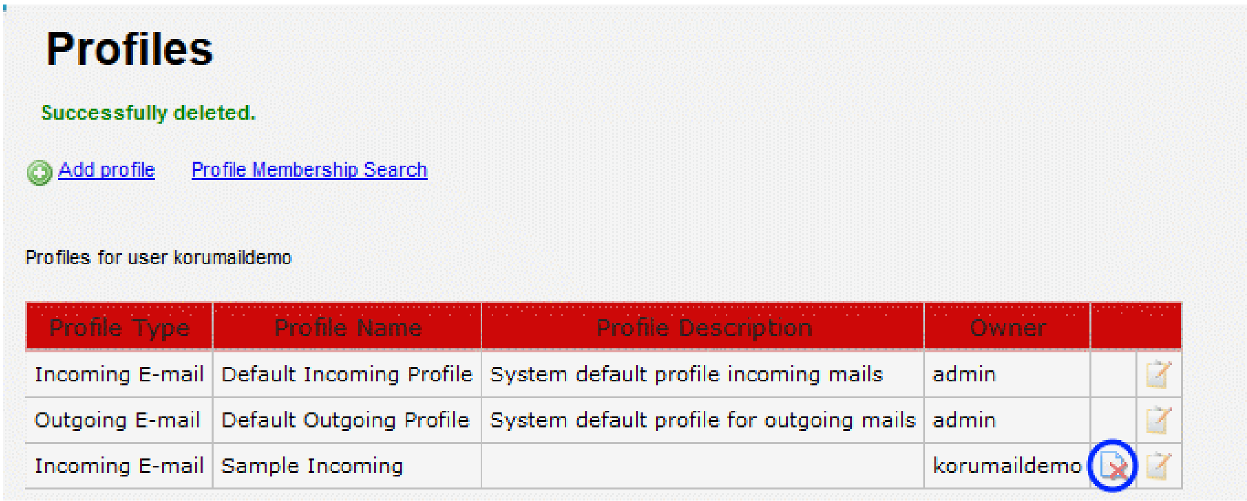
E-mail Members
You can enter any e-mail address here.

abc@gmail.com

- Edit the parameters as required. The procedure is similar to adding a new profile. See '**Add and Configure a New Profile**' for more details.

9.1.2 Delete a Profile

- Click 'Profile Management' > 'Profiles'
- Click the ✗ icon beside a profile in the 'Profiles' screen that you want to delete from the list.



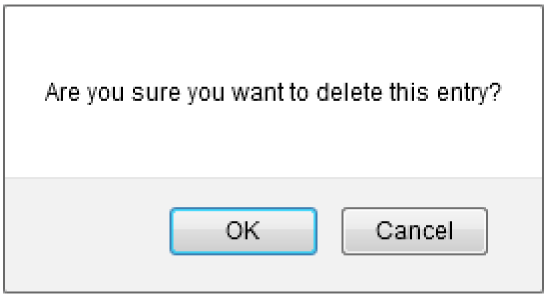
Profiles

Successfully deleted.

Profiles for user korumaildemo

Profile Type	Profile Name	Profile Description	Owner		
Incoming E-mail	Default Incoming Profile	System default profile incoming mails	admin		
Outgoing E-mail	Default Outgoing Profile	System default profile for outgoing mails	admin		
Incoming E-mail	Sample Incoming		korumaildemo		

- Click 'OK' to confirm the deletion.



Are you sure you want to delete this entry?

Note - if an incoming or outgoing profile is deleted, the default profile will be applied to the domain.

10 Reports

- The 'Reports' section lets you view and generate comprehensive activity reports on domains protected by KoruMail.
- There are multiple types of report you can view. Click the following links to find out more on each.
  - **Mail Logs Report**
  - **SMTP Queue Report**
  - **Delivery Logs Report**
  - **SMTP-AUTH Logs Report**
  - **Summary Report**
  - **Domain Report**
  - **Attachment Verdict Reports**
  - **Original Mail Request List**

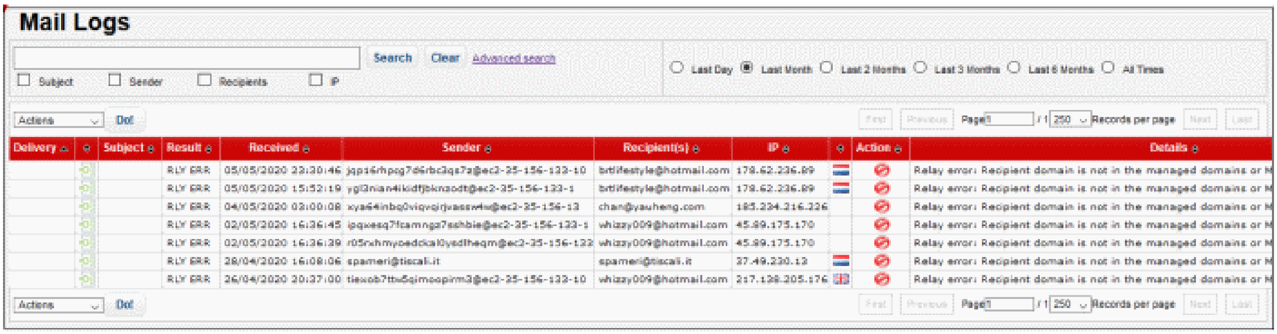
10.1 Mail Logs Report

- The 'Mail Log' report provides details of incoming and outgoing mails for all domains that have been added to KoruMail.
- The logs show the subject of the mail, date and time received by KoruMail, the result of the filtering process

and more.

To open the 'Mail Logs' interface

- Click 'Reports' > 'Mail Logs'



Mail Logs

Search | Clear | Advanced search

□ Subject □ Sender □ Recipients □ IP

○ Last Day ● Last Month ○ Last 2 Months ○ Last 3 Months ○ Last 6 Months ○ All Times

Actions | Do!

First | Previous | Page 1 / 1 | 250 | Records per page | Next | Last

Delivery		Subject	Result	Received	Sender	Recipient(s)	IP		Action	Details
			RLY ERR	05/05/2020 22:20:46	jqps6rhpcg7d6rbc3qs7s@ec2-35-156-133-10	brtlifestyle@hotmail.com	178.62.236.89		⊘	Relay error: Recipient domain is not in the managed domains or M
			RLY ERR	05/05/2020 15:52:19	ygl3nian4ikidfjbknaodt@ec2-35-156-133-1	brtlifestyle@hotmail.com	178.62.236.89		⊘	Relay error: Recipient domain is not in the managed domains or M
			RLY ERR	04/05/2020 02:00:08	xya64inbq0viqvqirjvassw4w@ec2-35-156-13	chan@yauheng.com	185.224.216.226		⊘	Relay error: Recipient domain is not in the managed domains or M
			RLY ERR	02/05/2020 16:36:45	ipqxesq7fcamngz7sshbie@ec2-35-156-133-1	whizzy009@hotmail.com	45.89.175.170		⊘	Relay error: Recipient domain is not in the managed domains or M
			RLY ERR	02/05/2020 16:36:39	r05rxhmyoedckal0yedlheqm@ec2-35-156-133	whizzy009@hotmail.com	45.89.175.170		⊘	Relay error: Recipient domain is not in the managed domains or M
			RLY ERR	28/04/2020 16:08:06	spameri@tiscali.it	spameri@tiscali.it	37.49.230.13		⊘	Relay error: Recipient domain is not in the managed domains or M
			RLY ERR	26/04/2020 20:37:00	tiexob7ttw5qimoopirm3@ec2-35-156-133-10	whizzy009@hotmail.com	217.138.205.176		⊘	Relay error: Recipient domain is not in the managed domains or M

Actions | Do!

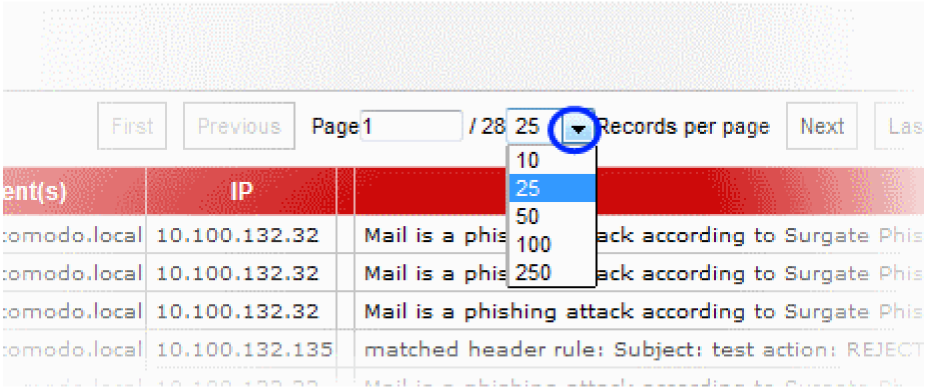
First | Previous | Page 1 / 1 | 250 | Records per page | Next | Last

Mail Logs Report - Table of Column Descriptions	
Column Header	**Description**
Delivery	Indicates the status of mail delivery. The statuses are: • Success • Temporary Error • Permanent Error
Icon	The arrow icon indicates whether the mail is incoming or outoing
Subject	The content of the email subject line.
Result	The verdict on a email after filtering. For example, 'CSPAM' means KoruMail found the mail was 'Certainly Spam'.
Received	Date and time KoruMail received the email.
Sender	Email address information of the originator
Recipient(s)	Domain name of the receiver
IP	The network address of the system from where the mail was sent. The next column displays the flag of the originating country.
Action	Status of the mail after filtering. Place your mouse over an icon to view a description of the action. ✔ - Relayed: The mail successfully passed the filtering process and was passed onto the target mail server. ⊘ - Rejected: The mail was not accepted by KoruMail. A rejection message was sent to the sender. ⊗ - Discarded: Quarantined mail. ↻ - Delayed: Indicates the source is **greylisted**.
Details	Reason why a particular action was taken on a mail. For example, why it was rejected, delayed etc.

At the top and bottom of the screen, you have the option to set the number of records to be displayed per page and export the report in CSV format.

To configure the number of records to be displayed per page

- Click the 'Records per page' drop-down

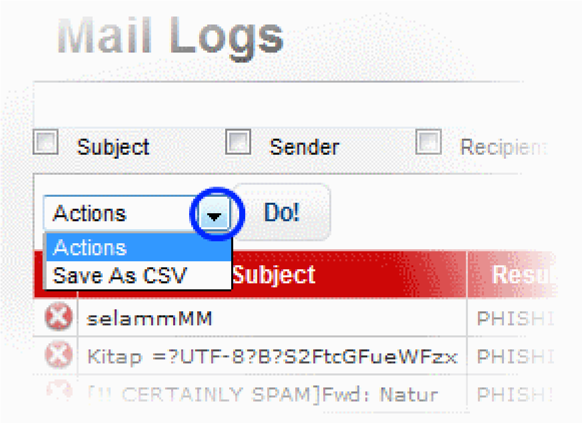


ent(s)	IP	
:omodo.local	10.100.132.32	Mail is a phis ack according to Surgate Phis
:omodo.local	10.100.132.32	Mail is a phis ack according to Surgate Phis
:omodo.local	10.100.132.32	Mail is a phishing attack according to Surgate Phis
:omodo.local	10.100.132.135	matched header rule: Subject: test action: REJECT

- Select the number of records per page to be displayed from the options.
- Click the 'First', 'Previous', 'Next' and 'Last' buttons to navigate to the respective pages.

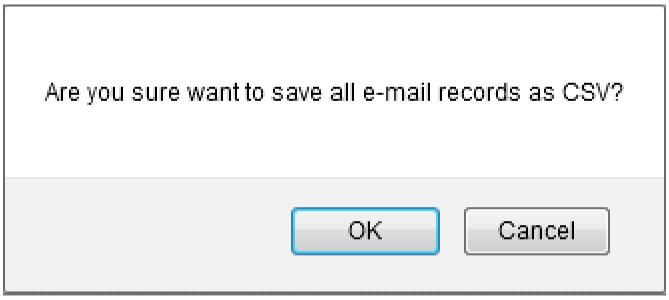
To export the report to a CSV file

- Click the 'Actions' drop-down



	Subject	Resul
☒	selammMM	PHISHI
☒	Kitap =?UTF-8?B?S2FtcGFueWFzx	PHISHI
☒	[!! CERTAINLY SPAM]Fwd: Natur	PHISHI

- Select 'Save As CSV' and click the 'Do!' button


Are you sure want to save all e-mail records as CSV?

- Click 'OK' in the confirmation dialog.

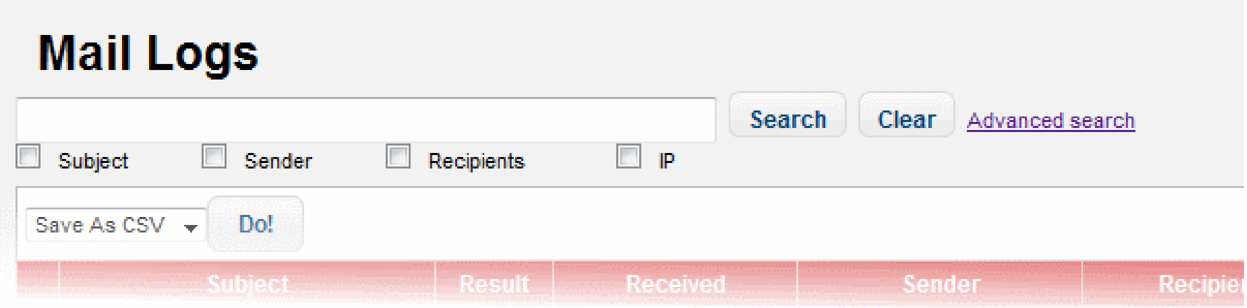
Search Options

You can search for a particular record or records in the report by using simple or advanced search feature.

- Simple Search
- Advanced Search

Simple Search

The simple search options allows you to search for a particular record or records based on 'Subject', 'Sender', 'Recipients' and / or 'IP' details only.

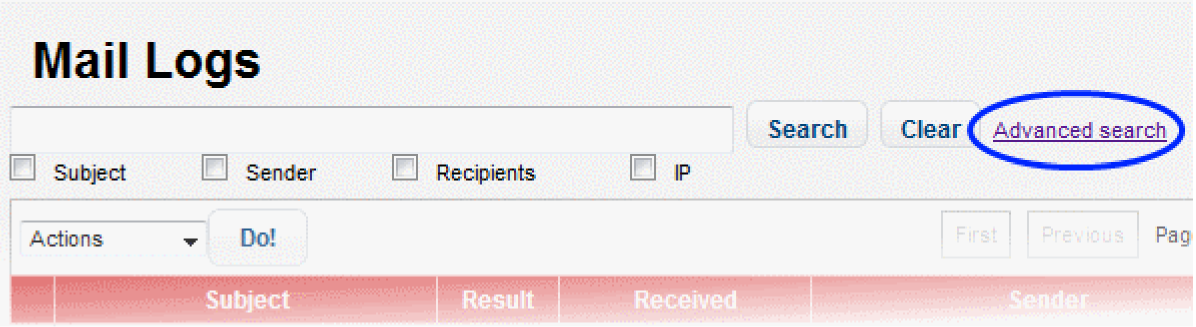


- To search for records based on the entries under 'Subject', 'Sender', 'Recipients' and / or 'IP' columns, enter the text or number fully or partially in the field and click the 'Search' button
- To search for records based on the entries under a particular column or columns, select the respective check boxes, enter the text or number fully or partially in the field and click the the 'Search' button. For example, if you want to search for a particular record for sender and recipients, select the 'Sender' and 'Recipients' check boxes, enter the text fully or partially in the field and click the 'Search' button.

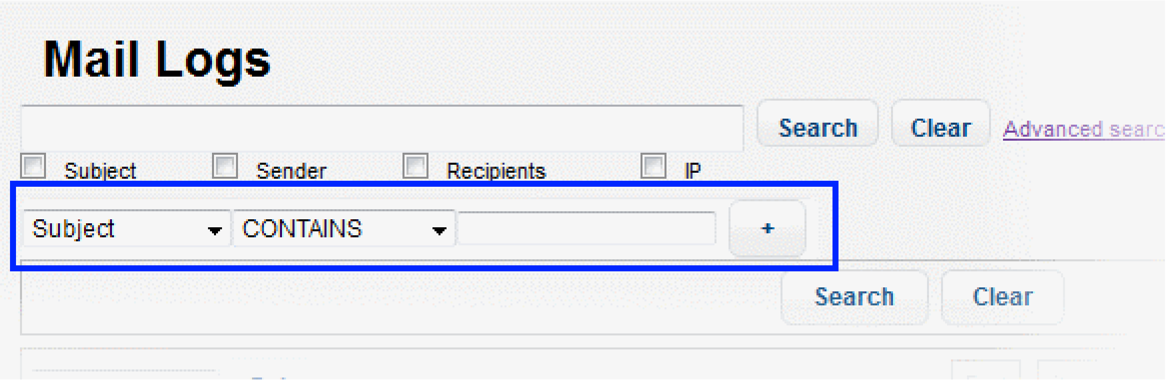
Advanced Search

The 'Advanced Search' option allows you a more granular search by including rules and filters.

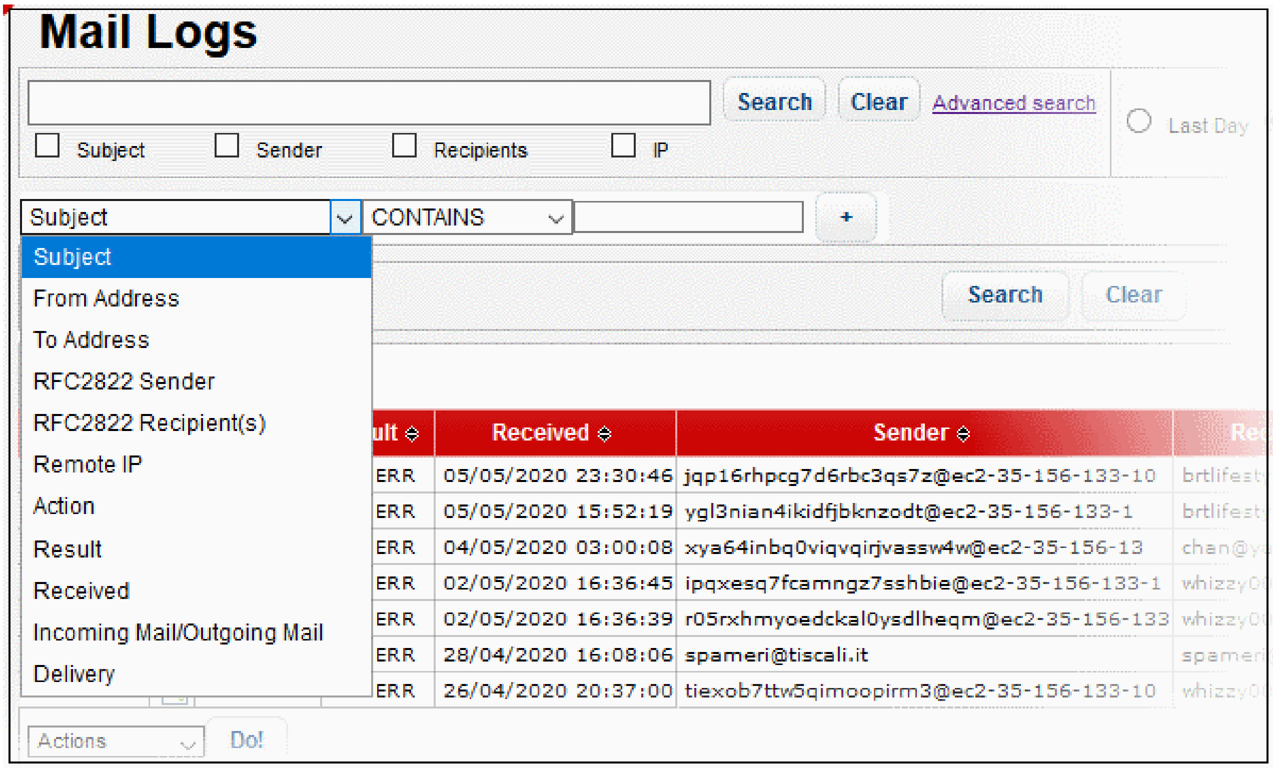
- Click the 'Advanced Search' link at the top of the screen.



The 'Advanced Search' option will be displayed.

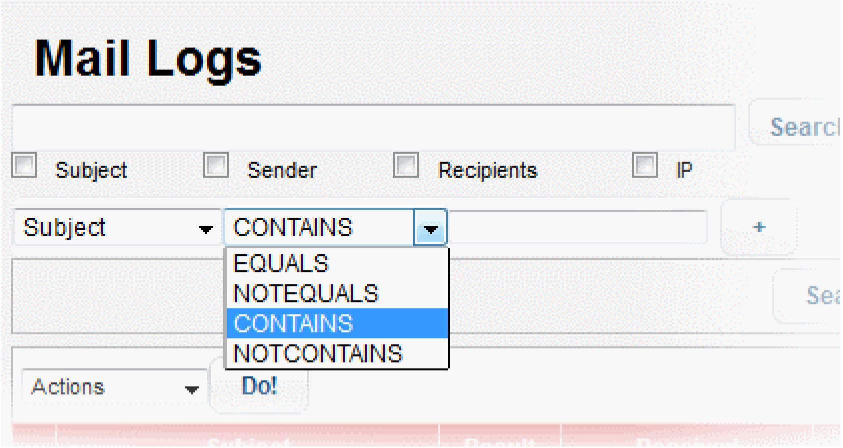


The first drop-down contains the column headers that can be selected for an advanced search.

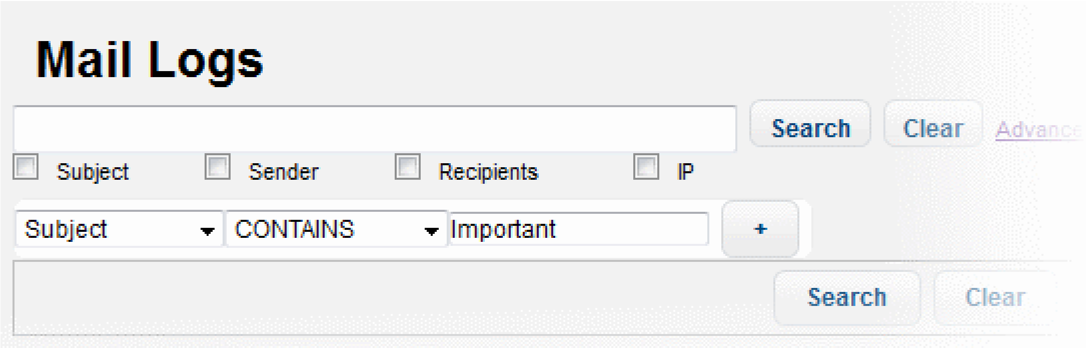


ult	Received	Sender	Re
ERR	05/05/2020 23:30:46	jqp16rhpcg7d6rbc3qs7z@ec2-35-156-133-10	brtlifest
ERR	05/05/2020 15:52:19	ygl3nian4ikidfjbknzodt@ec2-35-156-133-1	brtlifest
ERR	04/05/2020 03:00:08	xya64inbq0viqvqirjvassw4w@ec2-35-156-13	chan@y
ERR	02/05/2020 16:36:45	ipqxesq7fcamngz7sshbie@ec2-35-156-133-1	whizzy0
ERR	02/05/2020 16:36:39	r05rxhmyoedckal0ysdlheqm@ec2-35-156-133	whizzy0
ERR	28/04/2020 16:08:06	spameri@tiscali.it	spamen
ERR	26/04/2020 20:37:00	tiexob7ttw5qimoopirm3@ec2-35-156-133-10	whizzy0

The second column contains the condition for a search, which depends on the item selected in the first column and text/number entered or options selected in the third column.

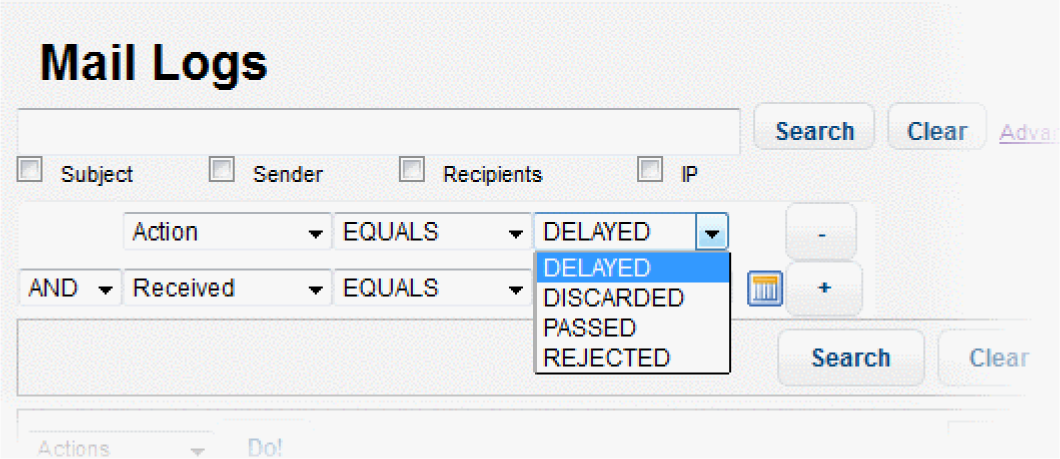


The third column allows you to enter the text/number or select from the options depending on the selection in the first column. For example, choosing 'Subject', 'From Address' or 'Remote IP' allows you to enter the text in the third column.



Subject | CONTAINS | Important

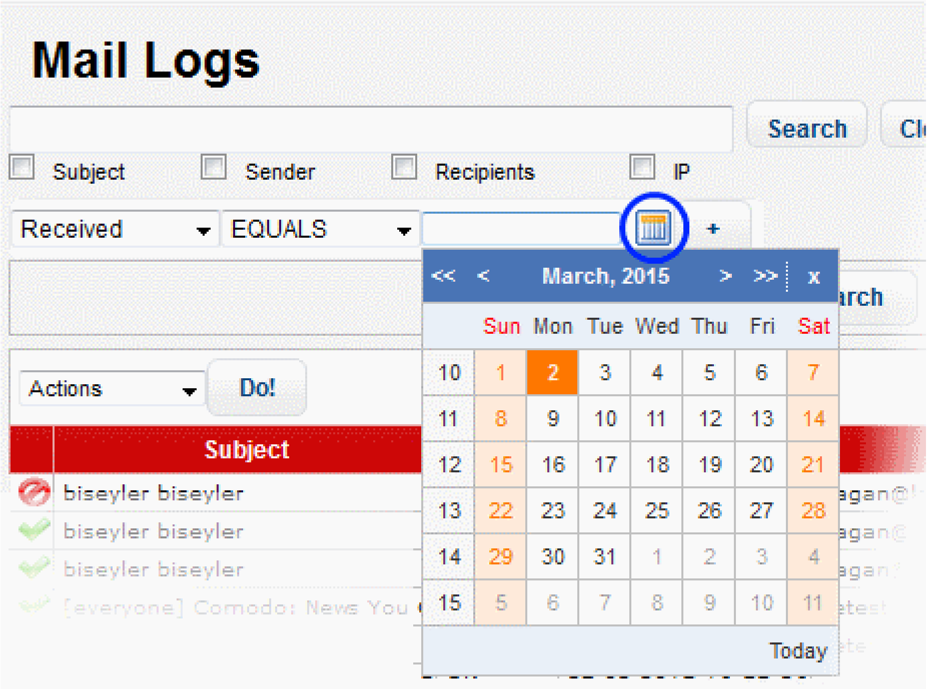
If you select 'Action' or 'Result' in the first column, then further options can be selected from the third column.



