



Comodo KoruMail

Software Version 6.0

Admin Guide

Guide Version 6.4.020317

Table of Contents

1 Introduction to KoruMail Messaging Gateway.....	5
2 Installing the Appliance.....	7
2.1 Prerequisites.....	7
2.2 Deployment in Data Centers.....	7
3 Accessing the Appliance.....	8
3.1 Accessing via CLI Console.....	8
3.2 Accessing via Web Console.....	11
3.3 The Main Interface	12
4 The Dashboard.....	13
4.1 System Usage Graphics.....	15
4.2 About Software.....	18
4.3 Changing your Password.....	25
5 User Management.....	26
5.1 Managing Administrative and End Users.....	26
5.1.1 Managing Administrative Users.....	28
5.1.2 Managing End Users.....	33
5.2 Managing Groups.....	35
6 System Configurations.....	39
6.1 Network Configuration.....	41
6.1.1 Interfaces.....	42
6.1.2 Network Settings.....	45
6.1.3 Network Time Protocol (NTP).....	46
6.1.4 Timezone.....	46
6.1.5 Static Routes.....	49
6.1.6 Simple Network Management Protocol (SNMP).....	52
6.2 Services.....	53
6.3 License.....	55
6.4 Configuring System Settings.....	61
6.4.1 System General Settings.....	62
6.4.2 Cache Settings	62
6.4.3 Session Settings.....	65
6.4.4 GUI Customization.....	66
6.4.5 System Backup	67
6.4.6 System Restore.....	70
6.4.7 Log Upload Settings.....	72
6.4.8 Postmaster Settings.....	73
6.4.9 SMTP TLS Settings.....	73
6.4.10 Update Database	74
6.4.11 Syslog Server.....	76
6.5 Logs.....	76
6.5.1 Log Files.....	77

6.5.2 Purge Files.....	79
6.5.3 Tools.....	80
6.5.4 Check Connectivity.....	84
6.5.5 Clear SMTP Queue.....	92
6.6 System Usage Statistics.....	93
7 SMTP Configuration.....	102
7.1 SMTP (Send E-Mail Protocol) Settings.....	103
7.1.1 General Settings.....	104
7.1.2 Advanced Settings.....	105
7.1.3 Outbound Delivery Queue.....	107
7.2 Manage Domains.....	110
7.2.1 Managing Domain Names.....	111
7.2.2 Managing Domain Routes.....	119
7.2.3 Managing Smart Hosts.....	125
7.2.4 Default Domain Routing.....	129
7.3 KoruMail SMTP AUTH Connector.....	130
7.3.1 SMTP Authentication Settings.....	130
7.3.2 Block Users.....	133
7.3.3 Anomaly Detection.....	139
7.4 LDAP/Local DB/My SQL User Database.....	141
7.4.1 LDAP Profile.....	141
7.4.2 Local DB Users.....	145
7.4.3 My SQL User Database.....	151
7.5 Greylist.....	154
7.5.1 Greylist Ignored IP Addresses/Domains.....	155
7.6 Managing RBL Servers.....	157
7.7 Disclaimer.....	161
7.8 SMPT Relay.....	162
7.9 DomainKeys Identified Mail (DKIM).....	162
7.10 Outgoing SMTP Limits.....	165
7.11 Incoming SMTP Limits.....	172
8 Modules.....	178
8.1 Anti-spam.....	178
8.1.1 Anti-spam General Settings.....	179
8.1.2 Authorized Trainers.....	180
8.1.3 Advanced Anti-spam Settings.....	182
8.1.4 Bayesian Training.....	182
8.1.5 Content Filter.....	183
8.1.6 Signature Whitelist.....	185
8.2 Anti-Virus.....	188
8.2.1 Anti-Virus General Settings.....	189
8.2.2 Advanced Anti-Virus Settings.....	189
8.3 KoruMail Reputation Network (KRN).....	191

8.4 Anti-Spoofing.....	192
8.5 SMTP IPS/FW	197
8.5.1 SMTP IPS General Settings.....	198
8.5.2 Whitelist IP Addresses.....	200
8.5.3 Blocked IP Addresses.....	202
8.5.4 Rate Control.....	206
8.6 Auto Whitelist.....	207
8.7 Data Leak Prevention (DLP)	208
8.8 Promotional.....	209
8.9 Attachment Verdict System.....	209
9 Profile Management.....	211
9.1 Adding and Configuring a New Profile.....	213
9.2 Editing a Profile.....	236
9.3 Deleting a Profile.....	237
10 Reports.....	238
10.1 Mail Logs Report.....	239
10.2 SMTP Queue Report.....	248
10.3 Delivery Logs Report.....	249
10.4 SMTP-AUTH Logs Report.....	250
10.5 Summary Reports.....	252
10.6 Domain Reports.....	261
10.7 Attachment Verdict Reports.....	265
11 Quarantine & Archive.....	266
11.1 Quarantine & Archive Settings.....	267
11.1.1 Quarantine & Archive General Settings.....	267
11.1.2 Email Reports Settings.....	268
11.2 Quarantine Logs.....	270
11.3 Archived Mails.....	279
About Comodo.....	288

1 Introduction to KoruMail Messaging 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 Messaging Gateway is an antispam and threat prevention appliance 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
- RBL (Realtime Blocking Lists)
- MX
- Reverse DNS
- White / grey / black lists, add titles which are industrially proven filtering techniques
- SRN Reputation Network
- Active Directory Integration
- Quarantine Reporting, Quarantine Webmail
- Reporting

Guide Structure

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

- **Introduction to KoruMail Messaging Gateway**
- **Installing the Appliance**
- **Accessing the Appliance**
 - **Accessing via CLI Console**
 - **Accessing via Web Console**
 - **The Main Interface**
- **The Dashboard**
 - **System Usage Graphics**
 - **About Software**
 - **Changing your Password**
- **User Management**
 - **Managing Administrative and End Users**
 - **Managing Groups**
- **System Configurations**
 - **Network Configuration**
 - **Services**
 - **License**
 - **Configuring System Settings**

- [Logs](#)
- [Tools](#)
- [System Usage Statistics](#)
- [SMTP Configuration](#)
 - [SMTP \(Send E-Mail Protocol\) Settings](#)
 - [Manage Domains](#)
 - [Surgate SMTP AUTH Connector](#)
 - [LDAP/Local DB/My SQL User Database](#)
 - [Greylist](#)
 - [Managing RBL Servers](#)
 - [Disclaimer](#)
 - [SMTP Relay](#)
 - [DomainKeys Identified Mail \(DKIM\)](#)
 - [Outgoing SMTP Limits](#)
 - [Incoming SMTP Limits](#)
- [Modules](#)
 - [Anti-spam](#)
 - [Anti-Virus](#)
 - [KoruMail Reputation Network \(KRN\)](#)
 - [Anti-Spoofing](#)
 - [SMTP IPS/FW](#)
 - [Auto Whitelist](#)
 - [Data Leak Prevention \(DLP\)](#)
 - [Anti-Phishing](#)
 - [Promotional](#)
- [Profile Management](#)
 - [Adding and Configuring a New Profile](#)
 - [Editing a Profile](#)
 - [Deleting a Profile](#)
- [Reports](#)
 - [Mail Logs Report](#)
 - [SMTP Queue Report](#)
 - [Delivery Logs Report](#)
 - [SMTP-AUTH Logs Report](#)
 - [Summary Reports](#)
 - [Domain Reports](#)
 - [Attachment Verdict Reports](#)
- [Quarantine & Archive](#)
 - [Quarantine & Archive Settings](#)
 - [Quarantine Logs](#)
 - [Archived Mails](#)

2 Installing the Appliance

- [Prerequisites](#)
- [Deployment in Data Centers](#)

2.1 Prerequisites

Please ensure the following conditions are met before installing the KoruMail appliance:

1. The source IP of incoming mail traffic should not be changed by other devices. If the incoming emails are routed via a load balancer to KoruMail then make sure the balancer's settings are configured not to change the source IP. Else IP based filtering will not work properly.
2. An A and MX records should be entered for korumail.domain.com
3. For the protected domains, only one MX Reverse DNS record should exist and it must point to KoruMail. Otherwise, spam and viruses will pass from other servers in MX records without being filtered via KoruMail. Also, if possible SMTP port 25 should not be accessible from outside for the emails to be protected by KoruMail. Spammers can keep MX records in their memories before KoruMail installation and they can send spam/virus directly to actual mail server by-passing KoruMail.
4. Firewall should be permitted as follows:

Traffic to KoruMail:

1. Port 8080 and port 8443 (GUI interface and quarantine reports) must be open from outside to KoruMail
2. Port 25 must be open from outside to KoruMail
3. Port 22 should be open for KoruMail Support Center (78,186,198,152) to remote access

Traffic from KoruMail:

1. All connections to the outside must be accessible

2.2 Deployment in Data Centers

Note the following points before starting:

1. Switch off the appliance then unplug the AC power cable
2. Remove all the cables and communication tools plugged into the device
3. Empty static electric on your body

You must place the appliance into rack cabinet with the rail-kit.

Before starting to use KoruMail appliance, check the following:

1. Power and network cables have been plugged in
2. Device's network settings have been done properly as explained in the section [Accessing via CLI Console](#)

After completing the above steps you can do all other configurations in detail explained in the section [System Configuration](#).

3 Accessing the Appliance

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

There are two ways to access the appliance:

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

3.1 Accessing 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 appliance 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 appliance 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!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

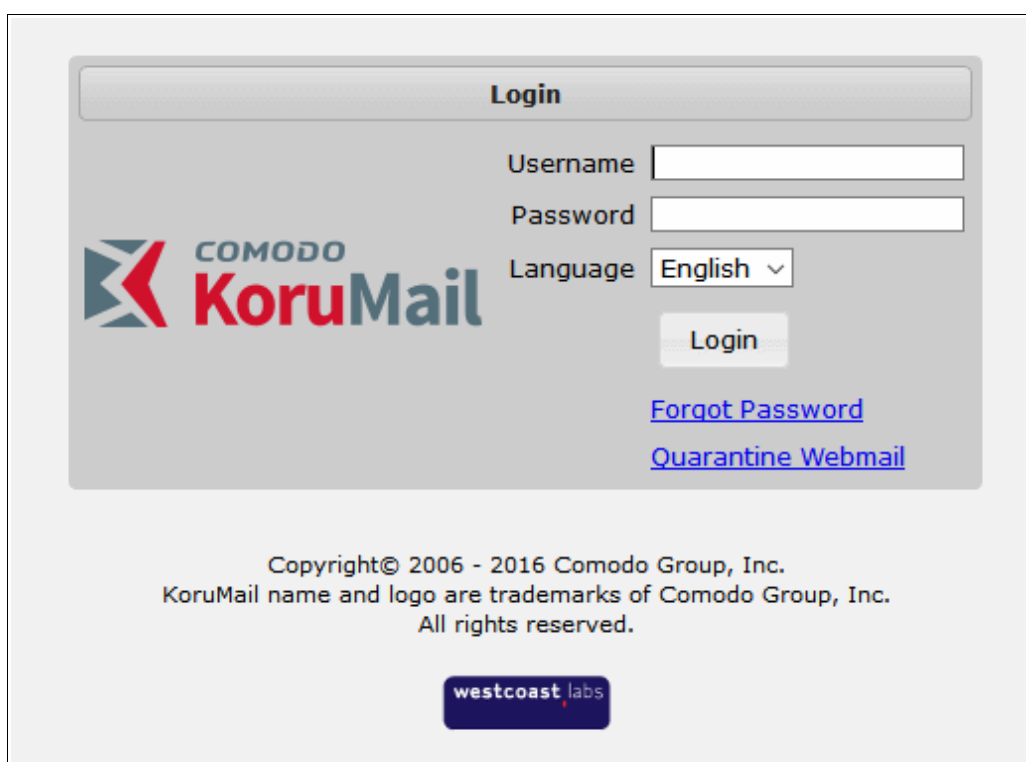
This option make changes on network settings
Do you want to proceed [y|n] (Default is none) ?
y
Enter the IP address of the system: 10.0.0.52
Enter the netmask of the system: 255.255.255.0
Enter the default gateway of the system: 10.0.0.1
Enter the first nameserver of the system: 10.0.0.1
Enter the second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

1. Enter KoruMail Messaging Gateway's IP or host name together with port 8080 (Example: <http://korumail.comodo.net:8080>) in the address bar of a browser
2. Enter your username and password. Default user name is 'admin'. For password please contact Comodo's sales representative
3. Choose one of the language options (English/Turkish)
4. Click the login button



Login

Username

Password

Language

Login

[Forgot Password](#)

[Quarantine Webmail](#)

Copyright© 2006 - 2016 Comodo Group, Inc.
KoruMail name and logo are trademarks of Comodo Group, Inc.
All rights reserved.

westcoast labs

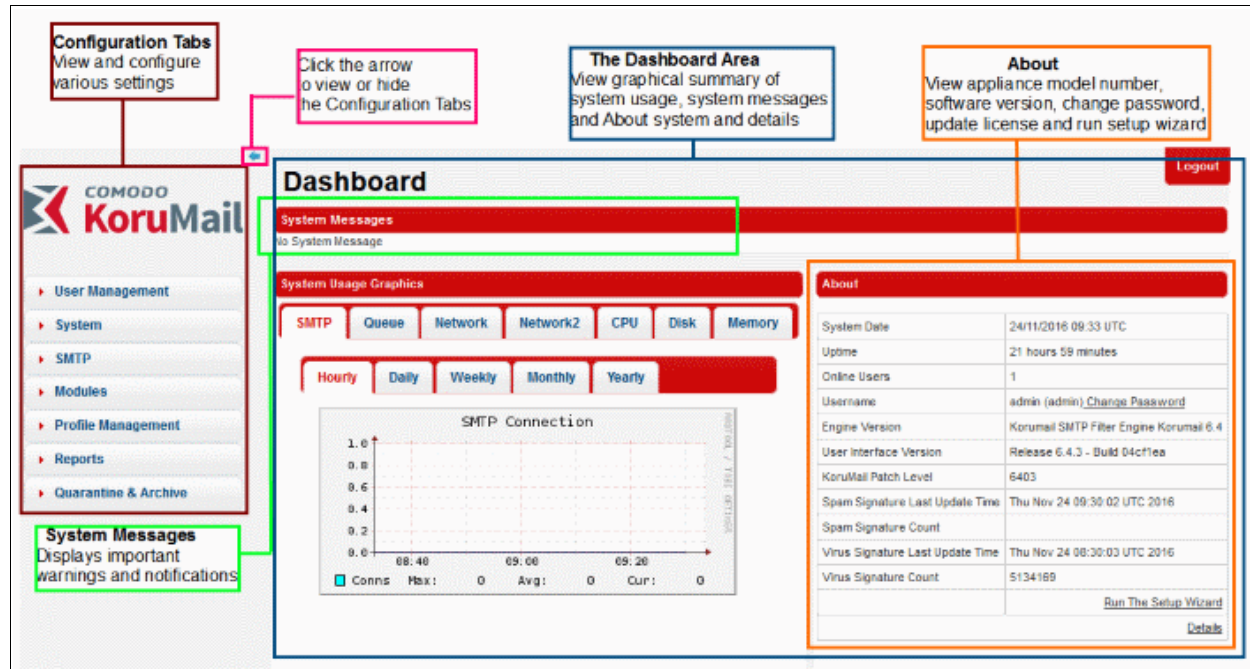
- To connect via secure HTTPS connection, click the 'SSL' icon and enter the credentials
- In case you have forgotten the password, click the 'Forgot Password' link, enter your email address and click the 'Send' button to receive a new password.
- Users can view their quarantined mails by clicking the 'Quarantine Webmail' link and providing their credentials in the KoruMail Quarantine Webmail interface. Refer to the '**Managing End Users**' section for more details.

Note: The credentials are case sensitive, and so should be entered as configured.

If there is no activity by the admin for a specified time (30 minutes by default) in KoruMail's control window then the session will time out. You should login again to access the KoruMail's control panel.

3.3 The Main Interface

The administrative console provides easy access to all modules, statistics and configuration screens in KoruMail Messaging Gateway.



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. Refer to the section '**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. Refer to the section '**System Configuration**' for more details.
- **SMTP:** Allows administrators to configure SMTP settings, add domains, add new LDAP profile, create greylist of domains, IP or network address, set outgoing limits and more. Refer to the section '**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. Refer to the section **Modules** for more details.
- **Profile Management:** Configure various settings such as anti-virus, anti-spam, blacklist and more for default incoming and outgoing profile. Refer to the section '**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. Refer to the section '**Reports**' for more details.
- **Quarantine & Archive:** Enables to configure Quarantine and Archive settings, view quarantined mail logs and archived mails. Refer to the section '**Quarantine & Archive**' for more details.

Dashboard

After logging-in to the console, the first screen displayed is the '**Dashboard**'. It provides 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 messaging gateway.
- **System Usage Graphics:** Provides a graphical representation of the system usage such as SMTP

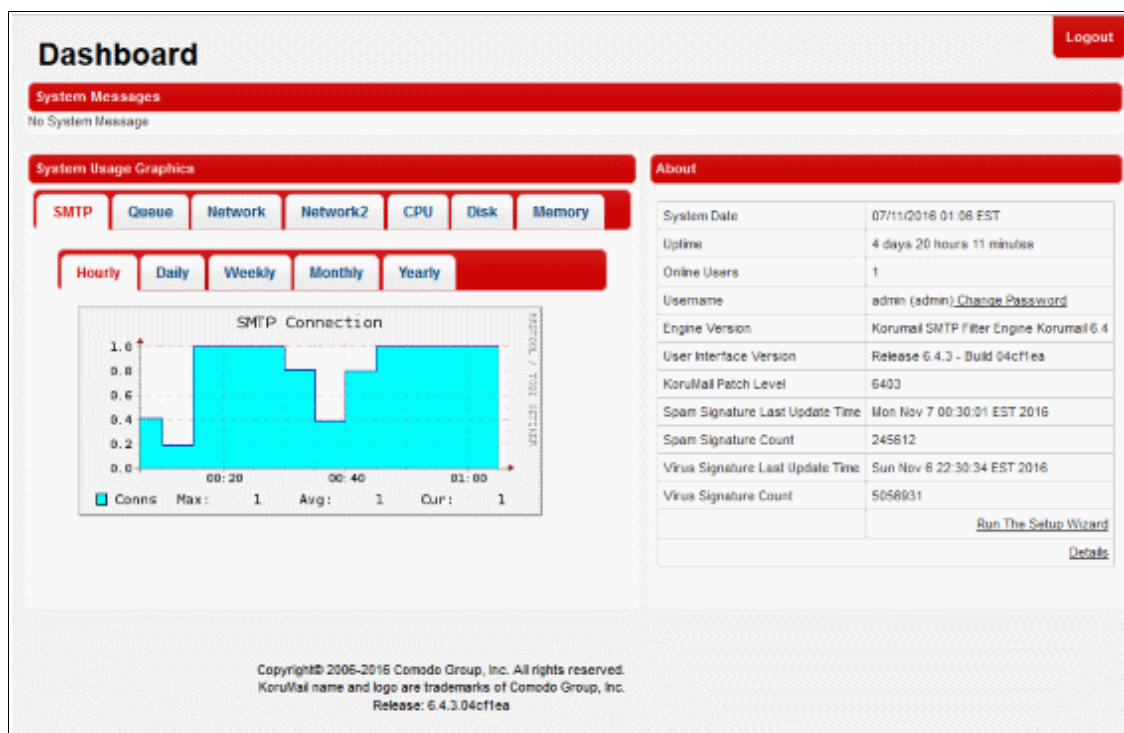
connection rate in hourly, daily, weekly, monthly or yearly basis, utilization of network, CPU, disk and memory. Refer to the section '[System Usage Graphic](#)' for more details.

- **About:** The 'About' area in the dashboard allows administrators to change the current password, view details of the appliance and software and manage the license. Refer to the section '[About Software](#)' and '[Changing your Password](#)' for more details.
- **Run the Setup Wizard:** Enables administrators to quickly configure the Korumail appliance.

4 The Dashboard

The Comodo KoruMail Dashboard provides at-a-glance statistical summary of the current running status, system messages and allows administrators to change the password and update license.

The Dashboard is displayed by default whenever you login to the administrative interface. To switch to 'Dashboard' from a different configuration screen, click on the 'KoruMail Messaging Gateway' logo at the top left.



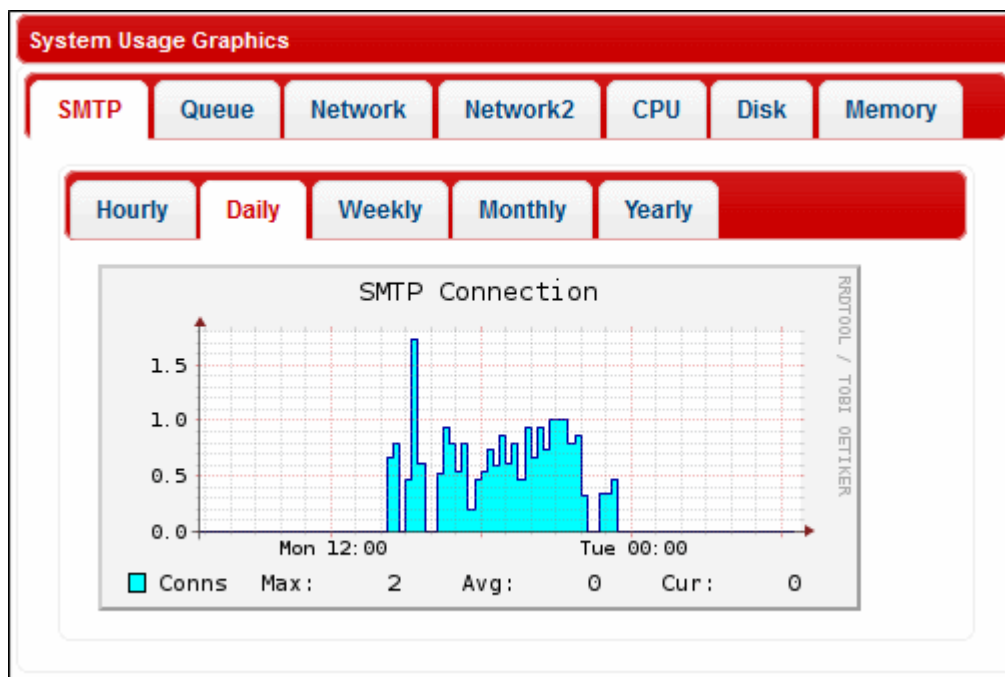
The 'System Messages' displays error messages or important notifications that might affect the performance of the messaging gateway.

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

- [System Usage Graphics](#)
- [About Software](#)
- [Changing your Password](#)

4.1 System Usage Graphics

The 'System Usage Graphics' area in the 'Dashboard' displays a graphical summary of SMTP connections, number of queued mails, network utilization rate, CPU utilization rate, disk usage ratio and system memory utilization rate. The tabs in the second row allow you to view summaries on an hourly, daily, weekly, monthly and yearly basis.



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

Refer to the **System Usage Statistics** section for more details about each of the item.

4.2 About Software

The 'About' section in the 'Dashboard' area displays hardware, software and virus update details and also allows you to change the web console access password.

About	
System Date	07/11/2016 01:06 EST
Uptime	4 days 20 hours 11 minutes
Online Users	1
Username	admin (admin) Change Password
Engine Version	Korumail SMTP Filter Engine Korumail 6.4
User Interface Version	Release 6.4.3 - Build 04cf1ea
KoruMail Patch Level	6403
Spam Signature Last Update Time	Mon Nov 7 00:30:01 EST 2016
Spam Signature Count	245612
Virus Signature Last Update Time	Sun Nov 6 22:30:34 EST 2016
Virus Signature Count	5056931
Run The Setup Wizard	
Details	

Clicking the 'Details' link at the bottom opens another 'About' screen that provides more details:

About

Logout

About KoruMail
System Admin

Engine Version	Korumail SMTP Filter Engine Korumail 6.4
User Interface Version	Release 6.4.3 - Build 04cf1ea
KoruMail Patch Level	6403
Spam Signature Last Update Time	Mon Nov 7 02:07:12 EST 2016
Spam Signature Count	245578
Virus Signature Last Update Time	Sun Nov 6 22:30:34 EST 2016
Virus Signature Count	5056931
Support	Comodo Group, Inc., korumailsupport@comodo.com
Sales	Comodo Group, Inc., korumailsales@comodo.com
Telephone	+90 530 016 99 03

Copyright© 2006-2016 Comodo Group, Inc. All rights reserved.
 KoruMail name and logo are trademarks of Comodo Group, Inc.
 Release: 6.4.3.04cf1ea

By default, the 'About KoruMail' will be displayed.

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

About Logout

About KoruMail **System Admin**

System Admin Name: John

System Admin Surname: Smith

System Admin Tel. No.: 123456789

System Admin E-mail: admin@example.com

[Save](#)

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

- Click 'Save' after the details are provided in the fields.

If the field 'System Admin E-mail' is left blank, then a error message will be displayed under the 'System Messages' in the 'Dashboard'.

Run a Setup Wizard

Allows you to quickly configure protection on a mail server.

To run the setup wizard:

- Click the 'Run the setup wizard' link.
- The 'User Preferences' screen will be displayed.
- The administrator can configure 'User Preferences', 'System Admin' details, 'Network Settings', 'Timezone', 'LDAP' profiles, 'Managed Domains', 'Routes' and 'Relay' details.

Dashboard Logout

System Messages
[Click for new update details.](#)
No System Message

System Usage Graphics

SMTP **Queue** **Network** **Network2** **CPU** **Disk**

Memory

Hourly **Daily** **Weekly** **Monthly** **Yearly**

SMTP Connection

Setup Wizard Logout

User Preferences

Permit Processing User Data ☒ Permit ☐ Anonymous ☐ None

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

[Next](#)

About

System Date	23/11/2016 00:31 EST
Uptime	21 hours 21 minutes
Online Users	1
Username	admin (admin) Change Password
Engine Version	Korumaill SMTP Filter Engine Korumail 6.4
User Interface Version	Release 6.4.3 - Build 04cf1ea
KoruMail Patch Level	6403
Spam Signature Last Update Time	Wed Nov 23 00:30:02 EST 2016
	242465
	Tue Nov 22 23:09:00 EST 2016
	5128747

[Run The Setup Wizard](#) [Details](#)

By permitting the processing of user data, administrators can upload certain spam messages for analysis to the Comodo support team. Refer to the section '[System General Settings](#)' for more details on user preferences.

- Clicking 'Next', you can enter admin details such as 'System Admin Name', 'System Admin Surname', 'System Admin Tel. No' and 'System Admin E-mail'.

Setup Wizard

Logout

System Admin

System Admin Name	<input type="text" value="Erhan"/>
System Admin Surname	<input type="text" value="Ceran"/>
System Admin Tel. No.	<input type="text" value="12345678"/>
System Admin E-mail	<input type="text" value="erhan.ceran@comodo.com"/>

Prev

Next

- Click 'Next', to enter network details.

Setup Wizard **Logout**

Network Settings

Hostname:	<input type="text" value="10.108.51.98"/>
IPv4 Default Gateway:	<input type="text" value="46 . 101 . 192 . 1"/>
IPv6 Default Gateway:	<input type="text"/> <input type="checkbox"/> Remove IPv6 settings
Primary DNS Server:	<input type="text" value="195.175.39.39"/>
Secondary DNS Server:	<input type="text" value="195.175.39.40"/>

Prev **Next**

Refer to the section **Network Settings** for more details on this section.

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

Setup Wizard **Logout**

Timezone

Continent	<input type="text" value="Europe"/>
City	<input type="text" value="Istanbul"/>
Current timezone	Europe/Istanbul

Prev **Next**

Refer to the **Timezone** section for more details.

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

Setup Wizard

[Logout](#)

LDAP

[+ Add LDAP profile](#)

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

[Prev](#)
[Next](#)

Refer to the **LDAP** section for more details.

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

Setup Wizard

[Logout](#)

Managed Domains

Managed Domain Name	Generate Report	Owner	Action
<input type="text"/>	<input type="checkbox"/>		
mail.postmanllc.net	<input checked="" type="checkbox"/>	admin	
www.mail.yahoo.com	<input checked="" type="checkbox"/>	admin	

[Prev](#)
[Next](#)

Refer to the **Managed Domains** section for more details.

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

Setup Wizard

[Logout](#)

Routes

Managed Domain Name	Routing Type	SMTP Server	Port Number	User Verification	LDAP/DB Profile	Action
<input type="text" value="-Choose-"/>	<input type="text" value="IPv4"/>	<input type="text"/>	<input type="text" value="25"/>	<input type="text" value="None"/>	<input type="text" value="None"/>	
mail.postmanllc.net	IPv4	178.62.89.150	25	LDAP	Default AD	
www.mail.yahoo.com	IPv4	172.62.89.150	25	LocalUserDB	LocalUserDB	

[Prev](#)
[Next](#)

Refer to the [Routes](#) section for more details.

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

Setup Wizard Logout

Relay

IP Range

There are no available records.

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)

Prev End

Refer to the [Relay](#) section for more details.

4.3 Changing your Password

You can change your current password anytime from the 'About' area. To change your password, from the 'Dashboard' screen click the 'Change Password' link in the 'Username' row.

About	
System Date	07/11/2016 01:06 EST
Uptime	4 days 20 hours 11 minutes
Online Users	1
Username	admin (admin) Change Password
Engine Version	Koremail SMTP Filter Engine Korumail 6.4
User Interface Version	Release 6.4.3 - Build 04cf1ea
KoruMail Patch Level	6403
Spam Signature Last Update Time	Mon Nov 7 00:30:01 EST 2016
Spam Signature Count	245612
Virus Signature Last Update Time	Sun Nov 6 22:30:34 EST 2016

In the 'Change Password' screen, enter the current password and then enter the new password and confirm it in the last field.

Change Password

Logout

Old Password:

New Password:

New Password (again):

Save

- Click the 'Save' button.

The password details will be updated and you have to use the new password to access the KoruMail's web console.

5 User Management

The 'User Management' area allow administrators to create new admins and configure their privileges. The 'Quarantine Webmail User' tab allows administrators to add email recipients' details so that they can log into the console to view their quarantined emails. The interface also allows the creation of user 'Groups' with different access levels.

Users

Logout

Administrative Users

Quarantine Webmail Users

+ Add user

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

Click the following links for more details:

- [Managing Administrative and End Users](#)
- [Managing Groups](#)

5.1 Managing Administrative and End Users

The KoruMail's web console can be accessed by administrators according to their designated privileges. The 'User Management' area also allows administrators to add end users so that the email recipients can access the web console and view their quarantined emails. A new administrator must have a group assigned to them, so make sure an appropriate group already exists. Refer to the section '[Managing Groups](#)' for more details.

- To open the 'Users' screen, click the 'User Management' tab on the left menu and click 'Users'.

Users

Administrative Users | Quarantine Webmail Users

[Add user](#)

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

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

Click the following links for more details:

- [Managing Administrative Users](#)
- [Managing End Users](#)
























5.1.1 Managing Administrative Users



- To open the 'Administrative Users' screen, click the 'User Management' tab on the left menu and click the 'Administrative Users' tab from the 'Users' screen.

Users

Administrative Users
Quarantine Webmail Users

[+ Add user](#)

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

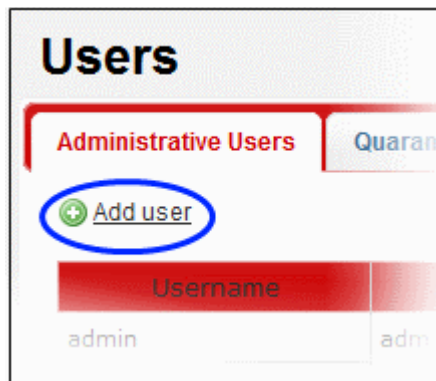
Administrative Users – Table of Column Descriptions	
Column Header	Description
Username	The username provided at the time of adding the administrator to access the web console.
Group	Displays the name of the group to which the administrator belongs. Refer to the section ' Managing Groups ' for more details.
Action	 Administrators with appropriate privileges can delete other admins by clicking this icon. Please note logged-in admin cannot be deleted by himself/herself.
	 Administrators with appropriate privileges can edit other admins' details. Refer to the section ' Editing an Administrator ' for more details.
Status	Indicates whether the admin is in enabled or disabled status. Disabled admins cannot log into the web console. Refer to the section ' Enabling/Disabling 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

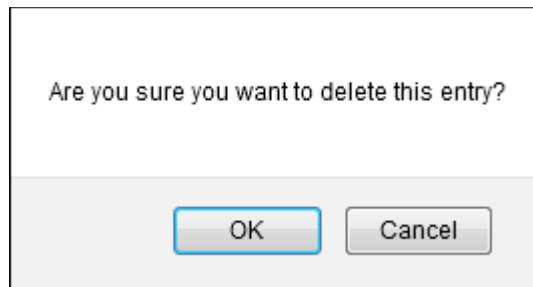


The 'Add New User' screen will be displayed.

- **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. Refer to the section '**Managing Groups**' for more details.
- Click the 'Save' button to add the new admin user.


To delete an administrative user

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



- 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

Logout

Username *	snowman
Authentication Type	Local DB ▼
Password *	•••
Password *	•••
Name	John
Surname	Smith
E-mail *	adminuser1@example.
Group	test1 ▼



Save
Cancel

- Edit the details as required. The screen is similar to the 'Add New User' section. Refer to '[Add an administrative user](#)' for more details.
- Click the 'Save' button.

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.

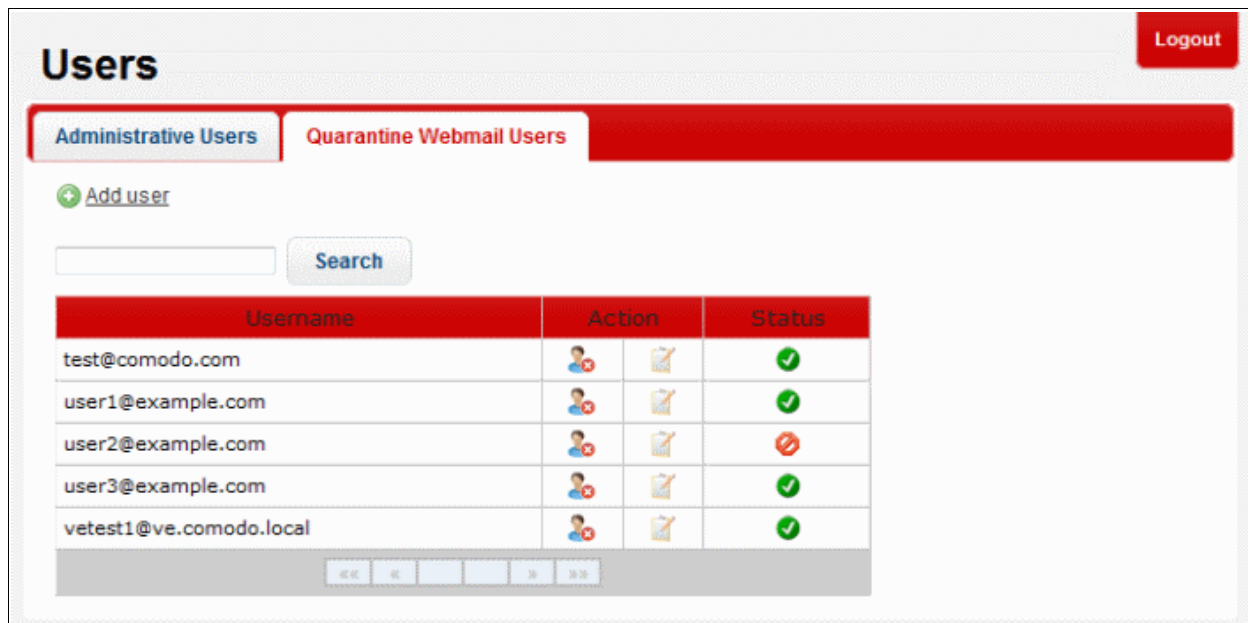
	Indicates the user is disabled and cannot login to the web console
	Indicates the user is enabled and can access the web console



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

5.1.2 Managing End Users

The 'Users' interface allows end users (email recipients) to view their quarantined emails. Administrators can provide them with web console access to view their mails. They can view only their quarantined mails. The 'Quarantine Webmail Users' tab in the 'Users' interface allow administrators to add end users, edit or delete them.

- To open the 'Quarantine Webmail Users' screen, click the 'User Management' tab on the left menu, click 'Users' and then click the 'Quarantine Webmail Users' tab from the 'Users' screen.



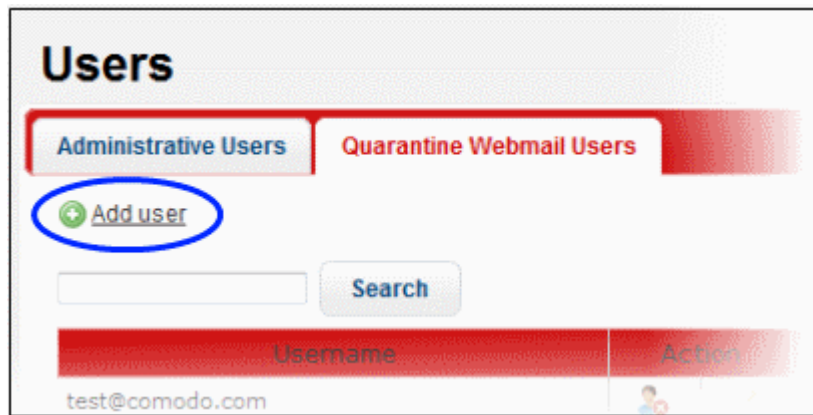
Quarantine Webmail Users – Table of Column Descriptions		
Column Header	Description	
Username	The username provided at the time of adding the end user to access the web console.	
Action		Administrators with appropriate privileges can delete the end user by clicking this icon.
		Administrators with appropriate privileges can edit end user's details. Refer to the section 'Editing an End User' for more details.
Status	Indicates whether the end user is in enabled or disabled status. Disabled end users cannot log into the web console. Refer to the section 'Enabling/Disabling End Users' for more details.	

From the this interface an appropriately privileged administrator can:

- 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

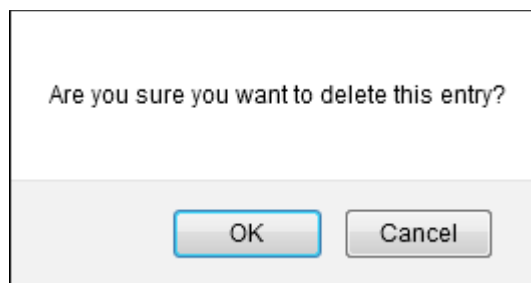


The 'Add New User' screen will be displayed.

- 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 the 'Save' button to add the new end user.

To delete an end user

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



- 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

Logout



E-mail *	user1@example.com
Name	John
Surname	Smith
Password *	...
Password *	...
Save Cancel	

- Edit the details as required. The screen is similar to the 'Add New User' section. Refer to '[Add an end user](#)' for more details.
- Click the 'Save' button.

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 Managing Groups

The 'Groups' interface allows the administrators with appropriate privileges to create administrator groups according to the needs of the organization. Each group can be configured with different permission levels. This simplifies the process of configuring permission levels for each administrator meaning new or existing administrators belonging to the account can be simply assigned a group with a preset policy. The admin interface will vary according to the user's permission level. Refer to the '[Managing Administrative Users](#)' section for more details on how to assign a group to admin users.

- To open the 'Groups' screen, click the 'User Management' tab on the left menu and click 'Groups'

Groups

[Add group](#)

Group Name	Group Description	Action
admin	Administrators	
domainmasters	Domain Masters	
operator	Operator Rights	
test	Test	
test1	Chennai Group	
trial	trial	
users	Incoming users	
viewer	View Only	

Copyright© 2006-2014 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 5.2.0.3055

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. Refer to the section ' 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

[Logout](#)

Group Name *	<input type="text"/>		
Group Description	<input type="text"/>		
Group Privileges	Privilege Name	Write	Read
	<input type="text" value="-Choose-"/>	All	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.



[Logout](#)

Add New Group


Group Name *	<input type="text"/>		
Group Description	<input type="text"/>		
Group Privileges	Privilege Name	Write	Read
	<u>All</u>	<u>All</u>	
	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #fff; padding: 2px 5px;">-Choose-</div> <div style="background-color: #00a0e3; color: white; padding: 2px 5px;">-Choose-</div> <div style="background-color: #fff; padding: 2px 5px;">All Privileges</div> <div style="background-color: #fff; padding: 2px 5px;">Anti-spam</div> <div style="background-color: #fff; padding: 2px 5px;">Anti-spoofing</div> <div style="background-color: #fff; padding: 2px 5px;">Anti-virus</div> <div style="background-color: #fff; padding: 2px 5px;">Auto Whitelist</div> <div style="background-color: #fff; padding: 2px 5px;">Archived Mails</div> <div style="background-color: #fff; padding: 2px 5px;">Delivery Logs</div> <div style="background-color: #fff; padding: 2px 5px;">Disclaimer</div> <div style="background-color: #fff; padding: 2px 5px;">DKIM</div> <div style="background-color: #fff; padding: 2px 5px;">DLP</div> <div style="background-color: #fff; padding: 2px 5px;">Domain Reports</div> <div style="background-color: #fff; padding: 2px 5px;">Attachment Verdict System</div> <div style="background-color: #fff; padding: 2px 5px;">Attachment Verdict Reports</div> <div style="background-color: #fff; padding: 2px 5px;">Greylist</div> <div style="background-color: #fff; padding: 2px 5px;">Groups</div> <div style="background-color: #fff; padding: 2px 5px;">SMTP IPS/FW</div> <div style="background-color: #fff; padding: 2px 5px;">LDAP/DB</div> <div style="background-color: #fff; padding: 2px 5px;">License</div> <div style="background-color: #fff; padding: 2px 5px;">Logs</div> </div>	+	

Copyright© 2006-2016 Comodo Security Solutions Inc. KoruMail name and logo are registered trademarks of Comodo Security Solutions Inc. Release: 2.0.0

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

Group Name *	<input type="text" value="Stores"/>								
Group Description	<input type="text" value="Stores Department"/>								
Group Privileges	<table border="1"> <thead> <tr> <th>Privilege Name</th> <th>Write</th> <th>Read</th> </tr> </thead> <tbody> <tr> <td>-Choose-</td> <td>All</td> <td>All</td> </tr> </tbody> </table>		Privilege Name	Write	Read	-Choose-	All	All	
	Privilege Name	Write	Read						
	-Choose-	All	All						
	Mail Logs		<input type="radio"/> <input checked="" type="radio"/> 						
Delivery Logs		<input type="radio"/> <input checked="" type="radio"/> 							
<div>Save Cancel</div>									

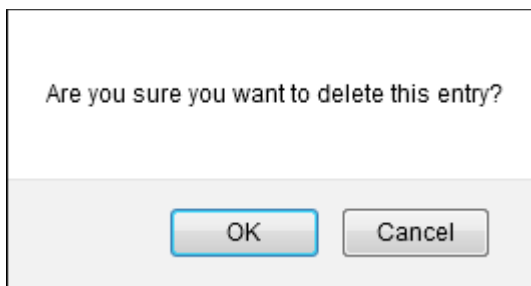
By default, the added privileges will have 'Read' rights only, meaning the features can be viewed and cannot be configured by the admin user.

- 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 the 'Save' button to add the new group.

Now this new group can be assigned to admin users. Refer to the section '[Managing Administrative 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



- 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 Logout

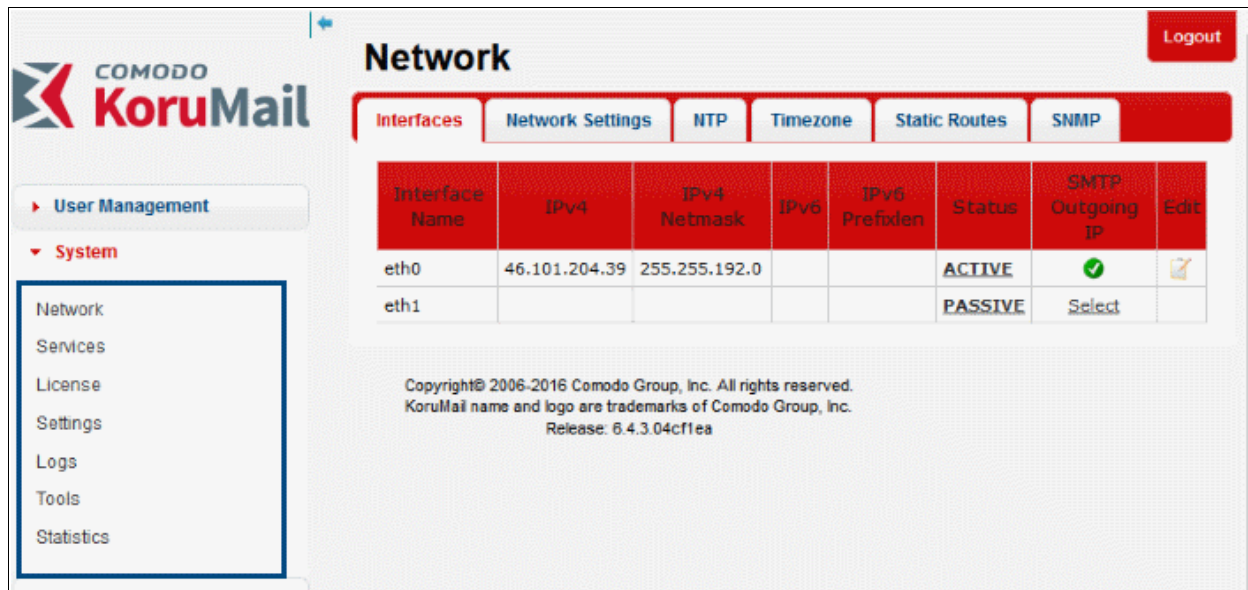
Group Name *	stores												
Group Description	Stores Department												
Group Privileges	<table border="1"> <thead> <tr> <th>Privilege Name</th> <th>Write</th> <th>Read</th> </tr> </thead> <tbody> <tr> <td>-Choose-</td> <td>All</td> <td>All</td> </tr> <tr> <td>Mail Logs</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Delivery Logs</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> </tbody> </table>	Privilege Name	Write	Read	-Choose-	All	All	Mail Logs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delivery Logs	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Privilege Name	Write	Read										
	-Choose-	All	All										
	Mail Logs	<input type="checkbox"/>	<input checked="" type="checkbox"/>										
Delivery Logs	<input type="checkbox"/>	<input checked="" type="checkbox"/>											
<div>Save Cancel</div>													

- Edit the details as required. The screen is similar to the 'Add New Group' section. Refer to '[Add a new group](#)' for more details.
- Click the 'Save' button.

The changes will be saved.

6 System Configurations

The 'System' tab on the left menu of the web console allows administrators to configure important parameters after initial configuration (see '[Installing the Appliance](#)').



- **Network:** Allows admin users to configure various network settings of KoruMail such as default gateways, DNS servers, NTP servers and more. Refer to the section '**Network Configuration**' for more details.
- **Services:** Allows admins to start or stop various services such as Delivery Agent, SMTP, Snmpd, Scheduler and more. Refer to the section '**Services**' for more details.
- **License:** View and update KoruMail licenses from this interface. Refer to the section '**License**' for more details.
- **Settings:** Configure various system settings such as Cache, Session, Backup and more. Refer to the section '**Configuring 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. Refer to the section '**Logs**' for more details.
- **Tools:** Allows admin users to check connectivity such as SMTP, Ping, Nslookup, Telnet as well as clear SMTP queue. Refer to the section '**Tools**' for more details.
- **Statistics:** View the graphical summary of system usage. Refer to the section '**System Usage Statistics**' for more details.

6.1 Network Configuration

The 'Network' tab allows administrators to configure various settings such as IP addresses for the network card (NIC), 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.

[Logout](#)

Network

Interfaces
Network Settings
NTP
Timezone
Static Routes
SNMP

Interface Name	IPv4	IPv4 Netmask	IPv6	IPv6 Prefixlen	Status	SMTP Outgoing IP	Edit
eth0	46.101.204.39	255.255.192.0			<u>ACTIVE</u>		
eth1					<u>PASSIVE</u>	<u>Select</u>	

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

- [Interfaces](#)
- [Network Settings](#)
- [Network Time Protocol \(NTP\)](#)
- [Time Zone](#)
- [Static Routes](#)
- [Simple Network Management Protocol \(SNMP\)](#)

6.1.1 Interfaces

The initial configuration of KoruMail is done at the time of installation using the Command Line Interface (CLI) console and can be edited and updated using the web console. Refer to the section '[Installing the Appliance](#)' for more details. The details of the Network Interface Card (NIC) can be edited/updated from the 'Interfaces' screen.

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

[Logout](#)


Network

Interfaces
Network Settings
NTP
Timezone
Static Routes
SNMP

Interface Name	IPv4	IPv4 Netmask	IPv6	IPv6 Prefixlen	Status	SMTP Outgoing IP	Edit
eth0	46.101.204.39	255.255.192.0			<u>ACTIVE</u>		
eth1					<u>PASSIVE</u>	<u>Select</u>	


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 appliance model. If two ports are available, then the

	appliance can be configured to route inbound and outbound emails on separate Ethernet 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 email 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. Refer to the section ' To edit the interface ' for more details.

From this screen, administrators can edit the interface settings.

To edit the interface

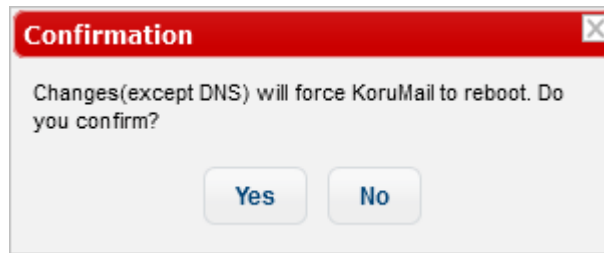
- Click the  icon beside the interface that you want to edit

The 'Edit interface' screen will be displayed.

Edit interface		Logout
Interface Name:	em0	
IPv4:	10 . 100 . 129 . 31	
IPv4 Netmask:	255 . 255 . 255 . 0	
IPv6:	<input type="text"/> <input type="checkbox"/> Remove IPv6 settings	
IPv6 Prefixlen:	<input type="text"/>	
Hostname:	<input type="text"/>	
IPv4 Default Gateway:	10 . 100 . 129 . 1	
IPv6 Default Gateway:	<input type="text"/>	
Primary DNS Server:	195 . 175 . 39 . 39	
Secondary DNS Server:	195 . 175 . 39 . 40	
Continent	Europe ▼	
City	Istanbul ▼	
Current timezone	Europe/Istanbul	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

- **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 appliance 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 the 'Save' button.

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



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

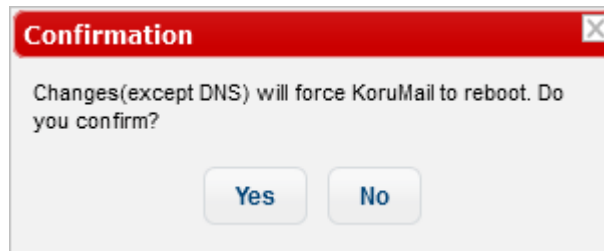
6.1.2 Network Settings

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' and 'Network Settings' from the 'Network' screen.

- **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 the 'Save' button.

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

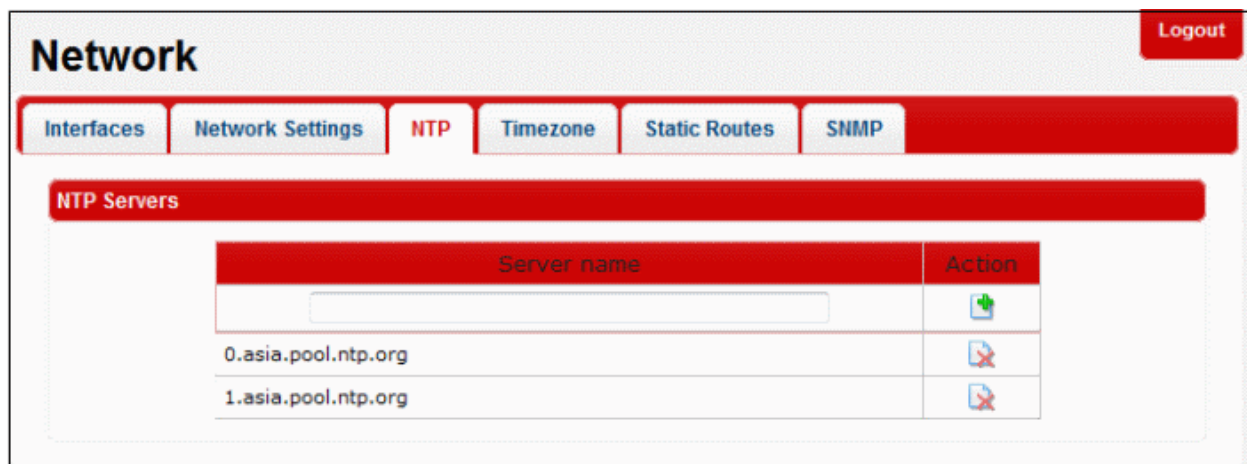


- Click 'Yes' to confirm the changes and reboot the system.

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' and 'NTP' from the 'Network' screen.



To add a new NTP server

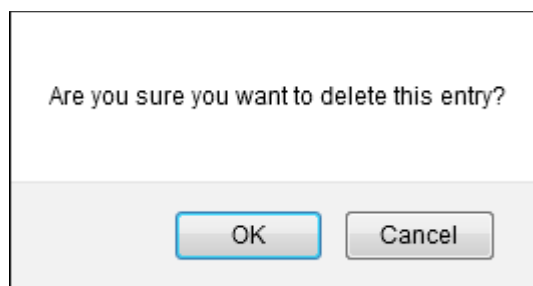
- Enter the name or IP address of the server in the 'Server name' field and click the 'Add' button

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.



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.

Network Logout

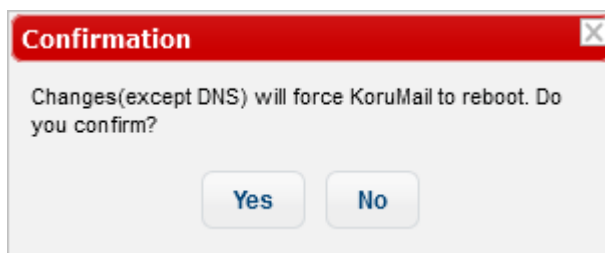
[Interfaces](#) [Network Settings](#) [NTP](#) [Timezone](#) [Static Routes](#) [SNMP](#)

Continent	Europe ▼
City	Istanbul ▼
Current timezone	Europe/Istanbul

[Save](#)

- **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.

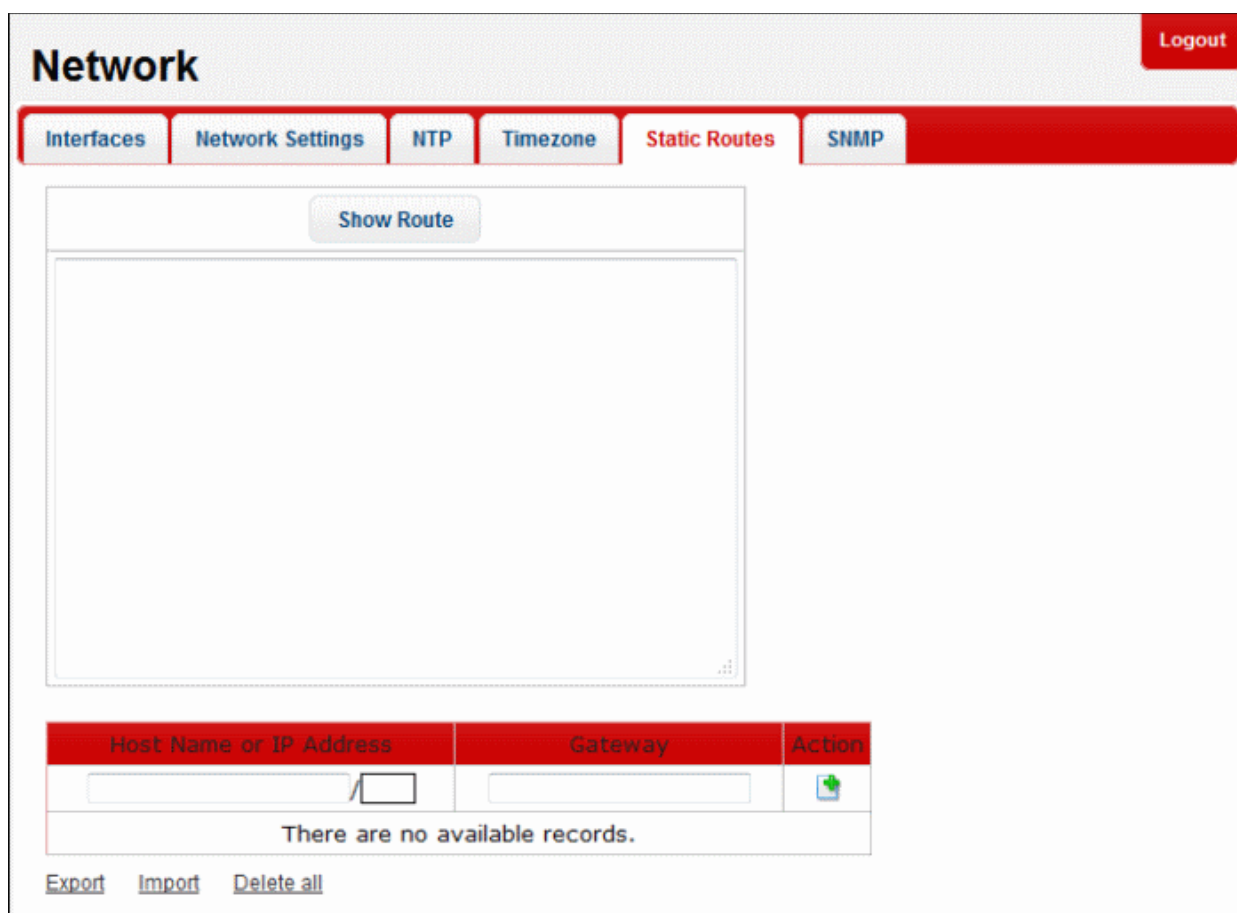


Click 'Yes' to confirm the changes and reboot the system. The changes done here will also be reflected in the '**Edit Interface**' of the NIC as explained in the previous section '**Interfaces**'.

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' and 'Static Routes' from the 'Network' screen.





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 / <input type="text"/>	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	Action
192.168.199.1 / <input type="text"/>	10.100.129.2	
192.168.199.1	10.100.129.2	

[Export](#) [Import](#) [Delete all](#)

The 'Import' dialog will be displayed.

Import

 Upload

Save

Close





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

The file will be added.




The 'Import' dialog box has a red header bar with the title 'Import'. Below the header, there is a light blue bar containing a '+ Upload' button on the left and a 'X Clear All' button on the right. The main area of the dialog is white and contains the text 'Static-Routes' and 'Done' on the left, and a 'Clear' link on the right. At the bottom of the dialog, there are two buttons: 'Save' and 'Close'.

- 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
<input type="text"/>	<input type="text"/>	
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	
Export Import Delete all		

- 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.

Static Routes

Show Route

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
<input type="text"/>	<input type="text"/>	
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.

Network

Logout

Interfaces

Network Settings

NTP

Timezone

Static Routes

SNMP


System Location

Chennai

System Contact

KoruMail Admin



Save

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 provides the current status of various KoruMail services. You can stop or restart a service and also shutdown or reboot KoruMail.

- To view and configure KoruMail services, click the 'System' tab on the left menu, then 'Services'

Services

Service	Status	Start / Stop	Restart
KoruMail Delivery Agent			
KoruMail SMTP Service			
KoruMail SMTP Submission Service			
KoruMail Main Filtering Engine			
Anti-spam Engine #1			
Anti-spam Engine #2			
KoruMail DB Connector			
Syslogd			
Snmpd Service			
Anti-virus Module			
Scheduler Service			

Legend

- Not Available
- Service is running
- Service is stopped
- Start service
- Stop service
- Restart service





Copyright© 2006-2014 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 5.2.0.3055


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

Description of the Services	
Column Header	Description
KoruMail Delivery Agent	The service forwards the emails processed by KoruMail to target email server.
KoruMail 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 the 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.
Submission SMTP Service	Submission port (587), is a mail delivery port as port 25 (SMTP) but it requires additional authentication. If you do not have an account on this server, you cannot send an e-mail.
KoruMail Main Filtering Engine	The emails that are filtered by 'SMTP Service' are passed to the main filtering engine software that checks for spam and virus in the mails. This module performs the actions specified by administrator such as rejecting, quarantining the infected email or saving the email to another register area or address. If e-mail is required to be sent to recipient then it is forwarded by the KoruMail Delivery Agent.
Anti-spam Engines	KoruMail antispam engines scans emails and specifies spam scores controlling thousands of spam signatures such as header and bayesian-based content filtering. This scores are used to define an e-mail as spam.
KoruMail DB Connector	The Postgre SQL services running on KoruMail's internal database of quarantined emails and archives.
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.
Anti-virus Module	KoruMail includes Comodo's anti-viurs programs as a built in solution.
Scheduler Service	This service organizes the programs that runs periodically. This feature in KoruMail Messaging 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, click on the  button.
- To reboot the KoruMail, click on the  button.