Action | EQUALS | DELAYED

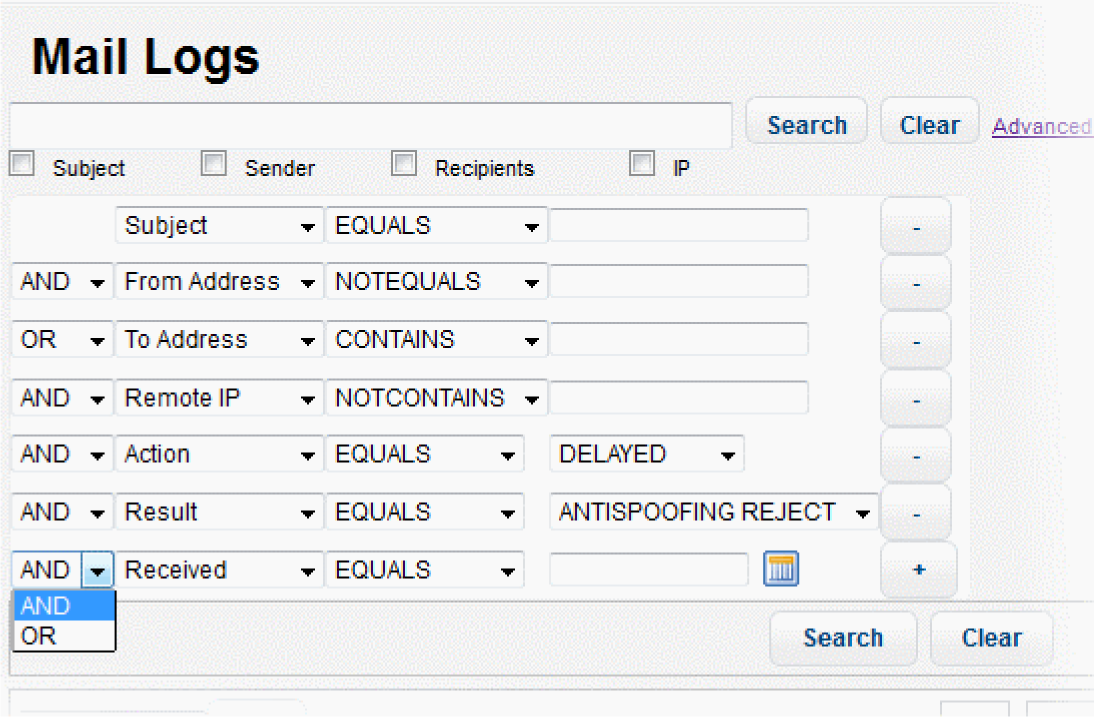
AND | Received | EQUALS

If you select 'Received' in the first column, then you can enter a date or select from the calendar.



Received | EQUALS

You can add more filters by clicking + for narrowing down your search.



Mail Logs

□ Subject □ Sender □ Recipients □ IP

	Subject	EQUALS		-
AND	From Address	NOTEQUALS		-
OR	To Address	CONTAINS		-
AND	Remote IP	NOTCONTAINS		-
AND	Action	EQUALS	DELAYED	-
AND	Result	EQUALS	ANTISPOOFING REJECT	-
AND	Received	EQUALS		+

You can remove a filter by clicking the - button beside it.

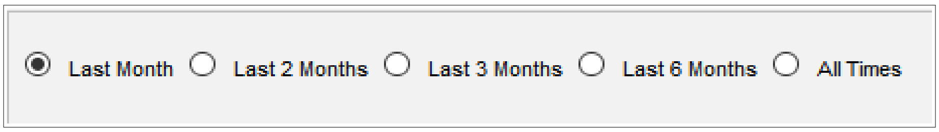
You can create a filter rule by selecting 'AND' or 'OR' option beside each of the added filter.

- Click 'Clear' to remove the advanced search rules.
- Click 'Search' to start the search per the filter rule.

The items will be searched for in the ascending order and results displayed.

- To remove the advanced search field, click the 'Advanced search' link again.

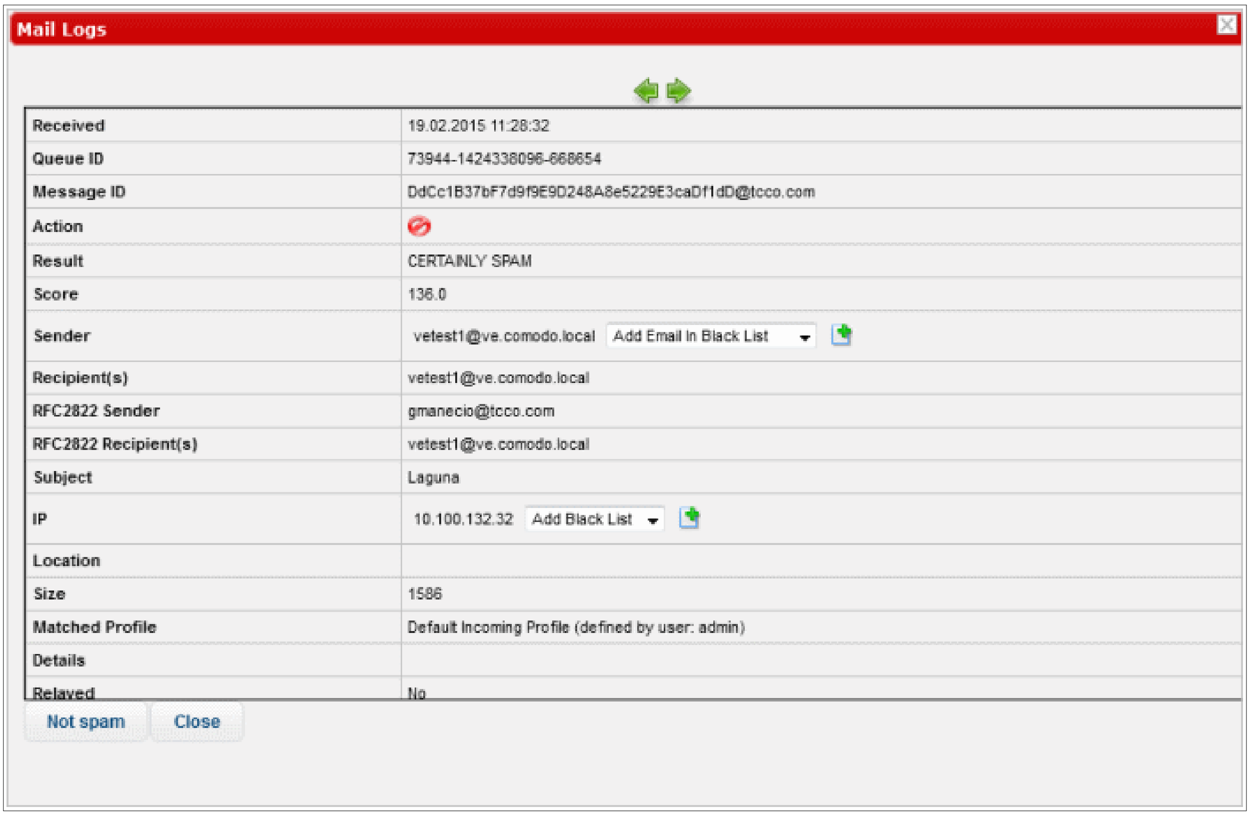
Administrators can filter results on monthly basis. The filters available are 'Last Month', 'Last 2 Months', 'Last 3 Months', 'Last 6 Months' and 'All Times'.



● Last Month ○ Last 2 Months ○ Last 3 Months ○ Last 6 Months ○ All Times

Details of a Log Entry

- Clicking anywhere on the row of a log record will display the details of the mail log.



Mail Logs

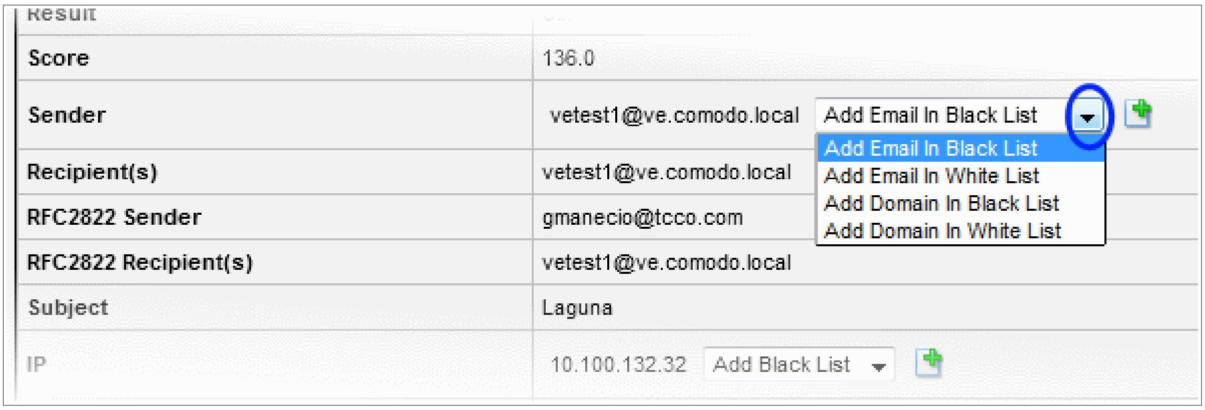
Received	19.02.2015 11:28:32
Queue ID	73944-1424338096-668654
Message ID	DdCc1B37bF7d9f9E9D248A8e5229E3caDf1dD@tcco.com
Action	
Result	CERTAINLY SPAM
Score	136.0
Sender	vetest1@ve.comodo.local Add Email In Black List
Recipient(s)	vetest1@ve.comodo.local
RFC2822 Sender	gmanecio@tcco.com
RFC2822 Recipient(s)	vetest1@ve.comodo.local
Subject	Laguna
IP	10.100.132.32 Add Black List
Location	
Size	1586
Matched Profile	Default Incoming Profile (defined by user: admin)
Details	
Relayed	No

The details screen allows you to mark the mail log as 'Spam' or 'Not spam' depending the mail category. You can also add the sender, sending domain and IP to blacklist or whitelist.

- To mark an email as 'Spam' or 'Not spam', click the relevant button at the bottom of the screen.

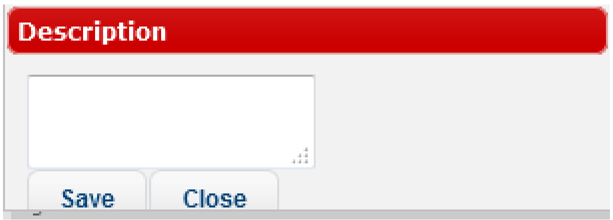
The changes will be saved and mails from the sender will be applied the new settings by KoruMail.

- To add the sender or domain to blacklist/whitelist, click the drop-down in the 'Sender' row.



Result	
Score	136.0
Sender	vetest1@ve.comodo.local Add Email In Black List
Recipient(s)	vetest1@ve.comodo.local
RFC2822 Sender	gmanecio@tcco.com
RFC2822 Recipient(s)	vetest1@ve.comodo.local
Subject	Laguna
IP	10.100.132.32 Add Black List

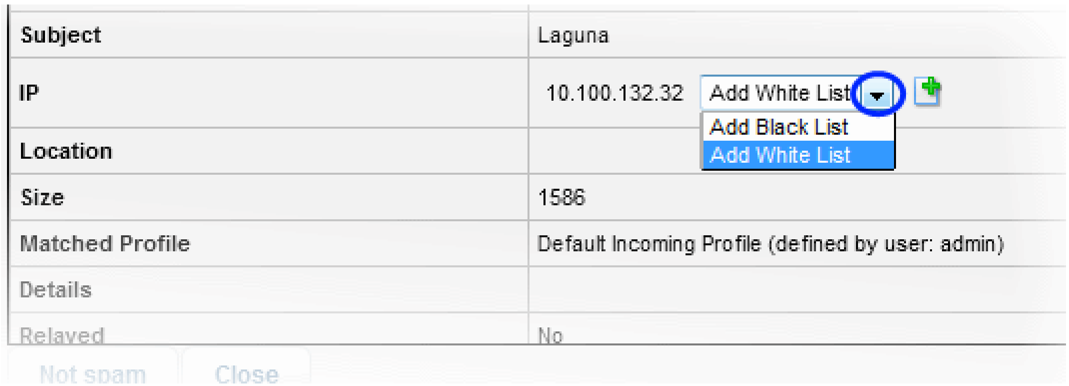
- Select the category from the options that you want to add the email and click the button beside it.



- Enter the reason for changing the category and click 'Save'.

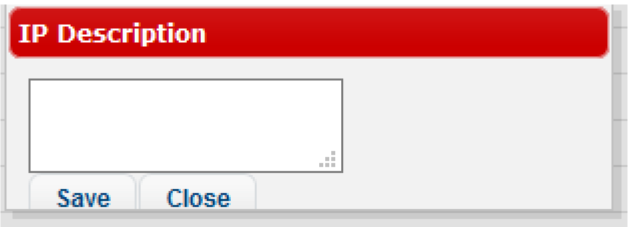
The changes will be saved and mails from the sender will be applied the new settings by KoruMail.

- To add the originating IP to blacklist/whitelist, click the drop-down in the 'IP' row.



Subject	Laguna
IP	10.100.132.32 Add White List
Location	
Size	1586
Matched Profile	Default Incoming Profile (defined by user: admin)
Details	
Relayed	No

- Select the category from the options that you want to add the IP and click the ➕ button beside it.



- Enter the reason for changing the category and click 'Save' .

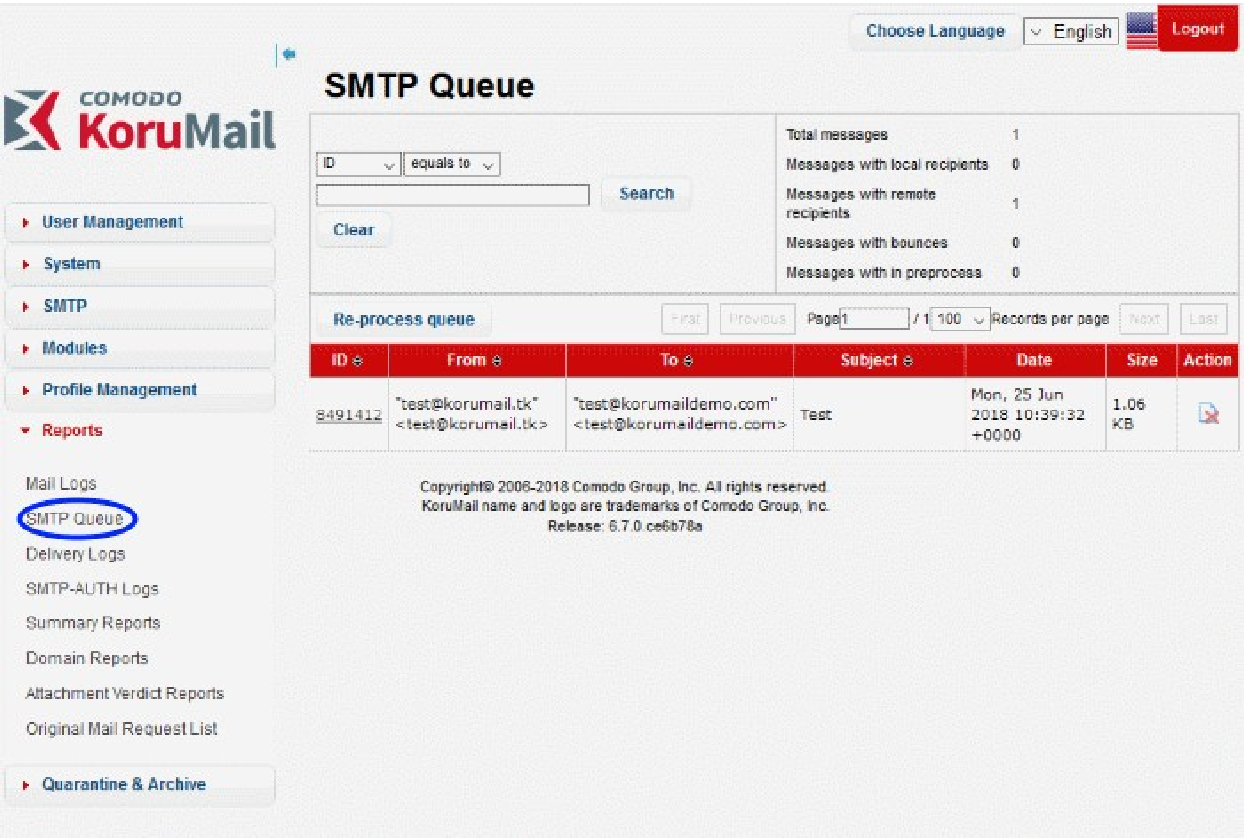
The changes will be saved and mails from the IP will be applied the new settings by KoruMail.

You can view the previous or next record by click the ⇦ ⇨ buttons at the top of a details screen.

10.2 SMTP Queue Report

The 'SMTP Queue' report shows details of mails that are queued for delivery.

- Click 'Reports' > 'SMTP Queue' to open the reports interface.



SMTP Queue

Total messages	1
Messages with local recipients	0
Messages with remote recipients	1
Messages with bounces	0
Messages with in preprocess	0

ID	From	To	Subject	Date	Size	Action
8491412	"test@korumail.tk" <test@korumail.tk>	"test@korumaildemo.com" <test@korumaildemo.com>	Test	Mon, 25 Jun 2018 10:39:32 +0000	1.06 KB	

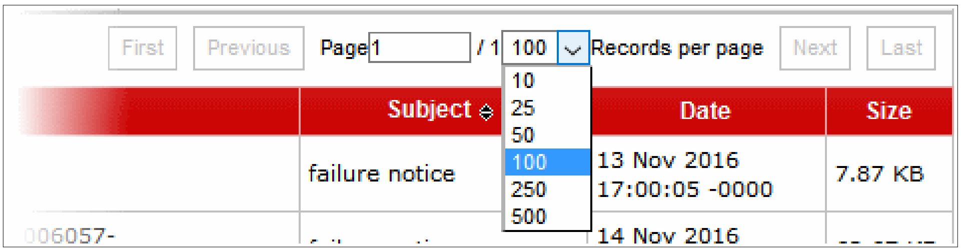
Copyright© 2006-2018 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 6.7.0.ce6b78a

SMTP Queue Report - Table of Column Descriptions	
Column Header	**Description**
ID	The identification number of the email queue that holds the status or message of the queue.
From	Sender's email address
To	Recipient's email address
Subject	The content of the email subject line.
Date	Date and time that the mail was sent
Size	Size of the file in kilobytes
Action	Delete the mail from the SMTP queue

At the top and bottom of the screen you have the option to set the number of records to be displayed per page.

Configure the number of records displayed per page

- Click the 'Records per page' drop-down



	Subject	Date	Size
	failure notice	13 Nov 2016 17:00:05 -0000	7.87 KB
006057-		14 Nov 2016	

- Select the number of records per page to be displayed from the options. The default is 100.

- Click the 'First', 'Previous', 'Next' and 'Last' buttons to navigate through the report.

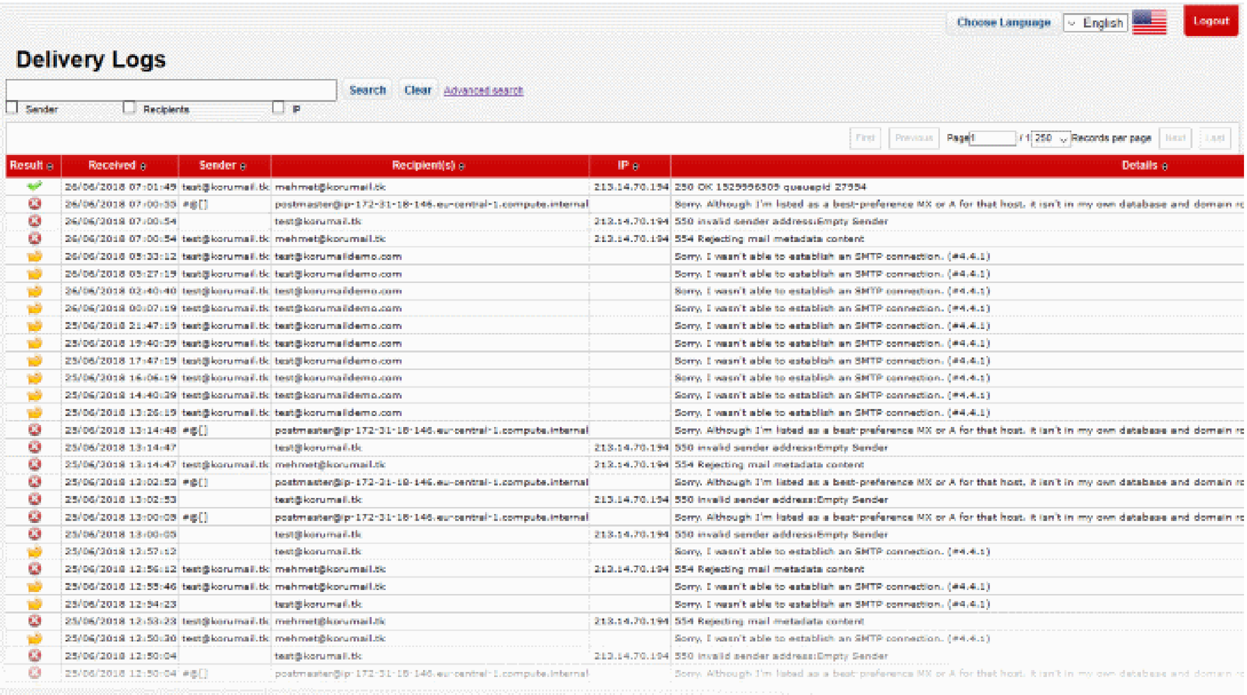
Search Options

You can search for a particular record by using the search field at the upper left. Use the drop-down menus to specify granular search criteria. This is similar to the **advanced search option** explained in the '**Mail Logs**' section.

10.3 Delivery Logs Report

While '**Mails Logs**' record all incoming and outgoing mail traffic, 'Delivery Logs' record only those mails accepted by mail servers.

- Click 'Reports' > 'Delivery Logs' to open the interface



Result	Received	Sender	Recipient(s)	IP	Details
✓	26/06/2018 07:01:49	test@korumail.tk	mehmet@korumail.tk	213.14.70.194	250 OK 1529996509 queueid 27554
☒	26/06/2018 07:00:55	#@[]	postmaster@ip-172-31-18-146.eu-central-1.compute.internal		Sorry, Although I'm listed as a best-preference MX or A for that host, it isn't in my own database and domain rc
☒	26/06/2018 07:00:54		test@korumail.tk	213.14.70.194	550 invalid sender address:Empty Sender
☒	26/06/2018 07:00:54	test@korumail.tk	mehmet@korumail.tk	213.14.70.194	554 Rejecting mail metadata content
↻	26/06/2018 05:33:12	test@korumail.tk	test@korumaildemo.com		Sorry, I wasn't able to establish an SMTP connection. (#4.4.1)
↻	26/06/2018 05:27:19	test@korumail.tk	test@korumaildemo.com		Sorry, I wasn't able to establish an SMTP connection. (#4.4.1)
↻	26/06/2018 02:40:40	test@korumail.tk	test@korumaildemo.com		Sorry, I wasn't able to establish an SMTP connection. (#4.4.1)
↻	26/06/2018 00:07:19	test@korumail.tk	test@korumaildemo.com		Sorry, I wasn't able to establish an SMTP connection. (#4.4.1)
↻	25/06/2018 21:47:19	test@korumail.tk	test@korumaildemo.com		Sorry, I wasn't able to establish an SMTP connection. (#4.4.1)
↻	25/06/2018 19:40:39	test@korumail.tk	test@korumaildemo.com		Sorry, I wasn't able to establish an SMTP connection. (#4.4.1)
↻	25/06/2018 17:47:19	test@korumail.tk	test@korumaildemo.com		Sorry, I wasn't able to establish an SMTP connection. (#4.4.1)
↻	25/06/2018 16:06:19	test@korumail.tk	test@korumaildemo.com		Sorry, I wasn't able to establish an SMTP connection. (#4.4.1)
↻	25/06/2018 14:40:39	test@korumail.tk	test@korumaildemo.com		Sorry, I wasn't able to establish an SMTP connection. (#4.4.1)
↻	25/06/2018 13:26:19	test@korumail.tk	test@korumaildemo.com		Sorry, I wasn't able to establish an SMTP connection. (#4.4.1)
☒	25/06/2018 13:14:48	#@[]	postmaster@ip-172-31-18-146.eu-central-1.compute.internal		Sorry, Although I'm listed as a best-preference MX or A for that host, it isn't in my own database and domain rc
☒	25/06/2018 13:14:47		test@korumail.tk	213.14.70.194	550 invalid sender address:Empty Sender
☒	25/06/2018 13:14:47	test@korumail.tk	mehmet@korumail.tk	213.14.70.194	554 Rejecting mail metadata content
☒	25/06/2018 13:02:53	#@[]	postmaster@ip-172-31-18-146.eu-central-1.compute.internal		Sorry, Although I'm listed as a best-preference MX or A for that host, it isn't in my own database and domain rc
☒	25/06/2018 13:02:53		test@korumail.tk	213.14.70.194	550 invalid sender address:Empty Sender
☒	25/06/2018 13:00:05	#@[]	postmaster@ip-172-31-18-146.eu-central-1.compute.internal		Sorry, Although I'm listed as a best-preference MX or A for that host, it isn't in my own database and domain rc
☒	25/06/2018 13:00:05		test@korumail.tk	213.14.70.194	550 invalid sender address:Empty Sender
↻	25/06/2018 12:57:12		test@korumail.tk		Sorry, I wasn't able to establish an SMTP connection. (#4.4.1)
☒	25/06/2018 12:56:12	test@korumail.tk	mehmet@korumail.tk	213.14.70.194	554 Rejecting mail metadata content
↻	25/06/2018 12:55:46	test@korumail.tk	mehmet@korumail.tk		Sorry, I wasn't able to establish an SMTP connection. (#4.4.1)
↻	25/06/2018 12:54:23		test@korumail.tk		Sorry, I wasn't able to establish an SMTP connection. (#4.4.1)
☒	25/06/2018 12:53:23	test@korumail.tk	mehmet@korumail.tk	213.14.70.194	554 Rejecting mail metadata content
↻	25/06/2018 12:50:30	test@korumail.tk	mehmet@korumail.tk		Sorry, I wasn't able to establish an SMTP connection. (#4.4.1)
☒	25/06/2018 12:50:04		test@korumail.tk	213.14.70.194	550 invalid sender address:Empty Sender
☒	25/06/2018 12:50:04	#@[]	postmaster@ip-172-31-18-146.eu-central-1.compute.internal		Sorry, Although I'm listed as a best-preference MX or A for that host, it isn't in my own database and domain rc

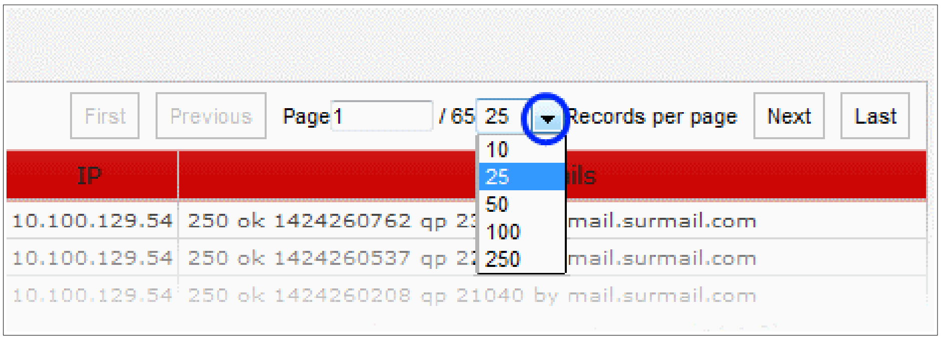
Delivery Logs Report - Table of Column Descriptions	
Column Header	**Description**
Result	The status of the mail processed by the mail server. The tool tip on hovering the mouse cursor over an icon displays the action. ✓ - Success: Indicates the mail has been successfully delivered to the recipient. ☒ - Permanent Error: Indicates the mail server failed to deliver the mail to the recipient. ↻ - Temporary: Indicates it is temporary error and the server will try again to deliver.
Received	Date and time KoruMail received the email.
Sender	Email address information of the originator
Recipient(s)	Email address information of the receiver
IP	The network address of the system from where the mail was sent. The next column displays the flag of the originating country.
Details	Provides information such as the message ID and reasons for permanent and temporary

	error

At the top and bottom of the screen, you have the option to set the number of records to be displayed per page.

To configure the number of records to be displayed per page

- Click the 'Records per page' drop-down



IP	ils
10.100.129.54	250 ok 1424260762 qp 23 mail.surmail.com
10.100.129.54	250 ok 1424260537 qp 22 mail.surmail.com
10.100.129.54	250 ok 1424260208 qp 21040 by mail.surmail.com

- Select the number of records per page to be displayed from the options.
- Click the 'First', 'Previous', 'Next' and 'Last' buttons to navigate to the respective pages.