6.3 License

The 'License' screen allows administrators to view current license details as well as to 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.

- To view and purchase a new KoruMail license, click the 'System' tab on the left menu, then 'License'

License								Logout
Licenses	License Activation	End User License Agreement						
CAM User e-mail Address	CAM Automatic Renewal	CAM Max Users	CAM Max Servers	CAM Activation Limit	CAM License First Installation Date	CAM License Expiration Date	CAM License Status	
mylicense@comodo.com	No	100	1	3	2015-02-24	2016-02-24	VALID	
Click here to get CAM license key								

From here an administrator can:

- [View the details of your current license](#)
- [Purchase a license](#)
- [Activate your license](#)

- [Read End User License Agreement \(EULA\)](#)

To view the details of current license

- Click the 'Licenses' tab

License Logout

Licenses | License Activation | End User License Agreement

CAM User e-mail Address	CAM Automatic Renewal	CAM Max Users	CAM Max Servers	CAM Activation Limit	CAM License First Installation Date	CAM License Expiration Date	CAM License Status
admin@comodo.com	No	100	1	3	2015-02-24	2016-02-24	VALID

[Click here to get CAM license key](#)

License – Table of Column Descriptions	
Column Header	Description
CAM User e-mail Address	The email ID provided at the time of CAM sign-up.
CAM Automatic Renewal	Indicates whether automatic renewal of license is opted.
CAM Max Users	Maximum number of users that can be enrolled
CAM Max Servers	Maximum number of servers that Korumail can be installed.
CAM Activation Limit	The number of times the same license key can be used to activate Korumail in the same machine.
CAM License First Installation Date	Indicates the date when the license was activated.
CAM License Expiration Date	Indicates the license expiry date
CAM License Status	Indicates the status of the license, whether it is valid or expired.

To purchase a license

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

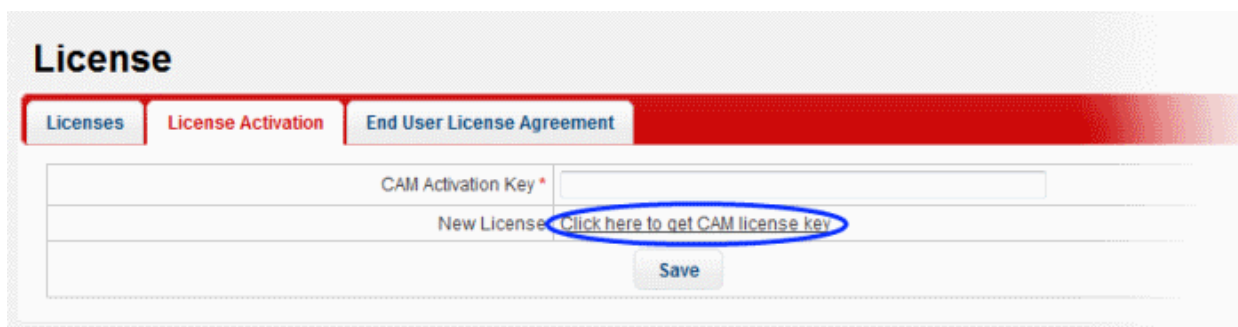
License

Licenses | License Activation | End User License Agreement

CAM User e-mail Address	CAM Automatic Renewal	CAM Max Users	CAM Max Servers
admin@comodo.com	No	100	1

[Click here to get CAM license key](#)

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



License

Licenses **License Activation** **End User License Agreement**

CAM Activation Key *

New License [Click here to get CAM license key](#)

Save

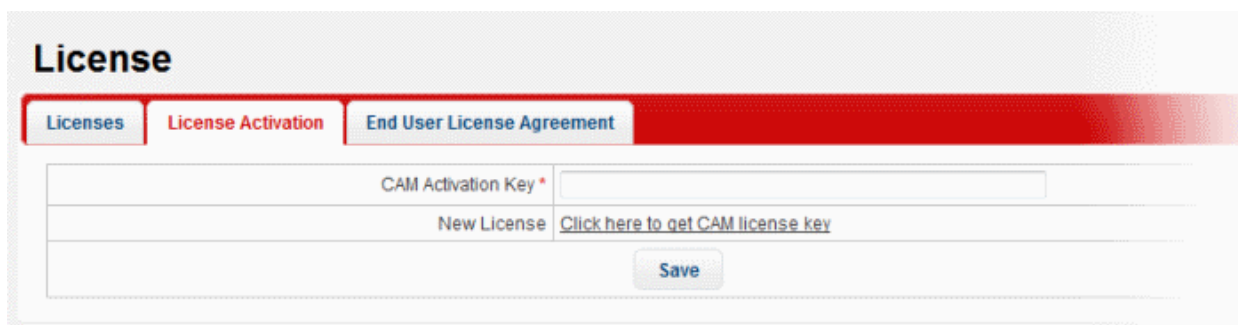
You will be taken to Comodo Accounts Manager (CAM) login page at <https://accounts.comodo.com/account/login>

- 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.

To activate your license

- Click the 'License Activation' tab.



License

Licenses **License Activation** **End User License Agreement**

CAM Activation Key *

New License [Click here to get CAM license key](#)

Save

- 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.

License Logout

Licenses License Activation **End User License Agreement**

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 Yazilim A.S. Turkey, a Turkish company, with offices at Halici Yazilim Evi Zemin Kat ODTÜ Teknokent Gankaya Ankara Turkey ("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 the Services.

- Read the EULA fully.

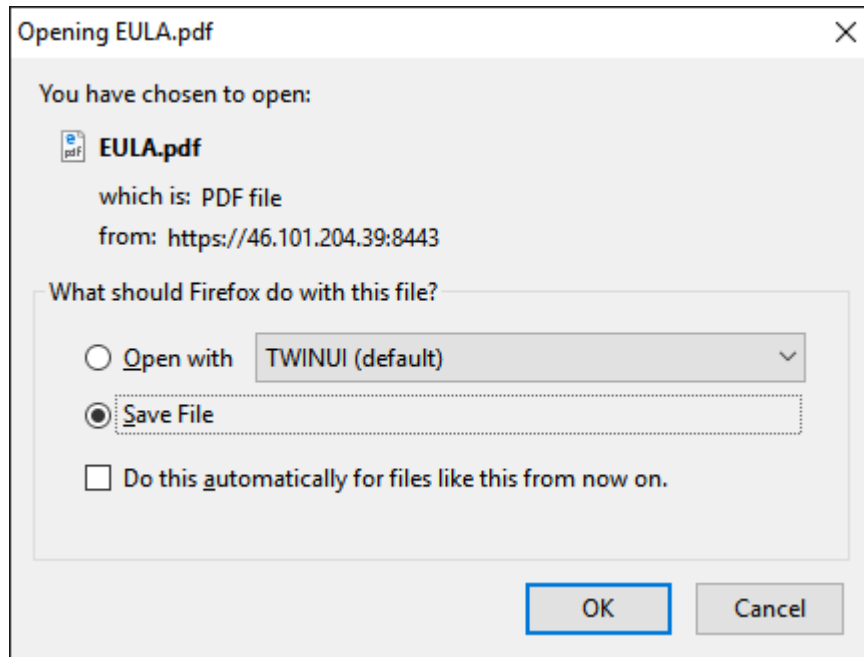
You can also download the EULA from the screen by clicking the 'Download As PDF' link at the bottom.

EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL SENDMAIL, INC., THE REGENTS OF THE UNIVERSITY OF CALIFORNIA OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

[Download As PDF](#) 

Copyright© 2006-2014 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 5.2.0.3055

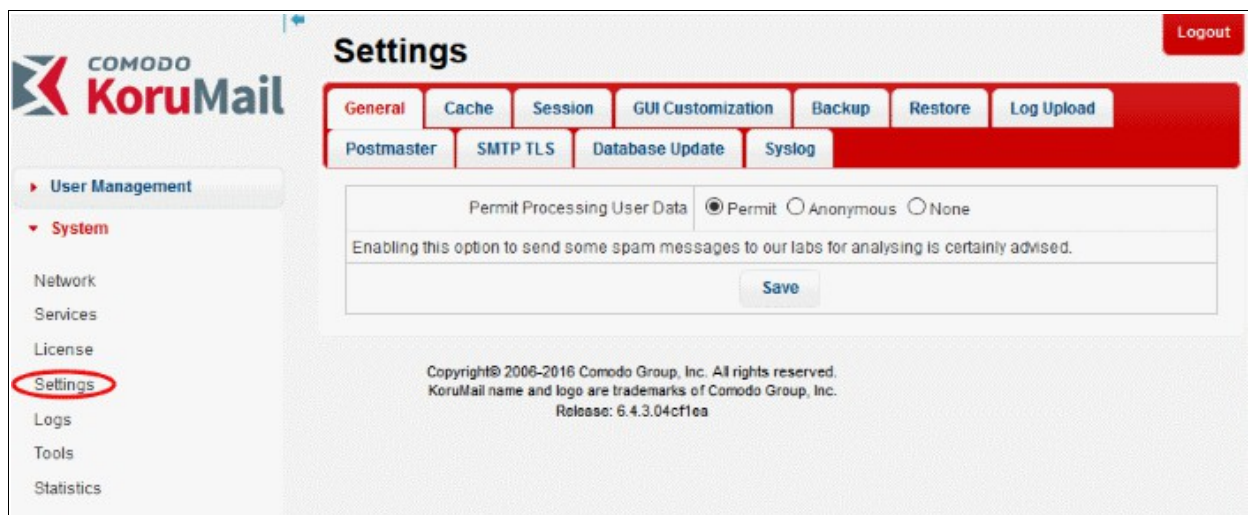
- Click 'OK' to download the file to your system.



6.4 Configuring System Settings

The 'Settings' interface allows administrators to configure various parameters such as cache settings for Greylist IP, LDAP, SMTP-Auth logs, user session timeout duration, system backup and restore, log upload settings and more.

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



Click the following links for more details:

- [General](#)
- [Cache](#)
- [Session](#)
- [GUI Customization](#)
- [Backup](#)
- [Restore](#)
- [Log Upload](#)
- [Postmaster](#)

- [SMTP TLS](#)
- [Database Update](#)
- [Update Database](#)
- [Syslog](#)

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' and 'General' tab.

Settings Logout

General Cache Session GUI Customization Backup Restore Log Upload

Postmaster SMTP TLS Database Update Syslog

Permit Processing User Data ☒ Permit ☐ Anonymous ☐ None

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

Save

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

6.4.2 Cache Settings

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

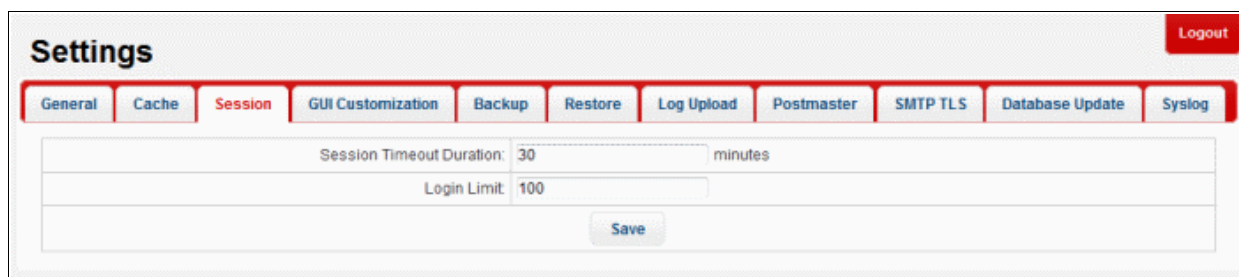
- To open the 'Cache' settings interface, click the 'System' tab on the left menu, then 'Settings' and 'Cache' tab.

- **Greylist IP Cache expire time:** KoruMail greylists IP addresses from which emails are received for the first time and rejects it. If the sender is using a proper mail server, it automatically resends the email. The greylisted IP becomes whitelisted and email is not rejected. If the mail is from a spam source, then normally it will not resend mails. Enter the time for which the greylisted IPs should be cached. If within this time emails are resent from greylisted IPs, they are whitelisted. After the entered time, the greylisted IPs are deleted from the greylist.
- **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 the 'Save' button 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.



The screenshot shows the 'Settings' page with a 'Session' tab selected. The page has a header with a 'Logout' button. Below the header is a navigation bar with tabs: General, Cache, Session (active), GUI Customization, Backup, Restore, Log Upload, Postmaster, SMTP TLS, Database Update, and Syslog. The main content area contains two input fields: 'Session Timeout Duration' set to 30 minutes and 'Login Limit' set to 100. A 'Save' button is located at the bottom of the form.

- **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 the 'Save' button 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.

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

The screenshot shows the 'Settings' page with the 'GUI Customization' tab selected. The 'Company' field contains 'KoruMail'. The 'Logo' section has an 'Upload' button and a text box with the instruction: 'Logo size must not be greater than 150x100 (widthxheight) pixels and format must be PNG.' Below this is a checkbox for 'Use default choose.' The 'Theme' dropdown is set to 'Blitzer (Default)'. A 'Save' button is at the bottom right.

- **Company:** Enter the name of the company to be displayed
- **Logo:** To upload the logo to be displayed, click the 'Upload' button, navigate to the location where it is saved and click 'Open'.

This screenshot shows the same 'Settings' page after a logo upload. The 'Logo' section now displays 'test_logo.png' with a 'Done' status and a 'Clear' link. There are also 'Upload' and 'Clear All' buttons. The 'Theme' remains 'Blitzer (Default)' and the 'Save' button is still present.

The image will be uploaded and displayed in the interface. Please note the image should be in .png format and its size should not be greater than 150 width x 100 length.

- To remove the logo, click the 'Clear' link.
- Click the 'Save' button to upload the logo.
- **Theme:** The 'Themes' drop-down allows you to choose the colors and appearance of the GUI as you prefer (Default = Redmond Theme).
- Click the 'Save' button 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' and 'Backup' tab.

The screenshot shows the 'Settings' page with the 'Backup' tab selected. The 'Backup Password' field is filled with dots. The 'Create Backup' button is highlighted. The 'Enable Auto Backup' checkbox is checked. The 'Save' button is at the bottom.

Settings		Logout								
General	Cache	Session	GUI Customization	Backup	Restore	Log Upload	Postmaster	SMTP TLS	Database Update	Syslog
Backup Password		••••••••								
Backup Password		••••••••								
		Create Backup Cancel								
Enable Auto Backup		<input checked="" type="checkbox"/>								
		Save								

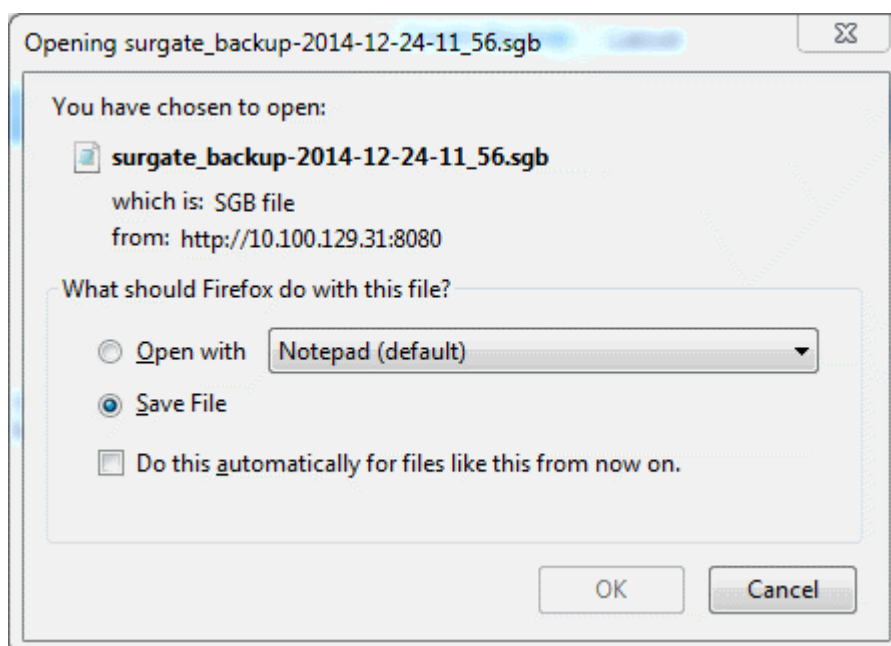
Instant Backup

- 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.

The screenshot shows the 'Settings' page with the 'Backup' tab selected. It features two password fields for 'Backup Password', a 'Create Backup' button, and a 'Click here to download backup' link highlighted with a blue circle. There is also an 'Enable Auto Backup' checkbox and a 'Save' button at the bottom.

- Click the 'Click here to download backup' link.



- Click 'OK' to save the file in 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.

Settings Logout

General Cache Session GUI Customization **Backup** Restore Log Upload Postmaster SMTP TLS Database Update Syslog

Backup Password

Backup Password

Enable Auto Backup ☒

Host

User

Password

Password

Remote Path

Backup type

Days to backup ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday ☐ Sunday

Backup hour

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

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' and 'Restore' tab

Settings Logout

General Cache Session GUI Customization Backup **Restore** Log Upload Postmaster SMTP TLS Database Update Syslog

Backup File:

Backup Password:

- To restore, click the 'Upload' button, navigate to the location where the backup file is saved and click 'Open'.

After uploading, the backup file will be displayed on the screen.

Settings Logout

General Cache Session GUI Customization Backup **Restore** Log Upload Postmaster SMTP TLS Database Update Syslog

Backup File:

surgate_backup-2015-3-3-11_46.sgb
Done

Backup Password:

- To remove the file, click the 'Clear' link beside it.
- To restore the backup, enter the backup password and click the 'Restore' button.

KoruMail will be rebooted after restoring

For the restore operation to be completed, KoruMail has to be rebooted. 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' and 'Log Upload' tab

Settings Logout

General Cache Session GUI Customization Backup Restore **Log Upload** Postmaster SMTP TLS Database Update Syslog

Host *

User *

Password *

Password *

Remote path *

Upload type

Days to upload * ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday ☐ Sunday

Upload hour *

- **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 the 'Save' button. 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:** 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 SMTP TLS Settings

KoruMail allows administrators to enable Transport Layer Security (TLS) encryption to provide authentication and confidentiality for email traffic. In order to enable TLS encryption, a certificate should be installed in the mail server.

- To open the 'SMTP TLS' settings interface, click the 'System' tab on the left, then click 'Settings' > 'SMTP TLS' tab.

- **Enable SMTP TLS:** Select the check box to enable TLS encryption while transmitting message between Mail Transfer Agents (MTAs). If selected, the details of the certificate should be entered in the fields.

The screenshot shows the 'Settings' page in the Comodo KoruMail Admin interface. The 'SMTP TLS' tab is selected, highlighted in red. The page has a 'Logout' button in the top right corner. Below the tabs, there is a form for configuring SMTP TLS. The 'Enable SMTP TLS' checkbox is checked. The 'The number of days of validity of certificate' is set to 360. Below this are fields for 'Country', 'State', 'City', 'Department', 'Host Name or IP Address', 'E-mail', and 'Created Date'. A 'Save' button is located at the bottom of the form.

Settings	
General Cache Session GUI Customization Backup Restore Log Upload Postmaster SMTP TLS Database Update Syslog	
Enable SMTP TLS	<input checked="" type="checkbox"/>
The number of days of validity of certificate *	360
Country *	--
State *	
City *	
Department *	
Host Name or IP Address *	
E-mail *	
Created Date	
<input type="button" value="Save"/>	

- Click the 'Save' button.

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

6.4.11 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:** 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.

- **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 the 'Save' button.

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 Logout

Log Files **Purge Files**

Total Log size: Refresh

[SMTP Filtering](#) [SMTP Service](#) [SMTP Submission](#) [Korugan Engine](#) [E-mail Delivery](#)

<input type="checkbox"/>	File Name	File Date	File Size	Action
<input type="checkbox"/>	korumailauth.log-20161115	Nov 15 17:34	577K	Download
<input type="checkbox"/>	korumailauth.log-20161116	Nov 16 23:57	233K	Download
<input type="checkbox"/>	korumailauth.log-20161117	Nov 17 19:19	269K	Download
<input type="checkbox"/>	korumailauth.log-20161118	Nov 18 04:31	88K	Download
<input type="checkbox"/>	korumailauth.log-20161122	Nov 22 23:37	956K	Download
<input type="checkbox"/>	korumailauth.log-20161123	Nov 23 01:11	1.6K	Download
	smtpproxy.log	Nov 22 03:11	0	Download
<input type="checkbox"/>	smtpproxy.log-20161115	Nov 15 21:59	220K	Download
<input type="checkbox"/>	smtpproxy.log-20161116	Nov 16 23:37	178K	Download
<input type="checkbox"/>	smtpproxy.log-20161117	Nov 17 20:41	145K	Download
<input type="checkbox"/>	smtpproxy.log-20161118	Nov 18 03:32	6.0K	Download
<input type="checkbox"/>	smtpproxy.log-20161122	Nov 22 23:35	148K	Download
<input type="checkbox"/>	smtpproxy.log-20161123	Nov 23 06:02	67K	Download

The 'Logs' interface has the following tabs:

- Log Files**
- Purge Files**

6.5.1 Log Files

The 'Log Files' tab displays the list of available log files for different activities and connection attempts. These include:

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

Administrators can download the log files and delete unwanted logs from this interface.

Tip: You can also view the real-time logs from the Reports interface. Refer to the section **Reports** for more details.

- To open the 'Log Files' interface, click the 'System' tab on the left menu, then 'Logs' and 'Log Files' tab.













Logs

Logout


Log Files
Purge Files

Total Log size: Refresh

[SMTP Filtering](#)
[SMTP Service](#)
[SMTP Submission](#)
[Korumail Engine](#)
[E-mail Delivery](#)

<input type="checkbox"/>	File Name	File Date	File Size	Action
<input type="checkbox"/>	korumailauth.log-20161115	Nov 15 17:34	577K	 Download
<input type="checkbox"/>	korumailauth.log-20161116	Nov 16 23:57	233K	 Download
<input type="checkbox"/>	korumailauth.log-20161117	Nov 17 19:19	269K	 Download
<input type="checkbox"/>	korumailauth.log-20161118	Nov 18 04:31	88K	 Download
<input type="checkbox"/>	korumailauth.log-20161122	Nov 22 23:37	956K	 Download
<input type="checkbox"/>	korumailauth.log-20161123	Nov 23 01:11	1.6K	 Download
	smtpproxy.log	Nov 22 03:11	0	Download
<input type="checkbox"/>	smtpproxy.log-20161115	Nov 15 21:59	220K	 Download
<input type="checkbox"/>	smtpproxy.log-20161116	Nov 16 23:37	178K	 Download
<input type="checkbox"/>	smtpproxy.log-20161117	Nov 17 20:41	145K	 Download
<input type="checkbox"/>	smtpproxy.log-20161118	Nov 18 03:32	6.0K	 Download
<input type="checkbox"/>	smtpproxy.log-20161122	Nov 22 23:35	148K	 Download
<input type="checkbox"/>	smtpproxy.log-20161123	Nov 23 06:02	67K	 Download

- The interface displays the total size of all the log files available currently from the KoruMail system.
- Clicking 'Refresh' reloads the list of the available log files to include the latest log files generated.
- The links above the table enables the administrator to choose the category of log files to be downloaded or deleted.

Log Files – Table of Column Descriptions		
Column Header	Description	
File Name	Name of the log file	
File Date	The precise date and time at which the log file was created.	
File Size	The size of the log file.	
Actions		Allows the administrators to delete the log file.

	Download	Allows the administrators to download the log file.
--	--------------------------	---

To download a log file

- Select the category of the log files to be viewed from the links above the table


The list of available log files under the chosen category will be displayed.

- Click the 'Download' link in the row of the required log file to download the file.

To delete an unwanted log file

- Select the category of the log files to be viewed, from the links above the table

The list of available log files under the chosen category will be displayed.

- Click the Delete icon  in the row of the required log file to download the file.
- Click 'OK' in the confirmation dialog.

To delete several unwanted log files

- Select the category of the log files to be viewed from the links above the table

The list of available log files under the chosen category will be displayed.

- Select the log files to be deleted by selecting the checkboxes beside them
- Click the 'Delete' button at the bottom left of the list.
- Click 'OK' in the confirmation dialog.

6.5.2 Purge Files

The Purge Files interface allows administrators to configure the time limit for preserving the log files and archived mails. Log files, archived mails and quarantined mails that are older than the period specified from this interface will be automatically removed.

- To open the 'Purge Files' interface, click the 'System' tab on the left menu then 'Logs' then open the 'Purge Files' tab.

Logs

Log Files

Purge Files

Delete older mail log records in database (Days)	<input type="text" value="0"/>
Delete older archived mails (Days)	<input type="text" value="0"/>
Delete older quarantine mails (Days)	<input type="text" value="0"/>
<input type="button" value="Delete"/>	

- 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

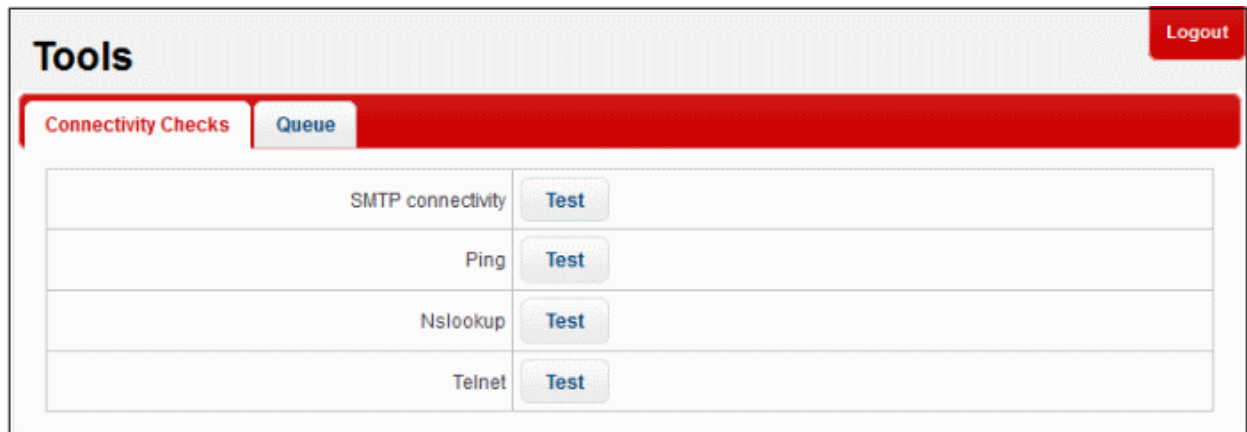
retained in the local database. Mails older than the days specified here, will be automatically deleted.

- 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 Checks**
- **SMTP Queue**

6.5.4 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.

Tools Logout

Connectivity Checks Queue

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 screenshot shows the 'Tools' section of the Comodo KoruMail Admin interface. It has two tabs: 'Connectivity Checks' and 'Queue'. Under 'Connectivity Checks', there is a table with columns 'SMTP connectivity', 'Ping', and 'Test'. The 'Test' button is circled in blue. A modal window titled 'Check remote SMTP Connectivity' is open, showing fields for 'Host Name or IP Address' (192.168.199.31), 'Port' (25), 'Sender', and 'Recipient'. A 'Result' field is at the bottom. 'Send' and 'Close' buttons are at the bottom right.

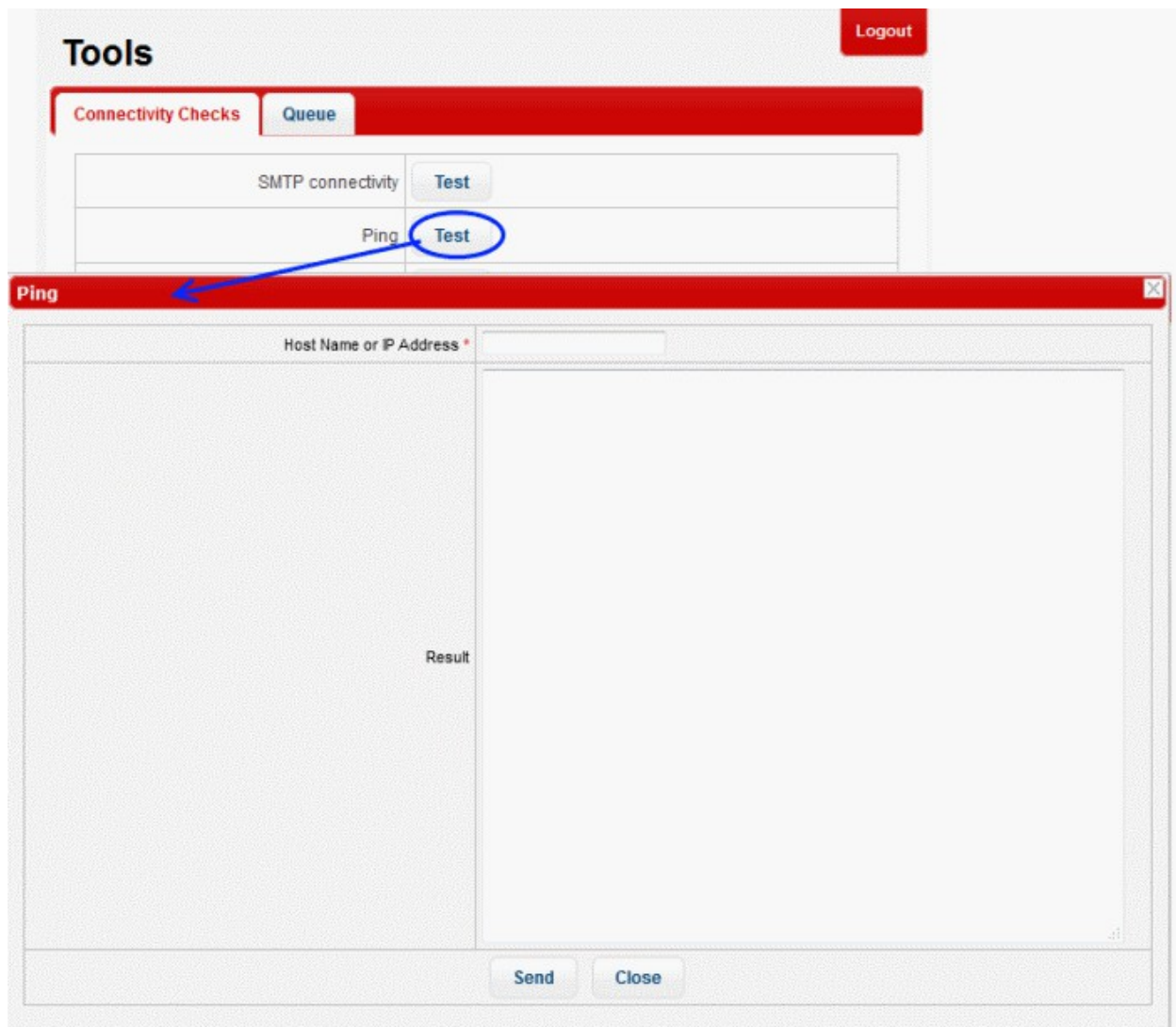
The 'Check remote SMTP Connectivity' interface will appear.