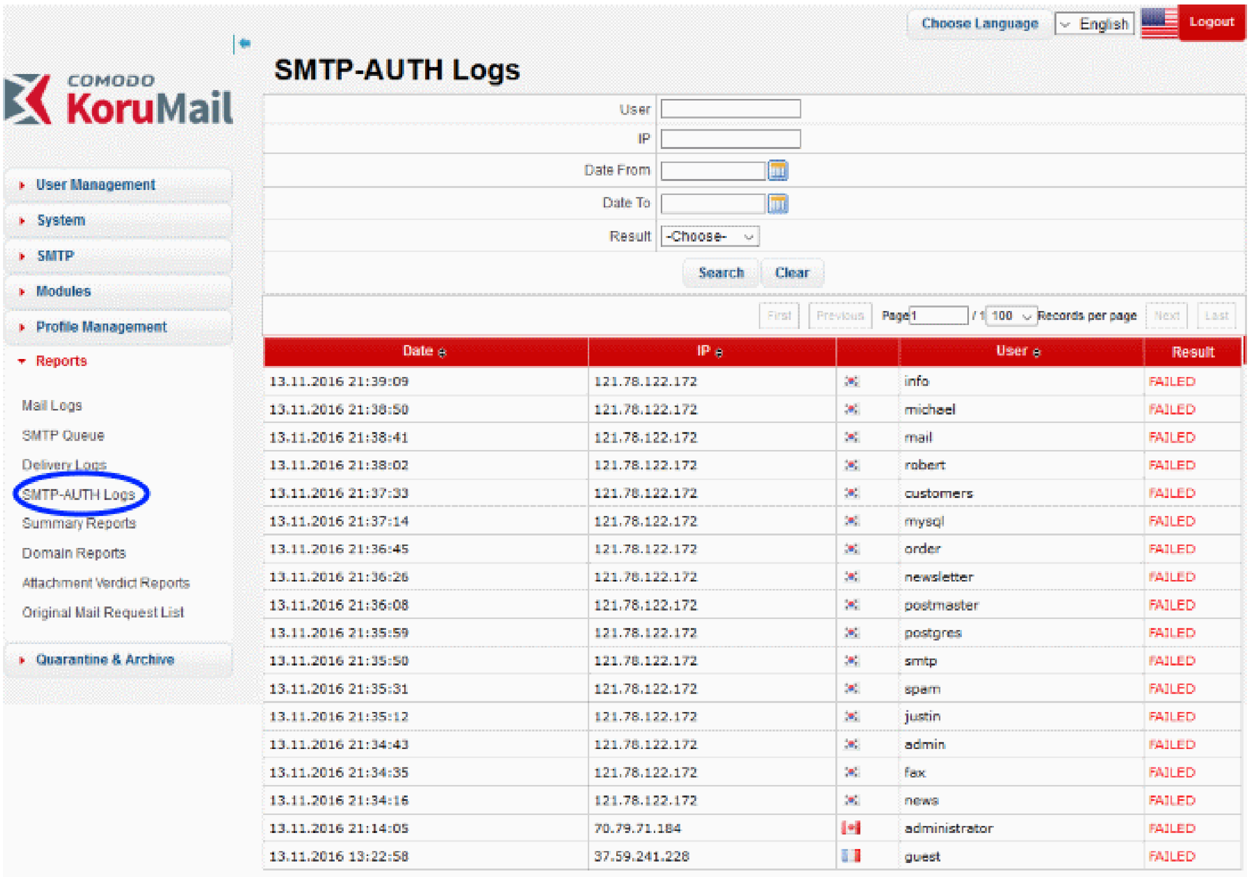
Search Options

You can search for a particular record or records in the report by using simple or advanced search feature. This is similar to the **search option** explained in the '**Mail Logs**' section.

10.4 SMTP-AUTH Logs Report

The 'SMTP-AUTH Logs Report' contains logs of every SMTP client log-in that required authentication.

- Click reports then 'SMTP-AUTH Logs' to open the interface.



SMTP-AUTH Logs

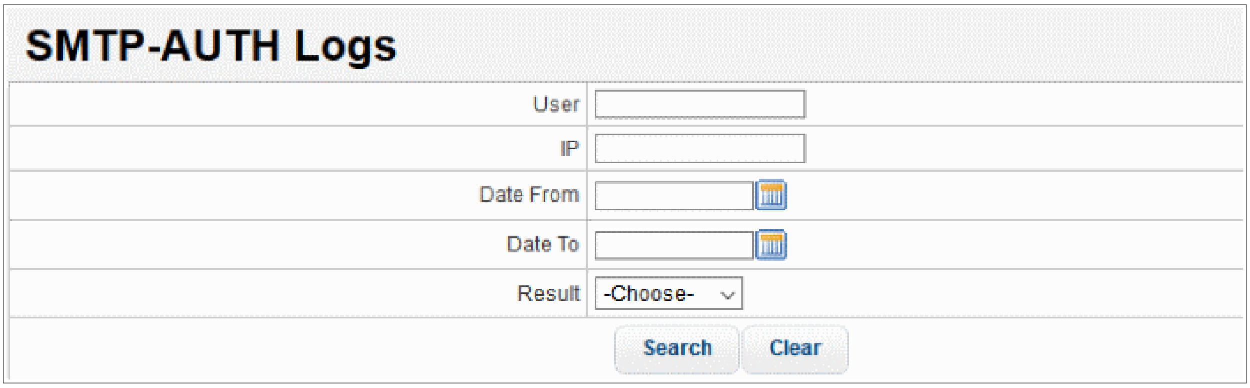
User	
IP	
Date From	
Date To	
Result	-Choose-

Page 1 / 1 100 Records per page

Date	IP		User	Result
13.11.2016 21:39:09	121.78.122.172		info	FAILED
13.11.2016 21:38:50	121.78.122.172		michael	FAILED
13.11.2016 21:38:41	121.78.122.172		mail	FAILED
13.11.2016 21:38:02	121.78.122.172		robert	FAILED
13.11.2016 21:37:33	121.78.122.172		customers	FAILED
13.11.2016 21:37:14	121.78.122.172		mysql	FAILED
13.11.2016 21:36:45	121.78.122.172		order	FAILED
13.11.2016 21:36:26	121.78.122.172		newsletter	FAILED
13.11.2016 21:36:08	121.78.122.172		postmaster	FAILED
13.11.2016 21:35:59	121.78.122.172		postgres	FAILED
13.11.2016 21:35:50	121.78.122.172		smtp	FAILED
13.11.2016 21:35:31	121.78.122.172		spam	FAILED
13.11.2016 21:35:12	121.78.122.172		justin	FAILED
13.11.2016 21:34:43	121.78.122.172		admin	FAILED
13.11.2016 21:34:35	121.78.122.172		fax	FAILED
13.11.2016 21:34:16	121.78.122.172		news	FAILED
13.11.2016 21:14:05	70.79.71.184		administrator	FAILED
13.11.2016 13:22:58	37.59.241.228		guest	FAILED

SMTP-AUTH Logs Report - Table of Column Descriptions	
Column Header	**Description**
Result	Indicates the status of the mail processed by SMTP mail server. Success : Indicates that the SMTP client has logged in successfully Failed: Indicates that the SMTP client login has failed
User	The name of the SMTP mail client
IP	The network address of the SMTP mail client
Date	Date and time information of the event log

The 'Search' options allows you to search for a particular record or records based on the 'User', 'IP', 'Date From', 'Date To' or 'Result' of the authentication of SMTP client log-in.



SMTP-AUTH Logs

User	
IP	
Date From	
Date To	
Result	-Choose-

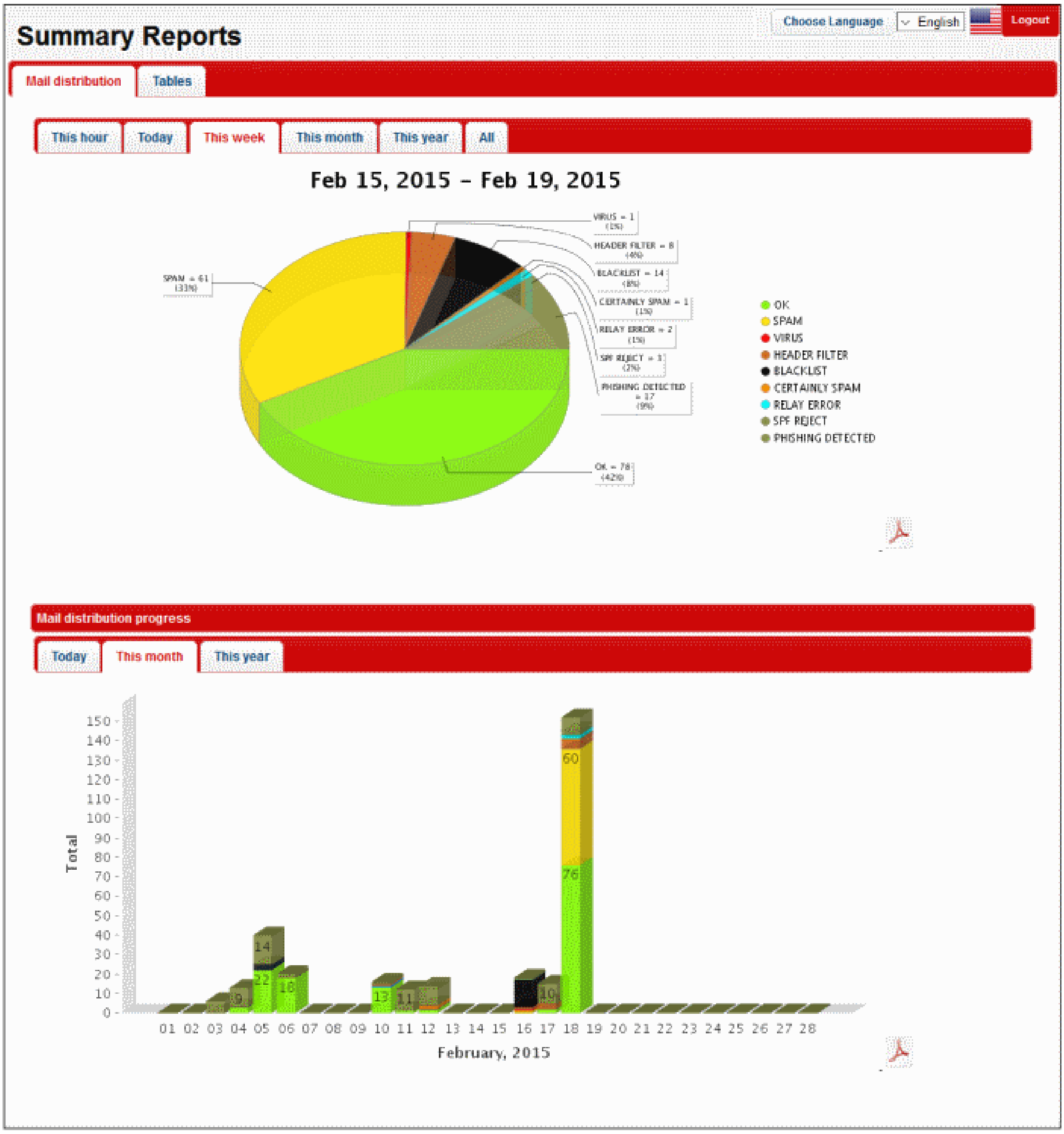
- To search for records based on the entries under 'User', 'IP', 'Date From', 'Date To' or 'Result', enter the text or number fully or partially in the field and click the 'Search' button
- To refresh search, click 'Clear'.

10.5 Summary Reports

- The 'Summary Reports' screen in KoruMail provides a comprehensive report of filtering results of mails for all domains that are enrolled.
- The summary report is available as pie chart, bar chart and table formats.
- The tabs at the top of the interface allows to view and download the reports in graphical or table format.
- The upper portion of the screen displays the report in pie chart format and is available for hourly, daily, weekly, monthly, yearly and full from the time of installation.
- The lower portion displays the results in bar chart format and is available on hourly, monthly and yearly basis.

To open the 'Summary Reports' interface

- Click 'Reports' and then click 'Summary Reports'



You can view and download the reports in graphical as well as in table format.

- Graphical Representation
- Table Representation

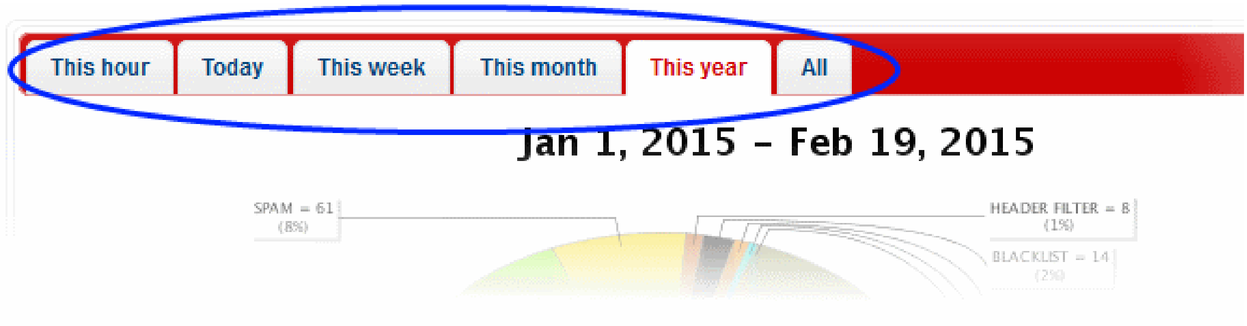
To view and download the report in graphical format

- Click the 'Mail Distribution' tab at the top

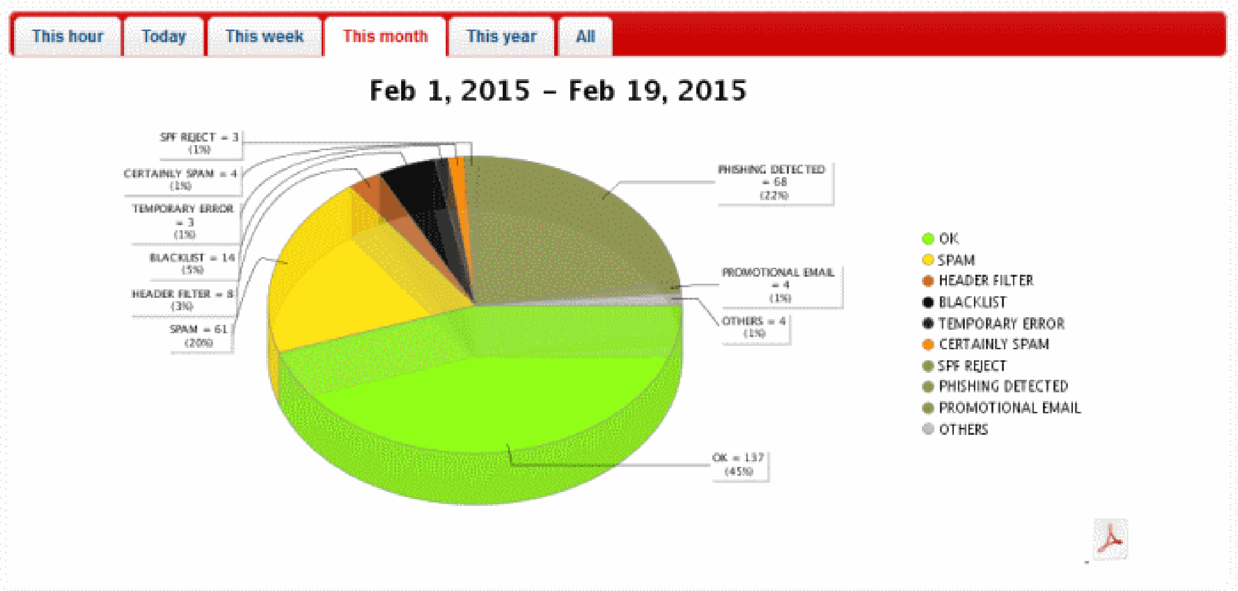
The results in **pie chart** format at the top and **bar chart** format at the bottom will be displayed.

- To view the results for a particular period, click the relevant tabs at the top.

Pie Chart



- Click the desired period for which you want to view and download the report. The available periods are hourly, daily, weekly, monthly, yearly and from the time of KoruMail installation.



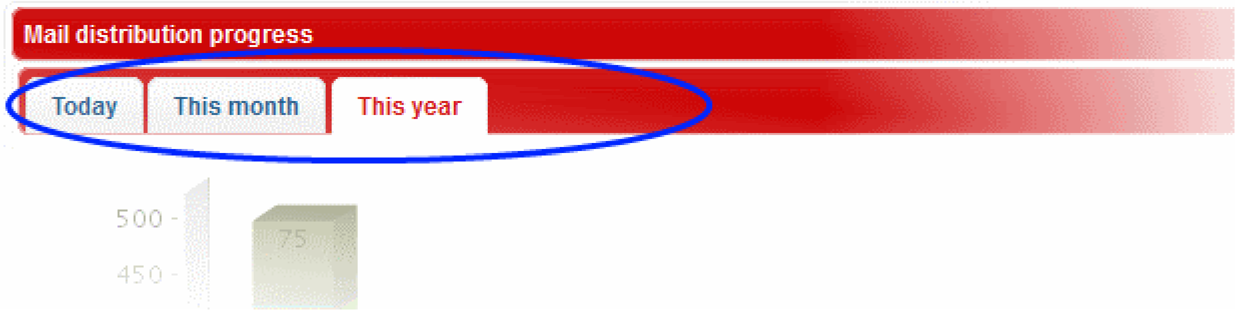
The different segments of the pie chart provides the details of the filtering results for the selected period such as mails categorized as spam, phishing, blacklisted and so on.

- To download the pie chart results, click the PDF icon

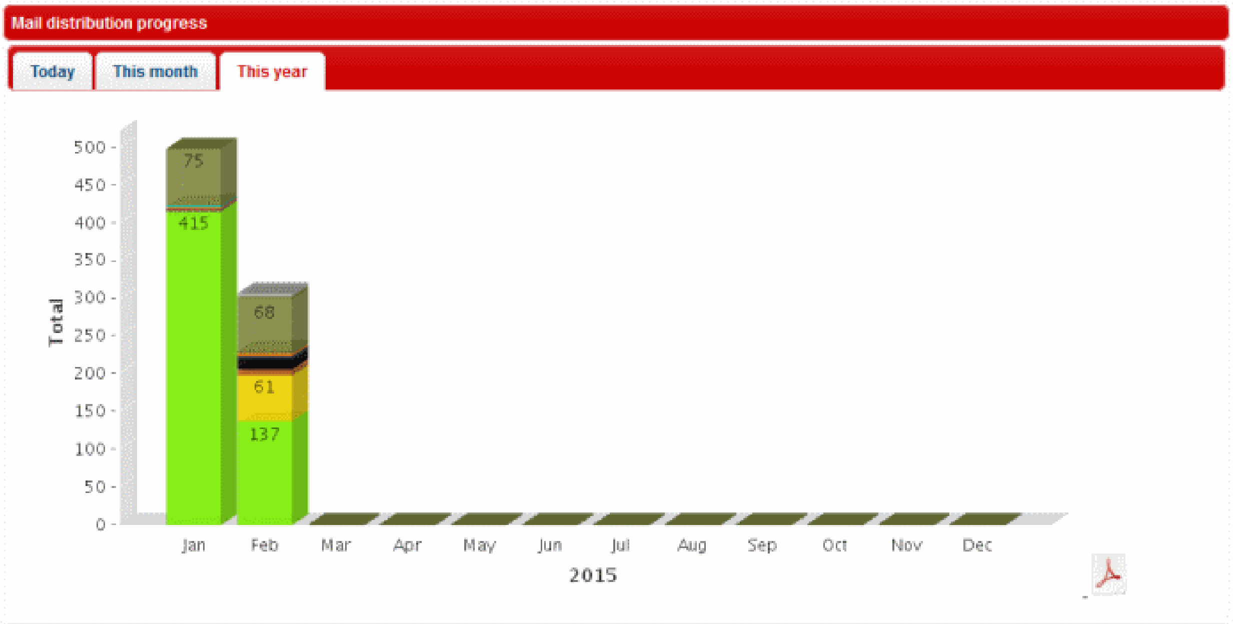
The pdf and xls files wil be downloaded to the local folder.

Bar Chart

- Click the desired period for which you want to view and download the report in bar chart format. The available periods are daily, monthly and yearly.



The report for the selected period will be displayed.



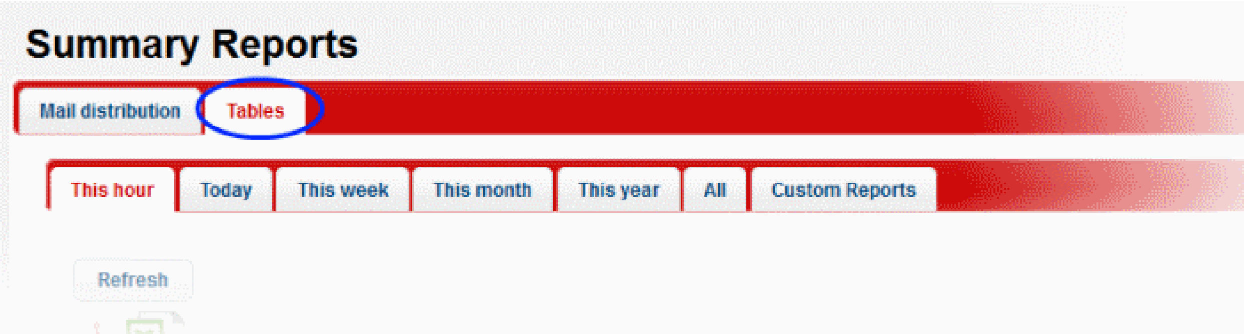
The Y-axis displays the number of mails and X-axis displays the hours/days/months for the selected period.

- To download the bar chart results, click the PDF icon

The pdf and xls files wil be downloaded to the local folder.

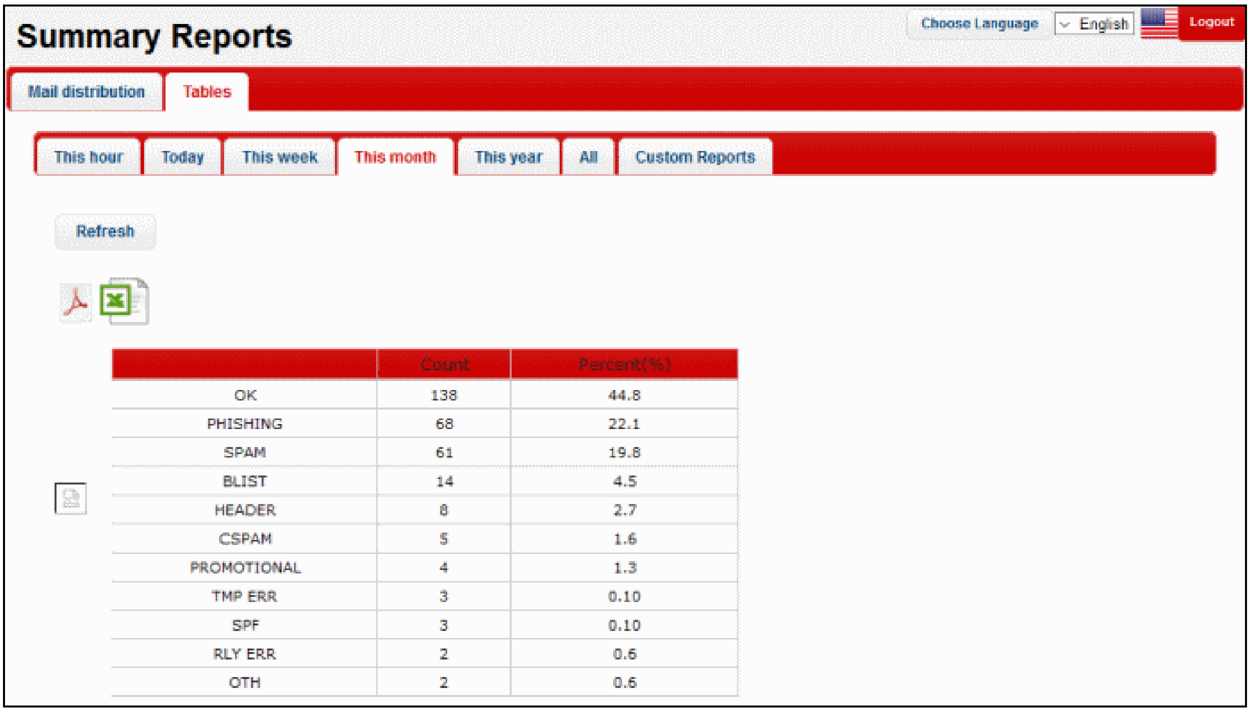
To view and download the report in table format

- Click the 'Tables' tab at the top of the 'Summary Reports' screen.



The report in table format is available for the periods hourly, daily, weekly, monthly, yearly and from the time of KoruMail installation. You can also define a period and generate a custom report.

- Click the desired period for which you want to view and download the report in table format.



	Count	Percent(%)
OK	138	44.8
PHISHING	68	22.1
SPAM	61	19.8
BLIST	14	4.5
HEADER	8	2.7
CSPAM	5	1.6
PROMOTIONAL	4	1.3
TMP ERR	3	0.10
SPF	3	0.10
RLY ERR	2	0.6
OTH	2	0.6

The report for the selected period will be displayed. The first column indicates the categorization of mails, the second column displays the number for each category and the third column provides the results in percentage for each category.

- To download the report in PDF format, click the PDF icon

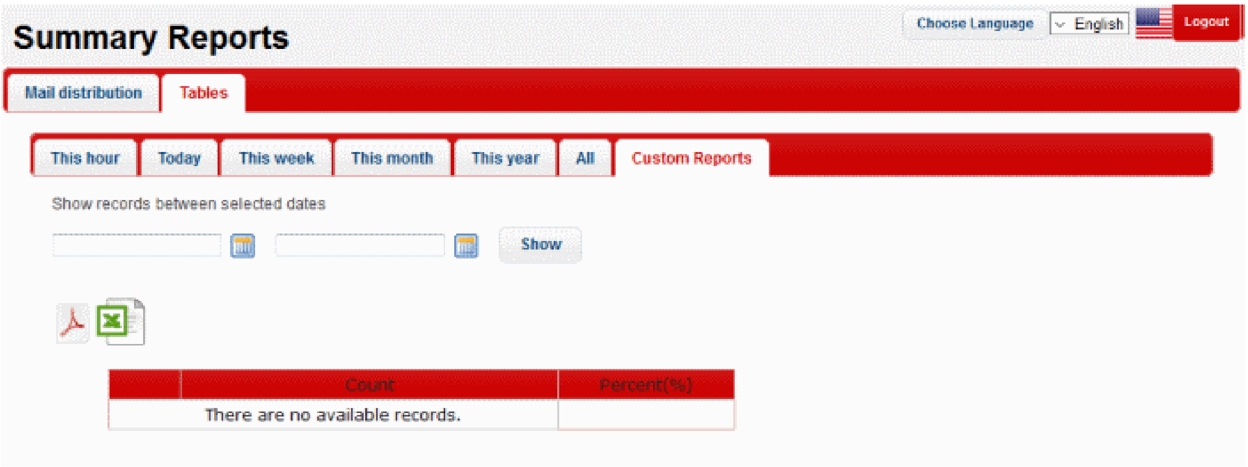
- To download the report in XLS (spreadsheet) format, click the XLS icon

The pdf and xls files will be downloaded to the local folder.

To generate a custom report in table format

- Click the 'Custom Reports' tab at the top

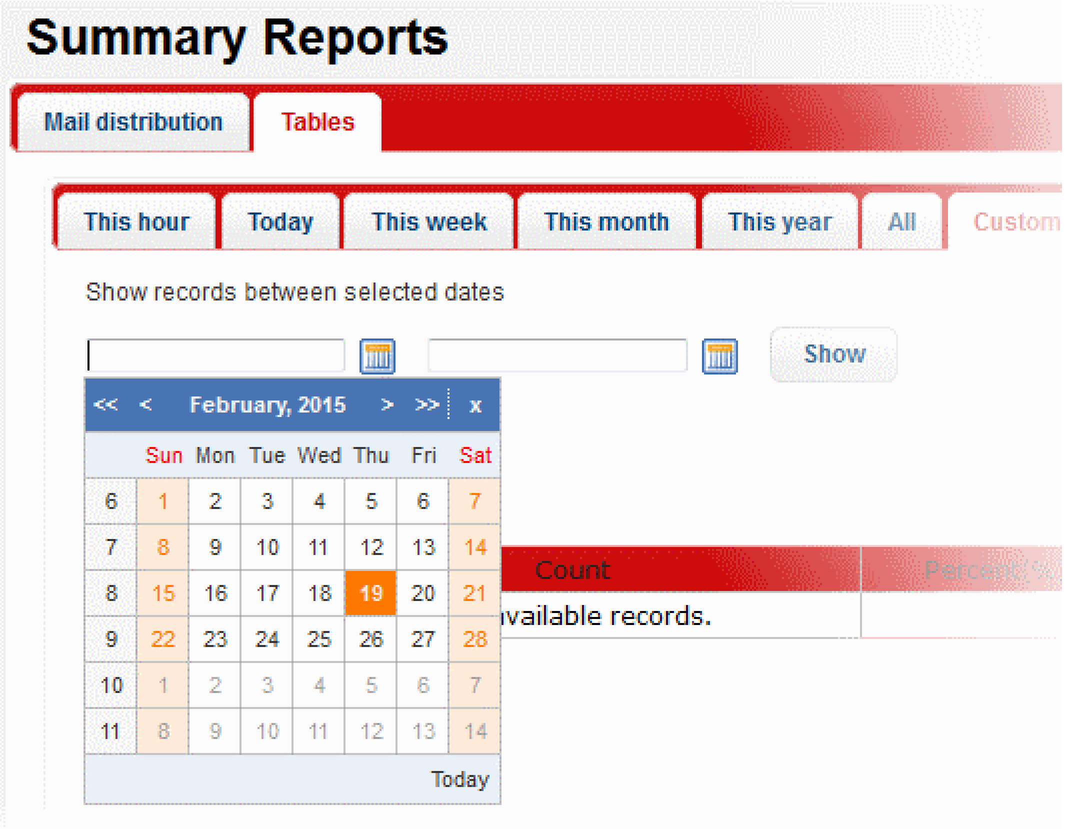
The fields to select the 'From' and 'To' period will be displayed.