- 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.



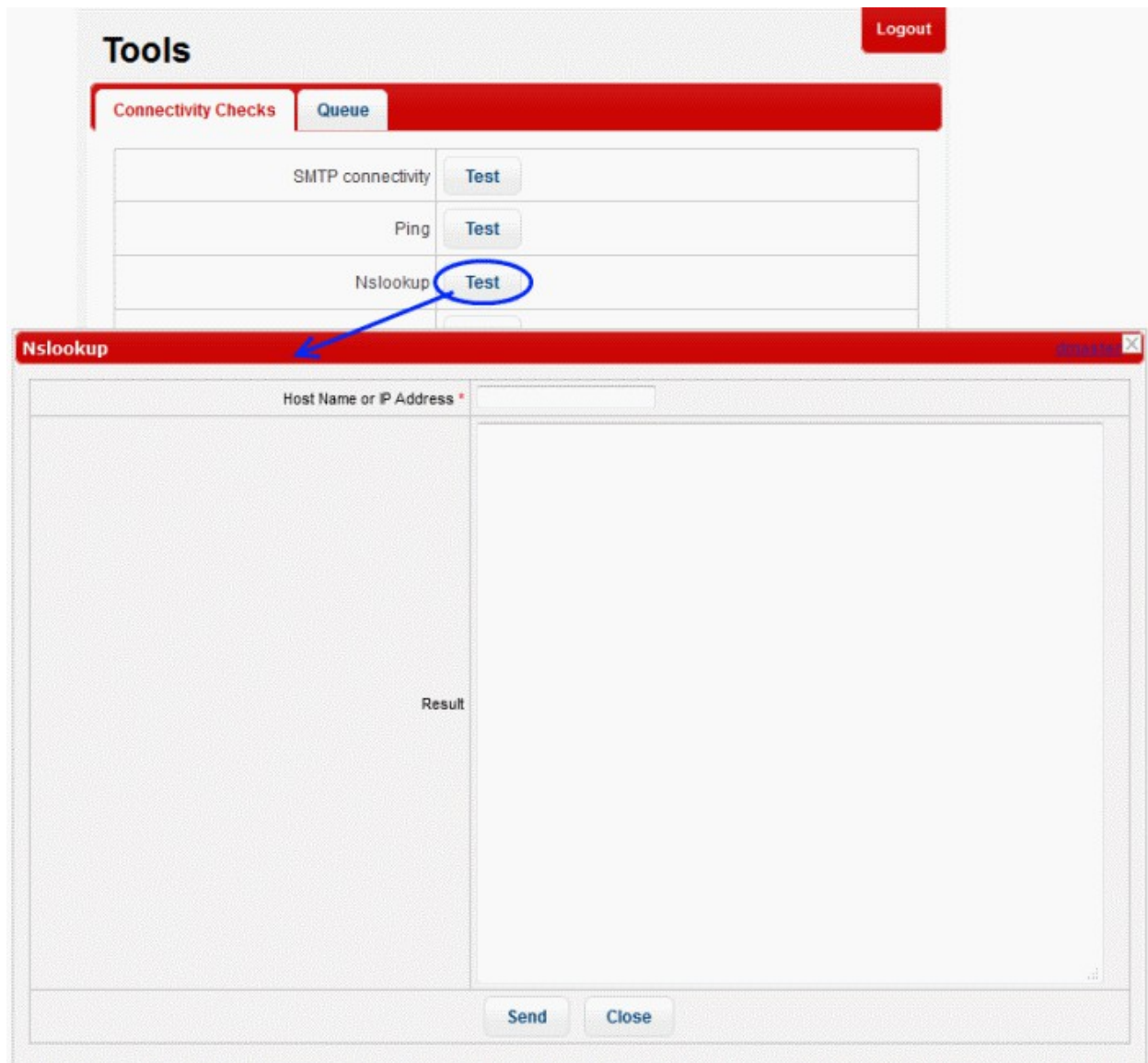
The 'Ping' interface will appear.

- 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.

Tools Logout

Connectivity Checks **Queue**

SMTP connectivity	Test
Ping	Test
Nslookup	Test
Telnet	Test

Telnet

Host Name or IP Address *

Port 25

Request GET /login.xhtml HTTP/1.0

Result

[Send](#) [Close](#)

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'

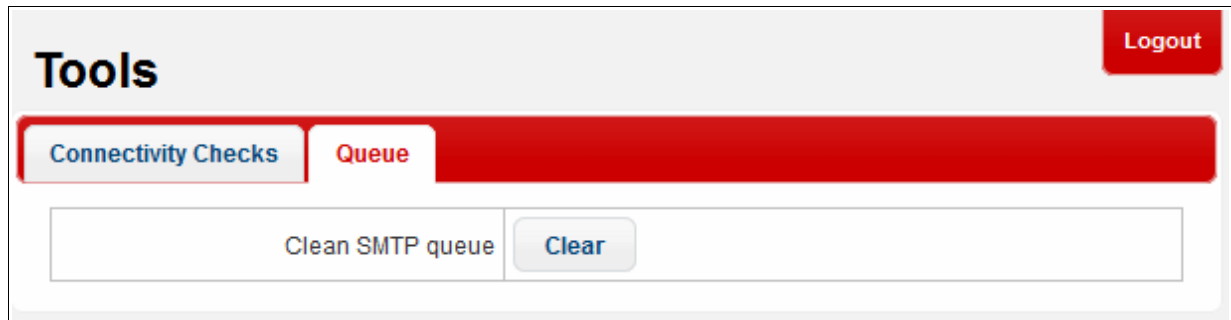
KoruMail will send the request to the remote host for checking the Telnet connectivity and display the results in the 'Result' field.

6.5.5 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' and 'Queue' tab.

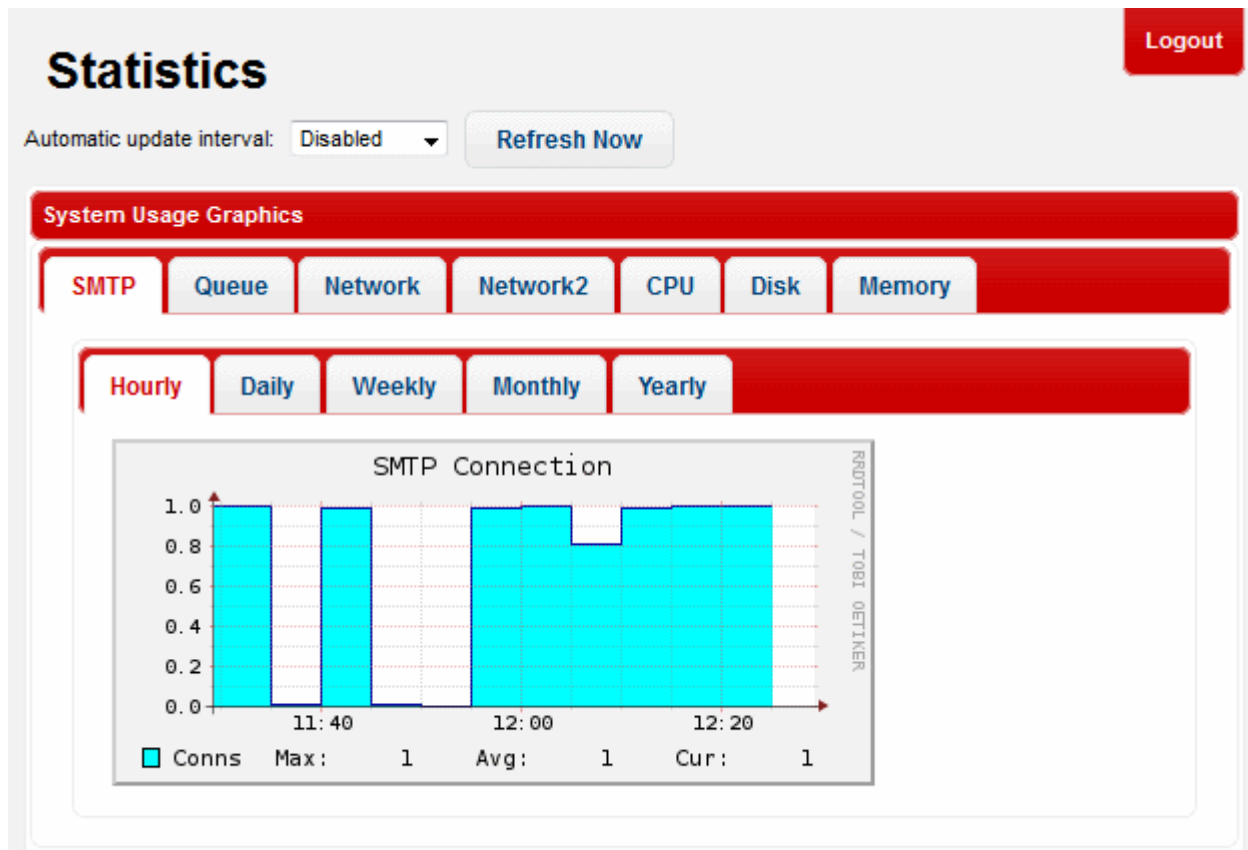


- Click the Clear button beside CLEAN SMTP queue.

6.6 System Usage Statistics

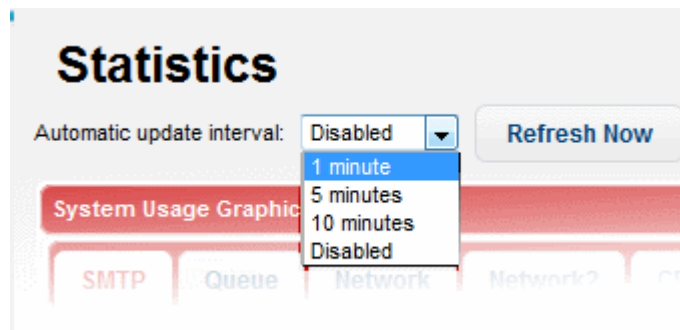
KoruMail displays SMTP connection statistics, mail statistics and utilization statistics of hardware and software resources like network, CPU, hard disks and system memory as graphs in the 'Statistics' interface.

- 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.



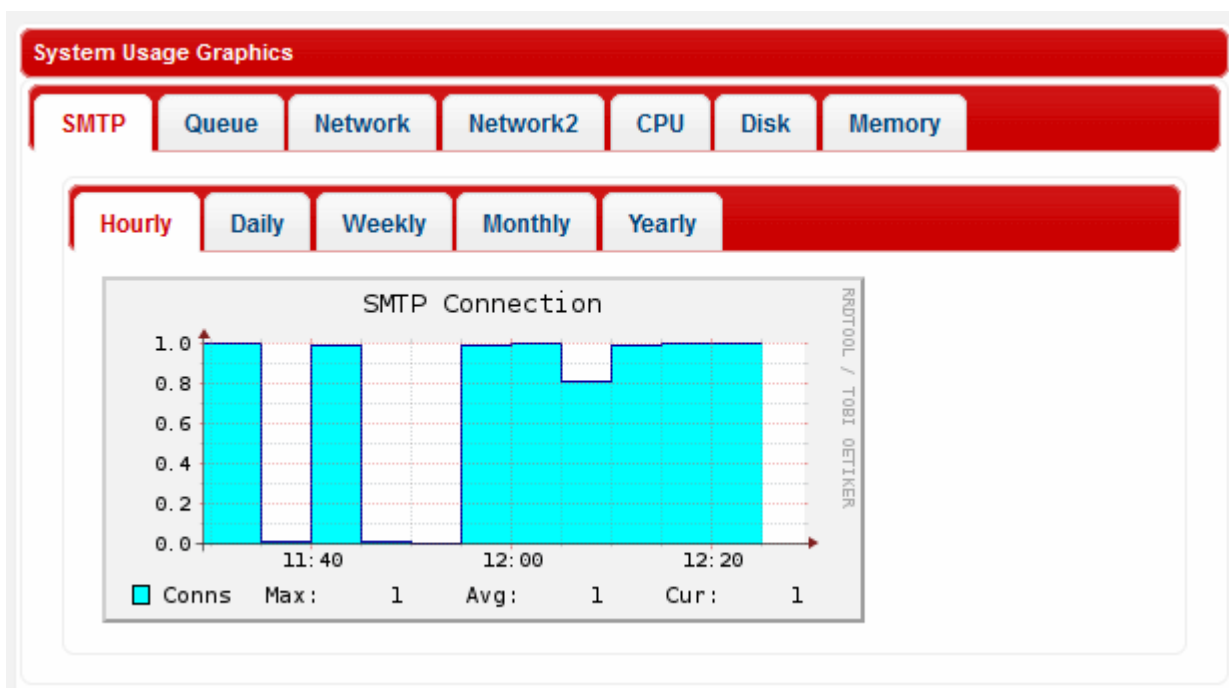
- To instantly update the statistics, click the 'Refresh Now' button.

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:

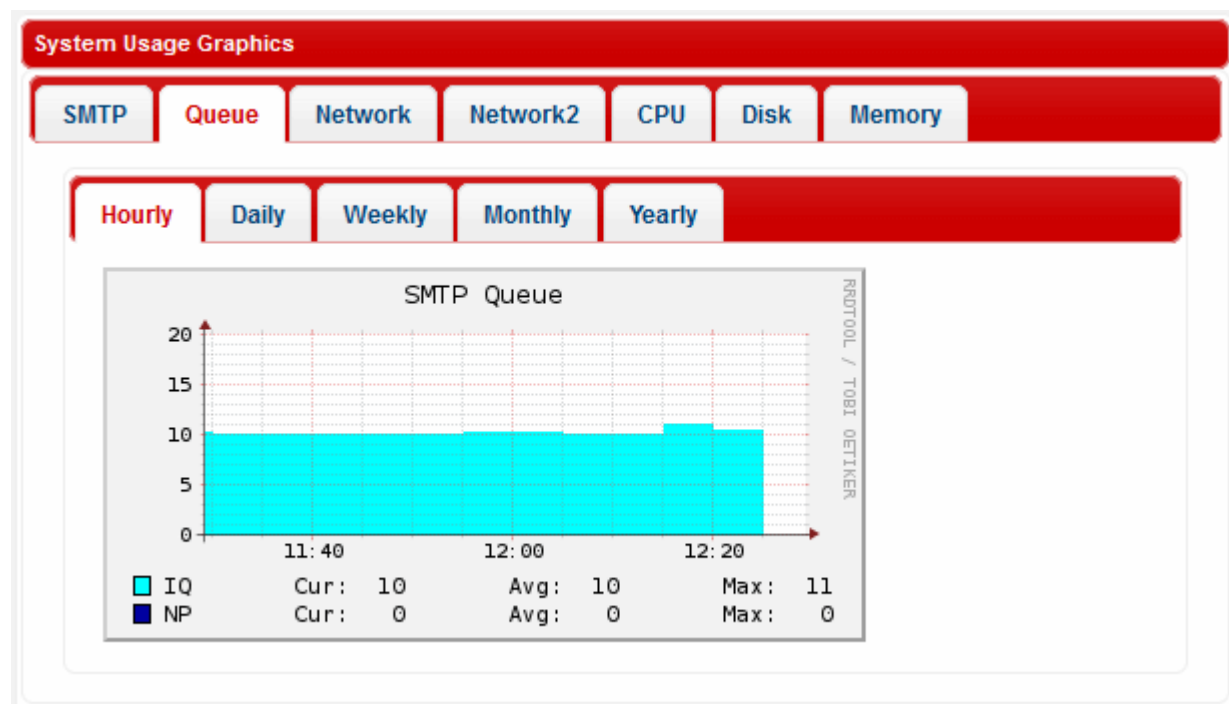


- Hourly - Shows the log of connections for the past one hour
- Daily - Shows the log of connections for the past 24 hours
- Weekly - Shows the log of connections for the past seven days
- Monthly - Shows the log of connections for the past four weeks
- Yearly - Shows the log of connections for the past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

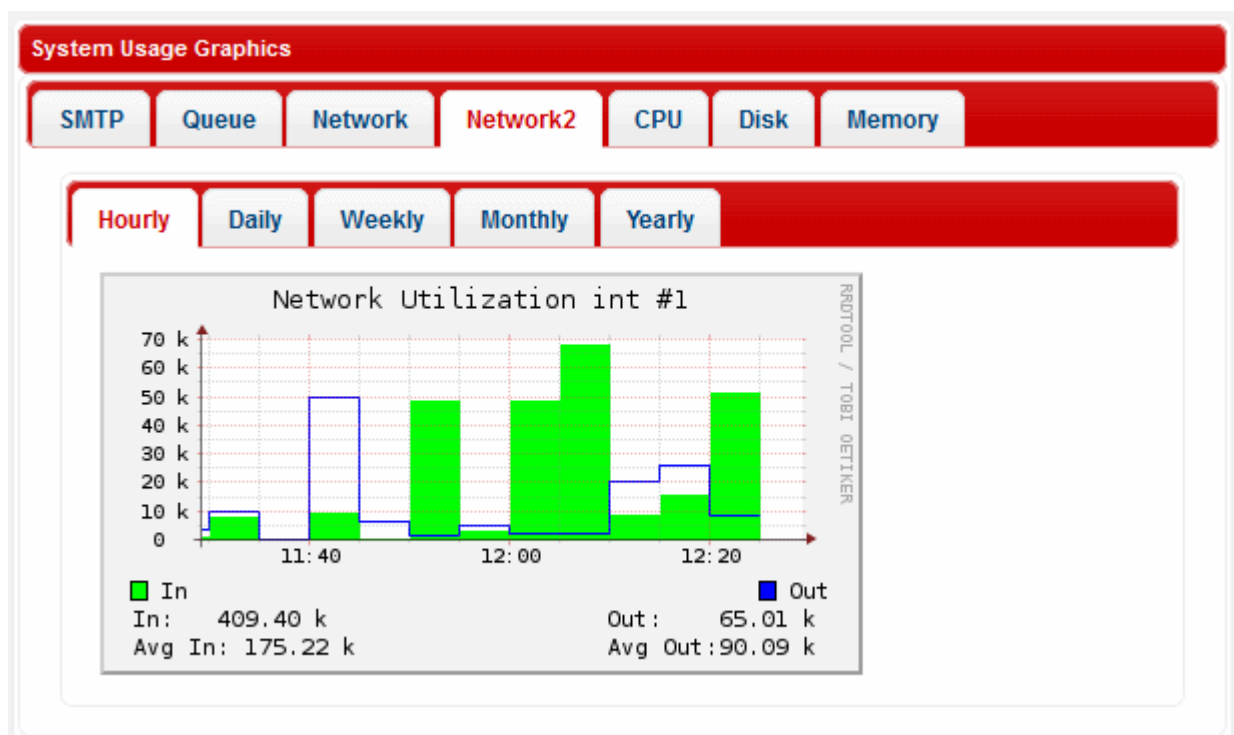


You can choose the time period for which you wish to see the logs from the sub tabs:

- 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

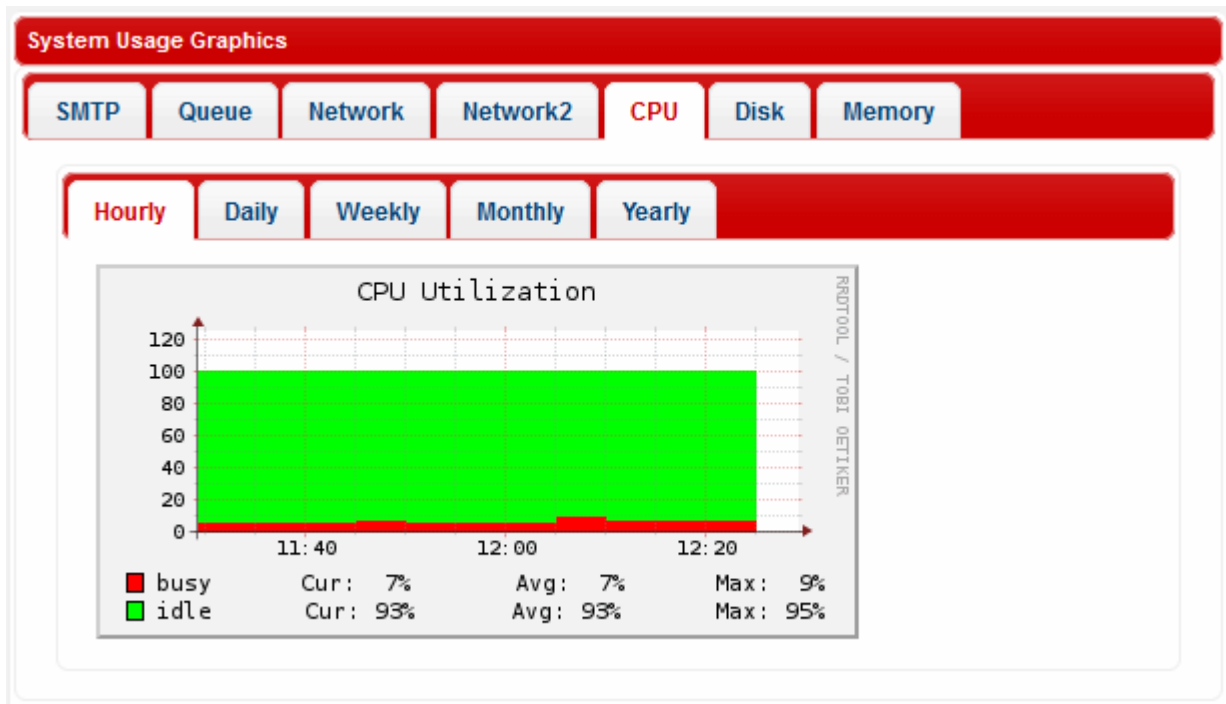
The incoming and outgoing traffic are represented with different colors in the graph.

- 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.



- 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

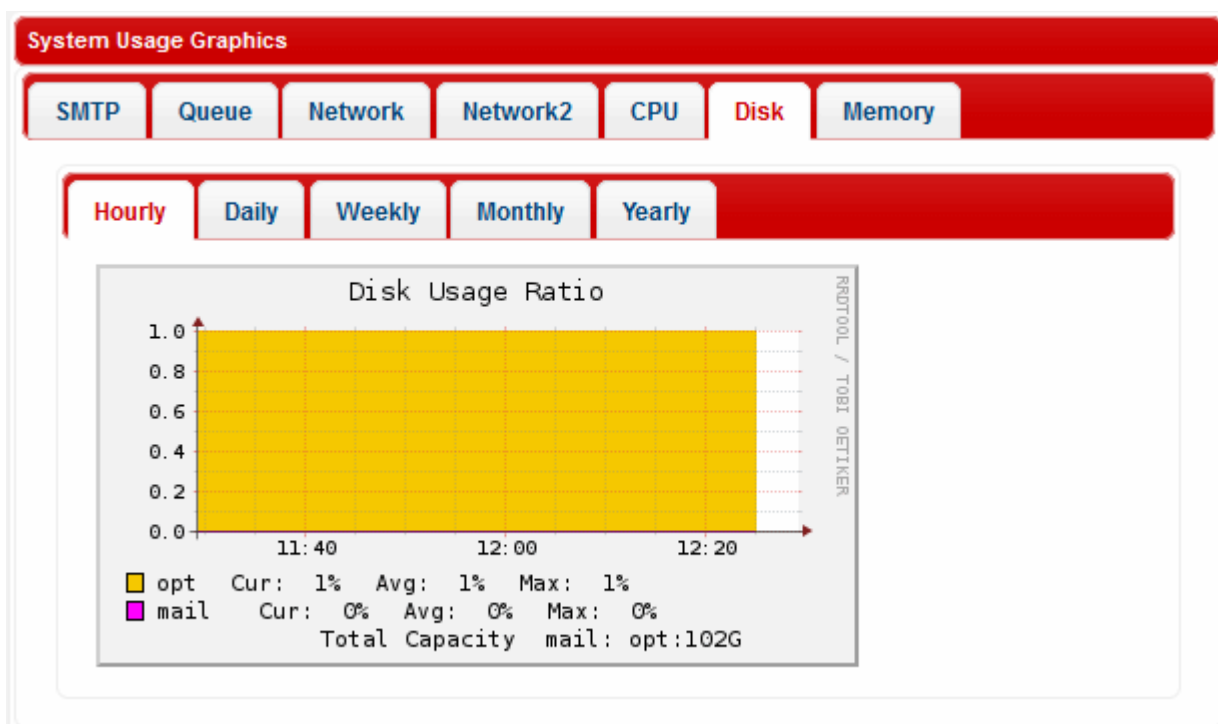
The processes that are responsible for CPU usage are indicated with different colors.

- 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.



- 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

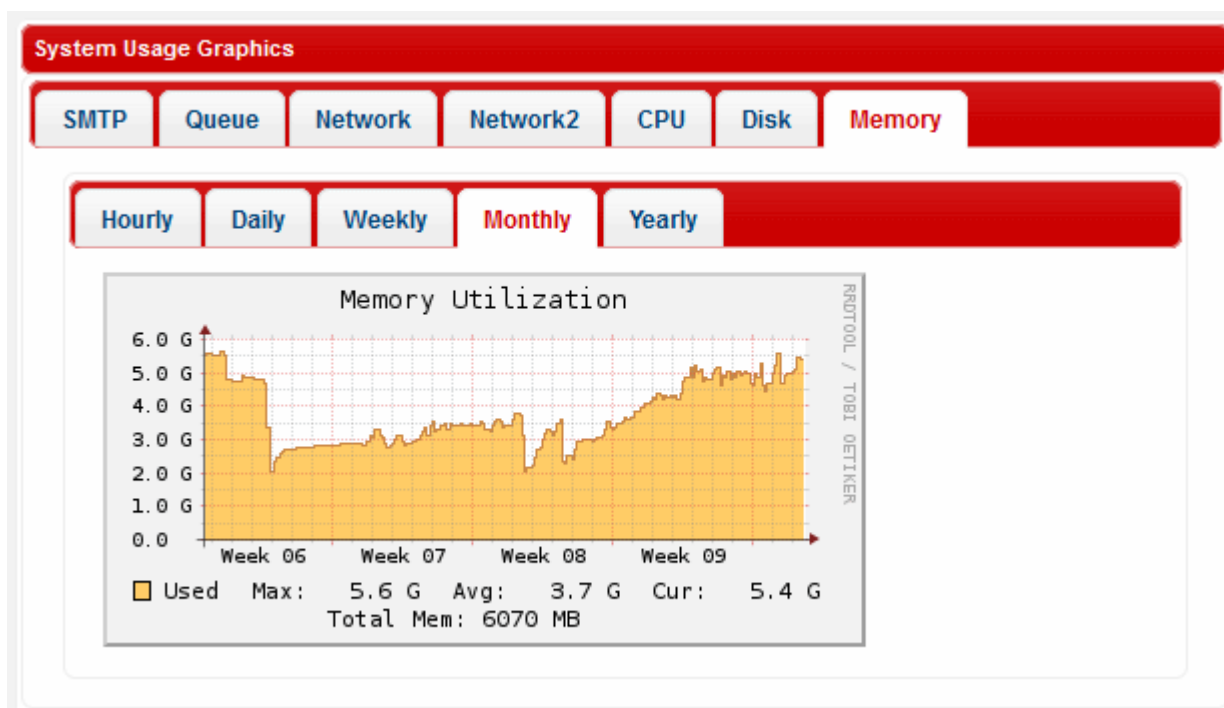
The disk usage by different types of data are indicated with different colors.

- 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.

The screenshot displays the Comodo KoruMail Admin interface. On the left, a sidebar menu lists various administrative sections: User Management, System, SMTP (highlighted), Domains, SMTP-AUTH, LDAP/DB, Greylist, RBL, Disclaimer, Relay, DKIM, Outgoing Limits, and Incoming Limits. Below these are Modules, Profile Management, Reports, and Quarantine & Archive. The main content area is titled 'SMTP' and features three tabs: General Settings, Advanced Settings, and Outbound Delivery Queue. The General Settings tab is active, showing a form with the following fields: 'SMTP server banner text' (set to 'Korunail Secure Email Gateway'), 'Maximum acceptable mail size' (20 MB), 'Activate DoS protection' (checked), 'Enable SMTP submission port' (checked), and 'Enable SPF' (set to '3 - Reject mail when SPF resolves to fail(deny)' with an option for 'Only for hosted domains'). A 'Save' button is located at the bottom of the form. At the very bottom of the page, a copyright notice states: 'Copyright© 2006-2016 Comodo Group, Inc. All rights reserved. KoruMail name and logo are trademarks of Comodo Group, Inc. Release: 6.4.3.04cf1ea'.

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](#)
- [SMTP 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' tab on the left menu and click 'SMTP'.

The screenshot shows the 'SMTP' configuration page in the Comodo KoruMail admin interface. The left sidebar contains a navigation menu with categories like 'User Management', 'System', 'SMTP', 'Domains', 'SMTP-AUTH', 'LDAP/DB', 'Greylist', 'REL', 'Disclaimer', 'Relay', 'DKIM', 'Outgoing Limits', 'Incoming Limits', 'Modules', 'Profile Management', 'Reports', and 'Quarantine & Archive'. The 'SMTP' section is expanded, showing sub-items like 'SMTP', 'Domains', 'SMTP-AUTH', 'LDAP/DB', 'Greylist', 'REL', 'Disclaimer', 'Relay', 'DKIM', 'Outgoing Limits', and 'Incoming Limits'. The main content area is titled 'SMTP' and has three tabs: 'General Settings' (selected), 'Advanced Settings', and 'Outbound Delivery Queue'. The 'General Settings' tab contains a table with the following fields:

SMTP server banner text	Korunmail Secure Email Gateway
Maximum acceptable mail size *	20 MB
Activate DoS protection *	<input checked="" type="checkbox"/>
Enable SMTP submission port *	<input checked="" type="checkbox"/>
Enable SPF Recommended value: 3	3 - Reject mail when SPF resolves to fail(deny) <input type="checkbox"/> Only for hosted domains

Below the table is a 'Save' button. At the bottom of the page, there is a copyright notice: 'Copyright© 2006-2016 Comodo Group, Inc. All rights reserved. KoruMail name and logo are trademarks of Comodo Group, Inc. Release: 6.4.3.04cf1ea'.

Click the following links for more details:

- [General Settings](#)
- [Advanced Settings](#)
- [Outbound Delivery Queue](#)

7.1.1 General Settings

The 'General Settings' allow administrators to configure settings such as the maximum size of mails that can be sent by clients and to enable DoS (Denial of Service) protection and SPF.

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

SMTP
Logout

General Settings
Advanced Settings
Outbound Delivery Queue

SMTP server banner text	KoruMail Labs - KoruMail SMTP Messagin
Maximum acceptable mail size *	50 MB
Activate DoS protection *	<input checked="" type="checkbox"/>
Enable SMTP submission port *	<input checked="" type="checkbox"/>
Enable SPF <small>Recommended value: 3</small>	3 - Reject mail when SPF resolves to fail(deny) <input type="checkbox"/> Only for hosted domains

Save

SMTP Settings – General Settings Table of Parameters	
Parameter	Description
SMTP server banner text	The welcome message displayed on the SMTP server when 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	If enabled, KoruMail activates DoS (Denial of Service) protection.
Enable SMTP submission port	If enabled, KoruMail doesn't accept outgoing messages from unauthenticated sources thus helping to protect your network and users from spam emails.
Enable SPF	<p>SPF (Sender Policy Framework) is a security standard to block the forgery of sender address.</p> <p>SPF values</p> <ol style="list-style-type: none"> Just add received-SPF header Return temporary failure in DNS query error If SPF result fails (ban) then reject it (recommended) If SPF result is softfail then reject it If SPF result is neutral then reject it If SPF result is not passed then reject it <p>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.</p>

- Click the 'Save' button 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'.

SMTP

Logout

General Settings

Advanced Settings

Outbound Delivery Queue

Minimum number of filter processors *	<input type="text" value="50"/>
Maximum number of filter processors *	<input type="text" value="150"/>
Maximum number of recipients per SMTP transaction *	<input type="text" value="0"/>
Incoming SMTP session timeout in seconds *	<input type="text" value="60"/>
RBL Timeout (second) *	<input type="text" value="2"/>
Early talker drop time (second)	<input type="text" value="0"/>
Reject invalid addresses	<input checked="" type="checkbox"/>
Queue life time (hour) *	<input type="text" value="24"/>
Enable tarpitting	<input type="checkbox"/>
Tarpit count	<input type="text" value="0"/>
Tarpit delay (second)	<input type="text" value="0"/>
Maximum number of SMTP sessions * Maximum: 500	<input type="text" value="500"/>
Maximum number of concurrent mail delivery *	<input type="text" value="500"/>
Main Filter engine log level	Info ▼

Save

SMTP Settings – Advanced Settings Table of Parameters	
Parameter	Description
Minimum number of filter processors	The minimum number of filter processes that the KoruMail filtering engine should use.
Maximum number of filter processors	The maximum number of filter processes that the KoruMail filtering engine should use.
Maximum number of recipients per SMTP transaction	Maximum number of recipients for each incoming SMTP request that comes to KoruMail.
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)	The SMTP server has a waiting time before sending a first greeting message after which the client replays with a HELO or a EHLO command. On receiving this (premature) message before the server sends greetings, then the client could be serving spam. The waiting time of SMTP server to send a greeting message is called Early talker drop time.
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. If a spammer sends an email to several recipients on your server during one SMTP session, enabling this feature will slow down the communication. 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 the 'Save' button 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'.

[Logout](#)



General Settings
Advanced Settings
Outbound Delivery Queue

SMTP



Queue 1

Concurrency Number	<input type="text" value="50"/>	Save
Domain	Action	
<input type="text"/>		
yahoo.com		
amazon.com		
Export Import Delete all		

Queue 2

Concurrency Number	<input type="text" value="100"/>	Save
Domain	Action	
<input type="text"/>		
aol.com		
Export Import Delete all		

Queue 3

Concurrency Number	<input type="text" value="150"/>	Save
Domain	Action	
<input type="text"/>		
att.net		
Export Import Delete all		

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.

SMTP

[General Settings](#)
[Advanced Settings](#)
[Outbound Delivery Queue](#)

Successfully Saved.

Queue 1

Concurrency Number	350	Save
Domain		Action
<input type="text"/>		
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 field and click the button under the 'Action' column.

SMTP

[General Settings](#)
[Advanced Settings](#)
[Outbound Delivery Queue](#)

Successfully Saved.

Queue 1

Concurrency Number	350	Save
Domain		Action
<input type="text" value="hotmail.com"/>		
yahoo.com		
amazon.com		

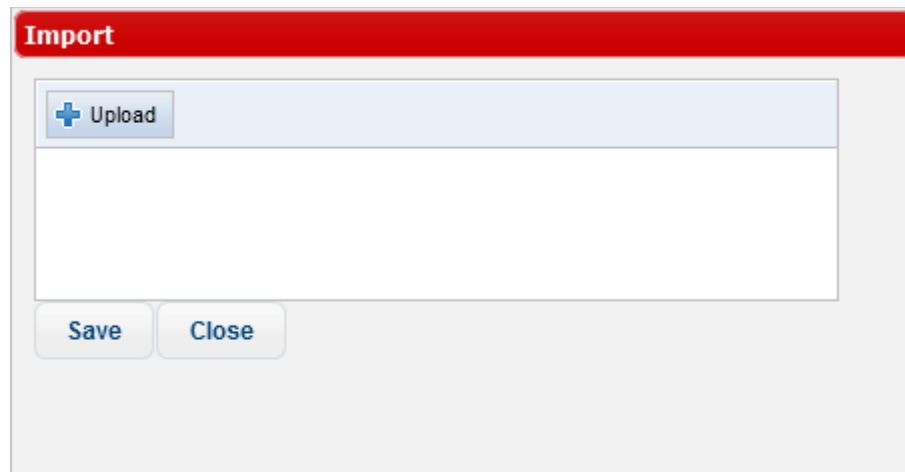
[Export](#) [Import](#) [Delete all](#)

Queue 2

<input type="text"/>		
----------------------	--	--

- 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 allow administrators to add domains and KoruMail applies all the rules and polices for emails belonging to the domains. The administrators in addition to edit the details of domains can also configure routes and SMTP servers, add 'Smart Hosts' for domains so as to route emails to an intermediate or relay server rather than delivering emails directly to the recipients' server.

- To open the 'Domains' screen, click the 'SMTP' tab on the left side and click 'Domains'.

Domains

Managed Domains | Routes | Smart Hosts

Filter: Filter! Clear Total: 45 domain(s)

Bulk Add

All None	Managed Domain Name	Generate Report	Owner	Action
<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>		
<input type="checkbox"/>	adtrustmedia.com	<input type="checkbox"/>	admin	
<input type="checkbox"/>	avilab.comodo.com	<input type="checkbox"/>	admin	
<input type="checkbox"/>	buyertrust.com	<input type="checkbox"/>	admin	
<input type="checkbox"/>	ccloud.com	<input type="checkbox"/>	admin	
<input type="checkbox"/>	chennai.comodo.com	<input type="checkbox"/>	admin	
<input type="checkbox"/>	chennai.comodo.local	<input checked="" type="checkbox"/>	snowman	
<input type="checkbox"/>	chennai.comodo.net	<input checked="" type="checkbox"/>	admin	
<input type="checkbox"/>	comodo.com	<input checked="" type="checkbox"/>	admin	
<input type="checkbox"/>	comodo.net	<input type="checkbox"/>	admin	
<input type="checkbox"/>	comodo.tv	<input type="checkbox"/>	admin	
<input type="checkbox"/>	comodoca.com	<input type="checkbox"/>	admin	
<input type="checkbox"/>	comodoca2.com	<input type="checkbox"/>	admin	
<input type="checkbox"/>	comodoca3.com	<input type="checkbox"/>	admin	
<input type="checkbox"/>	comodogroup.com	<input type="checkbox"/>	admin	
<input type="checkbox"/>	comodolabs.com	<input type="checkbox"/>	admin	
<input type="checkbox"/>	comodopcsupport.com	<input type="checkbox"/>	admin	
<input type="checkbox"/>	example.com	<input checked="" type="checkbox"/>	admin	
<input type="checkbox"/>	example.domain.com	<input checked="" type="checkbox"/>	admin	
<input type="checkbox"/>	geekbuddy.com	<input type="checkbox"/>	admin	
<input type="checkbox"/>	hackerguardian.com	<input type="checkbox"/>	admin	

Export Delete

Click the following the links for more details:

- [Managing domain names](#)
- [Managing domain routes](#)
- [Managing smart hosts](#)
- [Default domain routing](#)

7.2.1 Managing Domain Names

Administrators with appropriate privileges can add domain names that are to be managed and protected by KoruMail Messaging Gateway.

- To open the 'Managed Domains' screen, click the 'SMTP' tab on the left menu, click 'Domains' and then 'Managed Domains'.

Domains

Logout

Managed Domains

Routes

Smart Hosts

Filter:

Filter!

Clear

 Total: 45 domain(s)

+

 Bulk Add

All None	Managed Domain Name	Generate Report	Owner	Action
	<input type="text"/>	<input type="checkbox"/>		<div>+</div>
<input type="checkbox"/>	adtrustmedia.com	<input type="checkbox"/>	admin	<div>✓</div> <div>✕</div>
<input type="checkbox"/>	avlab.comodo.com	<input type="checkbox"/>	admin	<div>✓</div> <div>✕</div>
<input type="checkbox"/>	buyertrust.com	<input type="checkbox"/>	admin	<div>✓</div> <div>✕</div>
<input type="checkbox"/>	ccloud.com	<input type="checkbox"/>	admin	<div>✓</div> <div>✕</div>
<input type="checkbox"/>	chennai.comodo.com	<input type="checkbox"/>	admin	<div>✓</div> <div>✕</div>
<input type="checkbox"/>	chennai.comodo.local	<input checked="" type="checkbox"/>	snowman	<div>✓</div> <div>✕</div>
<input type="checkbox"/>	chennai.comodo.net	<input checked="" type="checkbox"/>	admin	<div>✓</div> <div>✕</div>
<input type="checkbox"/>	comodo.com	<input checked="" type="checkbox"/>	admin	<div>✓</div> <div>✕</div>
<input type="checkbox"/>	comodo.net	<input type="checkbox"/>	admin	<div>✓</div> <div>✕</div>
<input type="checkbox"/>	comodo.tv	<input type="checkbox"/>	admin	<div>✓</div> <div>✕</div>
<input type="checkbox"/>	comodoca.com	<input type="checkbox"/>	admin	<div>✓</div> <div>✕</div>
<input type="checkbox"/>	comodoca2.com	<input type="checkbox"/>	admin	<div>✓</div> <div>✕</div>
<input type="checkbox"/>	comodoca3.com	<input type="checkbox"/>	admin	<div>✓</div> <div>✕</div>
<input type="checkbox"/>	comodogroup.com	<input type="checkbox"/>	admin	<div>✓</div> <div>✕</div>
<input type="checkbox"/>	comodolabs.com	<input type="checkbox"/>	admin	<div>✓</div> <div>✕</div>
<input type="checkbox"/>	comodopcsupport.com	<input type="checkbox"/>	admin	<div>✓</div> <div>✕</div>
<input type="checkbox"/>	example.com	<input checked="" type="checkbox"/>	admin	<div>✓</div> <div>✕</div>
<input type="checkbox"/>	example.domain.com	<input checked="" type="checkbox"/>	admin	<div>✓</div> <div>✕</div>
<input type="checkbox"/>	geekbuddy.com	<input type="checkbox"/>	admin	<div>✓</div> <div>✕</div>
<input type="checkbox"/>	hackerguardian.com	<input type="checkbox"/>	admin	<div>✓</div> <div>✕</div>

1

2

»




»»

Export

Delete

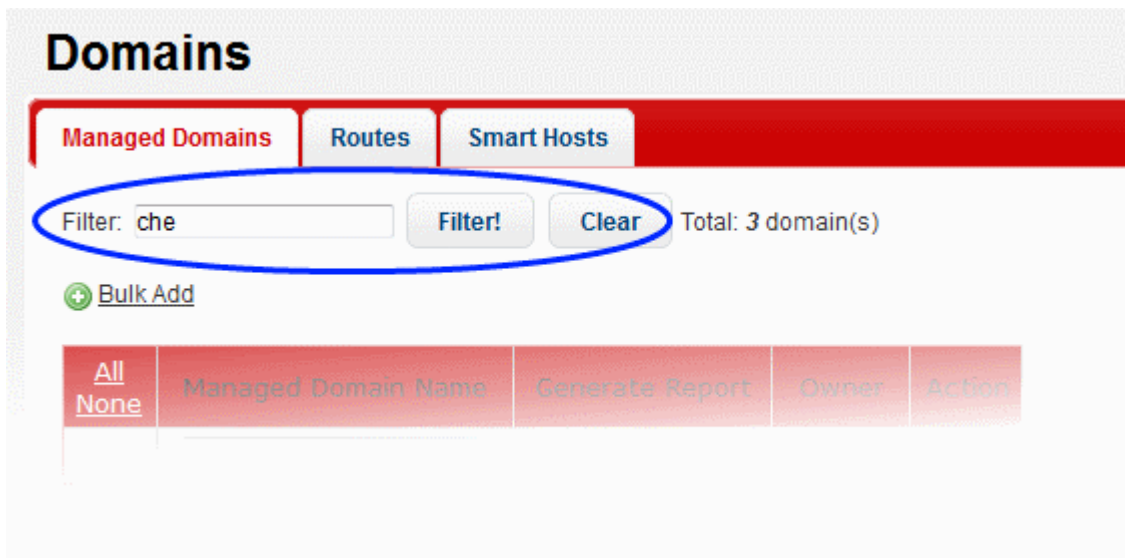
Managed Domains – Table of Column Descriptions

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

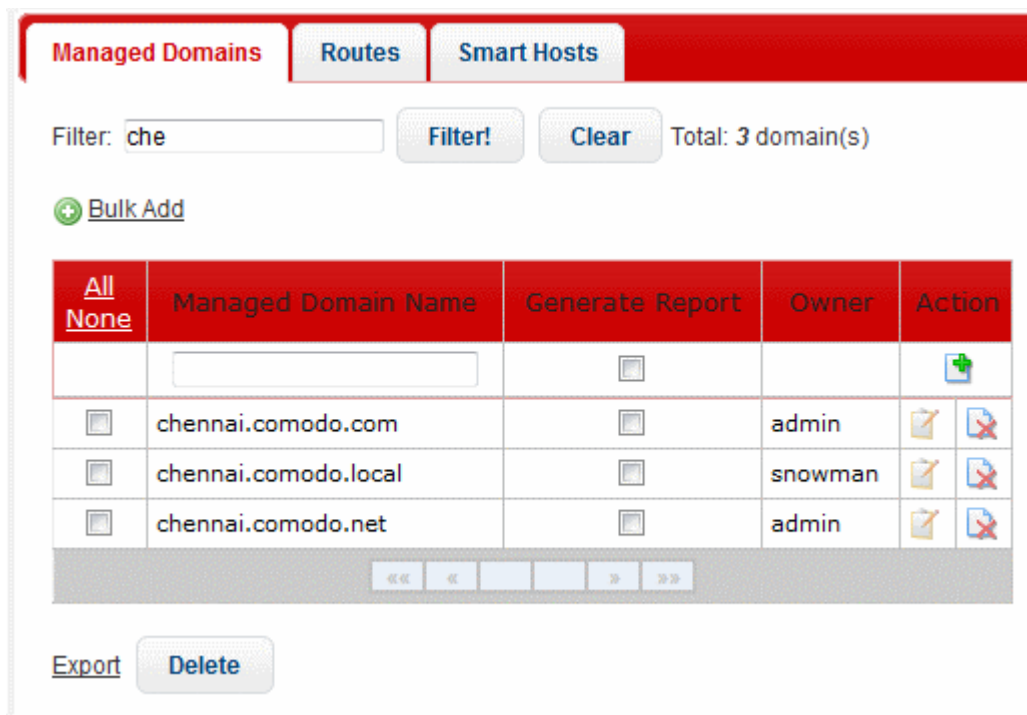
You can search for a particular domain(s) by using the filter.










The screenshot shows the 'Domains' management interface. At the top, there are tabs for 'Managed Domains', 'Routes', and 'Smart Hosts'. Below the tabs, there is a search filter section with a text input field containing 'che', a 'Filter!' button, and a 'Clear' button. To the right of the buttons, it says 'Total: 3 domain(s)'. Below the filter section, there is a '+ Bulk Add' link. At the bottom, there is a table with columns: 'All None', 'Managed Domain Name', 'Generate Report', 'Owner', and 'Action'.

- 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.



The screenshot shows the 'Domains' management interface after filtering. The 'Filter' field still contains 'che', and the 'Filter!' button is highlighted. The 'Total: 3 domain(s)' text is present. Below the filter section, there is a '+ Bulk Add' link. The table below shows the search results:

All None	Managed Domain Name	Generate Report	Owner	Action
<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>		
<input type="checkbox"/>	chennai.comodo.com	<input type="checkbox"/>	admin	 
<input type="checkbox"/>	chennai.comodo.local	<input type="checkbox"/>	snowman	 
<input type="checkbox"/>	chennai.comodo.net	<input type="checkbox"/>	admin	 

At the bottom of the table, there are navigation buttons: '<<', '<', '>', '>>'. Below the table, there are 'Export' and 'Delete' buttons.

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

The interface allow administrators 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	<input type="checkbox"/>		
<input type="checkbox"/>	adtrustmedia.com	<input type="checkbox"/>	admin	
<input type="checkbox"/>	avlab.comodo.com	<input type="checkbox"/>	admin	
<input type="checkbox"/>	buyertrust.com	<input type="checkbox"/>	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

Managed Domains
Routes
Smart Hosts

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

Filter: Total: 46 domain(s)

Bulk Add

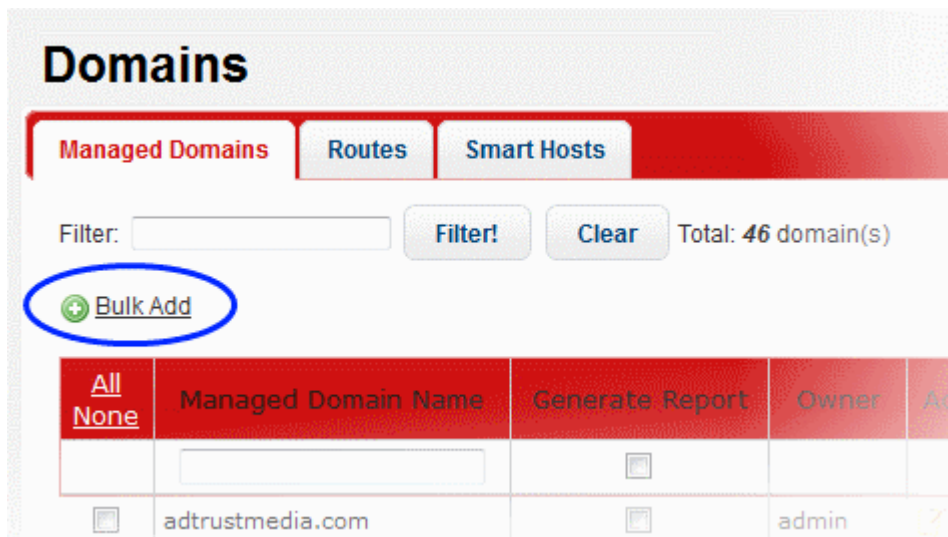
All None	Managed Domain Name	Generate Report	Owner	Action
	<input type="text"/>	<input type="checkbox"/>		
<input type="checkbox"/>	adtrustmedia.com	<input type="checkbox"/>	admin	
<input type="checkbox"/>	avlab.comodo.com	<input type="checkbox"/>	admin	
<input type="checkbox"/>	buvertrust.com	<input type="checkbox"/>	admin	

Refer to the section '**Managing Routes**' on how to add routes.

To add multiple domain names

The most significant feature of this menu is when you add the domain name you can route the domain name at the same time. For doing this lines must be written in Domain Name; Target IP Address; Port; LDAP name format. If target IP address is left blank no routing is done for this domain name. If port field left blank, port 25 is used as default.

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



The 'Bulk Add' screen will be displayed.

Add domains

Bulk Add

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

Add Cancel

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

Managed Domains
Routes
Smart Hosts

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.

Filter: **Filter!** **Clear** Total: **48** domain(s)

[Bulk Add](#)

All None	Managed Domain Name	Generate Report	Owner	Action
<input type="checkbox"/>	adtrustmedia.com	<input type="checkbox"/>	admin	<input type="checkbox"/>

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
Logout

Managed Domain Name	adtrustmedia.com
Owner	admin ▼
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- 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.

Managed Domains Routes Smart Hosts

Filter: [Filter!](#) [Clear](#) Total: 6 domain(s)

[Bulk Add](#)

All None	Managed Domain Name	Generate Report	Owner	Action
<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>		+
<input checked="" type="checkbox"/>	chennai.comodo.com	<input type="checkbox"/>	admin	✎ ✕
<input type="checkbox"/>	chennai.comodo.local	<input type="checkbox"/>	snowman	✎ ✕
<input checked="" type="checkbox"/>	chennai.comodo.net	<input type="checkbox"/>	admin	✎ ✕
<input type="checkbox"/>	chennai2.comodo.com	<input type="checkbox"/>	admin	✎ ✕
<input checked="" type="checkbox"/>	chennai3.comodo.com	<input type="checkbox"/>	admin	✎ ✕
<input type="checkbox"/>	mail1.chennai.comodo.local	<input type="checkbox"/>	admin	✎ ✕

Export [Delete](#)

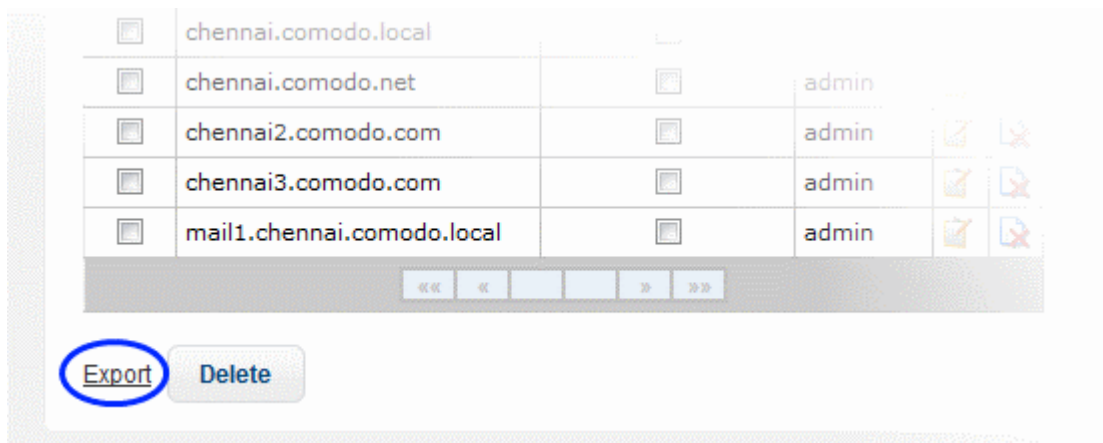
- Click 'OK' to confirm the deletion of the selected domains.

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

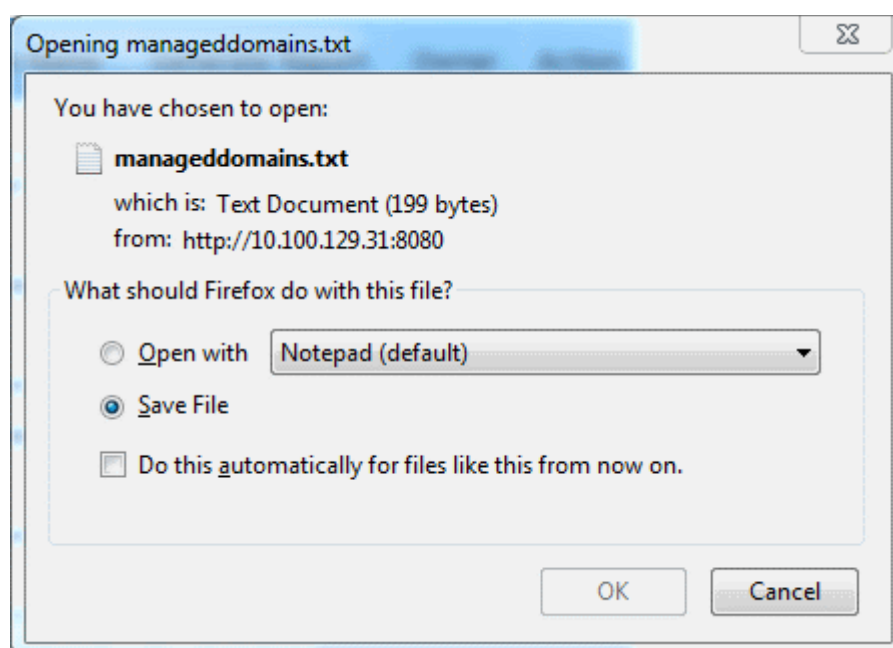
[OK](#)
[Cancel](#)

To export the domain names to a file

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



- Click 'OK' to download and save the domains list as a text file to your system.



7.2.2 Managing 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. Refer to the section '[Default Domain Routing](#)' for more details.

- To open the 'Routes' screen, click the 'SMTP' tab on the left menu, click 'Domains' and then 'Routes'.





[Logout](#)

Domains

[Managed Domains](#) | [Routes](#) | [Smart Hosts](#)

All None	Managed Domain Name	Routing Type	SMTP Server	Port Number	User Verification	LDAP/DB Profile	Action
	-Choose-	IPv4		25	None	None	
<input type="checkbox"/>	chennai.comodo.com	IPv4	mail1.chennai.comodo.com	25	LDAP	Default AD	
<input type="checkbox"/>	chennai.comodo.local	IPv4	10.100.129.55	25	None	-None-	
<input type="checkbox"/>	chennai.comodo.net	IPv4	192.168.199.31	25	MySQL	KoruMail	
<input type="checkbox"/>	example.com	IPv4	10.0.0.1	25	LocalUserDB	LocalUserDB	
<input type="checkbox"/>	ve.comodo.local	IPv4	10.100.129.54	25	None	-None-	

[Export](#) [Delete](#)

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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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

Managed Domains Routes Smart Hosts

All None	Managed Domain Name	Routing Type	SMTP Server	Port
<input type="checkbox"/>	-Choose-	IPv4		25
<input type="checkbox"/>	-Choose-	IPv4	mail1.chennai.comodo.com	25
<input type="checkbox"/>	adtrustmedia.com	IPv4	10.100.129.55	25
<input type="checkbox"/>	avlab.comodo.com	IPv4	192.168.199.31	25
<input type="checkbox"/>	buyertrust.com	IPv4	10.0.0.1	25
<input type="checkbox"/>	ccloud.com	IPv4	10.100.129.54	25
<input type="checkbox"/>	chennai2.comodo.com			
<input type="checkbox"/>	chennai3.comodo.com			
<input type="checkbox"/>	comodo.com			
<input type="checkbox"/>	comodo.net			
<input type="checkbox"/>	comodo.tv			
<input type="checkbox"/>	comodoca.com			
<input type="checkbox"/>	comodoca2.com			
<input type="checkbox"/>	comodoca3.com			
<input type="checkbox"/>	comodogroup.com			
<input type="checkbox"/>	comodolabs.com			
<input type="checkbox"/>	comodopcsupport.com			
<input type="checkbox"/>	comodoromania.com			
<input type="checkbox"/>	comodounite.com			
<input type="checkbox"/>	enterprisessl.com			
<input type="checkbox"/>	evbeacon.com			







Export



Copyright © 2006-2014 Comodo Group, Inc. All rights reserved.
Mail name and logo are trademarks of Comodo Group, Inc.
Release: 5.2.0.3055

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

Domains			
Managed Domains Routes Smart Hosts			
All None	Managed Domain Name	Routing Type	SMTP Server
	chennai2.comodo.com	IPv4	
<input type="checkbox"/>	chennai.comodo.com	IPv4	mail1.chennai.comodo.c
<input type="checkbox"/>	chennai.comodo.local	IPv6 HOSTNAME	10.100.129.55
<input type="checkbox"/>	chennai.comodo.net	MX RECORD	192.168.199.31
<input type="checkbox"/>	example.com	LDAP	10.0.0.1
<input type="checkbox"/>	vs.comodo.local	IPv4	10.100.129.55


- 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.

Verification	LDAP/DB Profile	Action
	Default AD	 
	Default AD	
	Default OpenLDAP	
	Default OpenLDAP AUTH	
	Default AD AUTH	
	Comodo Open LDAP	
	LocalUserDB	 
	-None-	 

- 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.


[Logout](#)

Edit domain route

Domain	chennai.comodo.com
Routing Type	IPv4
SMTP Server	mail1.chennai.comodo.com
Port Number	25
User Verification	LDAP
LDAP/DB Profile	Default AD
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- 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 domain routes

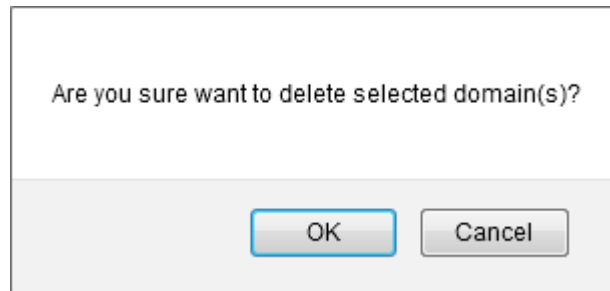
- To delete domain routes one at a time, click the  button under the 'Action' column header and confirm the deletion in the 'Confirmation' dialog.
- To delete multiple domain routes, select the check boxes beside them and click the 'Delete' button at the bottom.