Show records between selected dates

There are no available records.

- Click on the fields or calendar icon and select the period from the calendar.



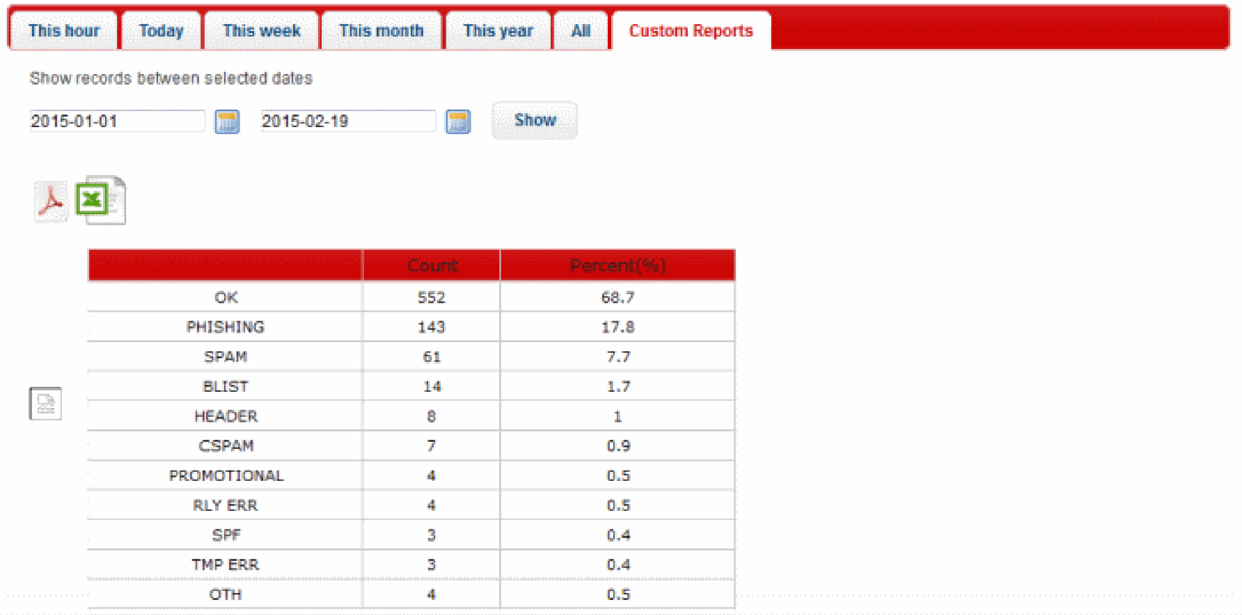
Show records between selected dates

February, 2015

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
6	1	2	3	4	5	6	7
7	8	9	10	11	12	13	14
8	15	16	17	18	19	20	21
9	22	23	24	25	26	27	28
10	1	2	3	4	5	6	7
11	8	9	10	11	12	13	14

ıvailable records.

- Click the 'Show' button after selecting the custom period.



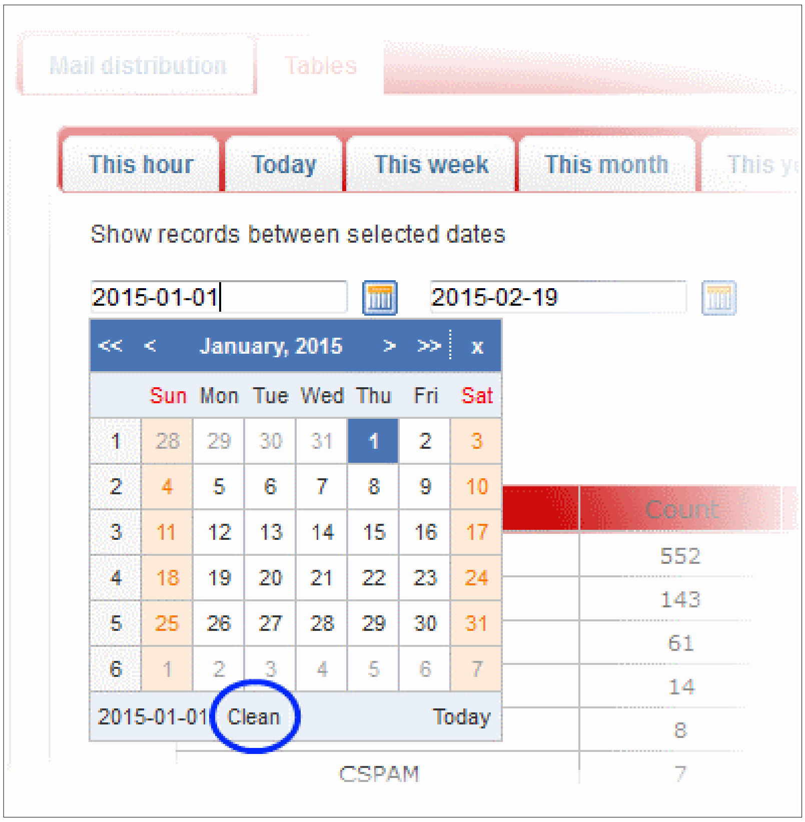
Show records between selected dates

2015-01-01 2015-02-19 Show

	Count	Percent(%)
OK	552	68.7
PHISHING	143	17.8
SPAM	61	7.7
BLIST	14	1.7
HEADER	8	1
CSPAM	7	0.9
PROMOTIONAL	4	0.5
RLY ERR	4	0.5
SPF	3	0.4
TMP ERR	3	0.4
OTH	4	0.5

The report for the selected custom period will be displayed. The first column indicates the categorization of mails, the second column displays the number for each category and the third column provides the results in percentage for each category.

- To download the custom report in PDF format, click the PDF icon and click 'OK' in the download dialogue to save the report.
- To download the custom report in XLS (spreadsheet) format, click the XLS icon and click 'OK' in the download dialogue to save the report.
- To clear the custom period, click on the period fields or calendar icon and click the 'Clean' button.



Show records between selected dates

2015-01-01 2015-02-19

<< < January, 2015 > >> x

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	28	29	30	31	1	2	3
2	4	5	6	7	8	9	10
3	11	12	13	14	15	16	17
4	18	19	20	21	22	23	24
5	25	26	27	28	29	30	31
6	1	2	3	4	5	6	7

2015-01-01 Clean Today

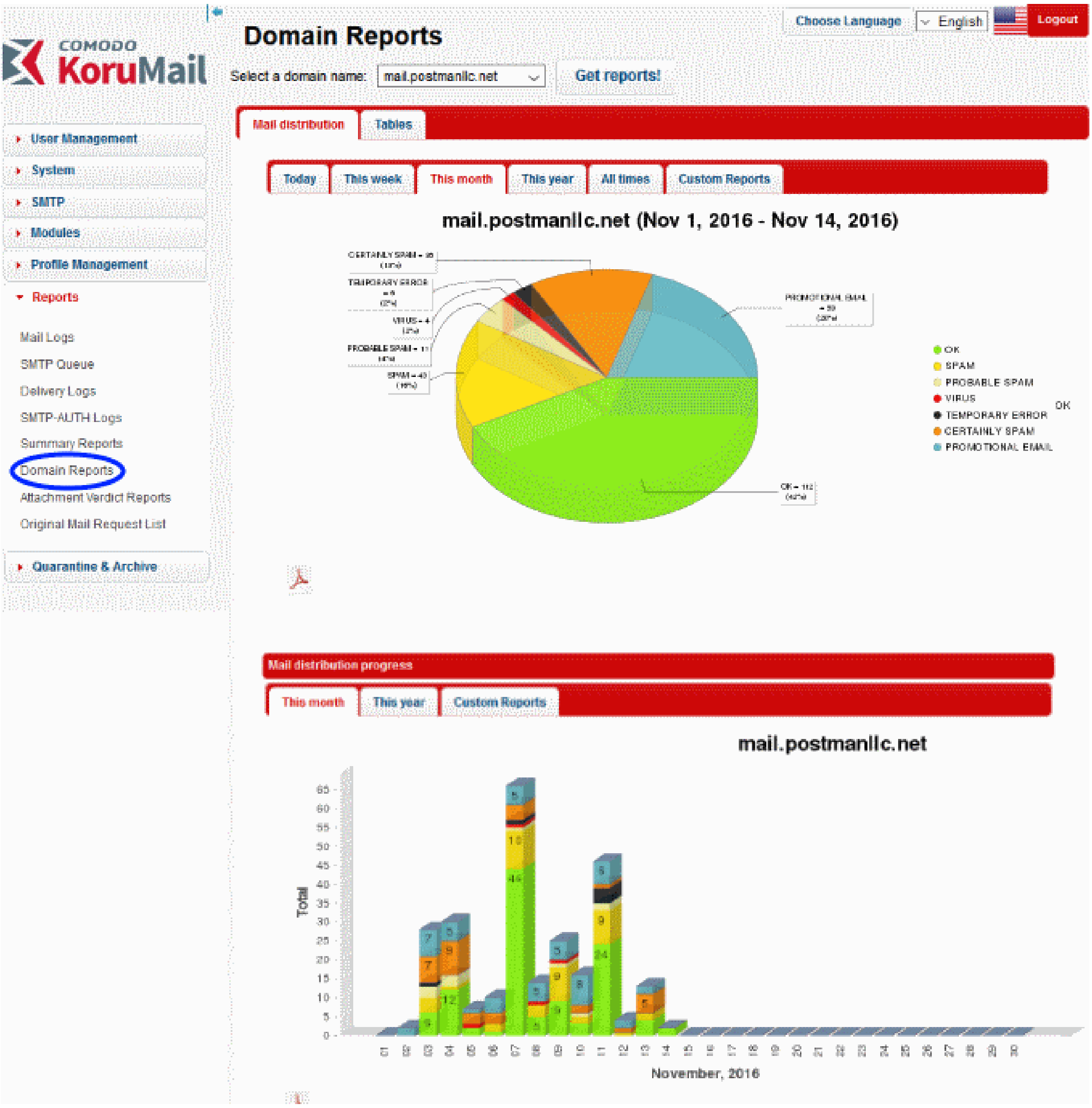
	Count
	552
	143
	61
	14
	8
CSPAM	7

10.6 Domain Reports

The 'Domain Reports' interface contains detailed statistics and graphs about your monitored domains.

To open the interface

- Click 'Reports' on the left then click 'Domains Reports':



Domain Reports

Select a domain name: mail.postmanllc.net

You can change the domain shown in the charts by using the drop-down menu at the top of the interface.

You can view and download the reports in graphical or table format.

- Graphical Representation
- Table Representation

Graphical Representation

Mail Distribution:

The 'Mail Distribution' chart categorizes mails sent/received on the specified domain according to mail category. Categories include 'OK', 'Spam', 'Probable Spam', 'Virus' etc. Use the tabs above the chart to change the time-period covered by the chart. Choices include 'Today', 'This Week', 'This Month', 'This Year' and 'All Time'.

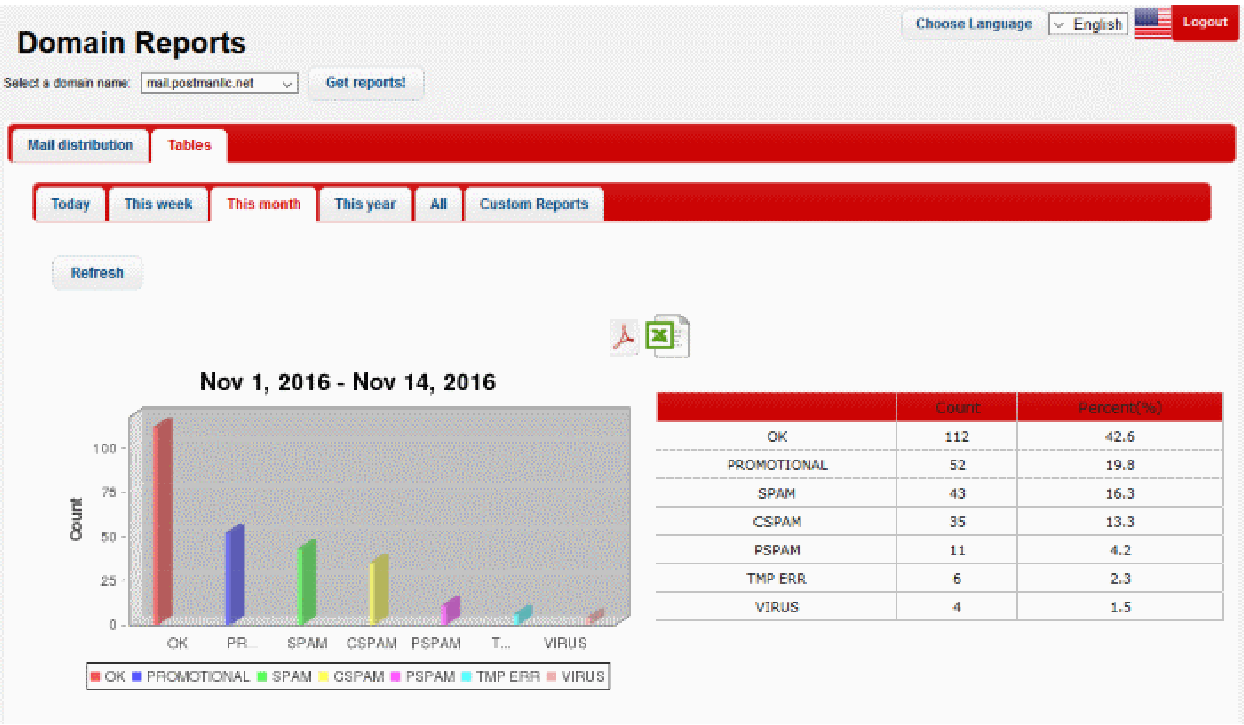
Mail Distribution Progress:

The 'Mail Distribution Progress' bar chart shows how many mails of each category were sent/received on each day. over a period of a month or a year.

- To export the report to PDF, click the PDF icon at the bottom-right of either of the two-chart types:

Tables:

The 'Tables' report displays the number of mails sent/received in each every mail category. The bar graph displays 'Count' on the x-axis against the category of mails on the y-axis.

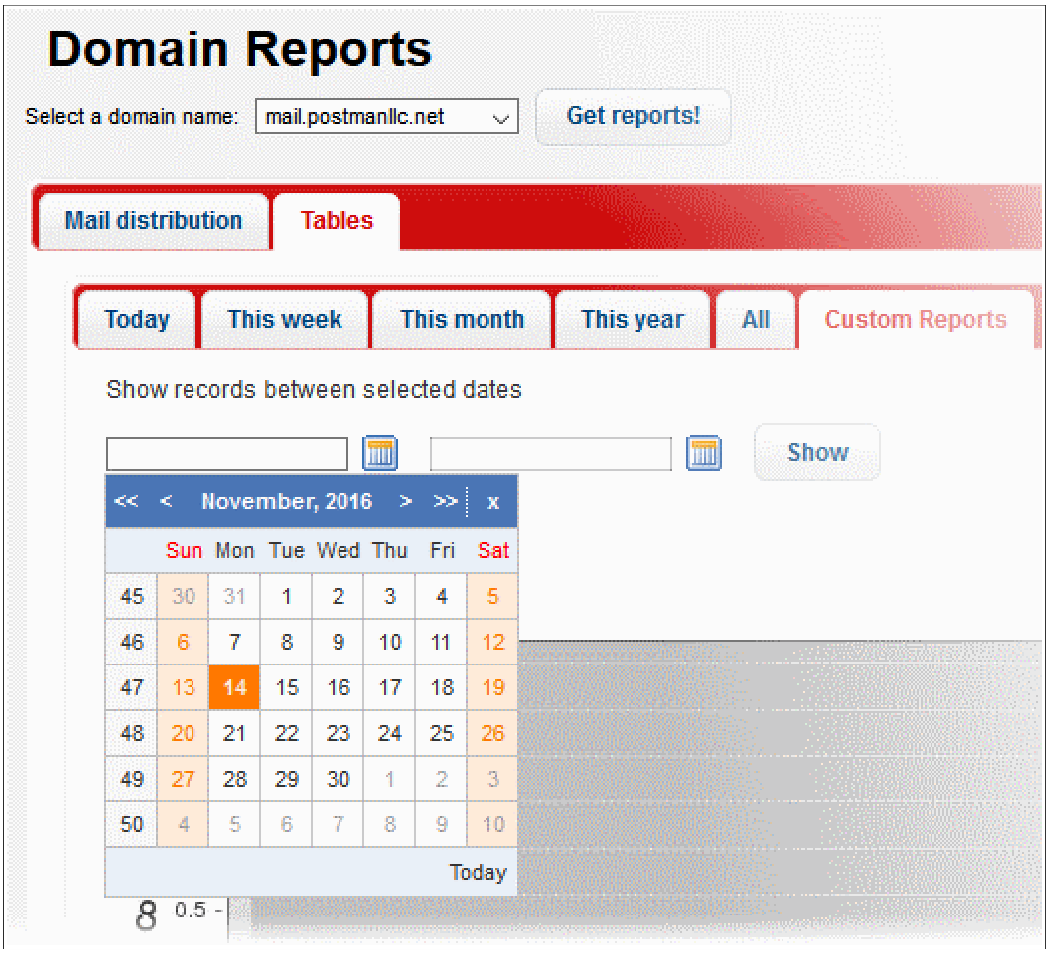


	Count	Percent(%)
OK	112	42.6
PROMOTIONAL	52	19.8
SPAM	43	16.3
CSPAM	35	13.3
PSPAM	11	4.2
TMP ERR	6	2.3
VIRUS	4	1.5

To generate a custom report in table format

- Click the 'Custom Reports' tab at the top

The fields to select the 'From' and 'To' period will be displayed.



Domain Reports

Select a domain name: mail.postmanllc.net ⌵ Get reports!

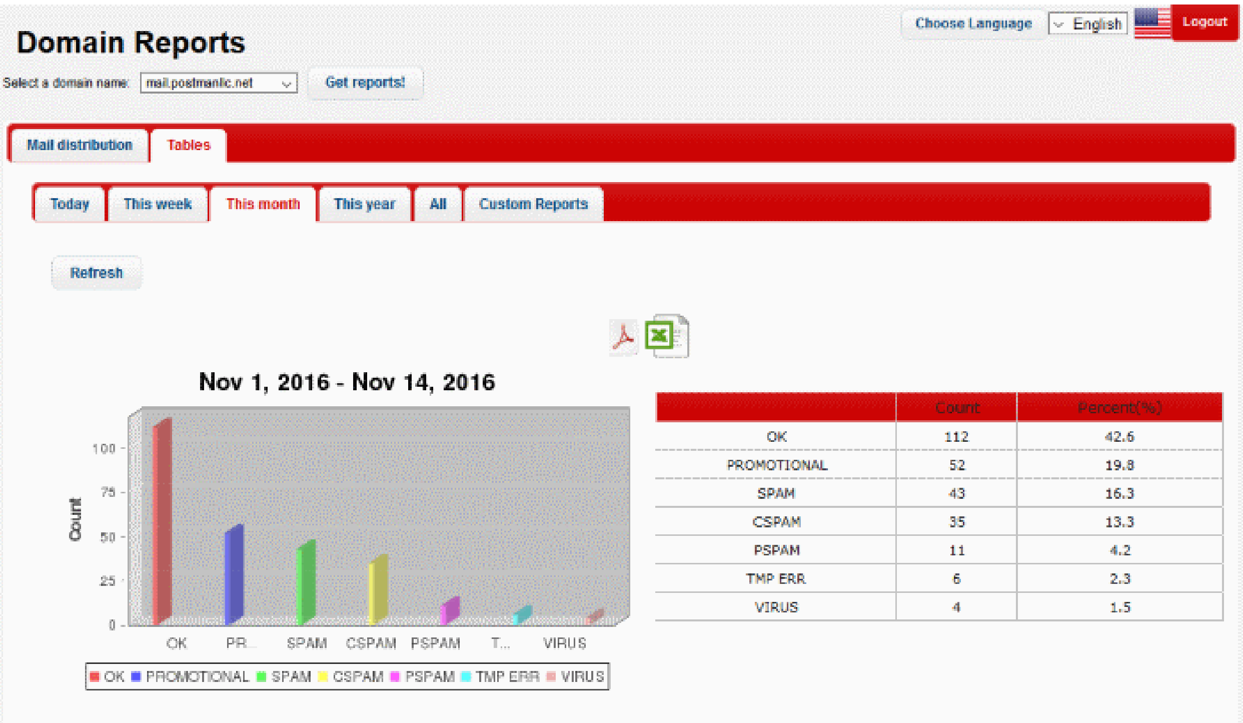
Show records between selected dates

<< < November, 2016 > >> x

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
45	30	31	1	2	3	4	5
46	6	7	8	9	10	11	12
47	13	14	15	16	17	18	19
48	20	21	22	23	24	25	26
49	27	28	29	30	1	2	3
50	4	5	6	7	8	9	10

Today

- Click on the fields or calendar icon and select the period from the calendar.
- Click 'Show' after selecting the custom period.



Domain Reports

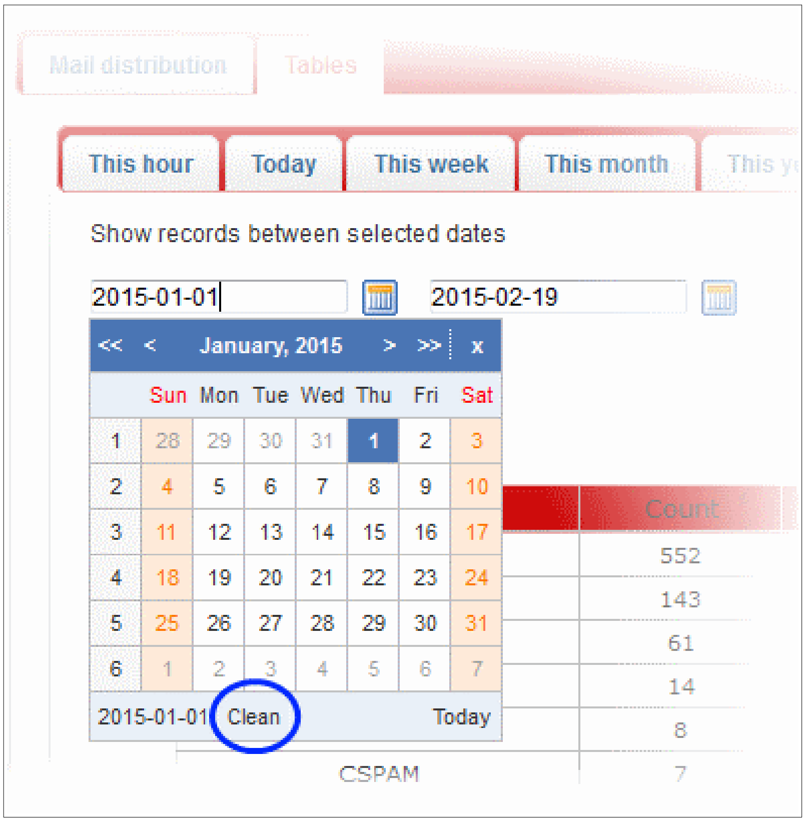
Select a domain name: mail.postmanllc.net ⌵ Get reports!

Nov 1, 2016 - Nov 14, 2016

	Count	Percent(%)
OK	112	42.6
PROMOTIONAL	52	19.8
SPAM	43	16.3
CSPAM	35	13.3
PSPAM	11	4.2
TMP ERR	6	2.3
VIRUS	4	1.5

The report for the selected custom period will be displayed. The first column indicates the categorization of mails, the second column displays the number for each category and the third column provides the results in percentage for each category.

- To download the custom report in PDF format, click the PDF icon and click 'OK' in the download dialogue to save the report.
- To download the custom report in XLS (spreadsheet) format, click the XLS icon and click 'OK' in the download dialogue to save the report.
- To clear the custom period, click on the period fields or calendar icon and click the 'Clean' button.



Show records between selected dates

2015-01-01 2015-02-19

<< < January, 2015 > >> x

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	28	29	30	31	1	2	3
2	4	5	6	7	8	9	10
3	11	12	13	14	15	16	17
4	18	19	20	21	22	23	24
5	25	26	27	28	29	30	31
6	1	2	3	4	5	6	7

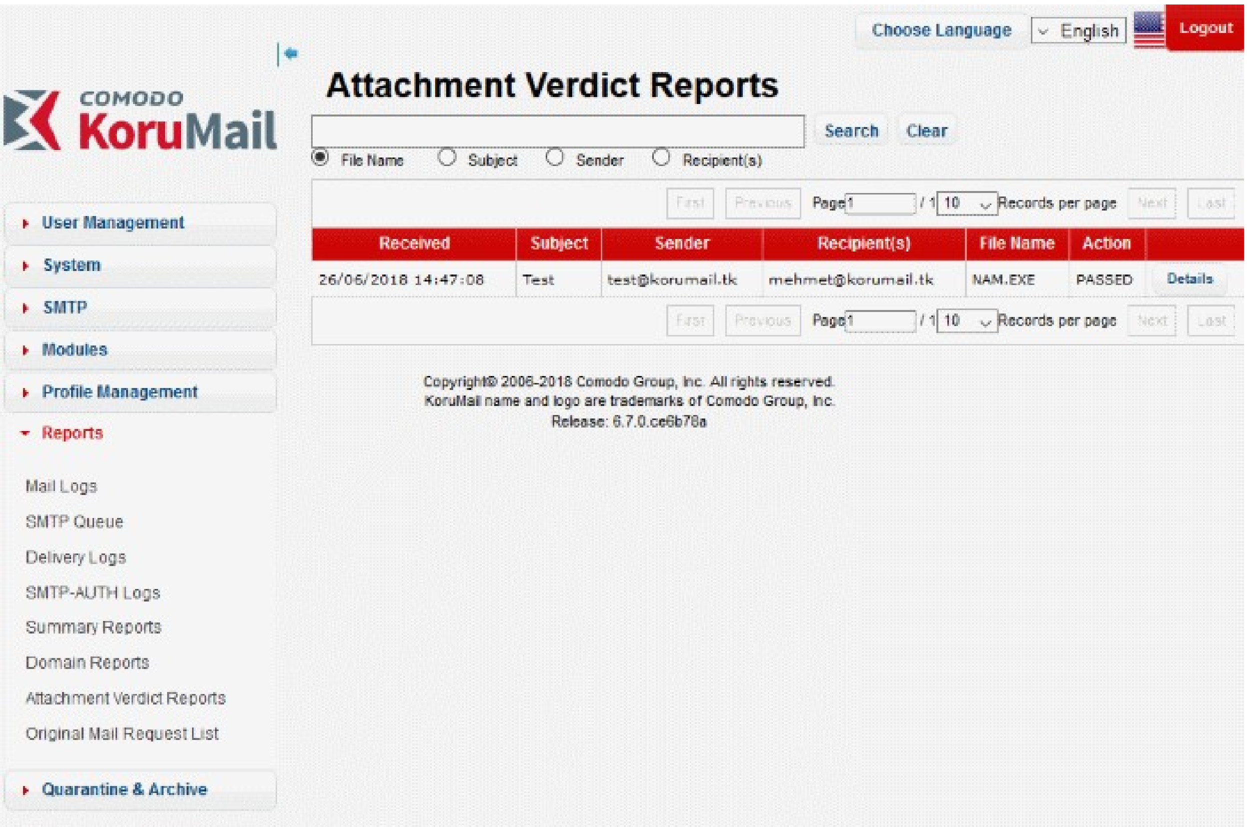
2015-01-01 Clean Today

10.7 Attachment Verdict Reports

The 'Attachment Verdict Reports' interface contains all the email attachment files for which Korumail has returned a verdict and the corresponding actions taken.

To open the interface

- Click 'Reports' on the left then click 'Attachment Verdict Reports'.