Domains

[Managed Domains](#) | [Routes](#) | [Smart Hosts](#)

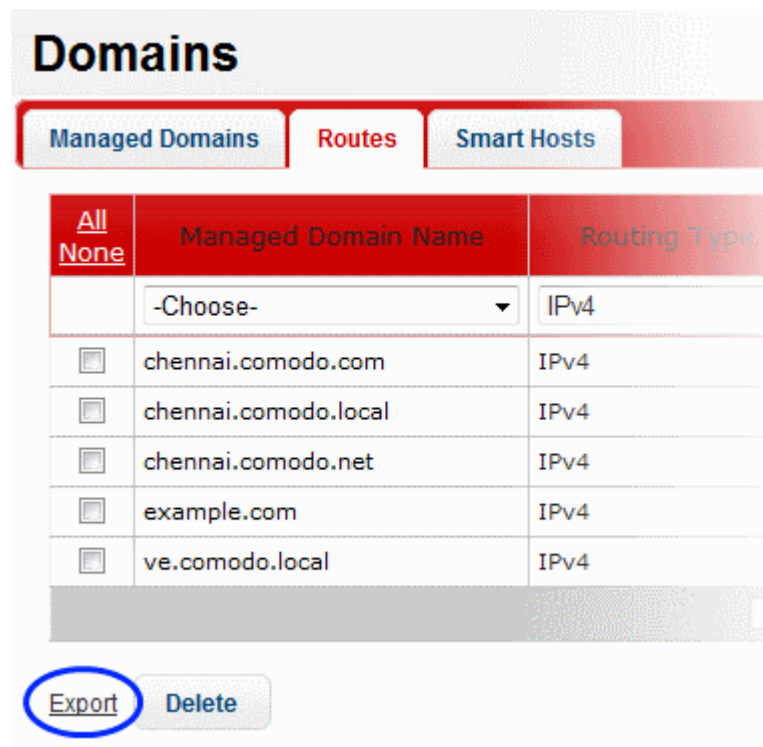
All None	Managed Domain Name	Routing Type	SMTP Server	Port Number	User
	-Choose-	IPv4		25	None
<input checked="" type="checkbox"/>	chennai.comodo.com	IPv4	mail1.chennai.comodo.com	25	LDAP
<input type="checkbox"/>	chennai.comodo.local	IPv4	10.100.129.55	25	None
<input checked="" type="checkbox"/>	chennai.comodo.net	IPv4	192.168.199.31	25	MySQL
<input checked="" type="checkbox"/>	example.com	IPv4	10.0.0.1	25	LocalUser
<input type="checkbox"/>	ve.comodo.local	IPv4	10.100.129.54	25	None

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

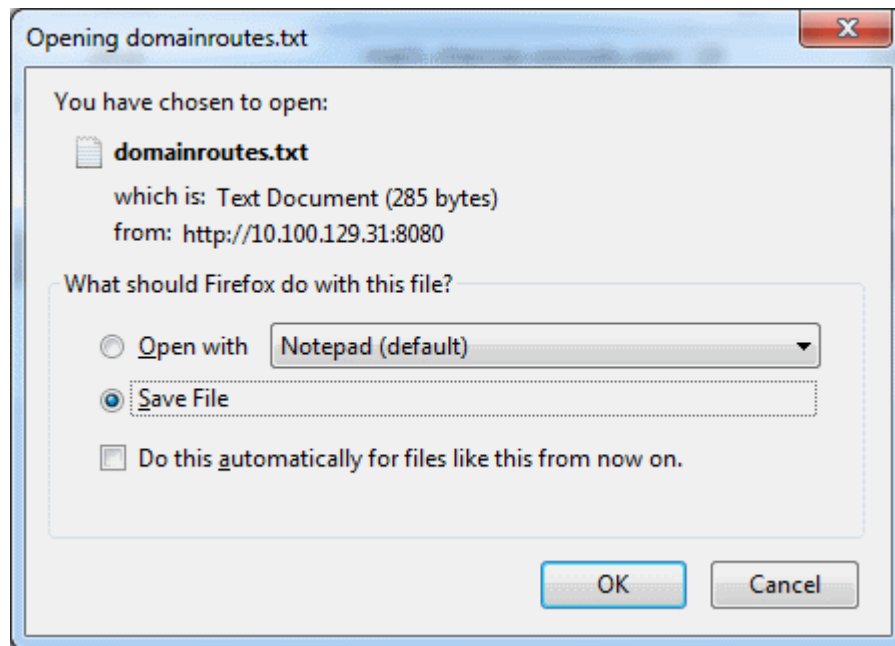


To export the domain routes to a file

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



- Click 'OK' to download and save the domain routes list as a text file to your system.



7.2.3 Managing Smart Hosts

Smart Hosts serve as an intermediate mail server that receive mail from an SMTP server and, after applying their own policy, forward them to end user mail boxes. KoruMail has the ability to route emails to 'Smart Hosts'. Please note that a domain added under 'Managed Domains' cannot be added for 'Smart Host' routing.

The interface also allows administrators to configure default domain routing. This applies to 'Managed Domains' whose routing has not been configured. Refer to the **Default Domain Routing** section for more details.

- To open the 'Smart Hosts' screen, click the 'SMTP' tab from the left menu and click 'Domains' > 'Smart Hosts'.

[Logout](#)

Domains

[Managed Domains](#) | [Routes](#) | [Smart Hosts](#)

Total: 3 domain(s)

[+ Bulk Add](#)

All None	Domain Name	Host Name or IP Address	Port	Action
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="25"/>	
<input type="checkbox"/>	comodo.chennai.com	mail1.comodo.chennai.com	25	
<input type="checkbox"/>	techwriting.comodo.com	mail1.comodo.chennai.com	25	
<input type="checkbox"/>	webdevs.comodo.chennai.com	mail1.comodo.chennai.com	25	

[Export](#) | [Delete](#)

Enable Default Domain Routing
☐

[Save](#)

Smart Hosts – Table of Column Descriptions

Column Header	Description	
Domain Name	The name of the domain added to KoruMail	
Host Name or IP Address	Host Name or IP address of the 'Smart Host'	
Port	The port number to which the KoruMail should forward the mail	
Action		To route the domain to a 'Smart Host', click this button after entering all the routing details.
		Allows the administrators to delete a domain 'Smart Host' route from the list.

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 the  button under the 'Action' column header.

To delete 'Smart Host' route for domains

- To delete 'Smart Host' routes one at a time, click the  button 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 the 'Delete' button at the bottom.



Domains

Managed Domains Routes Smart Hosts

Total: 3 domain(s)

 [Bulk Add](#)

All None	Domain Name	Host Name or IP
<input checked="" type="checkbox"/>	comodo.chennai.com	mail1.comodo.che
<input checked="" type="checkbox"/>	techwriting.comodo.com	mail1.comodo.che
<input type="checkbox"/>	webdevs.comodo.chennai.com	mail1.comodo.che

[Export](#) **Delete**

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

Managed Domains | Routes | Smart Hosts

Total: 3 domain(s)

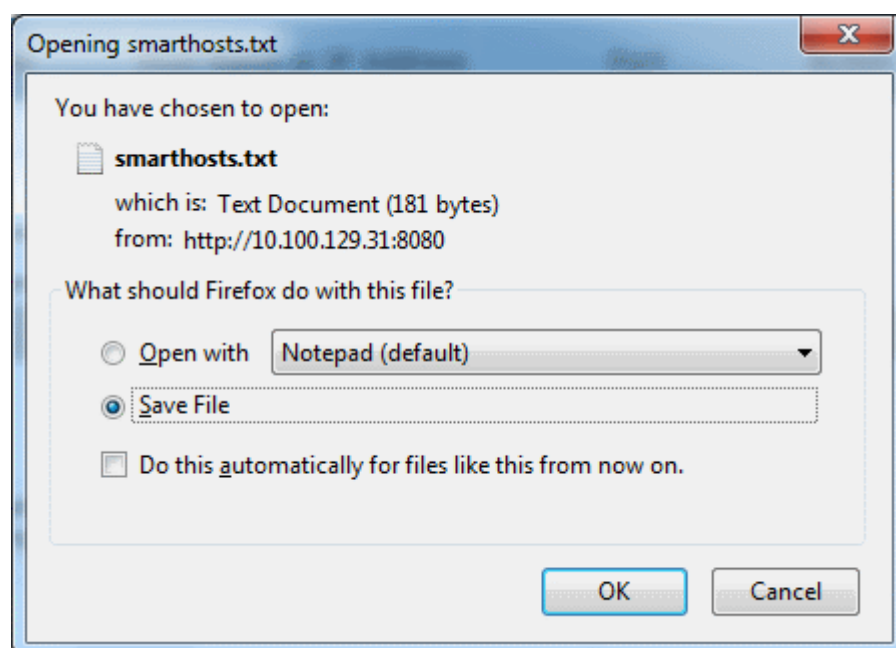
[Bulk Add](#)

All None	Domain Name	Host Name or IP Address	Port
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	25
<input type="checkbox"/>	comodo.chennai.com	mail1.comodo.chennai.com	25
<input type="checkbox"/>	techwriting.comodo.com	mail1.comodo.chennai.com	25
<input type="checkbox"/>	webdevs.comodo.chennai.com	mail1.comodo.chennai.com	25

[Export](#) [Delete](#)

Enable Default Domain

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



7.2.4 Default Domain Routing

KoruMail allows administrators to configure routing for '**Managed Domains**' that are protected by its filtering engine. Refer to the section '**Managing Domain Routes**' to find out how to configure routing for managed domains. If no routing is configured, then the default domain routing will apply for these domains. The default settings can be configured in the 'Smart Hosts' section.

- To open the 'Smart Hosts' screen, click the 'SMTP' tab on the left and click 'Domains' then 'Smart Hosts'.

Domains Logout

Managed Domains **Routes** **Smart Hosts**

Total: 3 domain(s)

[Bulk Add](#)

All None	Domain Name	Host Name or IP Address	Port	Action
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	25	
<input type="checkbox"/>	comodo.chennai.com	mail1.comodo.chennai.com	25	
<input type="checkbox"/>	techwriting.comodo.com	mail1.comodo.chennai.com	25	
<input type="checkbox"/>	webdevs.comodo.chennai.com	mail1.comodo.chennai.com	25	

[Export](#) [Delete](#)

Enable Default Domain Routing ☐

[Save](#)

- Select the 'Enable Default Domain Routing' check box

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

☐ webdevs.comodo.chennai.com mail1.comodo.chennai.com 25

[Export](#) [Delete](#)

Enable Default Domain Routing ☒

SMTP Server

SMTP Port 25

LDAP Profile -None- ▼

[Save](#)

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

7.3 KoruMail SMTP AUTH Connector

The 'SMTP-AUTH' section allows administrators to configure authentication settings for outgoing mails, block users and configure 'Anomaly Detection' (track the number of different IP addresses that are used for sending out mails for an email address).

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

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.


[Logout](#)



SMTP-AUTH

SMTP Authentication Settings
Block Users
Anomaly Detection

Enable SMTP Authentication	<input checked="" type="checkbox"/>
Only allow SMTP AUTH with TLS	<input type="checkbox"/>
Fake Sender Control	<input type="checkbox"/>
Authentication method	LDAP / AD ▾
Connection Timeout	<input type="text" value="5"/>
LDAP Profile	Default OpenLDAP AUTH ▾
<input type="button" value="Save"/>	

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.	
POP3/IMAP Authentication Method		
SMTP-AUTH server list	Authenticati on method	Select authentication method - either POP3 or IMAP.
	Connectio n 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.		

To 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.

Only allow SMTP AUTH with TLS ☐


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		
POP3	SSL	192.168.199.31	25	Yes	 
IMAP	TLS	192.168.199.30	25	Yes	 

Save

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

Authentication method	IMAP ▼
Connection type	TLS ▼
Hostname *	192.168.199.30
Port *	25
<input type="button" value="Save"/>	

- 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.

Block Users		Anomaly Detection
Enable SMTP Authentication	<input checked="" type="checkbox"/>	
Only allow SMTP AUTH with TLS	<input type="checkbox"/>	
Authentication method	LDAP / AD ▼	
Connection Timeout	5	
LDAP Profile	Default OpenLDAP AUTH ▼ Default AD Default OpenLDAP Default OpenLDAP AUTH Default AD AUTH Comodo Open LDAP	

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'.

The screenshot shows the 'SMTP-AUTH' admin interface. At the top right is a 'Logout' button. Below the title are three tabs: 'SMTP Authentication Settings' (active), 'Block Users', and 'Anomaly Detection'. A 'Search' link is on the left. The main area has a 'Blocking Lifetime' dropdown set to 'Unlimited' and a 'Save' button. Below this is a table with columns 'Date', 'Username', and 'Action'. The 'Username' column has a 'Starts With' dropdown and an input field. The table lists four blocked users with their dates and actions (a red 'X' icon). At the bottom are 'Export', 'Import', and 'Delete all' buttons.

Date	Username	Action
	Starts With <input type="text"/>	
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	






The interface allow administrators to:


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

To 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
	Starts With <input type="text"/>	
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	

- 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






Logout

SMTP Authentication Settings
Block Users
Anomaly Detection

[Search](#)

Blocking Lifetime Unlimited

Save

Date	Username	Action
	Starts With <input type="text"/>	
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	

[Export](#)
[Import](#)
Delete all

Blocking 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

SMTP Authentication Settings | **Block Users** | Anomaly Detection

[Search](#)

Blocking Lifetime: Unlimited ▾

- Unlimited
- 1 hour
- 6 hours
- 12 hours
- 24 hours

Date	Name	Action

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

SMTP-AUTH

[SMTP Authentication Settings](#)
[Block Users](#)
[Anomaly Detection](#)

Search

Blocking Lifetime

Date	Username	Action
	Starts With <input type="text"/>	
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.

SMTP-AUTH

[SMTP Authentication Settings](#)
[Block Users](#)
[Anomaly Detection](#)

Search

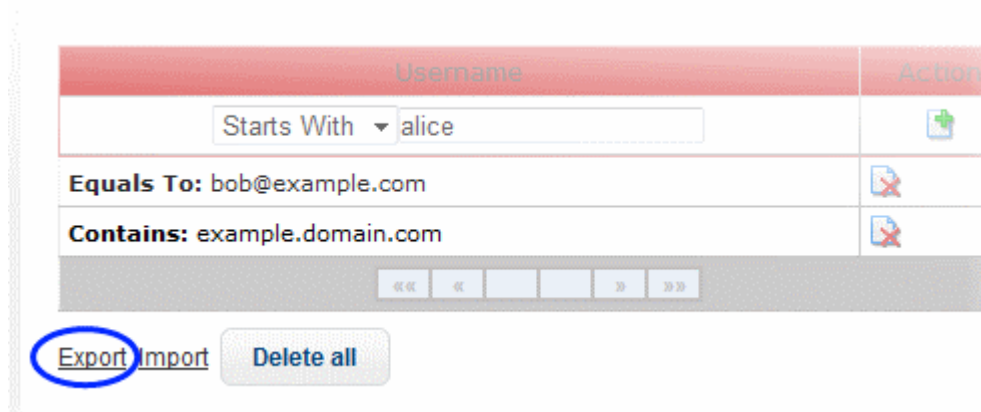
Blocking Lifetime

Date	Username	Action
	Starts With <input type="text"/>	
08.11.2016 02:29:12	Equals To: bob@example.com	
08.11.2016 02:29:34	Contains: example.domain.com	

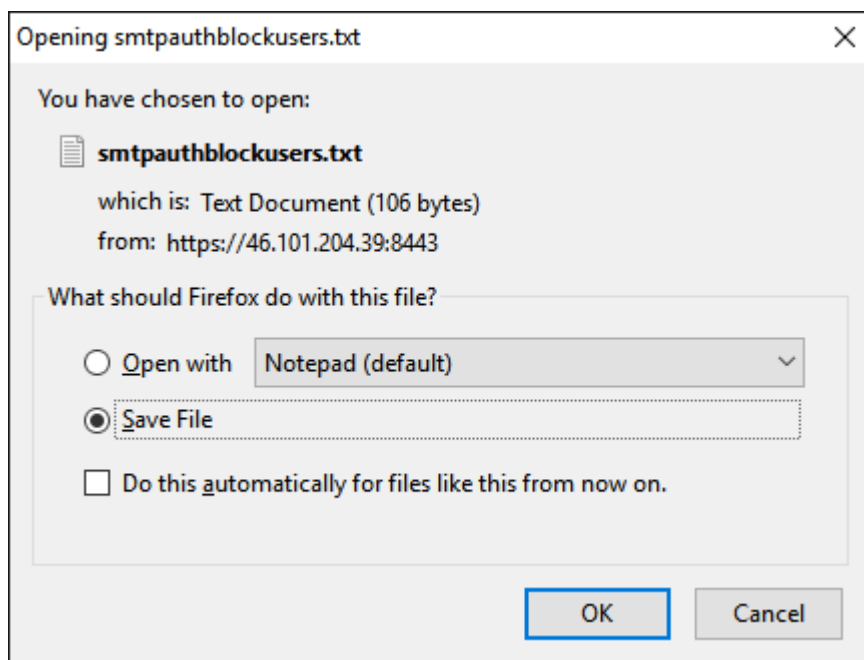
- To display all the items again, click the 'Clear' button.
- To remove the search field, click the 'Search' link again.

To export blocked users to file

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

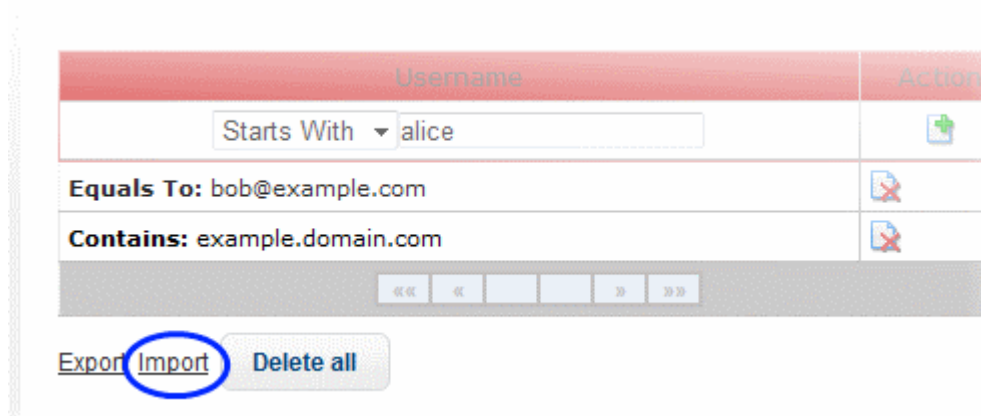


- Click 'OK' to download and save the blocked user list as a text file to your system.

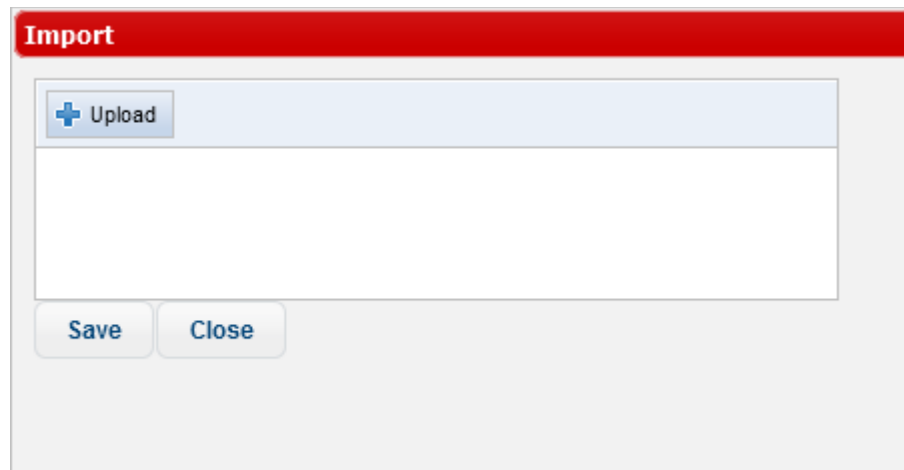


To import blocked users from file

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



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'.



- 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 admins to receive alerts when KoruMail detects a user/email address has sent messages from multiple IP addresses within a set time interval. Administrators 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 the 'SMTP' menu item on the left menu, then 'SMTP-AUTH' and then open the 'Anomaly Detection' tab.

SMTP-AUTH

SMTP Authentication Settings
Block Users
Anomaly Detection

Successfully Saved.

Enable Anomaly Detection	<input checked="" type="checkbox"/>
Enable Monitoring Mode	<input checked="" type="checkbox"/>
Interval(min)	<input type="text" value="30"/>
Number of failed SMTP-AUTH requests from a same IP to block that IP	<input type="text" value="5"/>
Number of users from the same IP that makes failed SMTP-AUTH requests	<input type="text" value="5"/>
Number of different IP addresses that makes successful SMTP-AUTH requests with same username	<input type="text" value="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-AUTH requests from a same IP to block that IP	Number of failed SMTP-AUTH requests from a particular IP before it is rejected.
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	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

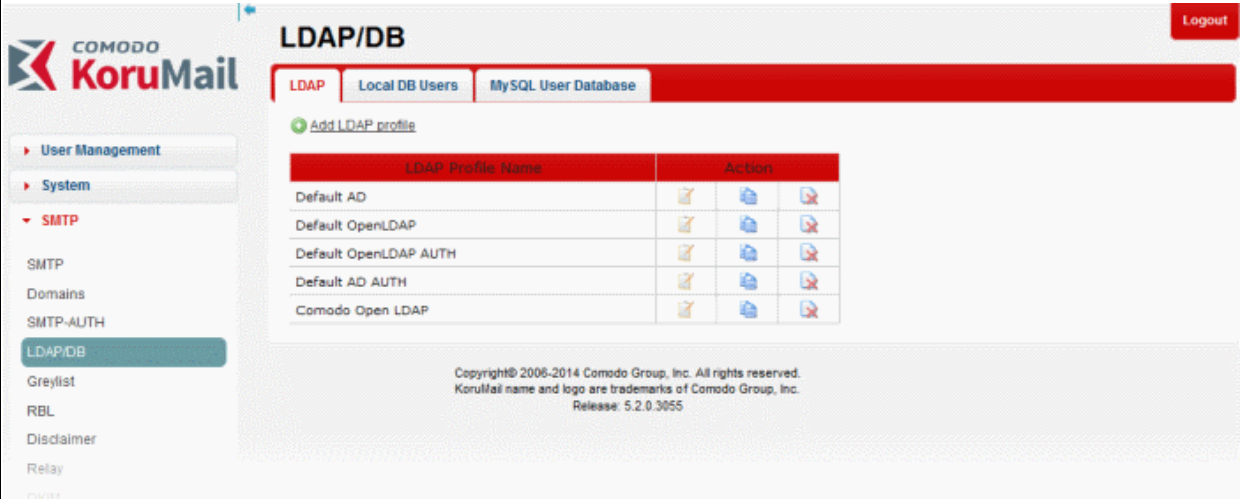
username

- 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 begins 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 and if not valid, reject the emails at SMTP level.

- To open the 'LDAP/DB' screen, click the 'SMTP' tab on the left menu and click 'LDAP/DB'.



The screenshot shows the 'LDAP/DB' configuration page in the KoruMail admin interface. The left sidebar has 'SMTP' selected, with 'LDAP/DB' as a sub-option. The main content area has tabs for 'LDAP', 'Local DB Users', and 'MySQL User Database'. Under the 'LDAP' tab, there is an 'Add LDAP profile' link and a table of existing profiles.

LDAP Profile Name	Action
Default AD	[Edit] [Add] [Delete]
Default OpenLDAP	[Edit] [Add] [Delete]
Default OpenLDAP AUTH	[Edit] [Add] [Delete]
Default AD AUTH	[Edit] [Add] [Delete]
Comodo Open LDAP	[Edit] [Add] [Delete]

Copyright© 2006-2014 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 5.2.0.3055

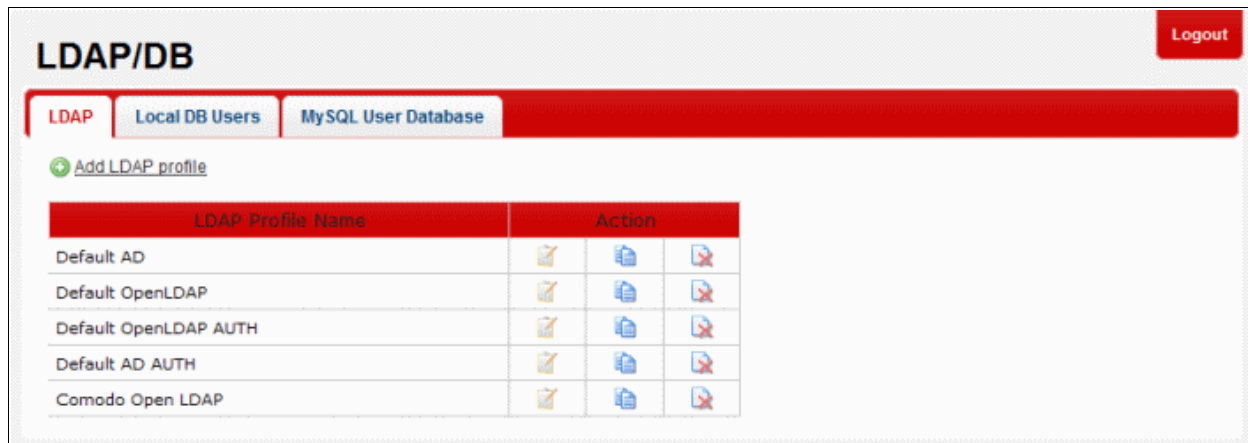
Refer to the following sections for more details:




- [LDAP \(Lightweight Directory Access Protocol\)](#)
- [Local DB Users](#)
- [MySQL User Database](#)

7.4.1 LDAP Profile

The Lightweight Directory Access Protocol, or LDAP, is an application protocol for querying and modifying 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 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 – 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

[Logout](#)

New LDAP Profile

Profile Name *	<input type="text"/>
Connection type	Plain ▾
Host Name or IP Address *	<input type="text"/>
Port *	389
Host Name or IP Address (Secondary)	<input type="text"/>
Port (Secondary)	0
Search Type	Realtime ▾
Cache Time (minutes) *	<input type="text" value="0"/>
Anonymous Access	<input type="checkbox"/>
Login DN *	<input type="text"/>
Password *	<input type="password"/>
Enable catch-all for this profile	<input type="checkbox"/>
Search Base *	<input type="text"/>
Search Pattern *	<div style="font-size: 0.8em;"> %u = "user" for "user@domain.com" %d = "domain.com" for "user@domain.com" %m = Whole e-mail address </div> <input type="text" value="(mail=%m)"/>
Test E-mail Address	<input type="text"/>
Email host attribute name	<input type="text"/>
Check Local DB Users Also	<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Verify"/> <input type="button" value="Cancel"/>	

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: <ul style="list-style-type: none"> • 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.

Logout

Edit LDAP profile

Profile Name *	Comodo Open LDAP
Connection type	Plain ▼
Host Name or IP Address *	192.168.199.31
Port *	389
Host Name or IP Address (Secondary)	
Port (Secondary)	0
Search Type	Realtime ▼
Cache Time (minutes) *	0
Anonymous Access	<input type="checkbox"/>
Login DN *	comodo
Password *	*****
Enable catch-all for this profile	<input type="checkbox"/>
Search Base *	ou=Support,dc=comodo
Search Pattern *	%u = "user" for "user@domain.com" %d = "domain.com" for "user@domain.com" %m = Whole e-mail address (mail=%m)
Test E-mail Address	
Email host attribute name	
Check Local DB Users Also	<input type="checkbox"/>

- 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 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 administrators to add users locally in its database for the managed domains so that fake emails or mails to invalid recipients will be rejected before the filtering processes is initiated. This helps to conserve the system's resources for better utilization. The users added here are available for selection in interfaces such as '**Managed Domains > Routes**'.

- To open the 'Local DB Users' screen, click the 'SMTP' tab on the left and click 'LDAP/DB' then 'Local DB Users'.

Logout

LDAP
Local DB Users
MySQL User Database

➕ Bulk Add

Actions ▾

Page 1
/ 2
10 ▾ Records per page

All None	E-mail	Action
	<input style="width: 100%;" type="text"/>	
<input type="checkbox"/>	bob@example.com	
<input type="checkbox"/>	smith@chennai.comodo.local	
<input type="checkbox"/>	user12@example.com	
<input type="checkbox"/>	user13@example.com	
<input type="checkbox"/>	user14@example.com	
<input type="checkbox"/>	user15@example.com	
<input type="checkbox"/>	user16@example.com	
<input type="checkbox"/>	user1@example.com	
<input type="checkbox"/>	user2@example.com	
<input type="checkbox"/>	user3@example.com	

Actions ▾

Page 1
/ 2
10 ▾ Records per page

Local DB Users – Table of Column Descriptions		
Column Header	Description	
Email	The name of the user added to KoruMail	
Actions		To add a user, click this button after entering the details in the field under 'E-mail' column.
		Allows the administrators to delete a user from the list.

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

Previous
Page 1
/ 2
10 ▾ Records per page
Next

E-mail	Ac
<input style="width: 100%;" type="text"/>	

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

The screenshot shows the 'Local DB Users' tab. At the top, there are tabs for 'LDAP', 'Local DB Users', and 'MySQL User Database'. Below these are search and clear buttons. A 'Bulk Add' link with a green plus icon is visible. A table with columns 'All None', 'E-mail', and 'Action' is shown. The first row has 'user21@example.com' in the 'E-mail' column, circled in blue, and a green plus icon in the 'Action' column. Other rows show 'bob@example.com' and 'smith@chennai.comodo.local'.

- Click the  button under the 'Action' column.

Note: You can add users for managed domains only.