Attachment Verdict Reports

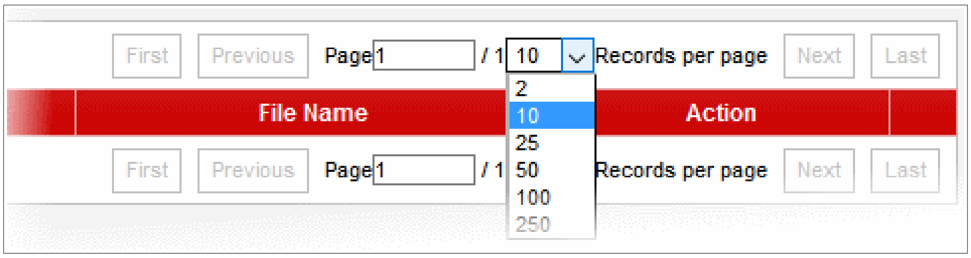
Received	Subject	Sender	Recipient(s)	File Name	Action	
26/06/2018 14:47:08	Test	test@korumail.tk	mehmet@korumail.tk	NAM.EXE	PASSED	Details

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

Attachment Verdict Report - Table of Column Descriptions	
Column Header	**Description**
Received	Date and time of email received by KoruMail.
Subject	Content in the 'Subject' line of the mails containing attachment.
Sender	Email address information of the originator
Recipient(s)	Domain name of the receiver
File Name	File that is given a verdict.
Action	Result of the valkyrie analysis verdict. For example 'Passed' or 'Rejected'

To configure the number of records to be displayed per page

- Click the 'Records per page' drop-down


First Previous Page 1 / 1 10 Records per page Next Last
File Name
Action
2
10
25
50
100
250
First Previous Page 1 / 1 50 Records per page Next Last

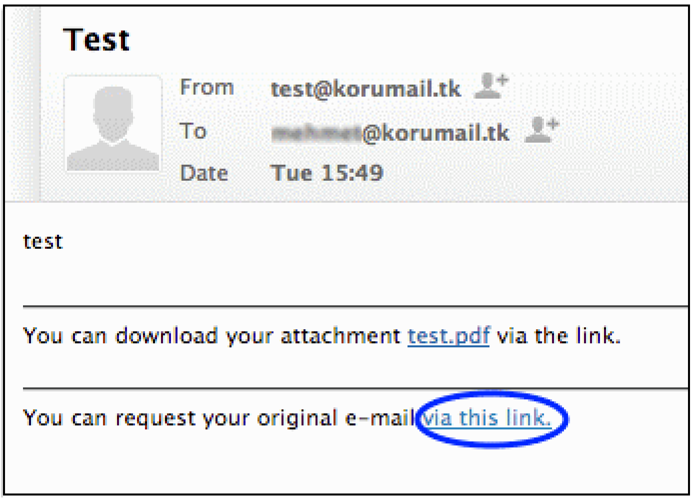
- Select the number of records per page to be displayed from the options. The default is 10.
- Click the 'First', 'Previous', 'Next' and 'Last' buttons to navigate through the report.

The 'Search' options allows you to search for a particular record or records based on the 'Filename', 'Subject', 'Sender' or 'Recipient(s)' of the file with verdict.

- To search for records based on the entries under 'Filename', 'Subject', 'Sender' or 'Recipient(s)' of the file with verdict reports, click any one of the radio buttons and enter the text or number fully or partially in the text field and then click the 'Search' button
- To refresh search, click 'Clear'.

10.8 Original Mail Request Sent

- The 'Original Mail Request Sent' section allows users to view original mails if containment feature is enabled.



Test

From test@korumail.tk

To [redacted]@korumail.tk

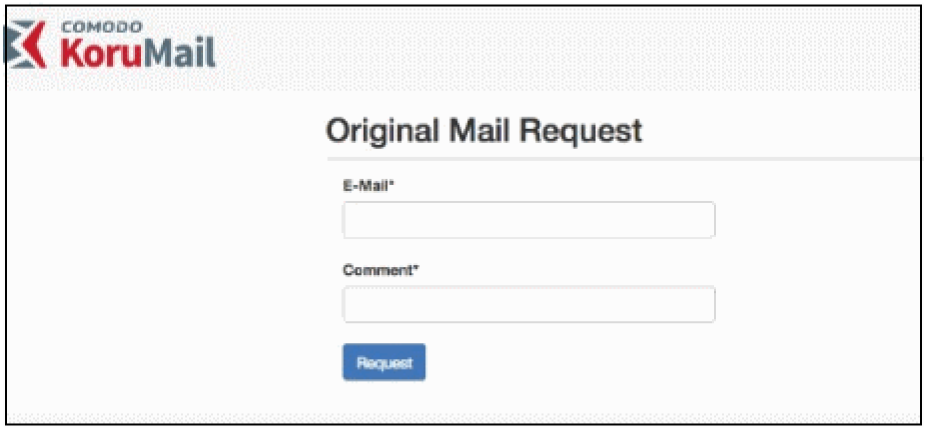
Date Tue 15:49

test

You can download your attachment test.pdf via the link.

You can request your original e-mail via this link.

- Click the original email link in that email and fill the form displayed as a record.



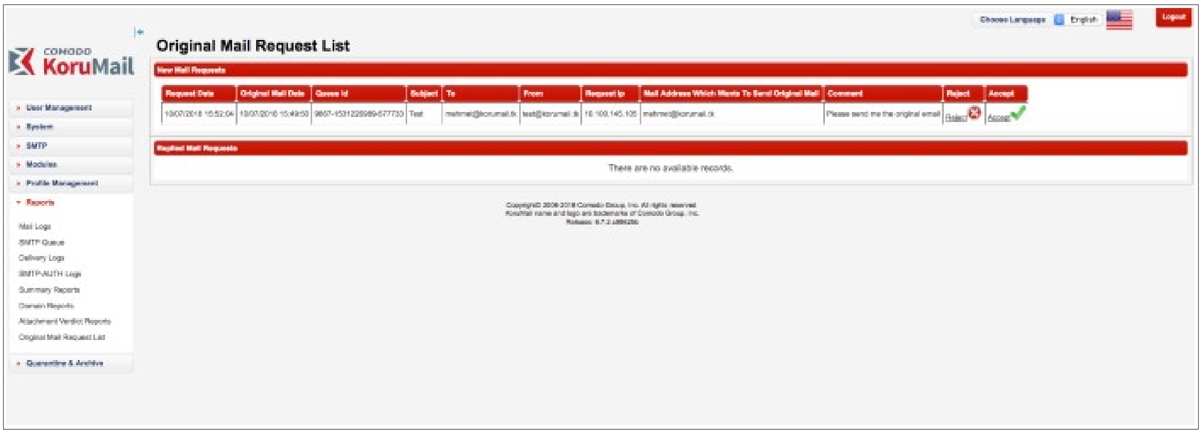
Original Mail Request

E-Mail*

Comment*

Request

- Fill the form and send to admins for approval.



Original Mail Request List

New Mail Requests

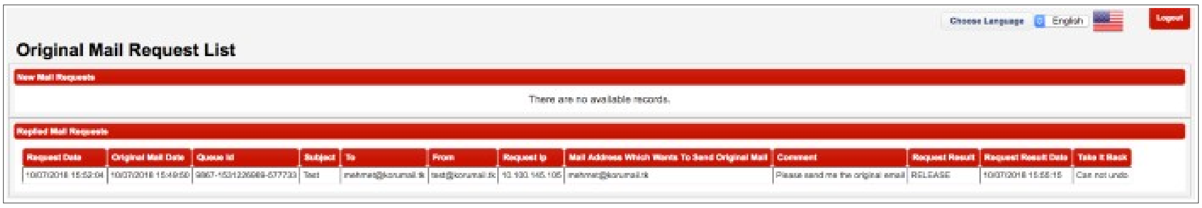
Request Date	Original Mail Date	Queue Id	Subject	To	From	Request Ip	Mail Address Which Wants To Send Original Mail	Comment	Reject	Accept
10/07/2018 15:52:04	10/07/2018 15:49:50	9867-1531228989-577733	Test	mehmet@korumail.tk	test@korumail.tk	10.100.145.105	mehmet@korumail.tk	Please send me the original email	Reject	Accept ✓

Replied Mail Requests

There are no available records.

Copyright© 2006-2018 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 6.7.3.a886256

- The administrator will reply by clicking 'Accept' or 'Reject' against the request row in the 'New Mail Request' section



Original Mail Request List

New Mail Requests

There are no available records.

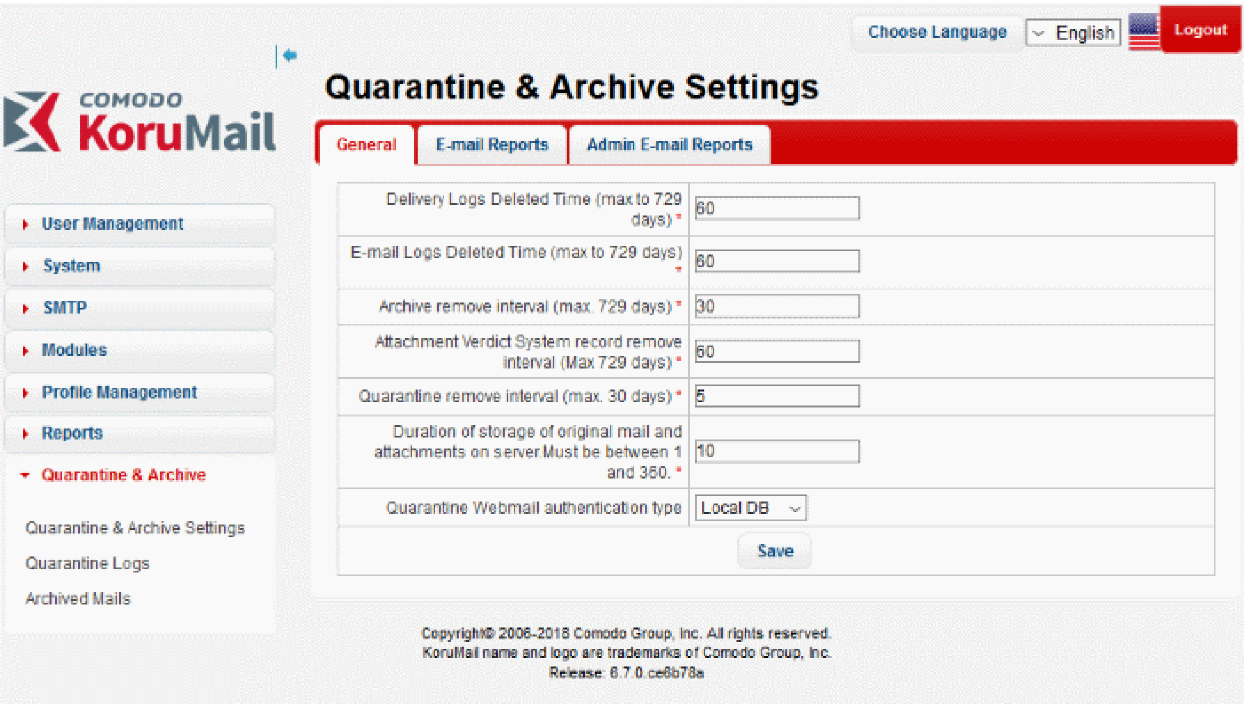
Replied Mail Requests

Request Date	Original Mail Date	Queue Id	Subject	To	From	Request Ip	Mail Address Which Wants To Send Original Mail	Comment	Request Result	Request Result Date	Take It Back
10/07/2018 15:52:04	10/07/2018 15:49:50	9867-1531226989-677733	Test	mehmet@korumail.tk	test@korumail.tk	10.100.145.105	mehmet@korumail.tk	Please send me the original email	RELEASE	10/07/2018 15:55:15	Can not undo

Admins can view the request result record listed in the 'Replied Mail Requests' section in the Original Mail Request List' interface.

11 Quarantine & Archive

- The 'Quarantine & Archive' sections allows administrators to configure the number of days that logs and archived files should be retained in KoruMail.
- Details of 'Quarantine Logs' and 'Archived Mails' can also be viewed, category changed and records exported to a CSV file.



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 following links for more details:

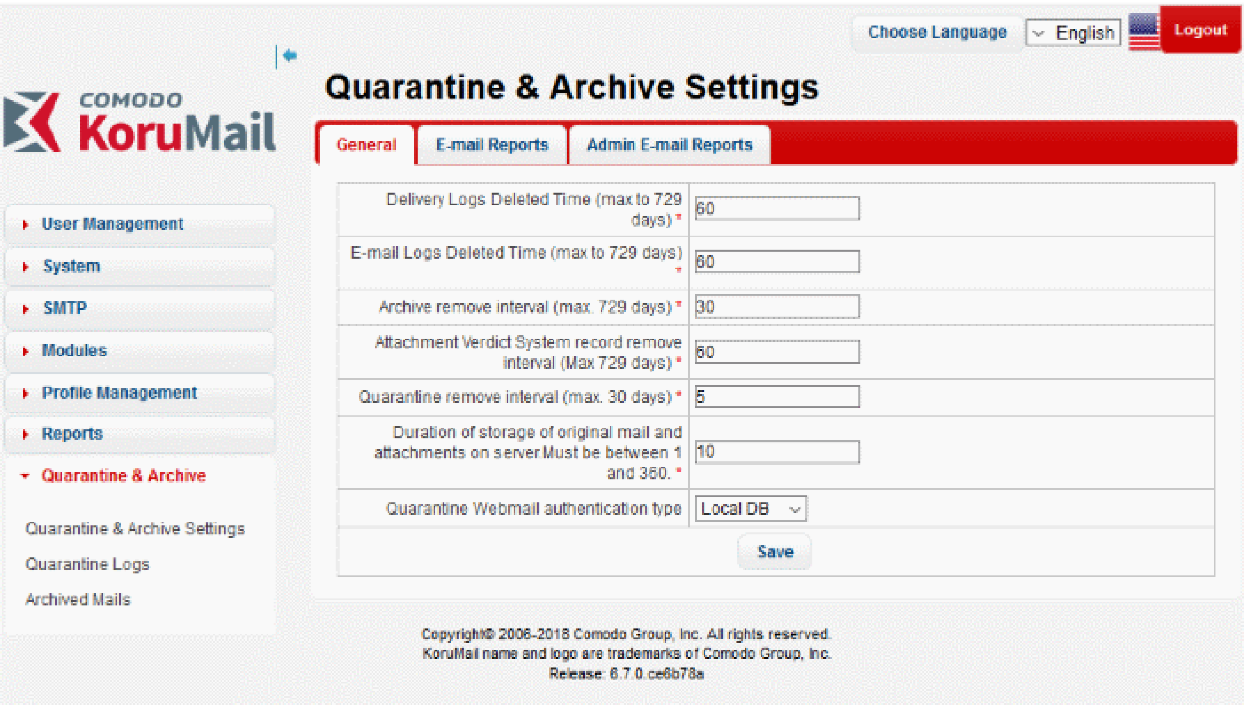
- Quarantine & Archive Settings
- Quarantine Logs
- Archived Mails

11.1 Quarantine & Archive Settings

- The 'Quarantine & Archive Settings' interface allows administrators to set the period to retain 'Mail Logs', 'Archived Mails' and 'Quarantine Logs' in KoruMail.
- You can also set the method of user authentication for accessing their quarantined email at 'Quarantine Webmail' interface.
- Admins can also create a mail template that is sent to users as notification to access their quarantined mails.

To open the interface,

- Click 'Quarantine & Archive' and then click '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 following links for more details:

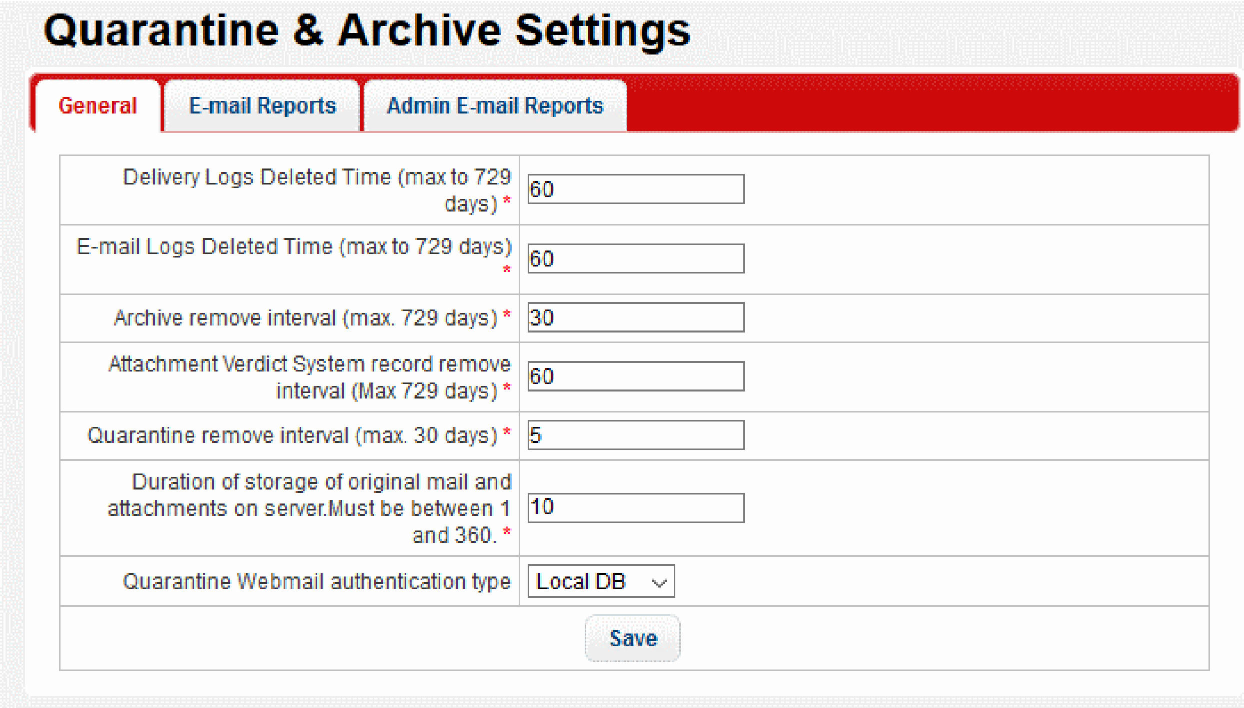
- **Quarantine & Archive General Settings**
- **Email Reports Settings**
- **Admin Email Reports Settings**

11.1.1 Quarantine & Archive General Settings

- The 'General' tab in 'Quarantine & Archive Settings' allows administrators to set the period to retain 'Mail Logs', 'Archived Mails' and 'Quarantine Logs' in KoruMail.
- Admins can also set the method of user authentication for users who access their quarantined emails at 'Quarantined Webmail' interface.

To open the interface,

- Click the 'General' tab in the 'Quarantine & Archive' screen



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

Quarantine & Archive General Settings - Table of Parameters	
Parameter	**Description**
Delivery Logs Deleted Time	Enter the number of days for which the delivery logs will be retained. The maximum period is729 days. See '**Delivery Logs Report**' for more details
E-mail Logs Deleted Time	Enter the number of days for which the email logs will be retained. The maximum period is 729 days. See '**Mail Logs Report**' for more details.
Archive remove interval	Enter the number of days for which the archived mail records will be retained. The maximum period is 729 days. See '**Archived Mails**' for more details.
Attachment Verdict System record remove Interval	Enter the number of days for which the Attachment verdict records will be retained. The maximum period is 729 days. See '**Attachment Verdict System**' for more details.
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. See '**Quarantine Logs**' for more details.
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 on the KoruMail server. 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.

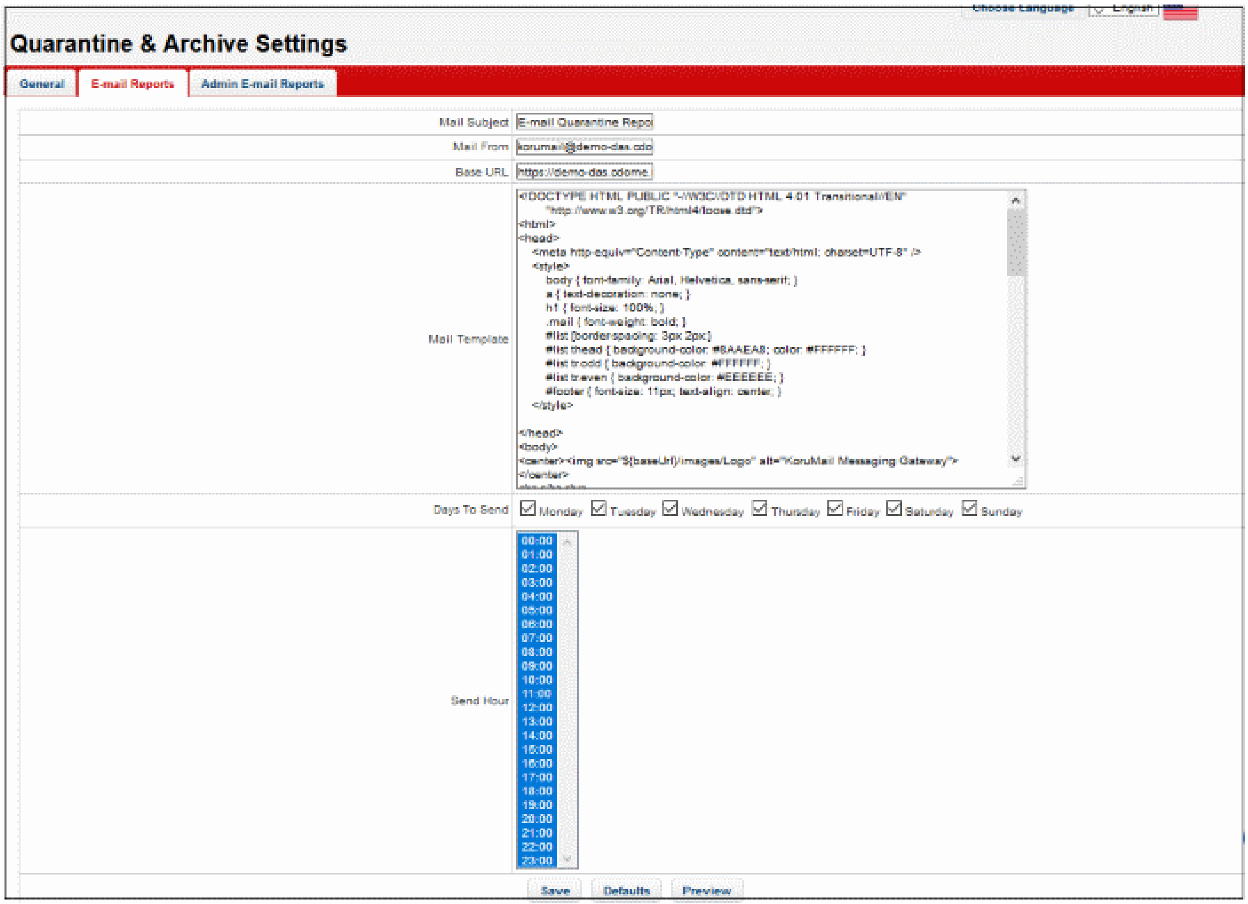
- Click 'Save' to apply your changes.

11.1.2 Email Reports Settings

- KoruMail allows users to access their quarantined emails via a separate web based quarantine page that contains all their quarantined messages.
- The 'Email Report' section allows admins to configure the URL of the 'Quarantine Webmail' page, the email notification subject line, from address, mail message template and the days and time the email should be sent to users.
- Please note the users should be added in '**Quarantine Webmail Users**' and password set for them to access the 'Quarantine Webmail' page.
- The 'Send daily quarantine report to recipients' check box should also be enabled in the '**Archive And Quarantine**' tab of the profile if applied to the users.
- Quarantine report is sent only for the following mail types:
  - Spam
  - Probable spam
  - RFC blacklist
  - Promotional mails

To open the 'E-mail Reports' interface,

- Click the 'E-mail Reports' tab in the 'Quarantine & Archive' screen.



Mail Subject: E-mail Quarantine Repo

Mail From: korumail@demo-das.cdo

Base URL: https://demo-das.cdome

Mail Template:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
      "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
   <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
   <style>
      body { font-family: Arial, Helvetica, sans-serif; }
      a { text-decoration: none; }
      h1 { font-size: 100%; }
      .mail { font-weight: bold; }
      #list {border-spacing: 3px 2px;}
      #list thead { background-color: #8AAEA8; color: #FFFFFF; }
      #list tr.odd { background-color: #FFFFFF; }
      #list tr.even { background-color: #EEEEEE; }
      #footer { font-size: 11px; text-align: center; }
   </style>

</head>
<body>
<center><img src="${baseUrl}/images/Logo" alt="KoruMail Messaging Gateway">
</center>
```

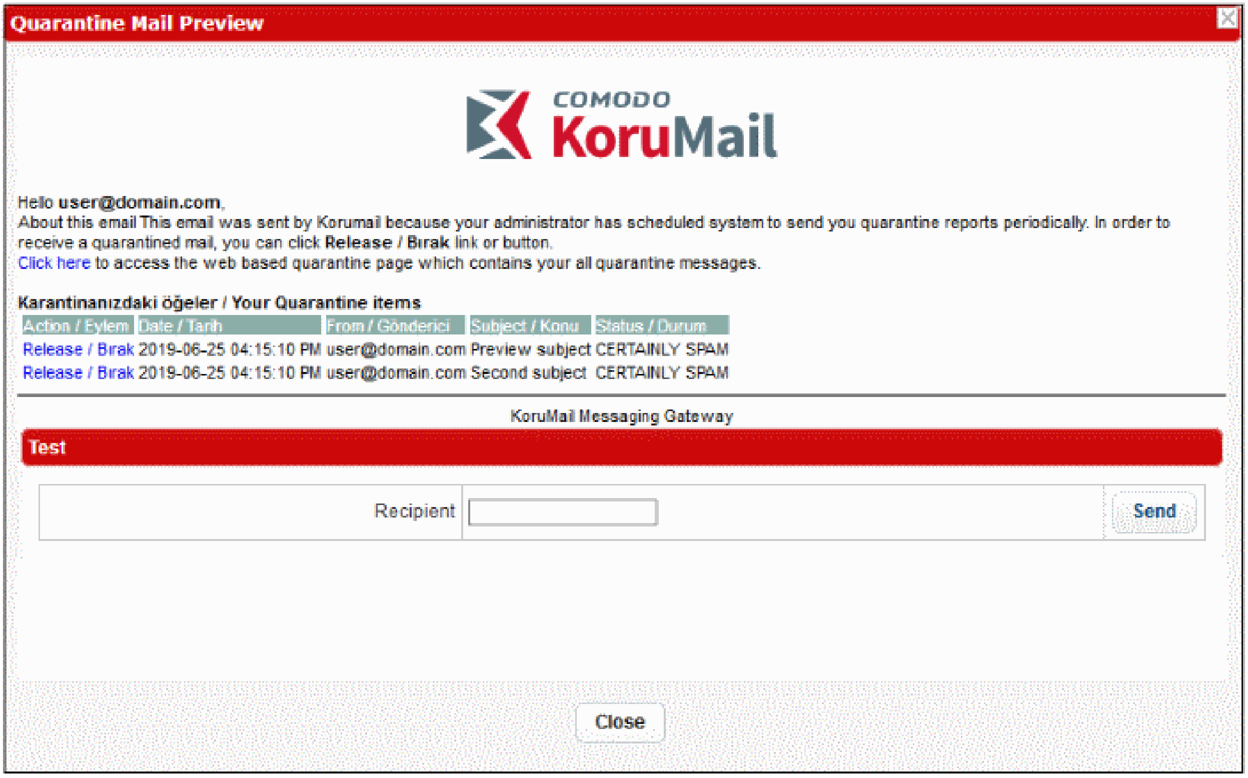
Days To Send: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Send Hour: 00:00, 01:00, 02:00, 03:00, 04:00, 05:00, 06:00, 07:00, 08:00, 09:00, 10:00, 11:00, 12:00, 13:00, 14:00, 15:00, 16:00, 17:00, 18:00, 19:00, 20:00, 21:00, 22:00, 23:00

Quarantine & Archive - E-mail Reports Settings - Table of Parameters	
Parameter	**Description**
Mail Subject	Enter the content for subject line for the automated email report

Mail From	Enter the address from which the email reports will be sent
Base URL	Enter URL of 'Quarantine Webmail' page that users should access to view their quarantined emails
Mail Template	The message body of the mail.
Days to Send	Select the day(s) when you want to send the email notifications
Send Hour	Select the hour of the day to send the email notifications for the selected days.

- Click 'Default' to restore the settings to default values.
- Click 'Preview' button to view the mail that will be sent to users



Hello **user@domain.com**,
About this email This email was sent by Korumail because your administrator has scheduled system to send you quarantine reports periodically. In order to receive a quarantined mail, you can click **Release / Bırak** link or button.
Click here to access the web based quarantine page which contains your all quarantine messages.

Karantinanızdaki öğeler / Your Quarantine items

Action / Eylem	Date / Tarih	From / Gönderici	Subject / Konu	Status / Durum
Release / Bırak	2019-06-25 04:15:10 PM	user@domain.com	Preview subject	CERTAINLY SPAM
Release / Bırak	2019-06-25 04:15:10 PM	user@domain.com	Second subject	CERTAINLY SPAM

KoruMail Messaging Gateway

- To test if the mails are delivered successfully, enter the user's email address in the 'Recipient' field and click 'Send'
- Click 'Close' to return to the 'E-mail Reports' interface.

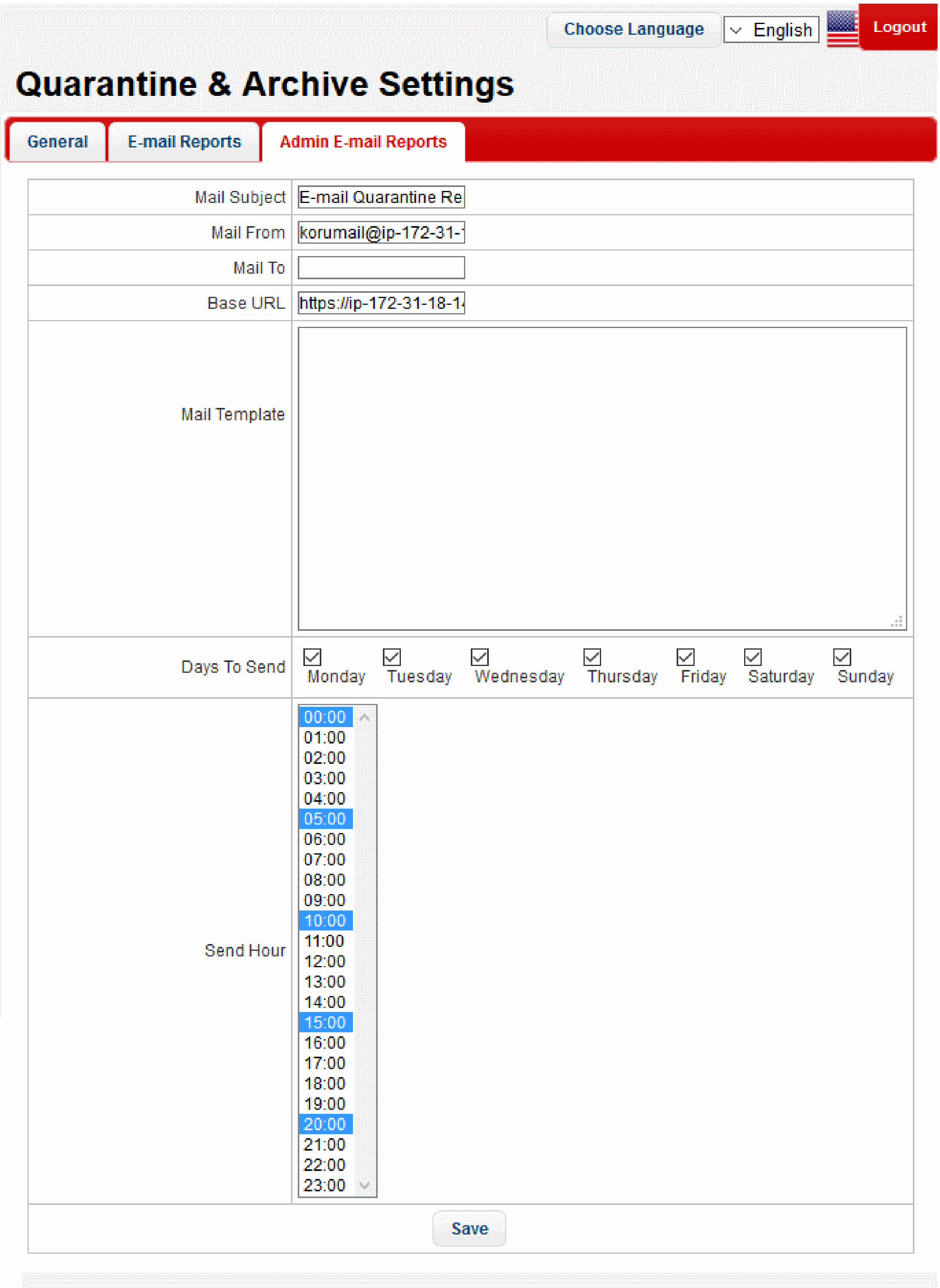
- Click 'Save' to apply your changes.

11.1.3 Admin Email Reports Settings

- KoruMail allows administrators to access all quarantined emails via a separate web based quarantine page that contains all their quarantined messages.
- The 'Admin Email Reports' section allows admins to configure the URL of the 'Quarantine Webmail' page, the email notification subject line, from address, to address mail message template and the days and time the email should be sent to users.

To open the 'Admin E-mail Reports' interface,

- Click 'Quarantine & Archive Settings' > 'Admin E-mail Reports' tab in the 'Quarantine & Archive' screen.



Quarantine & Archive Settings

Mail Subject	E-mail Quarantine Re
Mail From	korumail@ip-172-31-1
Mail To	
Base URL	https://ip-172-31-18-1
Mail Template	
Days To Send	☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday
Send Hour	00:00, 05:00, 10:00, 15:00, 20:00 selected (list 00:00 – 23:00)

Quarantine & Archive – Admin E-mail Reports Settings - Table of Parameters	
Parameter	**Description**
Mail Subject	Enter the content for subject line for the automated email report

Mail From	Enter the address from which the email reports will be sent
Mail To	Enter the administrator's email address at which the email reports will be received
Base URL	Enter URL of 'Quarantine Webmail' page that users should access to view their quarantined emails
Mail Template	The message body of the mail.
Days to Send	Select the day(s) when you want to send the email notifications
Send Hour	Select the hour of the day to send the email notifications for the selected days.

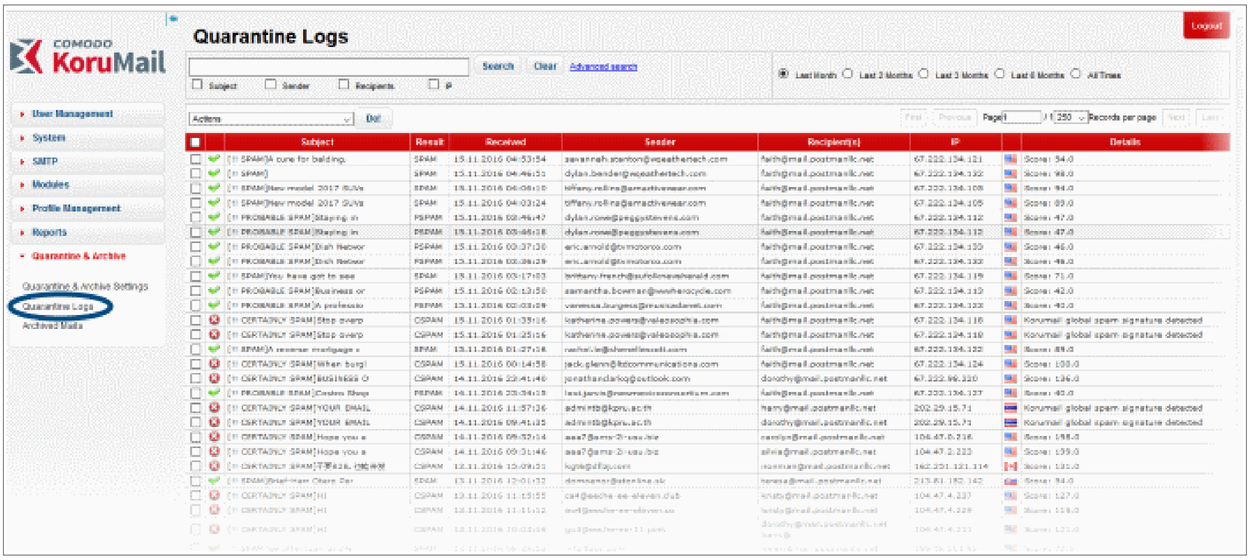
- Click 'Save' to apply your changes.

11.2 Quarantine Logs

- The 'Quarantine Logs' interface displays the log records of all quarantined mails.
- The number of days the logs are stored depends on the settings configured in the '**Quarantine & Archive General Settings**' screen.
- The interface allows administrators to take actions such as to delete, mark as not spam and more.

To open the interface,

- Click 'Quarantine & Archive' > 'Quarantine Logs'



Quarantine Logs

□ Subject □ Sender □ Recipients □ IP

● Last Month ○ Last 2 Months ○ Last 3 Months ○ Last 6 Months ○ All Times

Page 1 / 1 250 Records per page

□		Subject	Result	Received	Sender	Recipient(s)	IP		Details
□	✓	[!! SPAM]A cure for balding.	SPAM	15.11.2016 04:53:54	savannah.stanton@wpeathertech.com	faith@mail.postmanllc.net	67.222.134.121		Score: 34.0
□	✓	[!! SPAM]	SPAM	15.11.2016 04:46:51	dylan.bender@wpeathertech.com	faith@mail.postmanllc.net	67.222.134.132		Score: 98.0
□	✓	[!! SPAM]New model 2017 SUVs	SPAM	15.11.2016 04:06:10	tiffany.rollins@amactivewear.com	faith@mail.postmanllc.net	67.222.134.108		Score: 94.0
□	✓	[!! SPAM]New model 2017 SUVs	SPAM	15.11.2016 04:03:24	tiffany.rollins@amactivewear.com	faith@mail.postmanllc.net	67.222.134.105		Score: 89.0
□	✓	[!! PROBABLE SPAM]Staying in	PSPAM	15.11.2016 03:46:47	dylan.rose@peggystevens.com	faith@mail.postmanllc.net	67.222.134.112		Score: 47.0
□	✓	[!! PROBABLE SPAM]Staying in	PSPAM	15.11.2016 03:46:18	dylan.rose@peggystevens.com	faith@mail.postmanllc.net	67.222.134.112		Score: 47.0
□	✓	[!! PROBABLE SPAM]Dish Networ	PSPAM	15.11.2016 03:37:30	eric.arnold@bvmotorco.com	faith@mail.postmanllc.net	67.222.134.130		Score: 46.0
□	✓	[!! PROBABLE SPAM]Dish Networ	PSPAM	15.11.2016 03:36:29	eric.arnold@bvmotorco.com	faith@mail.postmanllc.net	67.222.134.133		Score: 46.0
□	✓	[!! SPAM]You have got to see	SPAM	15.11.2016 03:17:03	brittany.french@suffolknewsherald.com	faith@mail.postmanllc.net	67.222.134.119		Score: 71.0
□	✓	[!! PROBABLE SPAM]Business or	PSPAM	15.11.2016 02:13:58	samantha.bowman@wwheracycle.com	faith@mail.postmanllc.net	67.222.134.113		Score: 42.0
□	✓	[!! PROBABLE SPAM]A professio	PSPAM	15.11.2016 02:03:29	vanessa.burgess@musicadanet.com	faith@mail.postmanllc.net	67.222.134.133		Score: 40.0
□	✗	[!! CERTAINLY SPAM]Stop overp	CSPAM	15.11.2016 01:35:16	katherine.powers@valeosophia.com	faith@mail.postmanllc.net	67.222.134.116		Korumail global spam signature detected
□	✗	[!! CERTAINLY SPAM]Stop overp	CSPAM	15.11.2016 01:25:16	katherine.powers@valeosophia.com	faith@mail.postmanllc.net	67.222.134.118		Korumail global spam signature detected
□	✓	[!! SPAM]A reverse mortgage s	SPAM	15.11.2016 01:27:18	rachel.lee@sherwilliesalt.com	faith@mail.postmanllc.net	67.222.134.122		Score: 89.0
□	✗	[!! CERTAINLY SPAM]When burgl	CSPAM	15.11.2016 00:14:58	jack.glenn@lbdcommunications.com	faith@mail.postmanllc.net	67.222.134.124		Score: 100.0
□	✗	[!! CERTAINLY SPAM]BUSINESS O	CSPAM	14.11.2016 23:41:40	jonathandarkq@outlook.com	dorothy@mail.postmanllc.net	67.222.98.220		Score: 136.0
□	✓	[!! PROBABLE SPAM]Casino Shop	PSPAM	14.11.2016 23:34:18	lexi.jarvis@[illegible].com	faith@mail.postmanllc.net	67.222.134.127		Score: 40.0
□	✗	[!! CERTAINLY SPAM]YOUR EMAIL	CSPAM	14.11.2016 11:57:16	adminfb@kpru.ac.th	harry@mail.postmanllc.net	202.29.15.71		Korumail global spam signature detected
□	✗	[!! CERTAINLY SPAM]YOUR EMAIL	CSPAM	14.11.2016 09:41:35	adminfb@kpru.ac.th	dorothy@mail.postmanllc.net	202.29.15.71		Korumail global spam signature detected
□	✗	[!! CERTAINLY SPAM]Hope you a	CSPAM	14.11.2016 09:32:14	aaa7@ams-3-usa.biz	carolyn@mail.postmanllc.net	104.47.0.218		Score: 158.0
□	✗	[!! CERTAINLY SPAM]Hope you a	CSPAM	14.11.2016 09:31:46	aaa7@ams-3-usa.biz	silvia@mail.postmanllc.net	104.47.2.223		Score: 155.0
□	✗	[!! CERTAINLY SPAM][illegible]	CSPAM	13.11.2016 15:09:33	[illegible]	norman@mail.postmanllc.net	162.251.121.114		Score: 131.0
□	✓	[!! SPAM][illegible]	SPAM	13.11.2016 12:01:32	[illegible]	teresa@mail.postmanllc.net	213.81.152.142		Score: 34.0
□	✗	[!! CERTAINLY SPAM]HI	CSPAM	13.11.2016 11:15:55	[illegible]	kristy@mail.postmanllc.net	104.47.4.227		Score: 127.0
□	✗	[!! CERTAINLY SPAM]HI	CSPAM	13.11.2016 11:11:12	[illegible]	[illegible]	104.47.4.229		Score: 119.0
□	✗	[!! CERTAINLY SPAM]HI	CSPAM	13.11.2016 10:03:08	[illegible]	dorothy@mail.postmanllc.net harry@	104.47.4.231		Score: 121.0
□	✓	[illegible]	SPAM	[illegible]	[illegible]	[illegible]	[illegible]		[illegible]

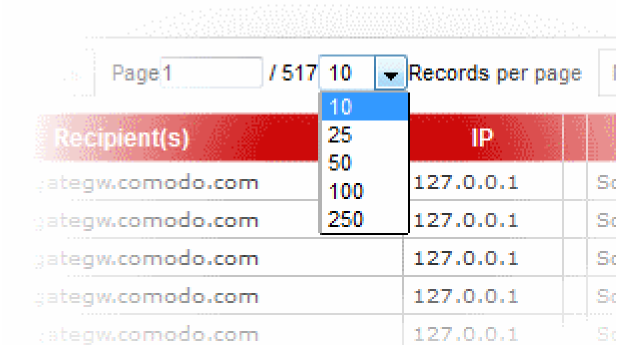
Quarantine Logs - Table of Column Descriptions	
Column Header	**Description**
Icon	Status of action for the mail applied by KoruMail after the filtering process. Placing your mouse cursor over an icon will show a description of the action. ✓ - Relayed: Indicates the mail has successfully passed the filtering process and user verified. ⊘ - Rejected: Indicates the mail is rejected by KoruMail after the filtering process and reject message sent to the sender mail server. ✗ - Discarded: Indicates the mail is quarantined

Subject	The content in the 'Subject' line of the mails
Result	The verdict on a email after filtering process. For example, 'CSPAM' means KoruMail found the mail was 'Certainly Spam'.
Received	Date and time of email was received by KoruMail
Sender	Email address information of the originator
Recipient(s)	Email address information of the receiver
IP	The network address of the system from where the mail was sent.
Details	Reason why a mail is quarantined and spam score if it is marked as spam.

At the top and bottom of the screen, you have the option to set the number of records to be displayed per page and take desired actions such as delete, mark as not spam and so on.

To configure the number of records to be displayed per page

- Click the 'Records per page' drop-down