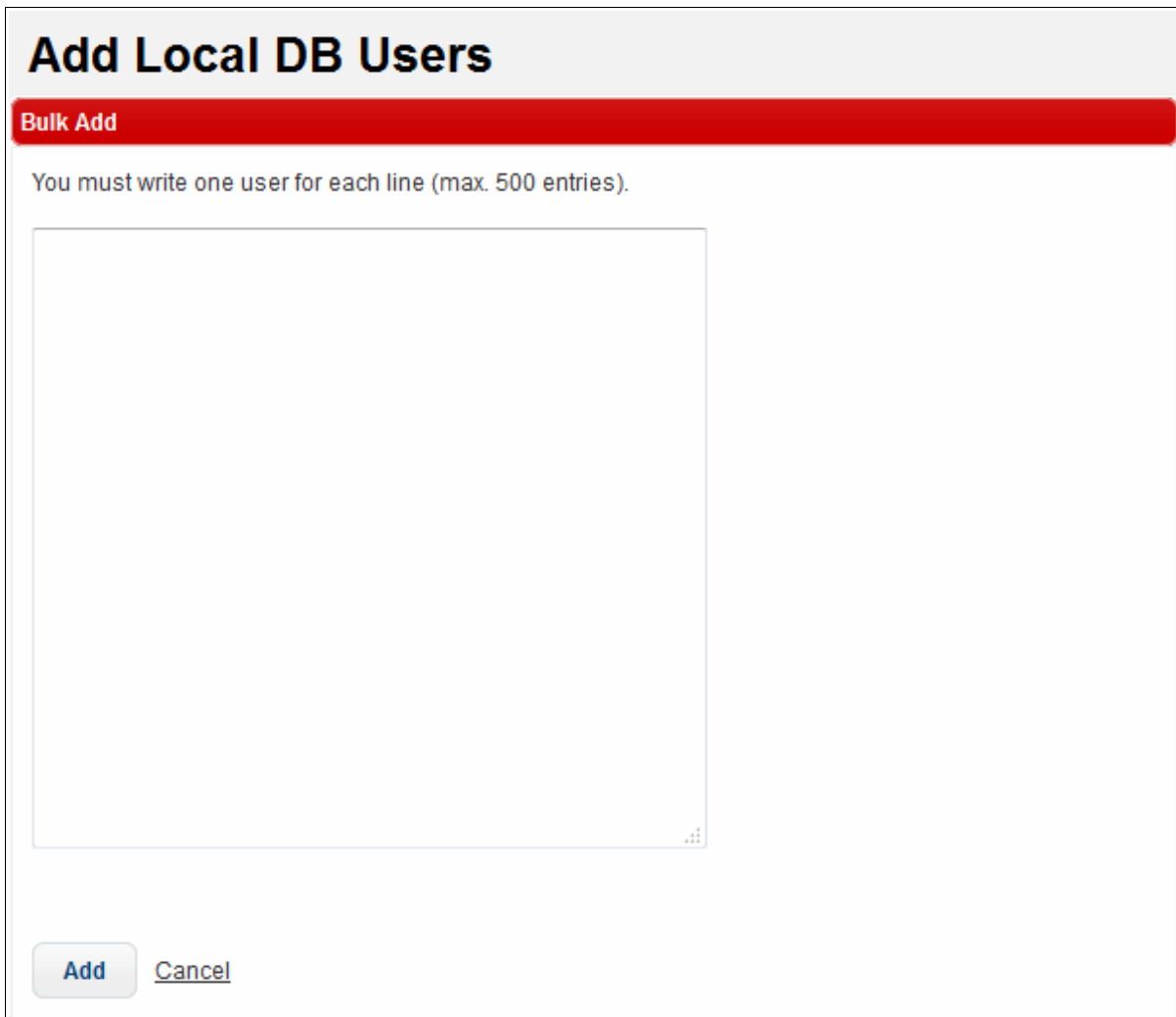
The user will be added and displayed in the list. You can also add multiple users at a time. Refer to the next section '[To add multiple users](#)' for more details.

To add multiple users

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

The screenshot shows the 'LDAP/DB' section. At the top, there are tabs for 'LDAP', 'Local DB Users', and 'MySQL User Database'. Below these are search and clear buttons. A 'Bulk Add' link with a green plus icon is visible and circled in blue. A table with columns 'All None', 'E-mail', and 'Action' is shown. The first row has 'user21@example.com' in the 'E-mail' column.

The 'Bulk Add' screen will be displayed.



Add Local DB Users

Bulk Add

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

[Add](#) [Cancel](#)

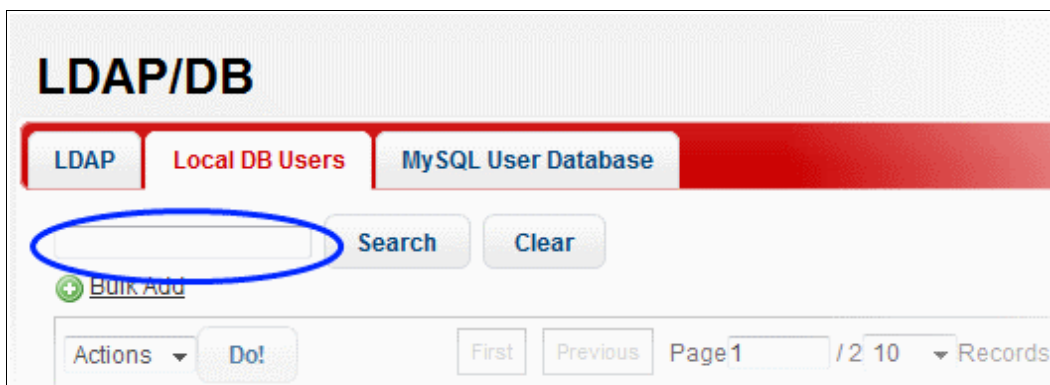
- Enter the users' email addresses each per line. The maximum allowed at a time is 500 users.
- Click the 'Add' button.

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

[LDAP](#) [Local DB Users](#) [MySQL User Database](#)

[Search](#) [Clear](#)

[+ Bulk Add](#)

[Actions](#) [Do!](#) [First](#) [Previous](#) Page 1 / 2 10 [Records](#)

- Click the 'Search' button.

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

LDAP/DB Logout

LDAP **Local DB Users** **MySQL User Database**

user

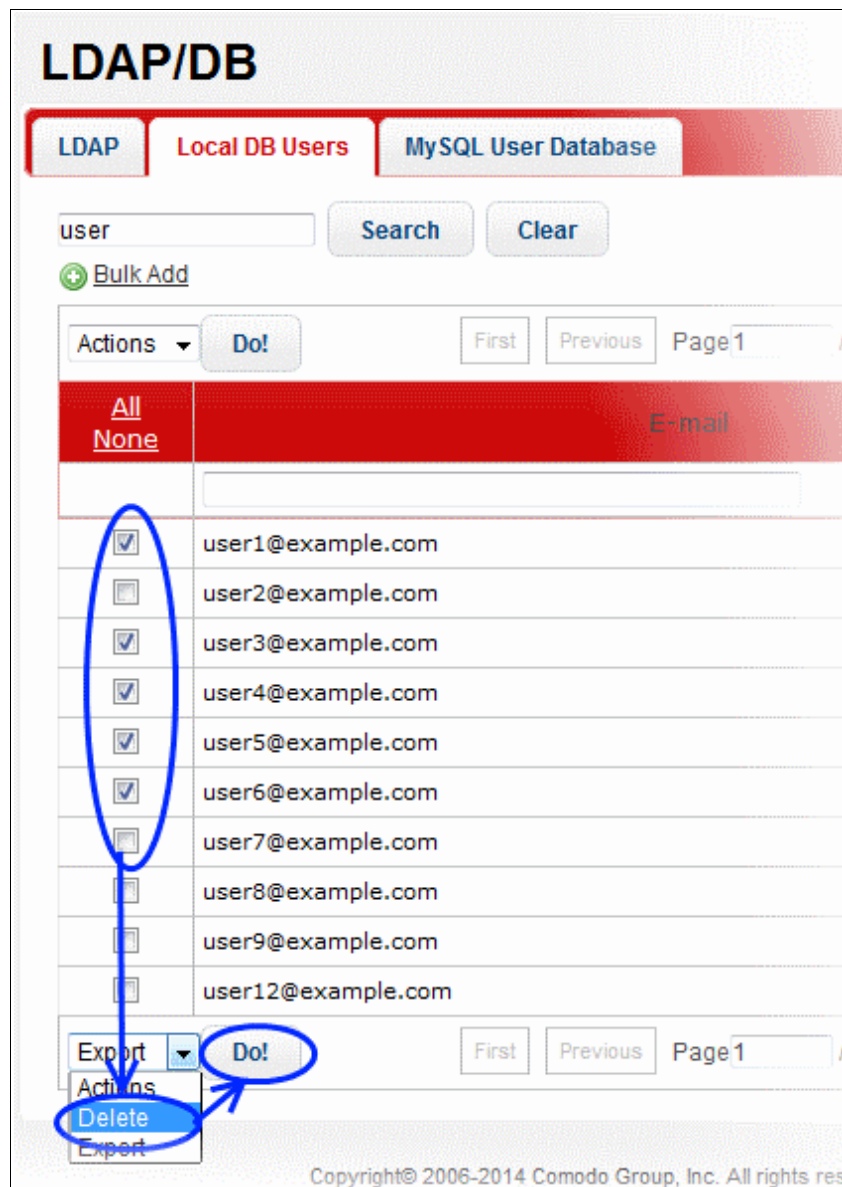
Actions First Previous Page 1 / 2 10 Records per page Next Last

All None	E-mail	Action
<input type="checkbox"/>	<input type="text"/>	
<input type="checkbox"/>	user1@example.com	
<input type="checkbox"/>	user2@example.com	
<input type="checkbox"/>	user3@example.com	
<input type="checkbox"/>	user4@example.com	
<input type="checkbox"/>	user5@example.com	
<input type="checkbox"/>	user6@example.com	
<input type="checkbox"/>	user7@example.com	

- 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.



- 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 'Actions' drop down, and select the 'Export' option.

LDAP/DB Logout

LDAP Local DB Users **MySQL User Database**

[Bulk Add](#)

Actions Page 1 / 1 50 Records per page

All None	E-mail	Action
	<input type="text"/>	
<input checked="" type="checkbox"/>	user1@comodo.com	
<input checked="" type="checkbox"/>	user2@comodo.com	
<input checked="" type="checkbox"/>	user3@comodo.com	

Export Page 1 / 1 50 Records per page

Export
Actions
Delete
Export

- Click 'Do' to 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 in 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'.



LDAP/DB Logout

LDAP Local DB Users **MySQL User Database**

[Add MySQL User Database](#)

Profile Name	Host Name or IP Address	Port	Database	SQL Clause	Action
KoruMail	192.168.199.31	25	KoruMail_database	mail='%m'	
KoruMail	192.168.199.32	25	SurGATE_database	mail='%m'	

MySQL User Database Profile – Table of Column Descriptions

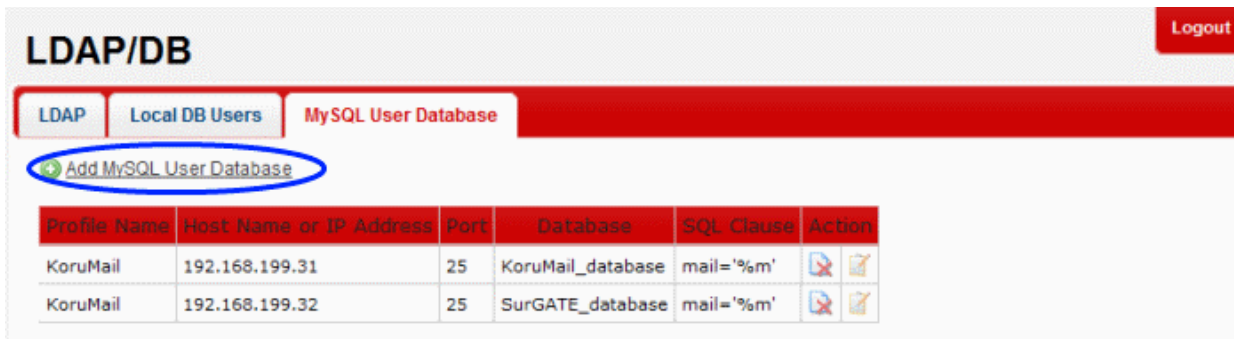
Column Header	Description	
Profile Name	The name of the MySQL User Database profile added to KoruMail	
Host Name or IP Address	Displays the address of the system where the 'MySQL User Database' is located.	
Port	Displays the port number to which KoruMail connects to.	
Database	The name of the 'MySQL 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 Logout

LDAP Local DB Users **MySQL User Database**

[Add MySQL User Database](#)

Profile Name	Host Name or IP Address	Port	Database	SQL Clause	Action
KoruMail	192.168.199.31	25	KoruMail_database	mail='%m'	 
KoruMail	192.168.199.32	25	SurGATE_database	mail='%m'	 

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

[Logout](#)

New MySQL User Database

Profile Name *	<input type="text"/>
Host Name or IP Address *	<input type="text"/>
Port *	<input type="text" value="0"/>
Search Type	Realtime ▾
Cache Time (minutes) *	<input type="text" value="0"/>
Database *	<input type="text"/>
Username *	<input type="text"/>
Password *	<input type="password"/>
SQL Clause *	<input type="text"/>
%m = Whole e-mail address	
Check Local DB Users Also	<input type="checkbox"/>
E-mail address for Testing *	<input type="text" value="admin@korumail.com"/>
<input type="button" value="Save"/> <input type="button" value="Verify"/> <input type="button" value="Cancel"/>	

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.

Logout

Edit MySQL User Database

Profile Name *	<input type="text" value="KoruMail"/>
Host Name or IP Address *	<input type="text" value="192.168.199.31"/>
Port *	<input type="text" value="25"/>
Search Type	<input type="text" value="Realtime"/>
Cache Time (minutes) *	<input type="text" value="0"/>
Database *	<input type="text" value="KoruMail_database"/>
Username *	<input type="text" value="admin"/>
Password *	<input type="password" value="*****"/>
SQL Clause * <small>%m = Whole e-mail address</small>	<input type="text" value="mail='%m'"/>
Check Local DB Users Also	<input type="checkbox"/>
E-mail address for Testing *	<input type="text"/>

- 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 the name of a method that controls source IP address/domains of each sent email, sender and recipient email addresses. Combination of these three information is named 'hash' and if this value does not exist in KoruMail Database then it acts as 'temporarily out of service' and the email is temporarily rejected.

Since spammers intend to send some millions of emails in a short time, most probably they do not try to send failed emails again. If the sender is Bot-Net client or a software used by spammers then the emails will not be resent. In this way spams are blocked quickly without using any content filtering algorithms. If the sender is a real MTA then it

will send the same email in a short time and message will be received by the recipient. If the same source sends an email again then the email will by-pass greylisting feature. In this way, the real email will be held for the first time only. You have the option to enable or disable this feature.






KoruMail can be configured to ignore the greylist record and accept emails from the sources first time itself without rejecting them.

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

[Logout](#)

Greylist

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

Greylist Type	Greylist Value	Action
IP or Network Address ▾	<input type="text"/>	
IP or Network Address	10.0.0.1	 
Domain	notsuredomain.com	 

[Export](#)

Refer to the next section '[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 creates a Greylist of source IP address/domains from where emails are sent to recipients protected by its filtering engine. The 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. Refer to the previous section '[Greylist](#)' for more details.




KoruMail can be configured to ignore the Greylist record and accept emails from the sources first time itself without rejecting them.

- To open the 'Greylist' screen, click the 'SMTP' tab from the left menu, then click 'Greylist'.

[Logout](#)

Greylist



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

Greylist Type	Greylist Value	Action
IP or Network Address ▾	<input type="text"/>	
IP or Network Address	10.0.0.1	 
Domain	notsuredomain.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

Logout

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	notsuredomain.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

Logout

The record is added successfully.

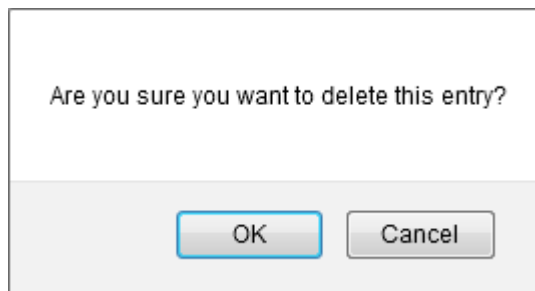
You can create greylist ignore record here for IP, Network and domains.

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

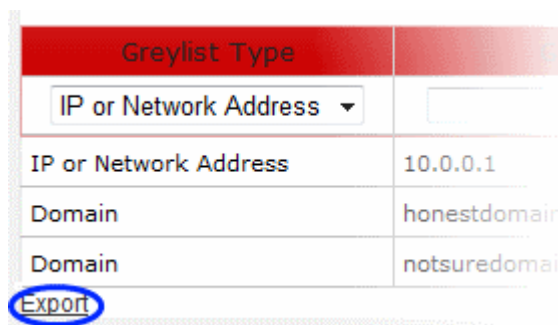
- To delete a domain name/IP address from the Greylist ignore list , click the  button under the 'Action' column header.



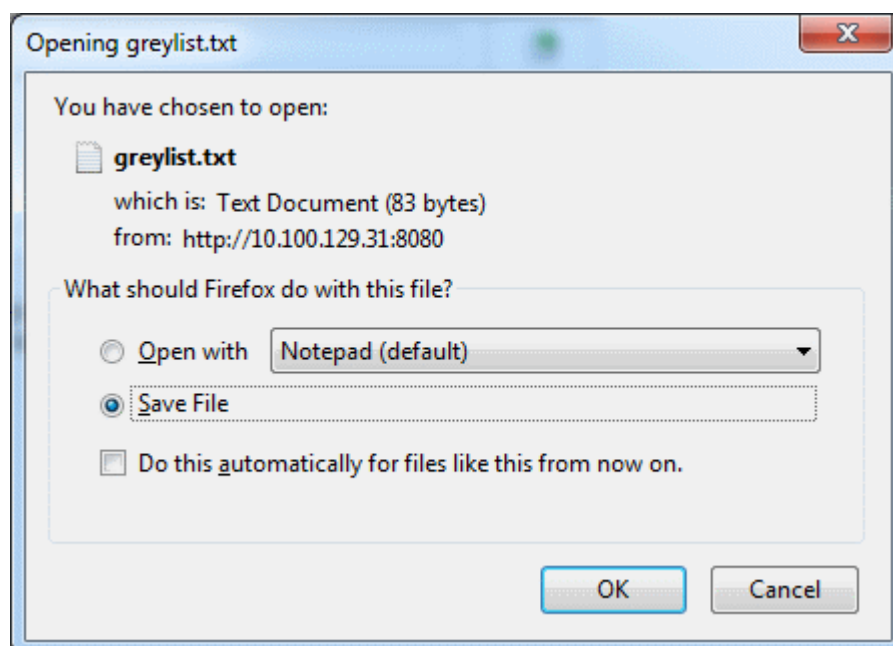
- Click 'OK' to confirm the deletion.

To export Greylist ignore list to a file

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



- Click 'OK' to download and save the list as a text file to your system.



7.6 Managing RBL Servers

Realtime Blackhole List (RBL) is one of the best ways to fight spam. RBL servers lists the server IP addresses that

proliferate spam, list of servers that are hijacked for spam relay, virus senders and so on. With RBL, KoruMail blocks SMTP connections that come from the IP addresses available in this database.

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

RBL

[Add RBL server](#)

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	

[Export](#)

Copyright© 2006-2014 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 5.2.0.3055

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 administrators 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

[+ Add RBL server](#)

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:

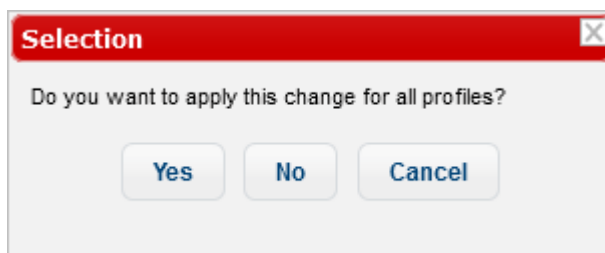
Add RBL server Logout

Server Host Address *	<input type="text"/>
Description	<input type="text"/>
Type	RBL ▾
Enable this RBL all profiles	<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- 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. Refer to the section '**Profile Management**' for more details about profiles.
- Click the 'Save' button to add the new RBL server.

To enable/disable a RBL server

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

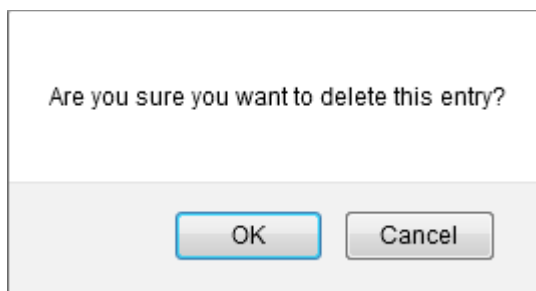


- Click 'Yes' to enable the server for all the profiles.
- Click 'No' to enable the server for the current profile.

The RBL servers can be enabled/disabled independently also for the profiles available in KoruMail. Refer to the section '[Profile Management](#)' for more details.

To delete a RBL server

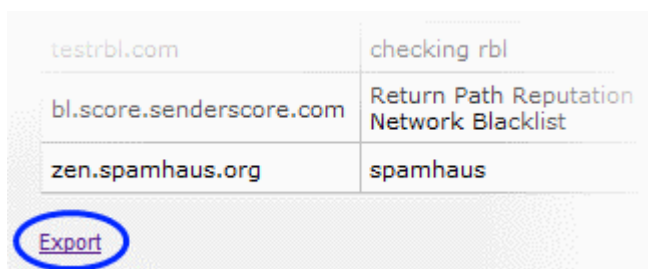
- To delete a RBL server from the list, click the  button.



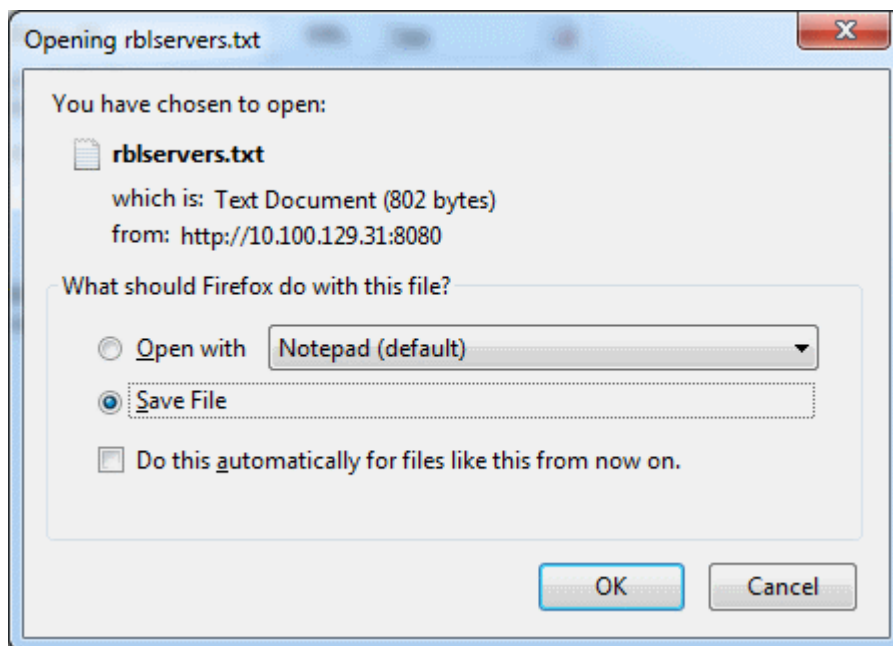
- Click 'OK' to confirm the deletion.

To export RBL server list to a file

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



- Click 'OK' to download and save the list as a text file to your system.



7.7 Disclaimer

KoruMail allows administrators to insert disclaimers in outgoing 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'.

Disclaimer

Logout

Managed Domain Name *	-Choose-
Enabled	<input type="checkbox"/>
Text Footer	<div></div>
HTML Footer	<div></div>
<div>Save</div> <div>Cancel</div>	

- **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 the 'Save' button

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 SMTP Relay

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

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

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.

- Click 'OK' to confirm the deletion.

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 refer 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'.

- 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'



- To remove the selected file from the field, click 'Clear'
- To upload the private key, click the 'Save' button.
- 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:

- Select the 'Create New Domainkey' check box.
- Click the 'Create' button to generate a new domain key for the selected domain.

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

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 allows administrators to set limits for outgoing mails for users as well as for domain names. KoruMail can be configured to allow only a certain number of outgoing mails per hour and per day. The interface allows you to 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'.

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**

Configuring outgoing limits for domains and users

To configure outgoing limits for domains and users:

- Click the 'General' tab

Outgoing Limits Logout

General Settings Usage

[Add new limit](#) [Add bulk domain limit](#) [Add bulk user limit](#)

Limitation type	Limitation object	Description	Limit per-hour	Limit per-day	Action
Domain	comodo.com	co	250	0	
Domain	example.com	ex	100	0	
Username	user1@example.com	user limit	50	200	

Outgoing 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 outgoing mails allowed per hour	
Limit per-day	Indicates the number of outgoing 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

Outgoing Limits Logout

General Settings Usage

[Add new limit](#) [Add bulk domain limit](#) [Add bulk user limit](#)

Limitation type	Limitation object	Description	Limit per-hour	Limit per-day	Action
Domain	comodo.com	co	250	0	
Domain	example.com	ex	100	0	
Username	user1@example.com	user limit	200	700	

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

- **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 the 'Save' button. 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

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

Logout

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 the 'Save' button.

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

Logout

Outgoing Limits

General Settings Usage

[+ Add new limit](#)
[+ Add bulk domain limit](#)
[+ Add bulk user limit](#)

Limitation type	Limitation object	Description	Limit per-hour	Limit per-day	Action
Domain	comodo.com	co	250	0	
Domain	example.com	ex	100	0	
Username	user1@example.com	user limit	200	700	

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



Add Bulk outgoing SMTP limit Logout

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 the 'Save' button to apply your changes.

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 outgoing SMTP limit' screen will be displayed.

Edit outgoing SMTP limit Logout

Limitation type	Domain
Limitation object *	example.com
Description:	ex
Limit per-hour *	100
Limit per-day *	0

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

Configuring 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

General
Settings
Usage

Default Template Loaded

SMTP AUTH is enabled by user name limit for outgoing e-mail * ☒

Enable the Limit for From Addresses * ☒

Default hourly limit *

Default daily limit

Envelope sender must match SMTP-AUTH username ☐

Default domain

SMTP-AUTH username format *

☐ Username
☐ Domain:

☒ user@domain.com
☐ user%domain.com

Enable System Admin e-mail notification for exceeded limits ☐

Mail Subject

Mail From

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 \$sysAdmin,

Merhaba \$sysAdmin,

<p>Giden e-posta limitini gecen hesap listesi</p>

Save
Defaults

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 the 'Save' button to apply your changes.

Viewing outgoing mail usage details for domains and users

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

Outgoing Limits Logout

General Settings **Usage**

Default Template Loaded

User				Domain			
Name	Time	Total(hourly)	Total(daily)	Name	Time	Total(hourly)	Total(daily)
There are no available records.				There are no available records.			

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 Logout

General Settings Usage

Default Template Loaded

User				Domain			
Name	Time	Total(hourly)	Total(daily)	Name	Time	Total(hourly)	Total(daily)
There are no available records.				There are no available records.			

- 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 administrators to set limits for incoming mails for users as well as for domain names. KoruMail can be configured to allow only a certain number of incoming mails per hour and per day. The interface allows you to 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'.

Incoming Limits Logout

General Settings Usage

[Add new limit](#)

Limitation type	Limitation object	Description	Limit per-hour	Limit per-day	Action
Domain	comodo.com	co	200	210	 
Domain	example.com	eg	50	100	 
Username	username@example.com	user1	300	1000	 

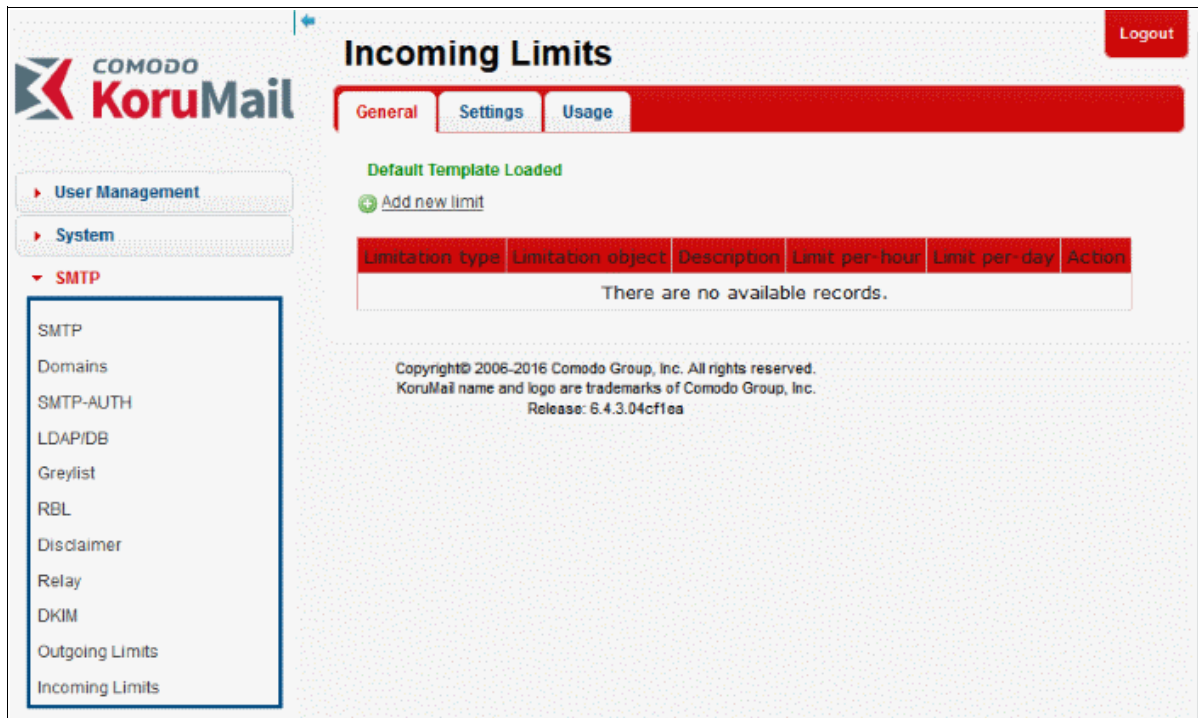
The interface allows administrators to:

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



Configuring Incoming limits for domains and users

To configure incoming limits for domains and users:

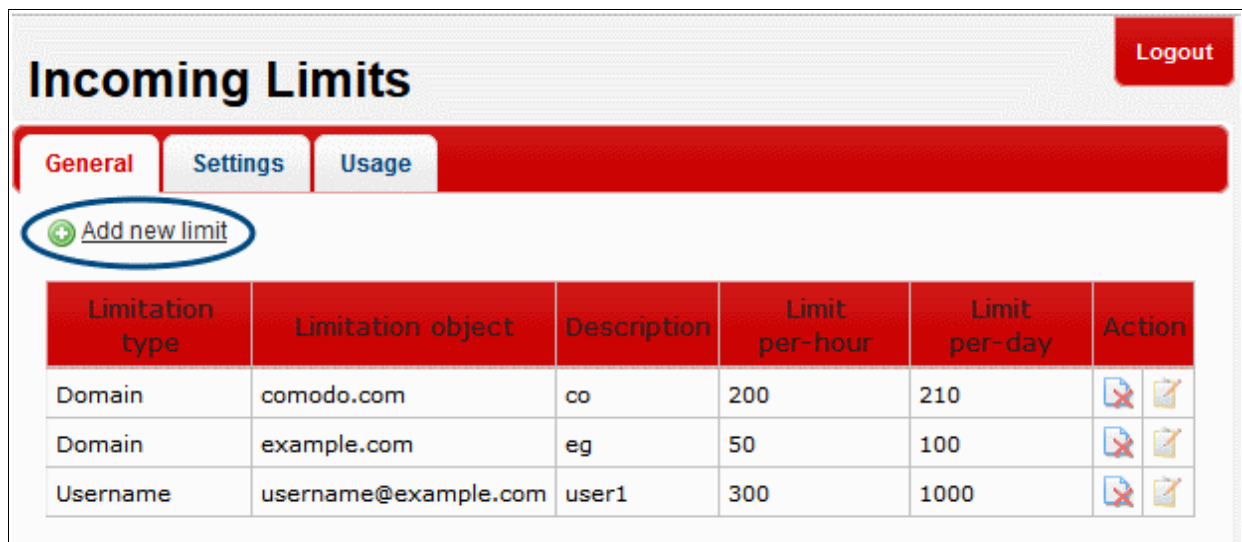
- Click SMTP > Incoming Limits and then click the 'General' tab



Incoming Limits: General – Table of Column Descriptions

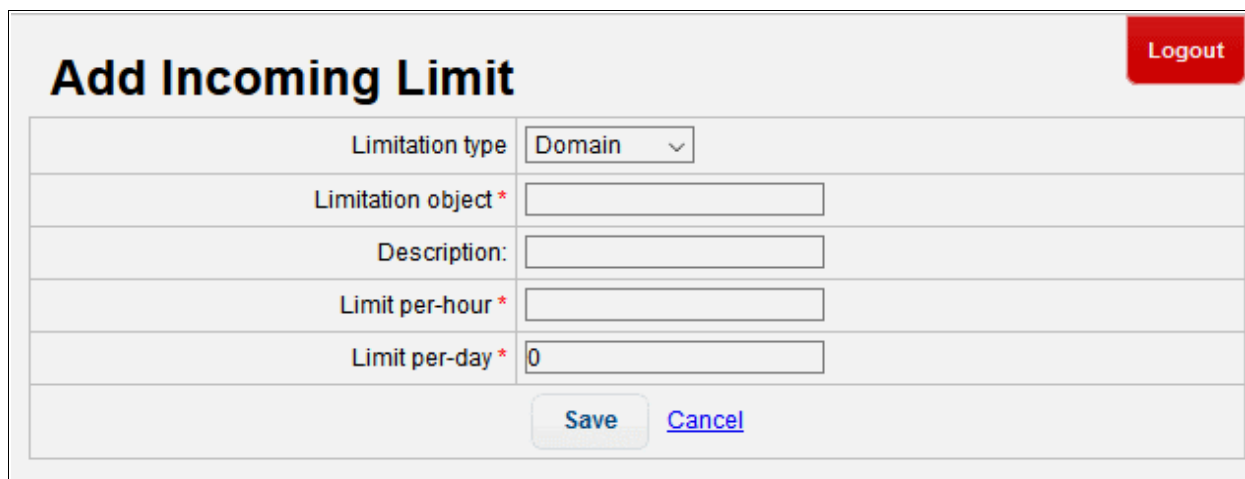
Column Header	Description	
Limitation Type	Indicates whether the limitation is for a domain or user	
Limitation Object	The details of the domain or the user	
Description	The description for the limitation	
Limit per-hour	Indicates the number of incoming mails allowed per hour	
Limit per-day	Indicates 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



Limitation type	Limitation object	Description	Limit per-hour	Limit per-day	Action
Domain	comodo.com	co	200	210	
Domain	example.com	eg	50	100	
Username	username@example.com	user1	300	1000	

The 'Add Incoming Limit' screen will be displayed.