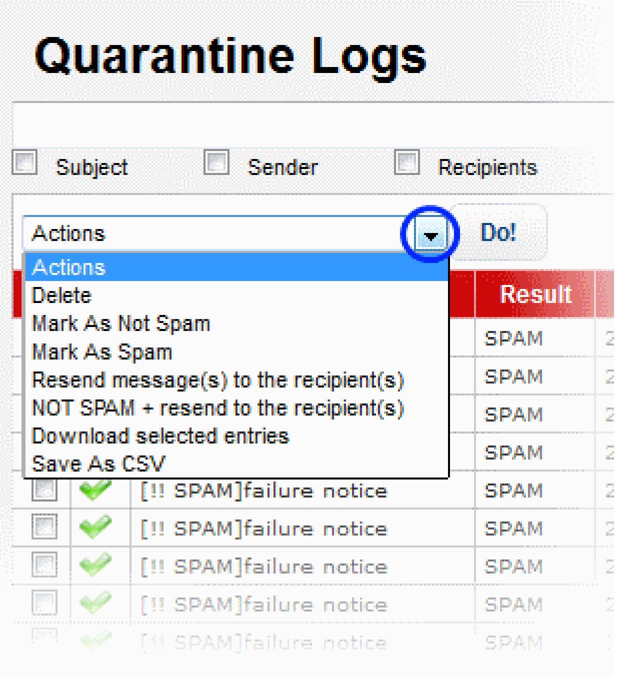


Recipient(s)	IP
ategw.comodo.com	127.0.0.1
ategw.comodo.com	127.0.0.1
ategw.comodo.com	127.0.0.1
ategw.comodo.com	127.0.0.1
ategw.comodo.com	127.0.0.1

- Select the number of records per page to be displayed from the options.
- Click the 'First', 'Previous', 'Next' and 'Last' buttons to navigate to the respective pages.

To act on log entries

- Click the 'Actions' drop-down


Quarantine Logs
□ Subject □ Sender □ Recipients
Actions
Do!
Actions
Delete
Mark As Not Spam
Mark As Spam
Resend message(s) to the recipient(s)
NOT SPAM + resend to the recipient(s)
Download selected entries
Save As CSV
Result
[!! SPAM]failure notice
SPAM

- Select the desired action from the drop-down and click the 'Do' button

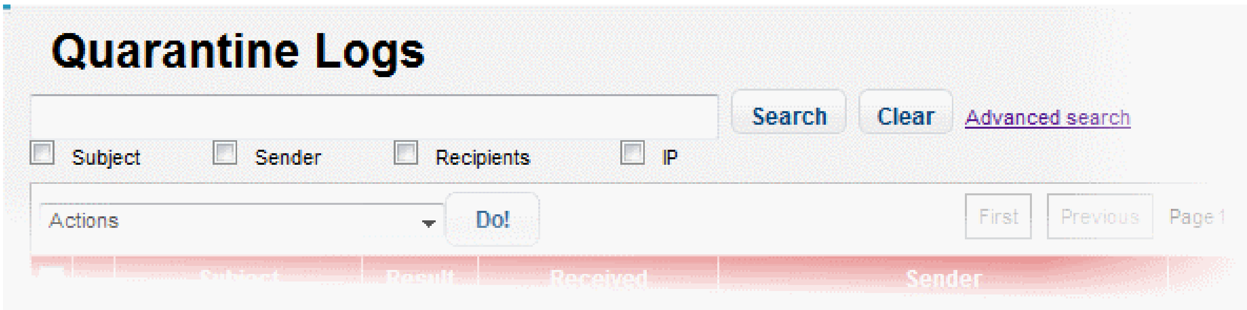
Search Options

You can search for a particular record or records in the quarantine log by using simple or advanced search feature.

- Simple Search
- Advanced Search

Simple Search

The simple search options allows you to search for a particular record or records based on 'Subject', 'Sender', 'Recipients' and / or 'IP' details only.

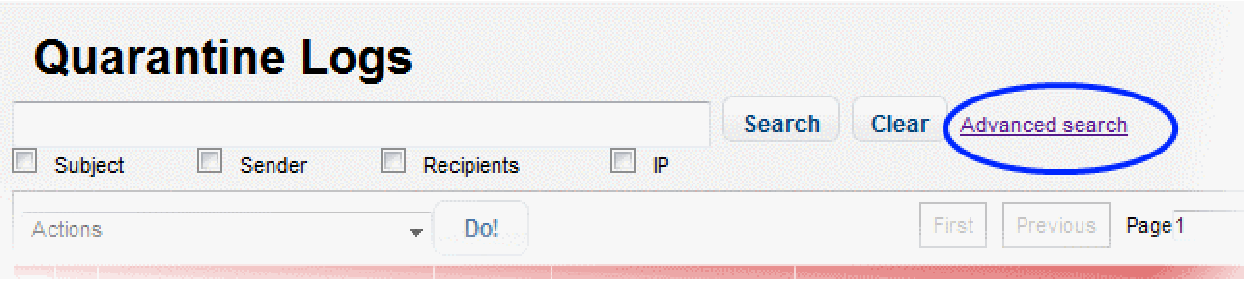


- To search for records based on the entries under 'Subject', 'Sender', 'Recipients' and / or 'IP' columns, enter the text or number fully or partially in the field and click the 'Search' button
- To search for records based on the entries under a particular column or columns, select the respective check boxes, enter the text or number fully or partially in the field and click the the 'Search' button. For example, if you want to search for a particular record for sender and recipients, select the 'Sender' and 'Recipients' check boxes, enter the text fully or partially in the field and click the 'Search' button.

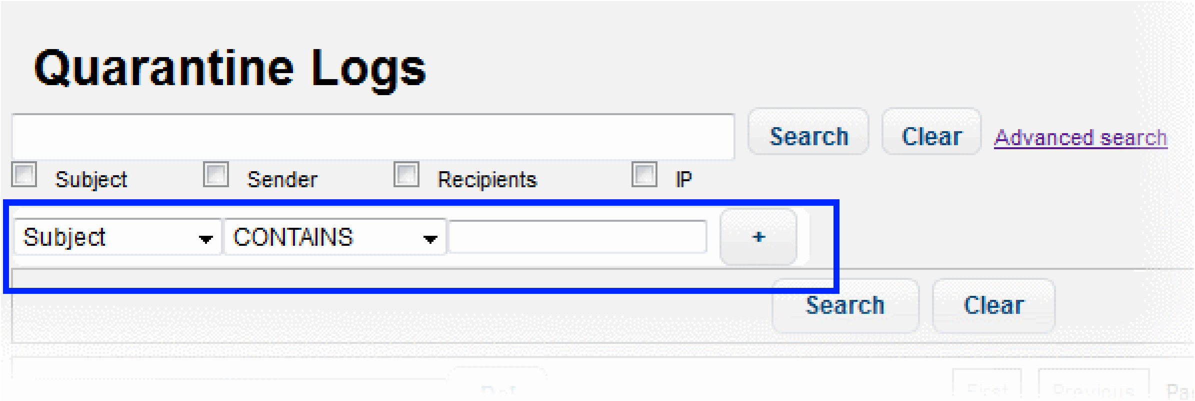
Advanced Search

The 'Advanced Search' option allows you a more granular search by including rules and filters.

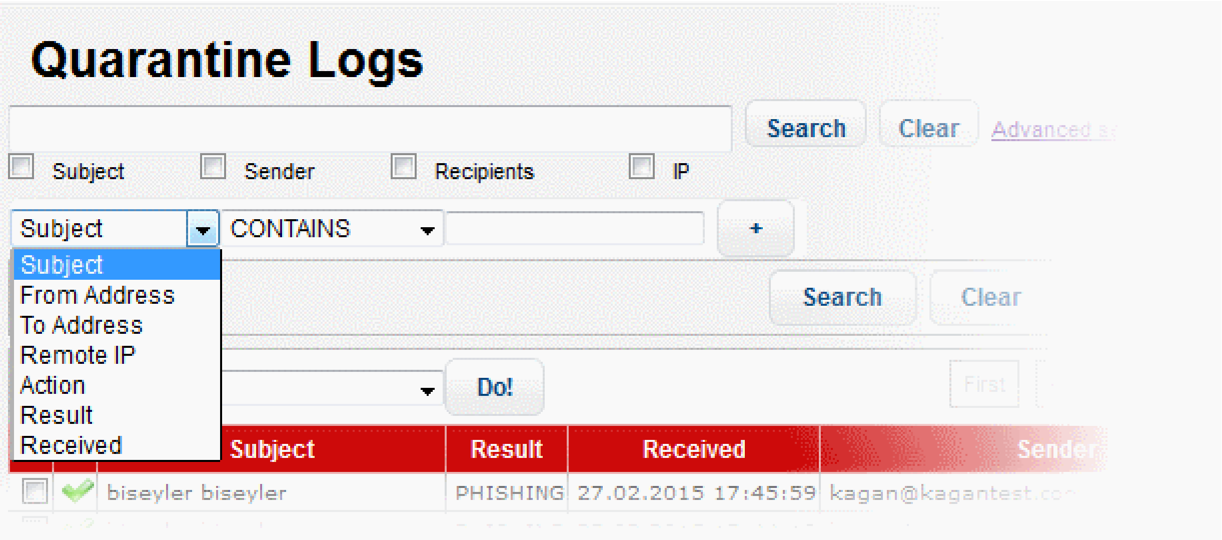
- Click the 'Advanced Search' link at the top of the screen.



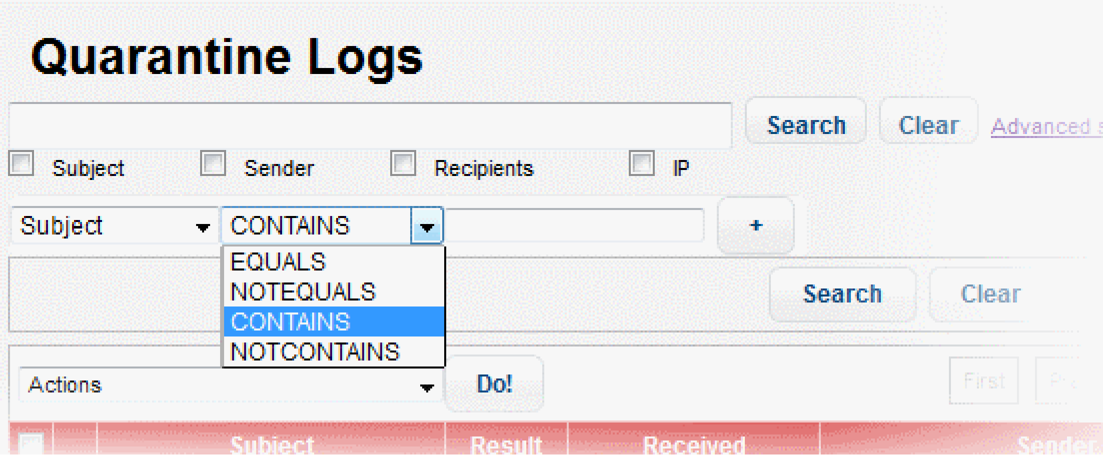
The 'Advanced Search' option will be displayed.



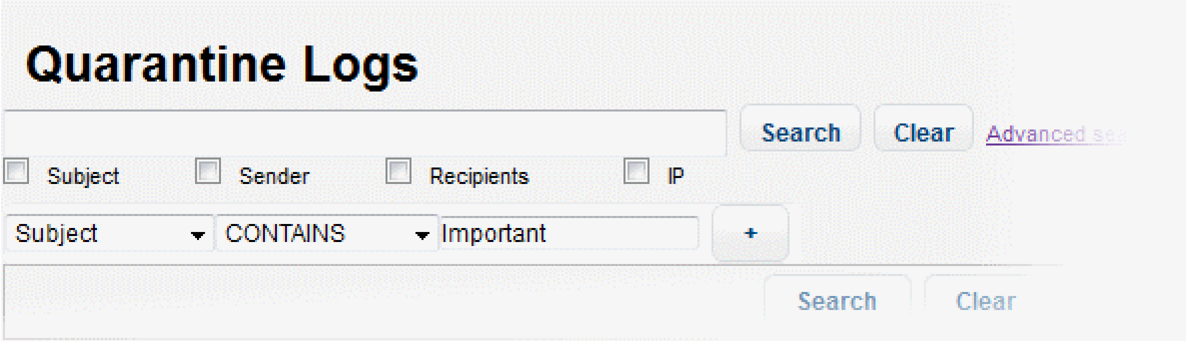
The first drop-down contains the column headers that can be selected for an advanced search.



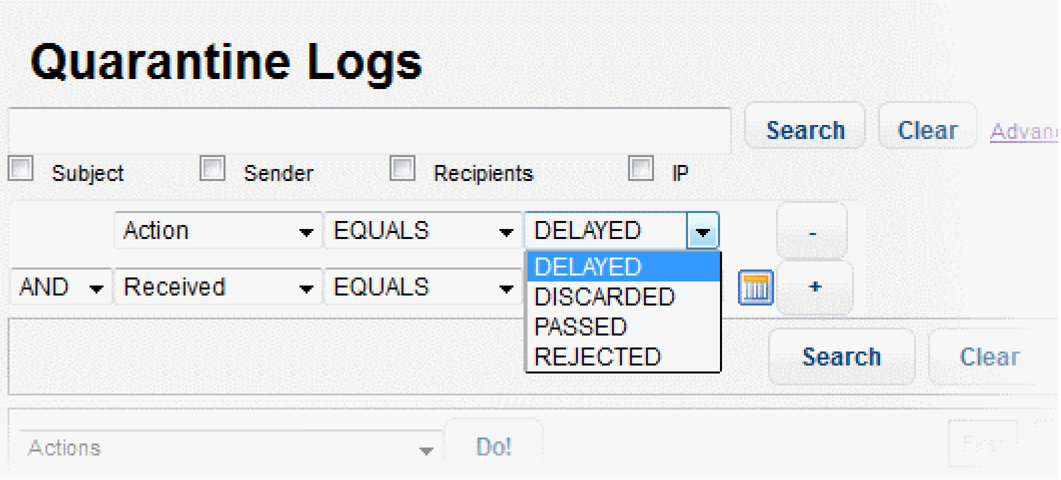
The second column contains the condition for a search, which depends on the item selected in the first column and text/number entered or options selected in the third column.



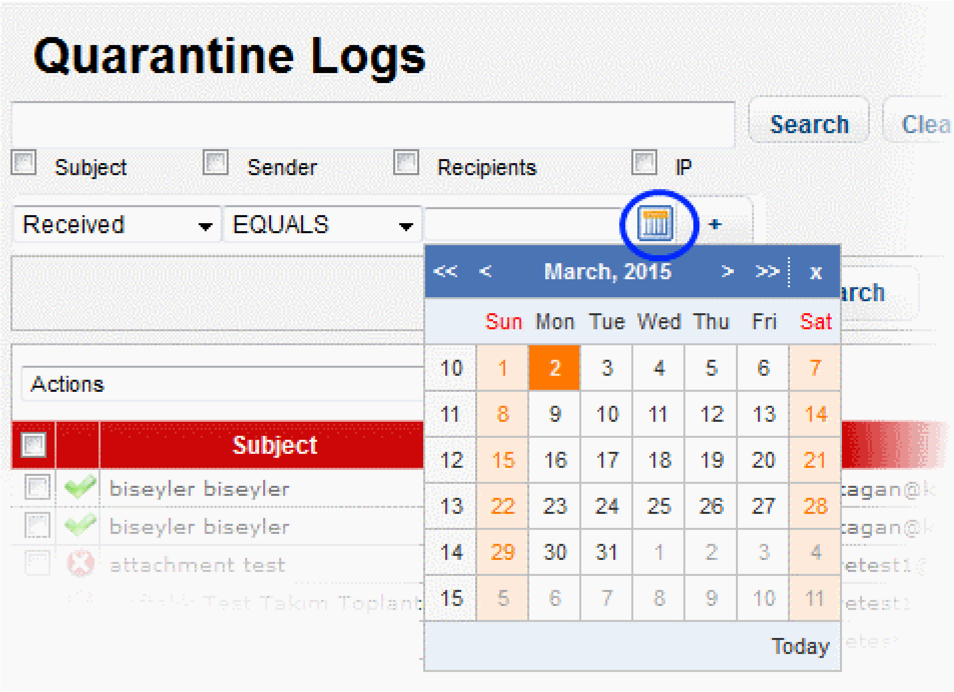
The third column allows you to enter the text/number or select from the options depending on the selection in the first column. For example, choosing 'Subject', 'From Address' or 'Remote IP' allows you to enter the text in the third column



If you select 'Action' or 'Result' in the first column, then further options can be selected from the third column.



If you select 'Received' in the first column, then you can enter a date or select from the calendar.



Quarantine Logs

Search | Clea

□ Subject □ Sender □ Recipients □ IP

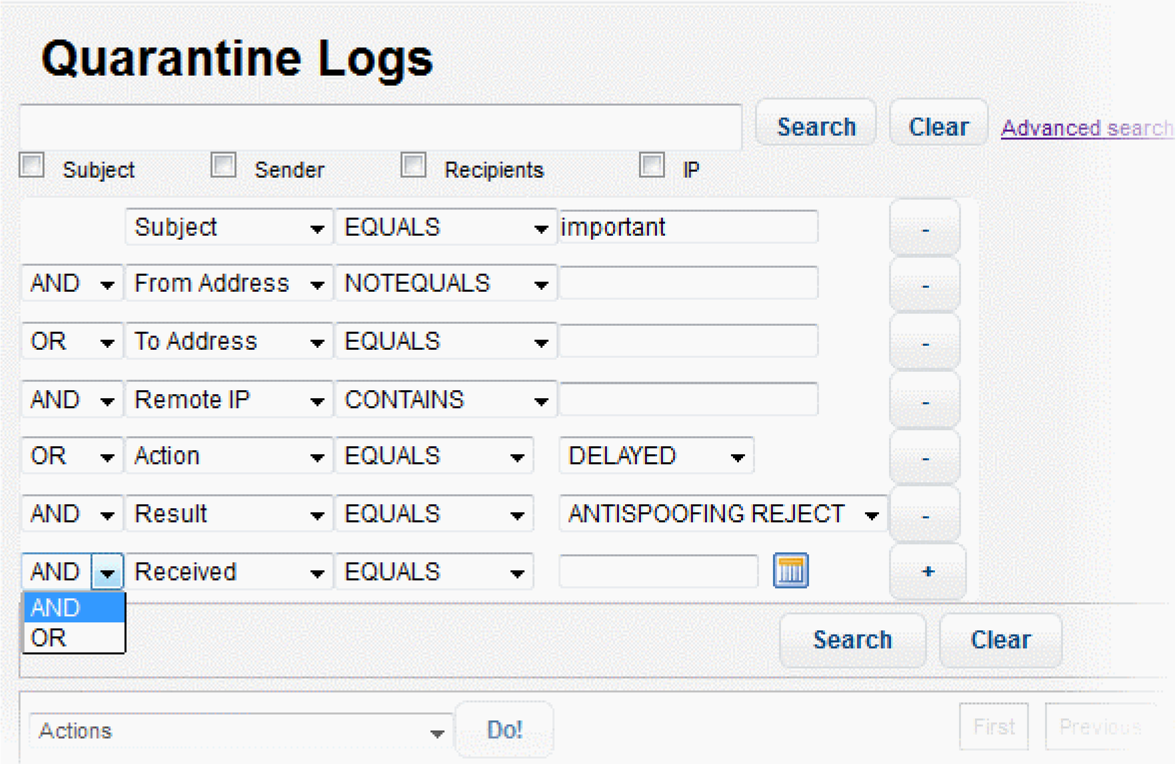
Received ▾ | EQUALS ▾ | | +

<< < March, 2015 > >> x

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
10	1	2	3	4	5	6	7
11	8	9	10	11	12	13	14
12	15	16	17	18	19	20	21
13	22	23	24	25	26	27	28
14	29	30	31	1	2	3	4
15	5	6	7	8	9	10	11

Today

You can add more filters by clicking + for narrowing down your search.



Quarantine Logs

Search | Clear | Advanced search

□ Subject □ Sender □ Recipients □ IP

	Subject ▾	EQUALS ▾	important	-
AND ▾	From Address ▾	NOTEQUALS ▾		-
OR ▾	To Address ▾	EQUALS ▾		-
AND ▾	Remote IP ▾	CONTAINS ▾		-
OR ▾	Action ▾	EQUALS ▾	DELAYED ▾	-
AND ▾	Result ▾	EQUALS ▾	ANTISPOOFING REJECT ▾	-
AND ▾	Received ▾	EQUALS ▾		+

You can remove a filter by clicking the - button beside it.

You can create a filter rule by selecting 'AND' or 'OR' option beside each of the added filter.

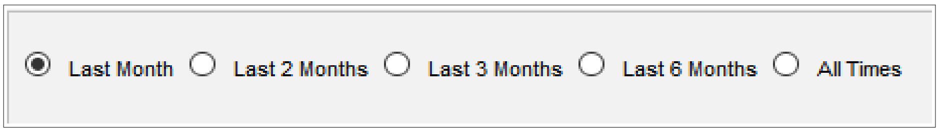
- Click 'Clear' to remove the advanced search rules.
- Click 'Search' to start the search per the filter rule.

The items will be searched for in the ascending order and results displayed.

- To remove the advanced search field, click the 'Advanced search' link again.

Administrators can filter results on monthly basis. The filters available are 'Last Month', 'Last 2 Months', 'Last 3 Months', 'Last 6 Months' and All Times.

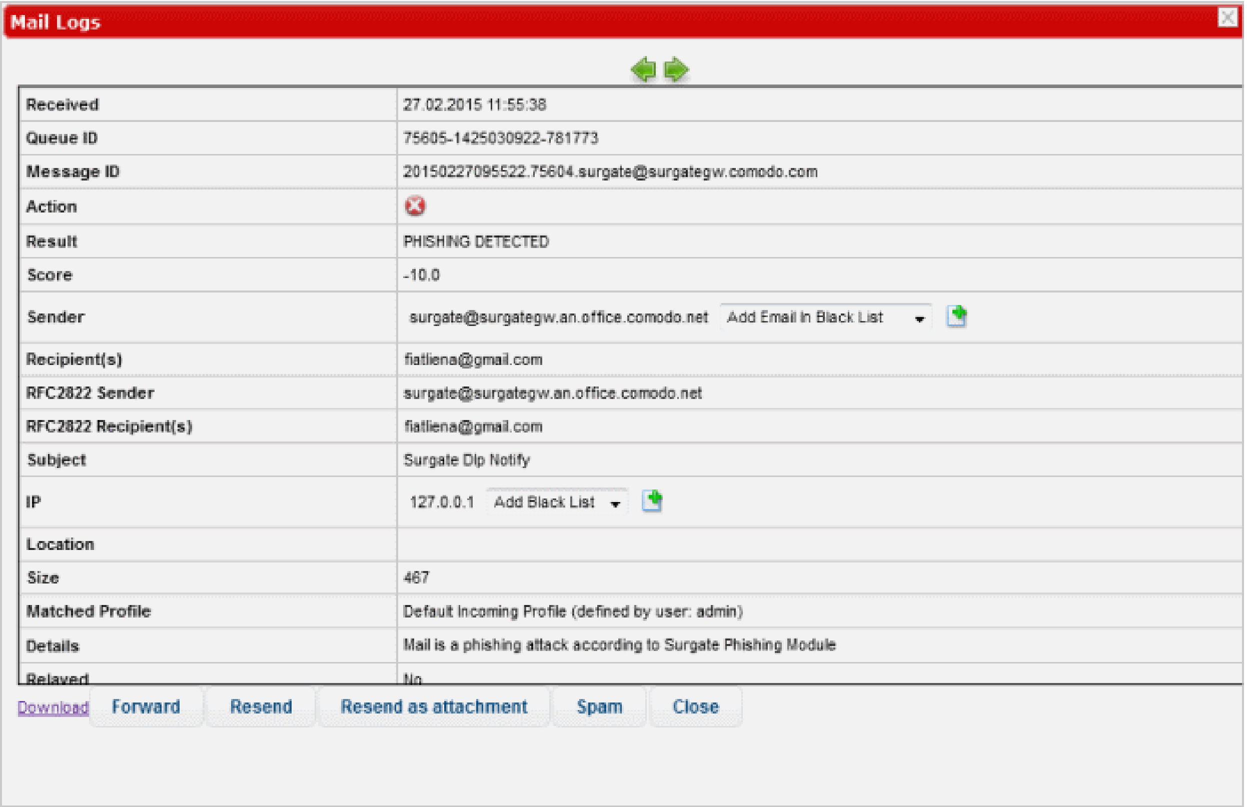
- To view the results of the last month, click the 'Last Month' radio button.



● Last Month ○ Last 2 Months ○ Last 3 Months ○ Last 6 Months ○ All Times

Details of a Log Entry

- Clicking anywhere on the row of a log record will display the details of the quarantined mail log.



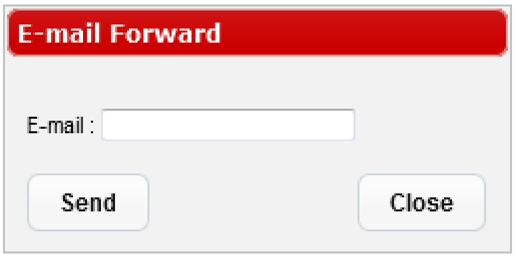
Received	27.02.2015 11:55:38
Queue ID	75605-1425030922-781773
Message ID	20150227095522.75604.surgate@surgategw.comodo.com
Action	✖
Result	PHISHING DETECTED
Score	-10.0
Sender	surgate@surgategw.an.office.comodo.net Add Email In Black List ▾
Recipient(s)	fiatliena@gmail.com
RFC2822 Sender	surgate@surgategw.an.office.comodo.net
RFC2822 Recipient(s)	fiatliena@gmail.com
Subject	Surgate Dlp Notify
IP	127.0.0.1 Add Black List ▾
Location	
Size	467
Matched Profile	Default Incoming Profile (defined by user: admin)
Details	Mail is a phishing attack according to Surgate Phishing Module
Relayed	No

The details screen allows you to mark the mail log as 'Spam' or 'Not spam' depending the mail category. You can also add the sender, sending domain and IP to blacklist or whitelist, forward, resend and resend as attachment.

- To mark an email as 'Spam' or 'Not spam', click the relevant button at the bottom of the screen.

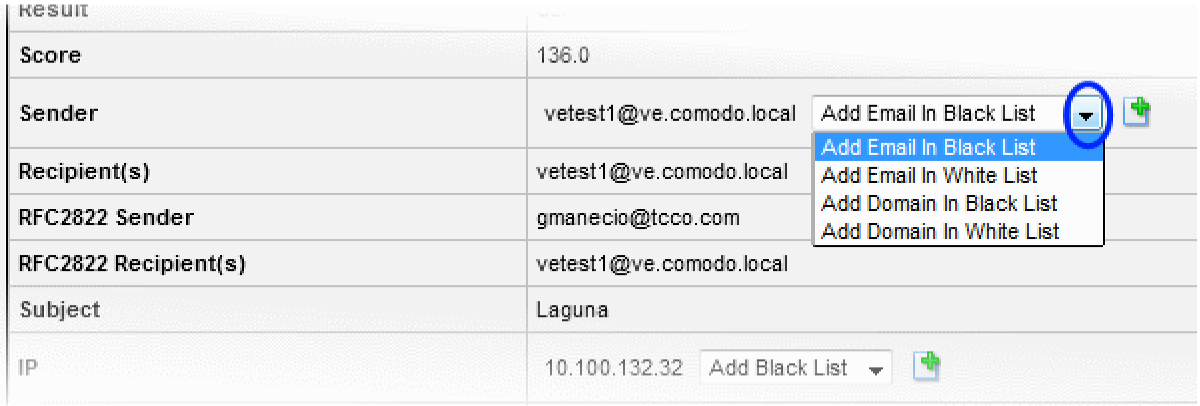
The changes will be saved and mails from the sender will be applied the new settings by KoruMail.

- To forward the mail, click the 'Forward' button, enter the mail ID in the 'Email Forward' dialog and click the 'Send' button.



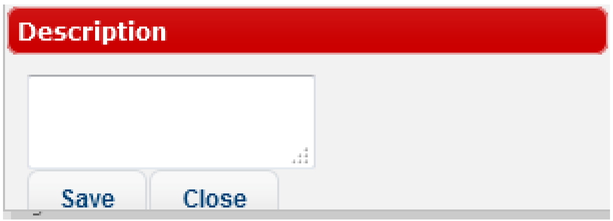
- Click the 'Resend' button to send the mail again.

- Click the 'Resend as attachment' button to send the mail as an attachment.
- To save the log record to your computer, click the 'Download' link and save the mail record.
- To add the sender or domain to blacklist/whitelist, click the drop-down in the 'Sender' row.



Result	
Score	136.0
Sender	vetest1@ve.comodo.local Add Email In Black List
Recipient(s)	vetest1@ve.comodo.local
RFC2822 Sender	gmanecio@tcco.com
RFC2822 Recipient(s)	vetest1@ve.comodo.local
Subject	Laguna
IP	10.100.132.32 Add Black List

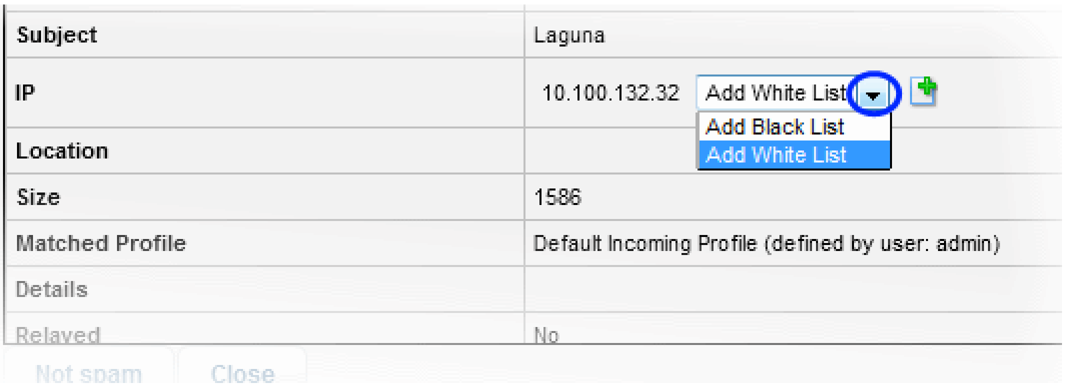
- Select the category from the options that you want to add the email and click the + button beside it.



- Enter the reason for changing the category and click the 'Save' button.

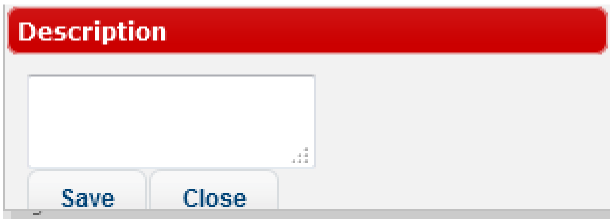
The changes will be saved and mails from the sender will be applied the new settings by KoruMail.

- To add the originating IP to blacklist/whitelist, click the drop-down in the 'IP' row.



Subject	Laguna
IP	10.100.132.32 Add White List
Location	
Size	1586
Matched Profile	Default Incoming Profile (defined by user: admin)
Details	
Relayed	No

- Select the category from the options that you want to add the IP and click the + button beside it.



- Enter the reason for changing the category and click the 'Save' button.

The changes will be saved and mails from the IP will be applied the new settings by KoruMail.

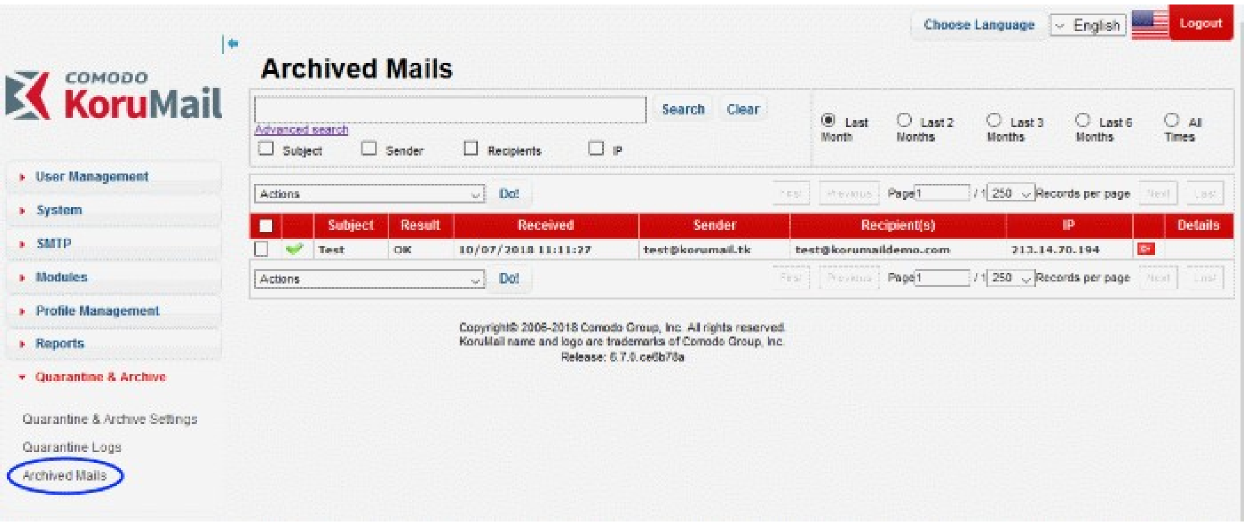
You can view the previous or next record by click the ⇦ ⇨ buttons at the top of a details screen.

11.3 Archived Mails

- The 'Archived Mails' interface displays the log records of all archived mails.
- The number of days the logs are stored depends on the settings configured in the '**Quarantine & Archive General Settings**' screen.
- The interface allows administrators to take actions such as to delete, mark as spam, mark as not spam and more.

To open the 'Archived Mails' interface,

- Click 'Quarantine & Archive' then 'Archived Mails'



□		Subject	Result	Received	Sender	Recipient(s)	IP		Details
□	✓	Test	OK	10/07/2018 11:11:27	test@korumail.tk	test@korumaildemo.com	213.14.70.194	🟥	

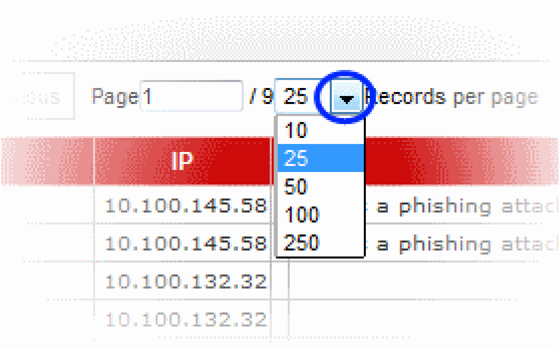
Copyright© 2006-2018 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 6.7.0.ce6b78a

Archived Mails - Table of Column Descriptions	
Column Header	**Description**
Icon	Indicates the status of action for the mail applied by KoruMail after the filtering process. Placing your mouse cursor over an icon will show a description of the action. ✓ - Relayed: Indicates the mail has successfully passed the filtering process and user verified. ⊘ - Rejected: Indicates the mail is rejected by KoruMail after the filtering process and reject message sent to the sender mail server. ☒ - Discarded: Indicates the mail is quarantined
Subject	The content in the 'Subject' line of the mails
Result	The verdict on an mail after the filtering process.
Received	Date and time Korumail received the email
Sender	Email address information of the originator
Recipient(s)	Email address information of the receiver
IP	The network address of the system from where the mail was sent.
Details	Reason why a mail is quarantined and spam score if it is marked as spam.

At the top and bottom of the screen, you have the option to set the number of records to be displayed per page and take desired actions such as delete, mark as not spam and so on.

To configure the number of records to be displayed per page

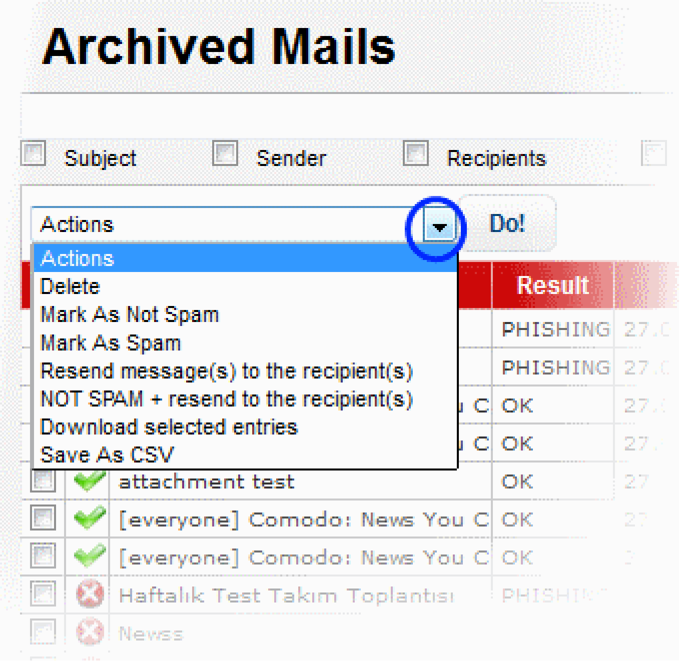
- Click the 'Records per page' drop-down



- Select the number of records per page to be displayed from the options.
- Click the 'First', 'Previous', 'Next' and 'Last' buttons to navigate to the respective pages.

To act on log entries

- Click the 'Actions' drop-down


Archived Mails
□ Subject
□ Sender
□ Recipients
Actions
Do!
Actions
Delete
Mark As Not Spam
Mark As Spam
Resend message(s) to the recipient(s)
NOT SPAM + resend to the recipient(s)
Download selected entries
Save As CSV
Result
PHISHING
PHISHING
OK
OK
attachment test
OK
[everyone] Comodo: News You C
OK
[everyone] Comodo: News You C
OK
Haftalık Test Takım Toplantısı
PHISHING
Newss

- Select the desired action from the drop-down and click the 'Do' button

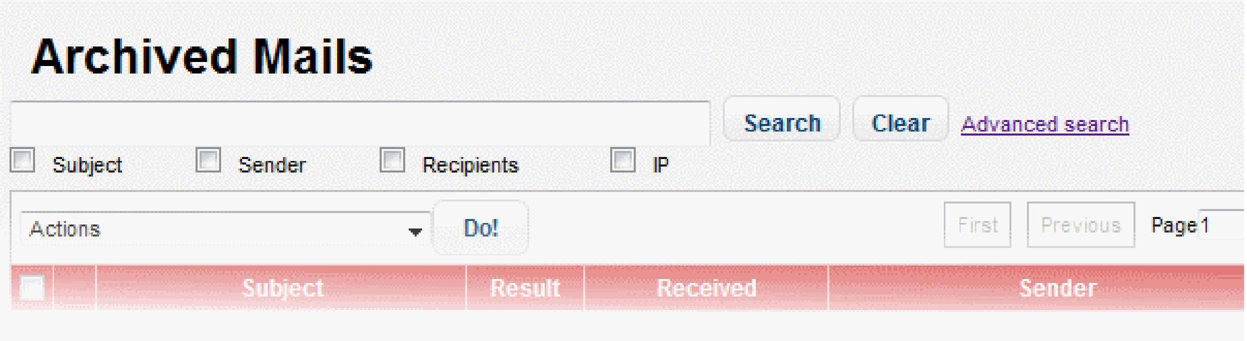
Search Options

You can search for a particular record or records in the quarantine log by using simple or advanced search feature.

- Simple Search
- Advanced Search

Simple Search

The simple search options allows you to search for a particular record or records based on 'Subject', 'Sender', 'Recipients' and / or 'IP' details only.

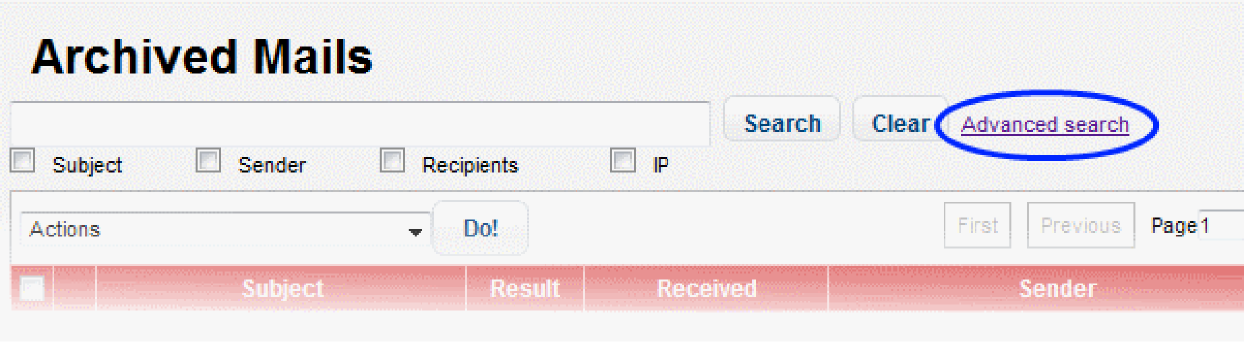


- To search for records based on the entries under 'Subject', 'Sender', 'Recipients' and / or 'IP' columns, enter the text or number fully or partially in the field and click the 'Search' button
- To search for records based on the entries under a particular column or columns, select the respective check boxes, enter the text or number fully or partially in the field and click the the 'Search' button. For example, if you want to search for a particular record for sender and recipients, select the 'Sender' and 'Recipients' check boxes, enter the text fully or partially in the field and click the 'Search' button.

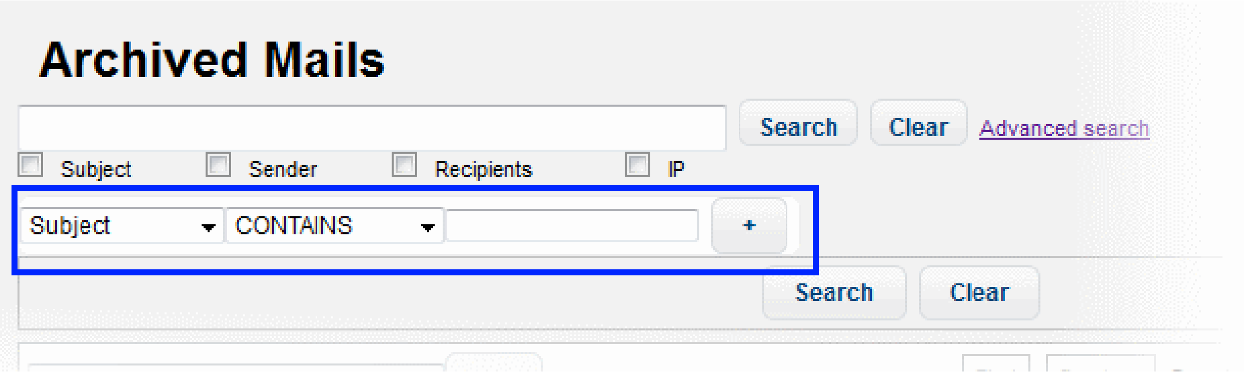
Advanced Search

The 'Advanced Search' option allows you a more granular search by including rules and filters.

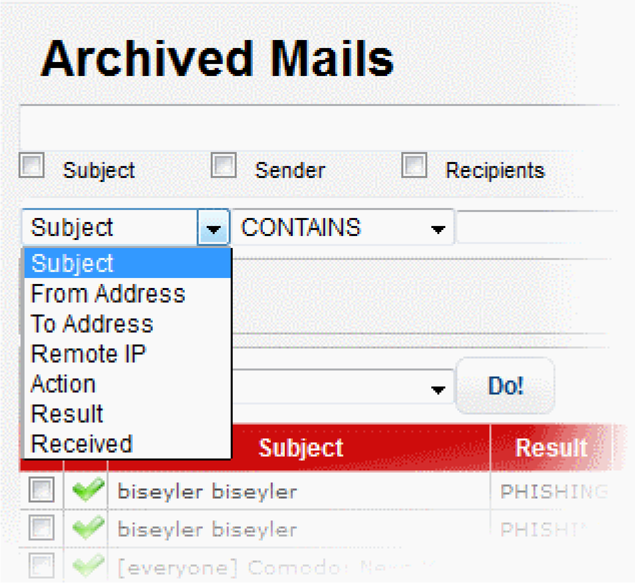
- Click the 'Advanced Search' link at the top of the screen.



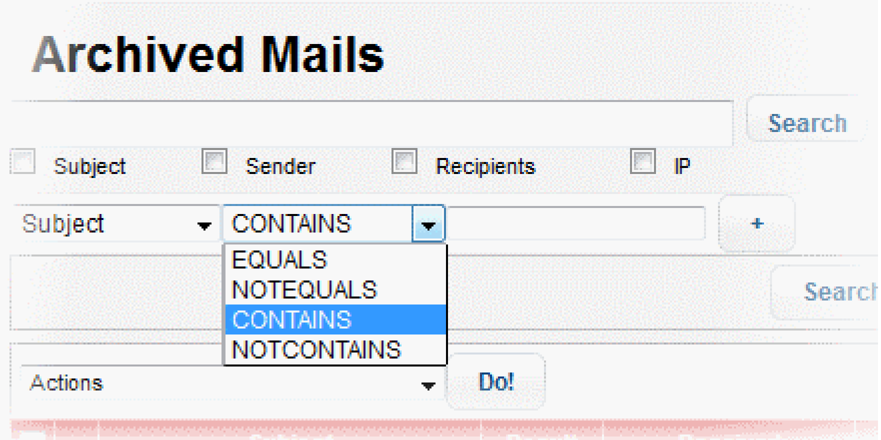
The 'Advanced Search' option will be displayed.



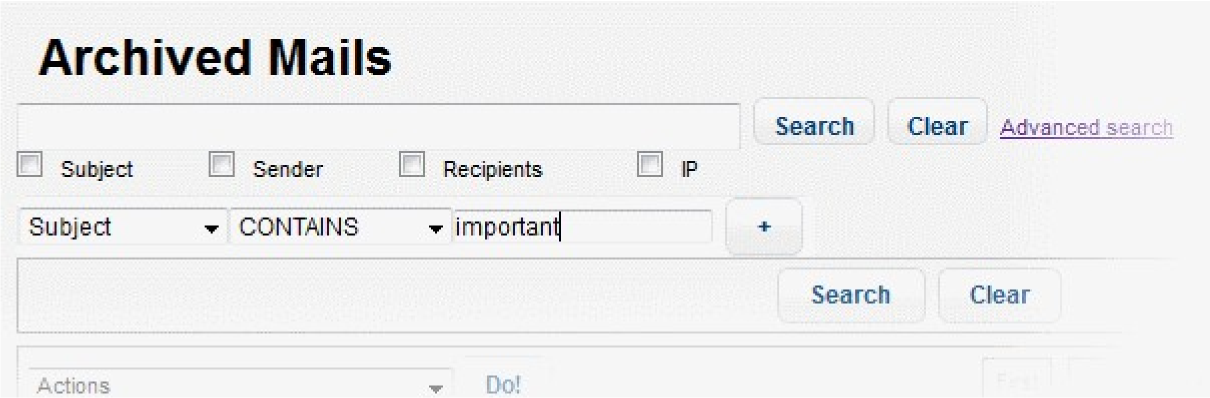
The first drop-down contains the column headers that can be selected for an advanced search.



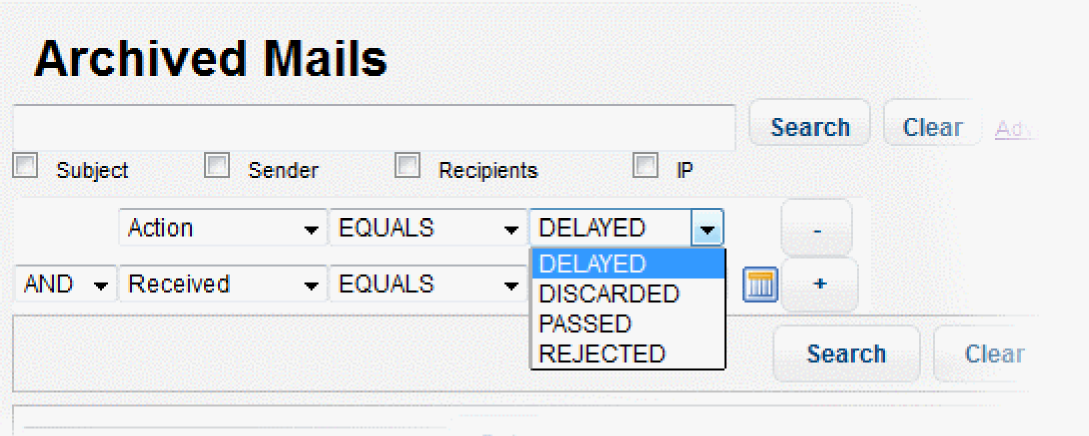
The second column contains the condition for a search, which depends on the item selected in the first column and text/number entered or options selected in the third column.



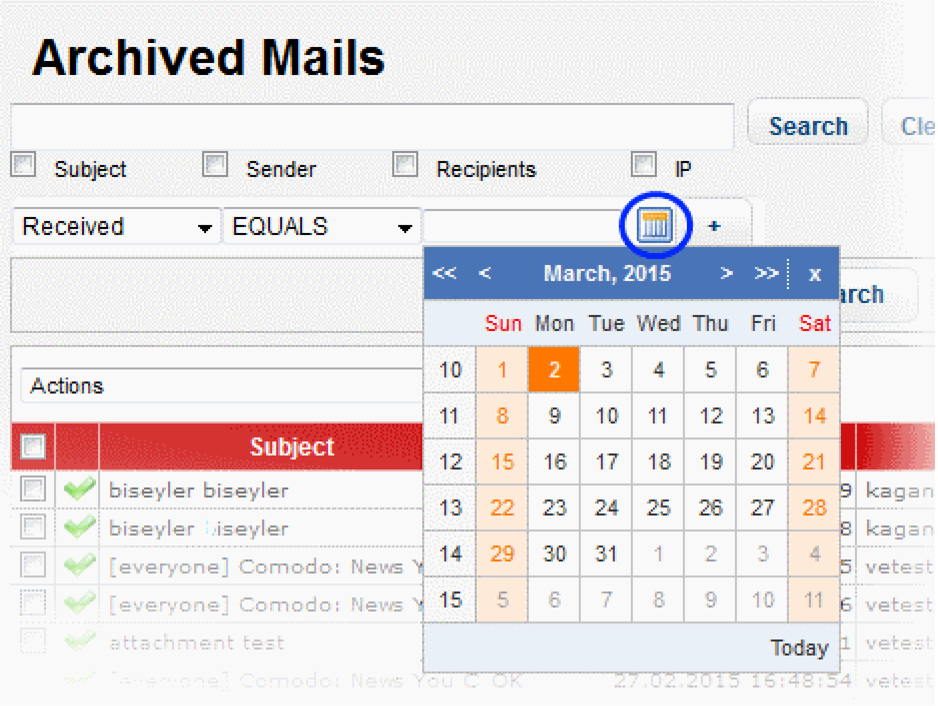
The third column allows you to enter the text/number or select from the options depending on the selection in the first column. For example, choosing 'Subject', 'From Address' or 'Remote IP' allows you to enter the text in the third column



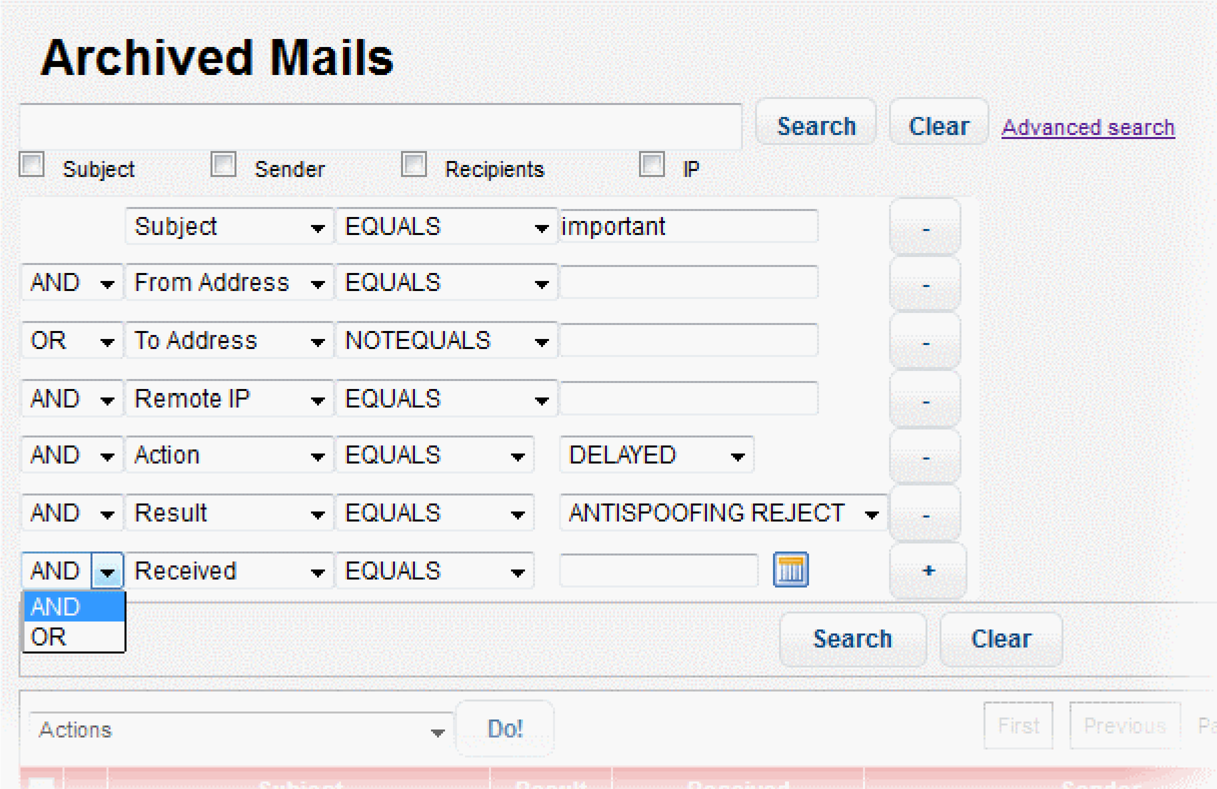
If you select 'Action' or 'Result' in the first column, then further options can be selected from the third column.



If you select 'Received' in the first column, then you can enter a date or select from the calendar.



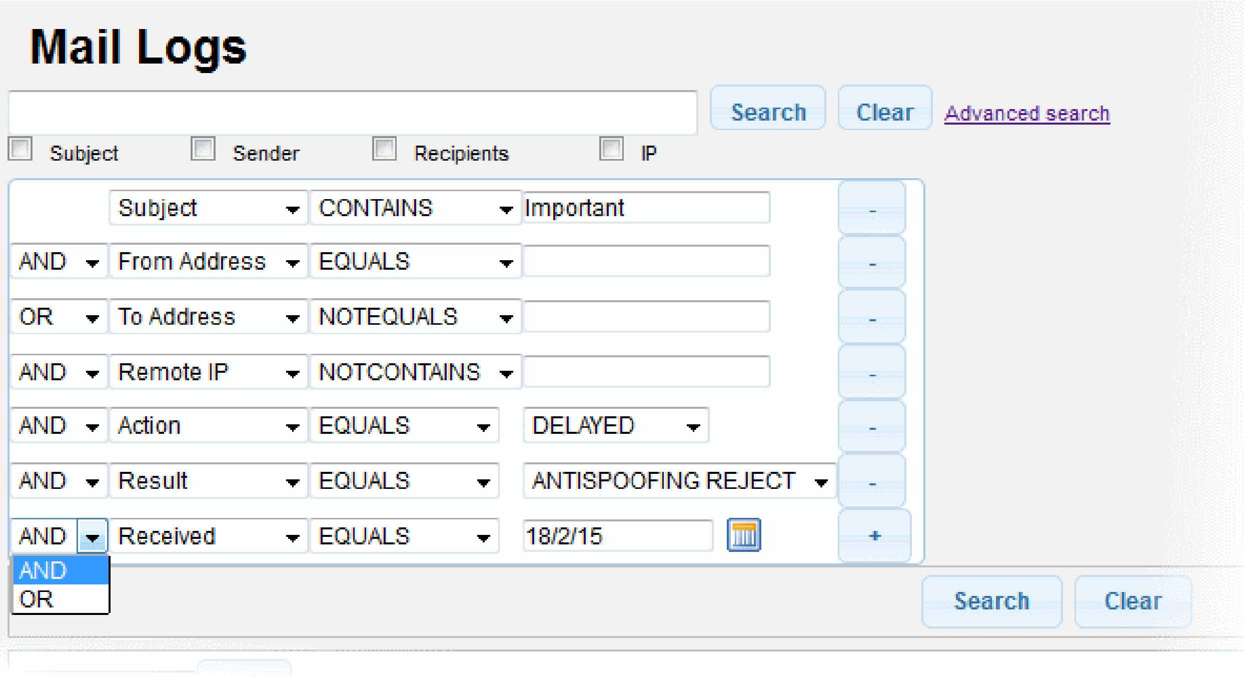
You can add more filters by clicking + for narrowing down your search.



Archived Mails

□ Subject □ Sender □ Recipients □ IP

	Subject	EQUALS	important	-
AND	From Address	EQUALS		-
OR	To Address	NOTEQUALS		-
AND	Remote IP	EQUALS		-
AND	Action	EQUALS	DELAYED	-
AND	Result	EQUALS	ANTISPOOFING REJECT	-
AND AND OR	Received	EQUALS		+



Mail Logs

□ Subject □ Sender □ Recipients □ IP

	Subject	CONTAINS	Important	-
AND	From Address	EQUALS		-
OR	To Address	NOTEQUALS		-
AND	Remote IP	NOTCONTAINS		-
AND	Action	EQUALS	DELAYED	-
AND	Result	EQUALS	ANTISPOOFING REJECT	-
AND AND OR	Received	EQUALS	18/2/15	+

You can remove a filter by clicking the - button beside it.

You can create a filter rule by selecting 'AND' or 'OR' option beside each of the added filter.

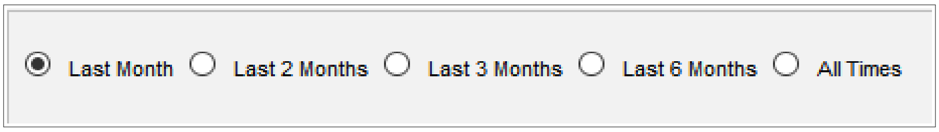
- Click 'Clear' to remove the advanced search rules.
- Click 'Search' to start the search per the filter rule.

The items will be searched for in the ascending order and results displayed.

- To remove the advanced search field, click the 'Advanced search' link again.

Administrators can filter results on monthly basis. The filters available are 'Last Month', 'Last 2 Months', 'Last 3 Months', 'Last 6 Months' and All Times.

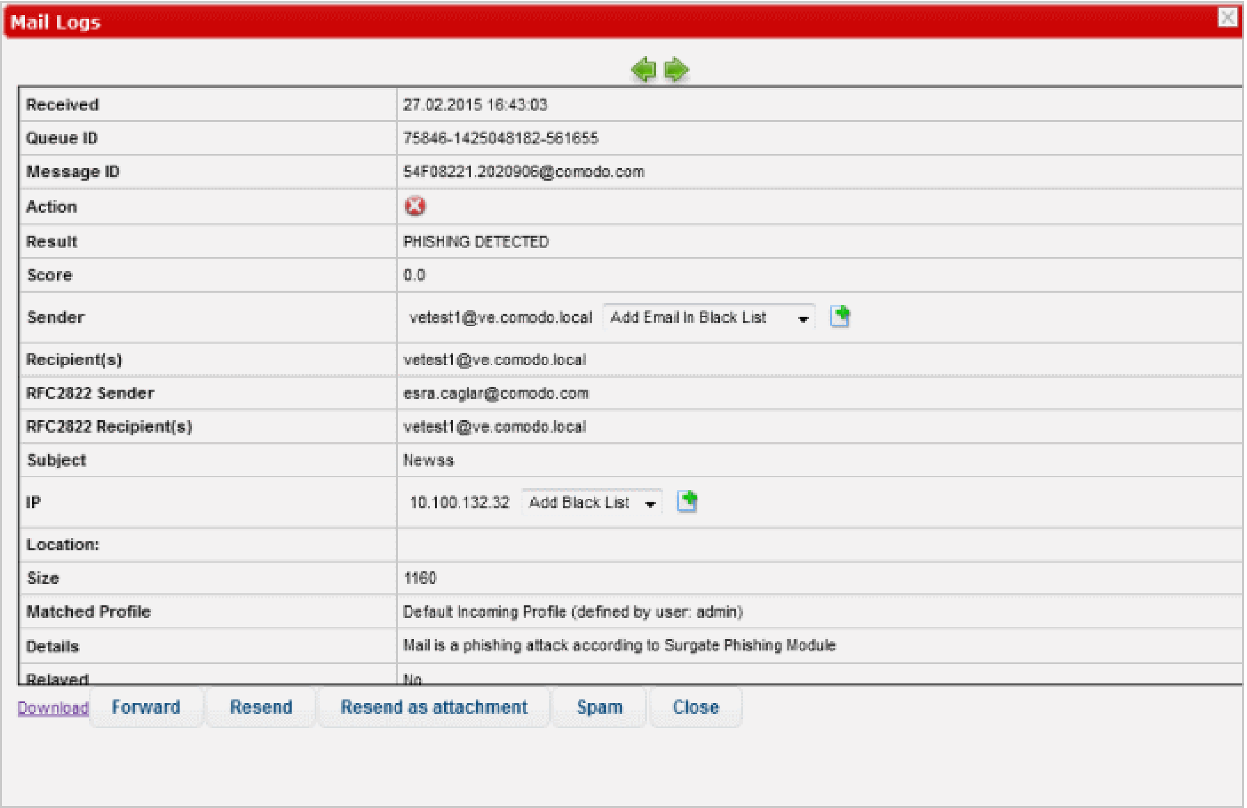
- To view the results of the last month, click the 'Last Month' radio button.



● Last Month ○ Last 2 Months ○ Last 3 Months ○ Last 6 Months ○ All Times

Details of a Log Entry

- Clicking anywhere on the row of a log record will display the details of the archived mail log.



Mail Logs

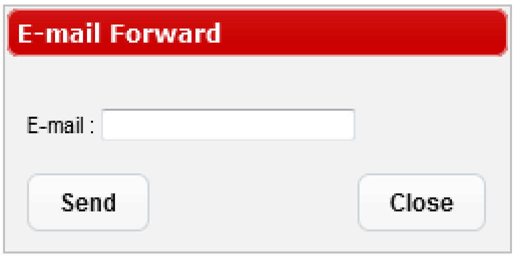
Received	27.02.2015 16:43:03
Queue ID	75846-1425048182-561655
Message ID	54F08221.2020906@comodo.com
Action	☒
Result	PHISHING DETECTED
Score	0.0
Sender	vetest1@ve.comodo.local Add Email In Black List
Recipient(s)	vetest1@ve.comodo.local
RFC2822 Sender	esra.caglar@comodo.com
RFC2822 Recipient(s)	vetest1@ve.comodo.local
Subject	Newss
IP	10.100.132.32 Add Black List
Location:	
Size	1160
Matched Profile	Default Incoming Profile (defined by user: admin)
Details	Mail is a phishing attack according to Surgate Phishing Module
Relayed	No

The details screen allows you to mark the mail log as 'Spam' or 'Not spam' depending the mail category. You can also add the sender, sending domain and IP to blacklist or whitelist, forward, resend and resend as attachment.

- To mark an email as 'Spam' or 'Not spam', click the relevant button at the bottom of the screen.

The changes will be saved and mails from the sender will be applied the new settings by KoruMail.

- To forward the mail, click 'Forward', enter the mail ID in the 'Email Forward' dialog and click 'Send'.

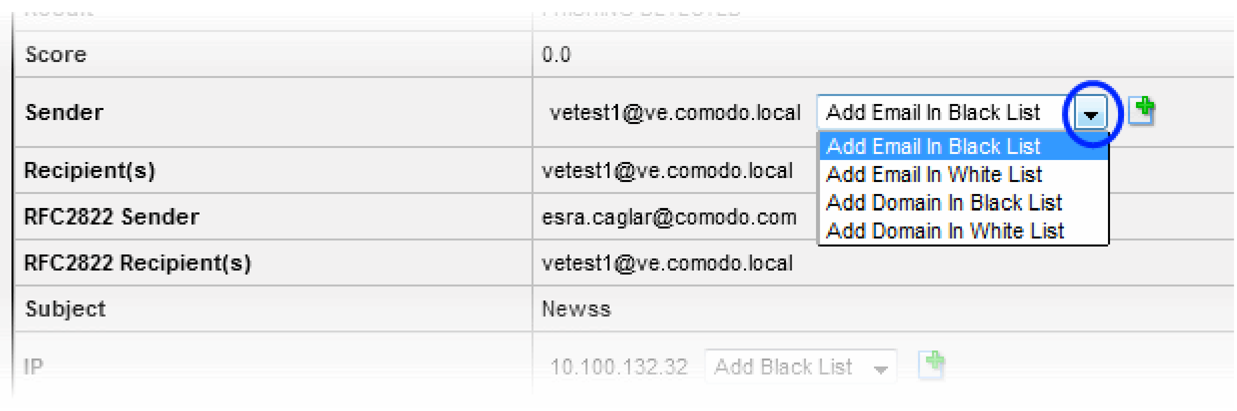


E-mail Forward

E-mail :

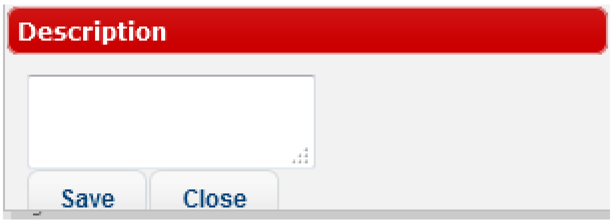
- Click 'Resend' to send the mail again.
- Click 'Resend as attachment' to send the mail as an attachment.
- To save the log record to your computer, click the 'Download' link and save the mail record.

- To add the sender or domain to blacklist/whitelist, click the drop-down in the 'Sender' row.



Result	PHISHING DETECTED
Score	0.0
Sender	vetest1@ve.comodo.local Add Email In Black List ▾ ✚
Recipient(s)	vetest1@ve.comodo.local
RFC2822 Sender	esra.caglar@comodo.com
RFC2822 Recipient(s)	vetest1@ve.comodo.local
Subject	Newss
IP	10.100.132.32 Add Black List ▾ ✚

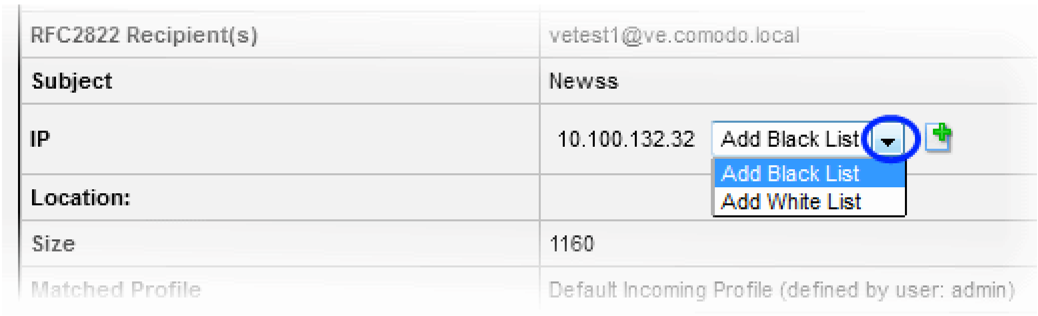
- Select the category from the options that you want to add the email and click the ✚ button beside it.



- Enter the reason for changing the category and click the 'Save' button.

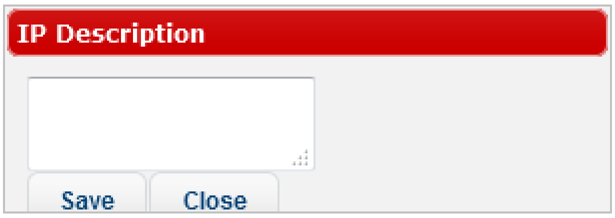
The changes will be saved and mails from the sender will be applied the new settings by KoruMail.

- To add the originating IP to blacklist/whitelist, click the drop-down in the 'IP' row.



RFC2822 Recipient(s)	vetest1@ve.comodo.local
Subject	Newss
IP	10.100.132.32 Add Black List ▾ ✚
Location:	
Size	1160
Matched Profile	Default Incoming Profile (defined by user: admin)

- Select the category from the options that you want to add the IP and click the ✚ button beside it.



- Enter the reason for changing the category and click the 'Save' button.

The changes will be saved and mails from the IP will be applied the new settings by KoruMail.

You can view the previous or next record by click the ◀ ▶ buttons at the top of a details screen.

Appendix - KoruMail Versions

Comodo KoruMail Editions - Table Description		
KoruMail Features	**Free Edition**	**Pro Edition**
Data Loss Prevention (DLP)	✗	✓
Auto Whitelisting	✓	✓
Set independent policies for incoming and outgoing mail	✓	✓
IPv6 Support	✓	✓
E-mail Archiving and Quarantine	✗	✓
SMTP IPS/firewall	✓	✓
Full Antispam and antivirus filtering	✓	✓
Antivirus Scanning (Comodo AV and Valkyrie integrations)	✓	✓
Intelligently learns and adapts to new spam techniques	✓	✓
Quickly analyze and composes spam signatures especially for promotional mails	✓	✓
User authentication (LDAP, Active Directory, MySQL, and LocalDB)	✓	✓
Set email attachment size limits	✓	✓
Multiple administrative tiers and permissions	✓	✓
Syslog & SNMP Support (Simple network management Protocol)	✓	✓
Domain Keys antispoofing network technology (DKIM)	✓	✓
Korumail Reputation Network (KRN)	✓	✓
Auto Back-up for Remote Server	✗	✓
E-mail, IP or Domain-dased Whitelist/Blacklist	Limited to 10 domains	✓
Banner and plugin filter	✗	✓
Sent E-mail limitation based on user name and domain	✓	✓
Recipient control through LDAP. Active Directory, MySQL, and local databases	✓	✓

Identification of various connection ports based on recipient's domains	✓	✓
Blocking invalid e-mail recipients and senders	✓	✓
Preventing Dos Attacks	✓	✓
Unlimited number of admins with different Authorization Levels	✓	✓
Delegation of management based on domains	✗	✓
Generation of domain an e-mail based policies	✓	✓
Saving all archived mails into disk or redirecting them to another e-mail address	✗	✓
Daily quarantine report	✓	✓
Instant controlling of quarantine e-mails through web interface	✓	✓
Reverse DNS Control	✓	✓
Filtering Sent Mails	✓	✓
Reporting in graphics and table formats	✓	✓
Support directly from Comodo support teams	✗	✓
Containment	✗	✓
Office 365 Support	✗	✓

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**