- **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 the 'Save' button. 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 [Logout](#)

Limitation type	Domain ▾
Limitation object *	<input type="text" value="comodo.com"/>
Description:	<input type="text" value="co"/>
Limit per-hour *	<input type="text" value="200"/>
Limit per-day *	<input type="text" value="210"/>
<input type="button" value="Save"/> Cancel	

The screen is similar to the 'Add Incoming Limit' interface. Refer to the section for '[Configuring incoming limits for domains and users](#)' for more details.

Configuring 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

[Logout](#)

Incoming Limits

[General](#) [Settings](#) [Usage](#)

Settings saved successfully.

Enable System Admin e-mail notification for exceeded limits	<input checked="" type="checkbox"/>
Mail Subject	<input type="text" value="Sender Limits Notifica"/>
Mail From	<input type="text" value="korumail@10.108.51."/>
Mail Template	<pre><!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 \${sysAdmin}, <p>Gelen e-posta limitini gecen hesap listesi</p></pre>

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 the 'Save' button to apply your changes.

Viewing 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.

Incoming Limits								Logout
General Settings Usage								
User				Domain				
Name	Time	Total(hourly)	Total(daily)	Name	Time	Total(hourly)	Total(daily)	
mehmet@mail.postmanilic.net	2016-11-09 06:00:00.0	7	7	seth.bernard@rajeshkhanasongs.com	2016-11-09 10:00:00.0	1	2	
seth.bernard@rajeshkhanasongs.com	2016-11-09 10:00:00.0	1	2	kaylee.house@dinosaurusfactsforkids.com	2016-11-09 16:00:00.0	2	2	
michael.ball@derroitnews.com	2016-11-09 17:00:00.0	2	2	588392645-2104237-107@be4.maropost.com	2016-11-08 01:00:00.0	1	1	
kaylee.house@dinosaurusfactsforkids.com	2016-11-09 16:00:00.0	2	2	service@thelotter.co.uk	2016-11-09 08:00:00.0	1	1	
ashley.navarro@robertsurf.com	2016-11-09 10:00:00.0	2	2	shelbydearhd212@gmail.com	2016-11-08 06:00:00.0	1	1	
services@365online.com	2016-11-08 07:00:00.0	2	2	bounces+132643-c052-ironman@mail.postmanilic.net@mtg.hubspot.com	2016-11-09 19:00:00.0	1	1	
jason.sullivan@tracyfingers.com	2016-11-08 16:00:00.0	2	2	a7ugq+ai+rjyx3wgvqzpq==_130220974469_af4kak+meewydsuphrra==@in.constantcontact.com	2016-11-09 19:00:00.0	1	1	
www-data@rayapple.ru	2016-11-08 08:00:00.0	1	1	jason.sullivan@tracyfingers.com	2016-11-08 16:00:00.0	2	2	
588392645-2104237-107@be4.maropost.com	2016-11-08 01:00:00.0	1	1	services@365online.com	2016-11-08 07:00:00.0	2	2	
service@thelotter.co.uk	2016-11-09 08:00:00.0	1	1	bestmetal@vip.sina.com	2016-11-08 08:00:00.0	1	1	

Incoming Limits: Usage – Table of Parameters		
Parameter	Description	
User	Name	Displays the email address of the recipient.
	Time	The time at which the mail is received.
	Total(Hourly)	The total number of emails received in an hour.
	Total(Daily)	The total number of emails received in a day.
Domain	Name	Displays the email address of the recipient on the limited domain.
	Time	The time at which the mail is received.
	Total(Hourly)	The total number of emails received in an hour.
	Total(Daily)	The 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'.

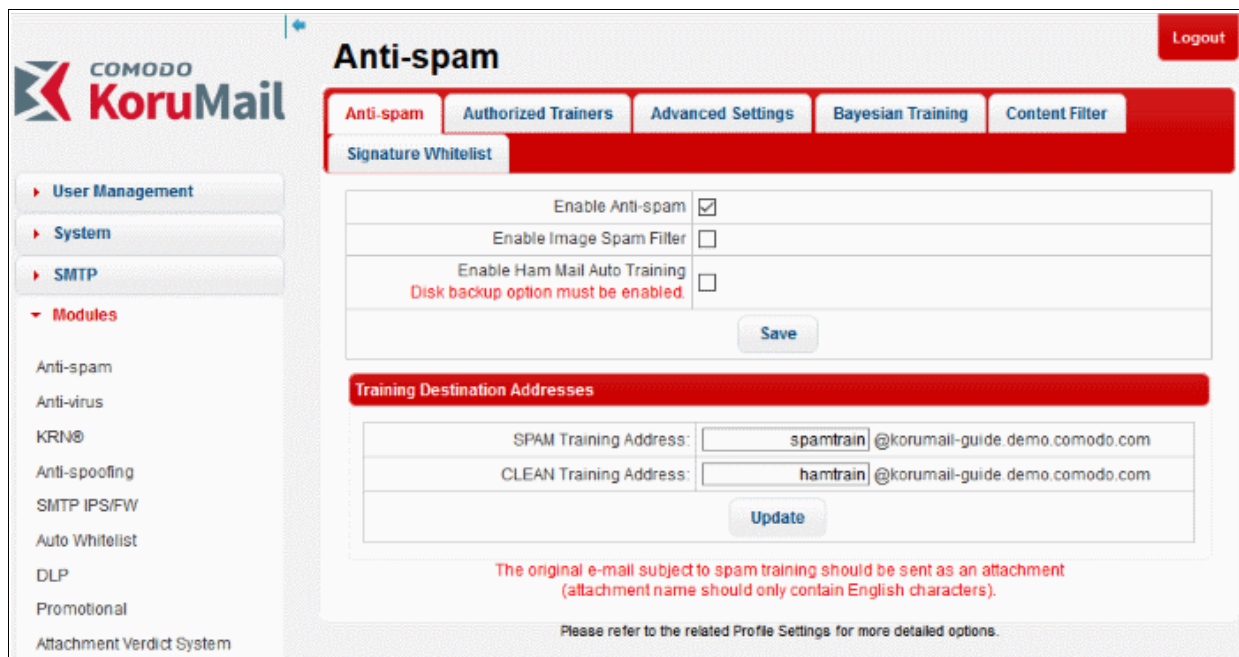
Incoming Limits								Logout
General Settings Usage								
User				Domain				
Name	Time	Total(hourly)	Total(daily)	Name	Time	Total(hourly)	Total(daily)	
mich				Kay				
michael.ball@derroitnews.com	2016-11-09 17:00:00.0	2	2	kaylee.house@dinosaurusfactsforkids.com	2016-11-09 16:00:00.0	2	2	
				kayla.clarke@handimusic.com	2016-11-09 11:00:00.0	1	1	

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 allows you to configure the core security components of KoruMail's email defense system. The 'Anti-spam' module allows administrators to configure anti-spam settings, add authorized trainers, add content filters and more. Administrators can also configure other modules including anti-virus, anti-spoofing and anti-phishing.



Click the following links for more details:

- [Anti-spam](#)
- [Anti-virus](#)
- [KRN® - KoruMail Reputation Network® Servers](#)
- [Anti-spoofing](#)
- [SMTP IPS/FW](#)
- [Auto Whitelist](#)
- [Data Loss Prevention \(DLP\)](#)
- [Promotional](#)
- [Attachment Verdict System](#)

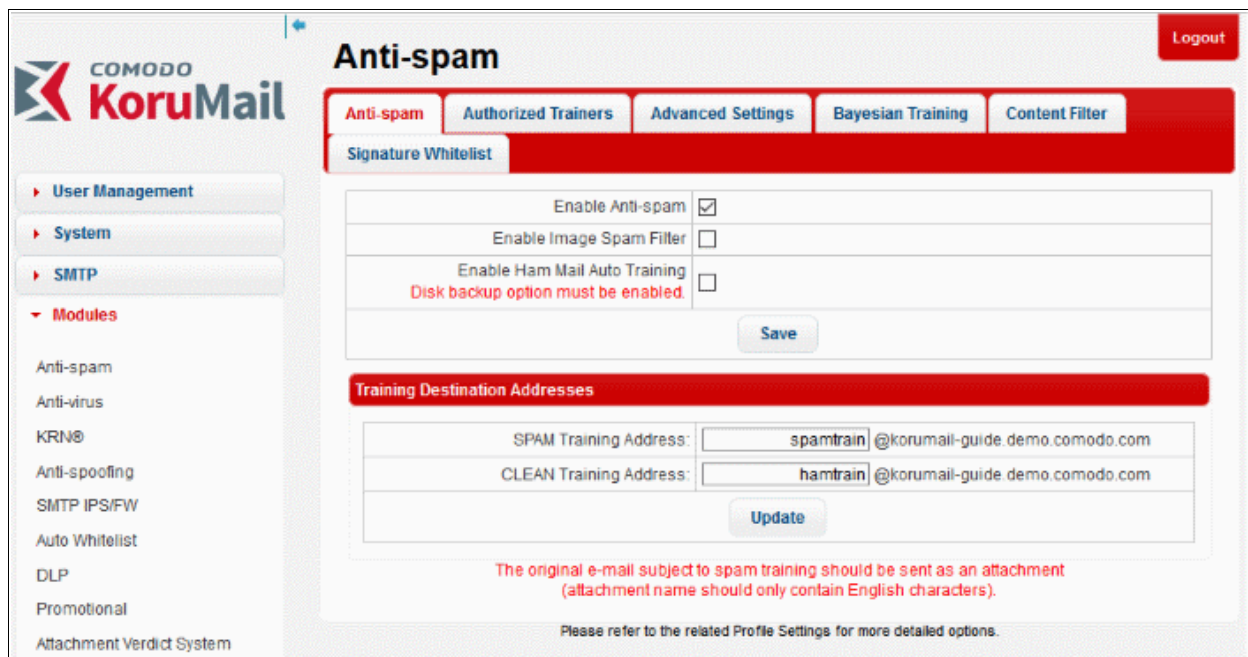
8.1 Anti-spam

The Anti-spam module allows administrators to 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.

Bayesian spam filtering is a statistical technique of email filtering. It makes use of a naive Bayes classifier to identify spam emails. 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 anti-spam parameters specified in profile settings. Refer to the '[Profile Management](#)' section for more details about profile settings.

- To open the 'Anti-spam' interface, click the 'Modules' tab on the left, then click 'Anti-spam'.



Refer to the following sections for more details:

- [Anti-spam General Settings](#)
- [Authorized Trainers](#)
- [Advanced Anti-spam Settings](#)
- [Bayesian Training](#)
- [Content Filter](#)
- [Signature Whitelist](#)

8.1.1 Anti-spam General Settings

In the 'Anti-spam' general settings screen, administrators can enable/disable various settings including anti-spam, image spam filter and Ham mail training. The anti-spam module must be enabled in order to activate the anti-spam parameters specified in profile settings. Refer to the '[Profile Management](#)' section for more details about profile settings.

- To open the 'Anti-spam' general settings screen, click the 'Anti-spam' tab in the Anti-spam interface.

[Logout](#)

Anti-spam

Anti-spam
Authorized Trainers
Advanced Settings
Bayesian Training
Content Filter

Signature Whitelist

Enable Anti-spam	<input checked="" type="checkbox"/>
Enable Image Spam Filter	<input type="checkbox"/>
Enable Ham Mail Auto Training <small>Disk backup option must be enabled.</small>	<input type="checkbox"/>
Save	

Training Destination Addresses

SPAM Training Address:	<input type="text" value="spamtrain@korumail-guide.demo.comodo.com"/>
CLEAN Training Address:	<input type="text" value="hamtrain@korumail-guide.demo.comodo.com"/>
Update	

Anti-spam General Settings – Table of Parameters	
Parameter	Description
Enable Anti-spam	Select this 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. Refer to the 'Profile Management' section 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 administrators to define the sources from which spam training emails can be sent. Submitting sample spam emails to KoruMail allows the system to learn, adapt and protect against new spam types. Training content sent from any other source will not be accepted by KoruMail.

- To open the 'Authorized Trainers' screen, click the 'Authorized Trainers' tab in the Anti-spam interface.

Anti-spam Logout

Anti-spam Authorized Trainers Advanced Settings Bayesian Training Content Filter Signature Whitelist

Authorized Trainers

Send Information Message ☒

Type	Value	Description	Add
E-mail ▼			+
E-mail	hamtraining@comodo.com	Ham training	–
IPv4	192.162.199.0	Spam training	–

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

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	+	Allows administrators to add a source ID after filling the fields in the row
	–	Allows administrators to 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?

OK Cancel

- Click 'OK' to confirm the removal of an authorized trainer.

8.1.3 Advanced Anti-spam Settings

The 'Advanced Settings' screen allows administrators to configure language settings. It allows to configure the languages for which the emails will be analyzed for spam using the Bayes spam classifier.

- To open the 'Advanced Settings' screen, click the 'Advanced Settings' tab in the Anti-spam interface.

- Accepted Languages:** The languages for which the Bayes spam engine should analyze the emails for spam. By default, a set of predefined languages is selected. To remove a language from the list, select it and click the 'Remove' button. To move a language to the right side, select it and click the 'Copy' button.

Click the 'Save' button to apply your changes.

8.1.4 Bayesian Training

In order to train the Bayesian spam engine in KoruMail to identify spam and clean emails, administrators can upload content from the 'Bayesian Training' screen. It allows to upload both spam and safe content for training.

- To open the 'Bayesian Training' screen, click the 'Bayesian Training' tab in the Anti-spam interface.

- 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



- 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)

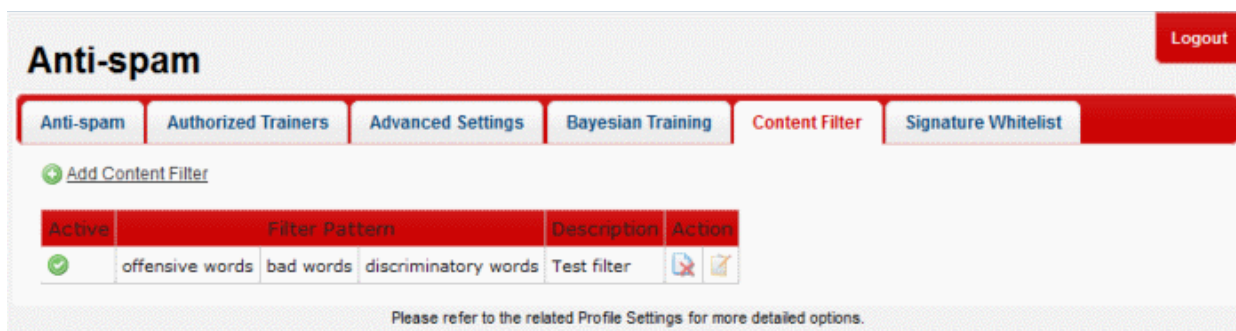


- Repeat the process to add more files
- To remove a file from the list, click the 'Clear' link beside it
- To remove all the files from the list, click the 'Clear All' button at the top
- To upload the files, click the 'Save' button

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 the 'Content Filter' tab in the Anti-spam interface.



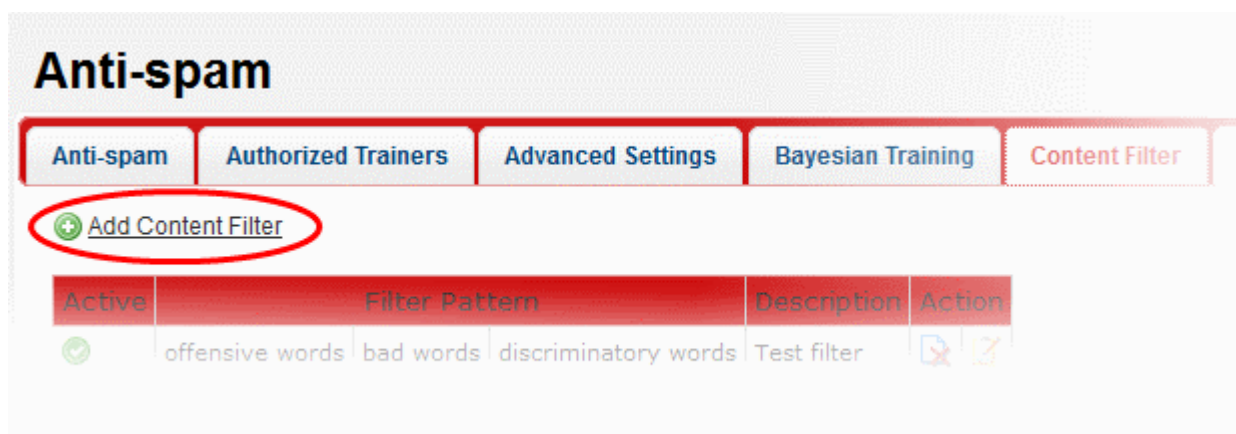
Content Filter – Table of Column Descriptions		
Column Header	Description	
Active	Indicates whether the 'Content Filter' is enabled or disabled	
Filter Pattern	Displays the details of the filter pattern.	
Description	The description for the added 'Content Filter'	
Action		Allows administrators to delete 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.



The 'New Content Filter' screen will be displayed.

New Content Filter Logout

Active ☒

Filter Pattern *
You must define at least one pattern.

Description *

[Save](#) [Cancel](#)

- **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 Logout

Active ☒

Filter Pattern *
You must define at least one pattern.

Description *

[Save](#) [Cancel](#)

- 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?

[OK](#) [Cancel](#)

- Click 'OK' to confirm the deletion of the filter

8.1.6 Signature Whitelist

The signature whitelist area is a list of digital signatures that came attached to white-listed emails. Administrators can manually whitelist mails from the 'Mail logs' interface.

Anti-spam

Signature Whitelist

Signature Description	Action
info@finn-neo.com	[X]
www.proactiv.com	[X]
X-Mailer: Microsoft Outlook Express 6.00.2600.0000	[X]

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

Copyright© 2006-2016 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 6.4.3.04cf1ea

To whitelist emails in 'Mail Logs':

- Click 'Mail Logs' from reports menu.

Mail Logs

Search Clear Advanced search

☐ Subject ☐ Sender ☐ Recipients ☐ IP

☒ Last Month ☐ Last 2 Months ☐ Last 3 Months ☐ Last 6 Months ☐ All Time

Result: EQUALS CERTAINLY SPAM

Search Clear

Actions: Del

Subject	Result	Received	Sender	Recipient(s)	IP	Details
[1] CERTAINLY SPAM]Why do all	CSAM	10.11.2016 20:31:57	brianna.monroe@lucapuncall.com	faith@mail.postmanic.net	199.229.249.201	Score: 129.0
[1] CERTAINLY SPAM]MAJOR -SEN	CSAM	10.11.2016 09:04:31	jefferybuchanan77@gmail.com	anthony@mail.postmanic.net	52.86.0.96	Korunail global spam signature detected
[1] CERTAINLY SPAM]U- K-6(发件人:1818)	CSAM	07.11.2016 10:18:26	info@finn-neo.com	chrisharry1@mail.postmanic.net	175.184.37.174	Korunail global spam signature detected
[1] CERTAINLY SPAM]Acne can r	CSAM	07.11.2016 10:01:01	chloe.blackwell@hyperionairline.com	faith@mail.postmanic.net	172.245.211.197	Korunail global spam signature detected
[1] CERTAINLY SPAM]Acne can r	CSAM	07.11.2016 09:56:50	chloe.blackwell@hyperionairline.com	faith@mail.postmanic.net	172.245.211.197	Korunail global spam signature detected
[1] CERTAINLY SPAM]RE: PRIZE	CSAM	07.11.2016 01:09:23	sanchezperezco@gmail.com	dorothy@mail.postmanic.net	186.40.111.74	Korunail global spam signature detected
[1] CERTAINLY SPAM]SYRIAN REF	CSAM	06.11.2016 09:08:02	johndmed651@gmail.com	harry@mail.postmanic.net	52.86.0.96	Score: 167.0
[1] CERTAINLY SPAM]RE: PRIZE	CSAM	06.11.2016 07:55:52	sanchezperezco@gmail.com	dorothy@mail.postmanic.net	199.254.123.22	Korunail global spam signature detected
[1] CERTAINLY SPAM]RE: PRIZE	CSAM	06.11.2016 01:52:31	amenchan@saalem.hic	harry@mail.postmanic.net	118.140.177.62	Korunail global spam signature detected
[1] CERTAINLY SPAM]([spam?]) RE	CSAM	05.11.2016 17:08:32	amenchan@saalem.hic	dorothy@mail.postmanic.net	118.140.177.62	Korunail global spam signature detected
[1] CERTAINLY SPAM]SYRIAN REF	CSAM	05.11.2016 15:58:49	johndmed651@gmail.com	dorothy@mail.postmanic.net	52.86.0.96	Score: 173.0
[1] CERTAINLY SPAM]SYRIAN REF	CSAM	05.11.2016 08:28:42	johndmed651@gmail.com	bridget@mail.postmanic.net	52.86.0.96	Score: 204.0
[1] CERTAINLY SPAM]SYRIAN REF	CSAM	04.11.2016 23:25:08	johndmed651@gmail.com	barbara@mail.postmanic.net	52.86.0.96	Score: 173.0
[1] CERTAINLY SPAM]Reply	CSAM	04.11.2016 22:57:32	kwamememash@ecobankgh.com	jessica@mail.postmanic.net	93.187.162.98	Korunail global spam signature detected
[1] CERTAINLY SPAM]Reply	CSAM	04.11.2016 21:22:44	kwamememash@ecobankgh.com	dorothy@mail.postmanic.net	93.187.162.98	Korunail global spam signature detected
[1] CERTAINLY SPAM]SYRIAN REF	CSAM	04.11.2016 18:35:14	johndmed651@gmail.com	anthony@mail.postmanic.net	52.86.0.96	Score: 173.0
[1] CERTAINLY SPAM]2009个国空	CSAM	04.11.2016 14:21:04	tsi@ajyou.com	carroll@mail.postmanic.net	42.51.216.11	Score: 120.0
[1] CERTAINLY SPAM]Bad Acne c	CSAM	04.11.2016 13:42:54	maggie.medina@ningtech.com	faith@mail.postmanic.net	38.99.252.11	Korunail global spam signature detected
[1] CERTAINLY SPAM]Bad Acne c	CSAM	04.11.2016 13:40:31	maggie.medina@ningtech.com	faith@mail.postmanic.net	38.99.252.11	Korunail global spam signature detected
[1] CERTAINLY SPAM]S Charity	CSAM	04.11.2016 08:24:33	sarahjmoal@test.com	harry@mail.postmanic.net	75.131.133.237	Korunail global spam signature detected
[1] CERTAINLY SPAM]OFFICIAL N	CSAM	04.11.2016 02:52:05	award@goolemail.com	dorothy@mail.postmanic.net	117.52.99.146	Korunail global spam signature detected
[1] CERTAINLY SPAM]RE: CONGRA	CSAM	03.11.2016 17:28:03	amenchan@saalem.hic	harry@mail.postmanic.net	220.241.212.153	Korunail global spam signature detected
[1] CERTAINLY SPAM]ACCOUNTS:	CSAM	03.11.2016 17:21:08	chow@zhuat.com	dorothy@mail.postmanic.net	89.253.252.22	Korunail global spam signature detected
[1] CERTAINLY SPAM]Simply the	CSAM	03.11.2016 17:13:43	amberhobbs@fashionfestivalbd.com	faith@mail.postmanic.net	198.8.81.11	Score: 110.0
[1] CERTAINLY SPAM]Simply the	CSAM	03.11.2016 17:13:09	amberhobbs@fashionfestivalbd.com	faith@mail.postmanic.net	198.8.81.11	Score: 110.0

Page 1 of 250 Records per page

- Click the 'Advanced search' link.
- Select 'Result' from the first drop down.

- Select 'EQUALS' from the second drop down and then choose 'CERTAINLY SPAM'.

Mail Logs

←

→

Received	04.11.2016 06:24:35	
Queue ID	32270-1478255075-343277	
Message ID	WASHINGTONCd7KKQpQ00001fce@mail.levybus.com	
Action		
Result	CERTAINLY SPAM	
Score	120.0	
Sender	sarahjiwool@test.com	<input type="button" value="Add Email In White List"/>
Recipient(s)	harry@mail.postmanllc.net	
RFC2822 Sender	" will fund for charity" <sarahjiwool@test.com>	
RFC2822 Recipient(s)		
Subject	[! CERTAINLY SPAM]\$ Charity Fundraising Money for Charity \$	
IP	75.151.133.237	<input type="button" value="Add White List"/>
Location	United States	
Size	4.97 KB	
Matched Profile	Default Incoming Profile (defined by user: admin)	
Details	Korumail global spam signature detected Show signature Add White Signature Lists	

- 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.

The screenshot shows the Comodo KoruMail Admin interface. On the left is a sidebar with a menu. The 'Modules' section is expanded, and 'Anti-spam' is selected. In the main content area, the 'Anti-spam' module is active, and the 'Signature Whitelist' tab is selected. A table lists whitelisted signatures. A blue arrow points from the 'Anti-spam' menu item to the 'Signature Whitelist' tab.

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© 2006-2016 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 6.4.3.04cf1ea

The email will automatically populate in the 'Signature Whitelist' tab in Anti-spam' module.

8.2 Anti-Virus

KoruMail is capable of virus scanning of all emails that pass through its engine. KoruMail 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. Refer to the '**Profile Management**' section for more details about profile settings.

- To open the 'Anti-virus' interface, click the 'Modules' tab on the left, then click 'Anti-virus'.

The screenshot shows the Comodo KoruMail Admin interface with the 'Anti-virus' module selected. The 'General Settings' tab is active. The 'Enable Anti-virus' checkbox is checked, and the 'Virus Scanner' is set to 'Comodo Anti-virus'. A 'Save' button is visible. The sidebar shows 'Anti-virus' selected under the 'Modules' section.

Enable Anti-virus ☒

Virus Scanner Comodo Anti-virus

[Save](#)

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

Copyright© 2006-2016 Comodo Group, Inc. All rights reserved.
KoruMail name and logo are trademarks of Comodo Group, Inc.
Release: 6.4.3.04cf1ea

Refer to the following sections for more details:

- [Anti-Virus General Settings](#)
- [Advanced Anti-Virus Settings](#)

8.2.1 Anti-Virus General Settings

In the 'Anti-virus' general settings screen, administrators can enable/disable the anti-virus module and select the anti-virus program that should be used for AV scanning. The anti-virus module must be enabled in order to activate the anti-virus parameters specified in profile settings. Refer to the ['Profile Management'](#) section for more details about profile settings.

- To open the 'Anti-virus' general settings screen, click the 'General Settings' tab in the 'Anti-virus' interface.

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. Refer to the 'Profile Management' section 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 the 'Save' button 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.

[Logout](#)

Anti-virus

[General Settings](#)
[Advanced Settings](#)

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	<input checked="" type="checkbox"/>	
Scan PDF File	<input type="checkbox"/>	
Enable Phishing Signature checks	<input checked="" type="checkbox"/>	
Enable Phishing URL Checks	<input checked="" type="checkbox"/>	
Scan Archive Files	<input checked="" type="checkbox"/>	

[Save](#)
[Default](#)
[Cancel](#)

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. Refer to the 'Profile Management' section for more details about profile settings.

- Click the 'Save' button to apply your changes.
- To restore the default 'Anti-virus 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®'

The screenshot shows the KoruMail Admin interface. On the left is a sidebar with a 'Modules' menu item circled in blue, with an arrow pointing to the 'KRN®' option, which is also circled. The main content area is titled 'KRN®' and has tabs for 'Servers' and 'Settings'. Below the tabs, there is a table titled 'KoruMail Reputation Network® Servers'.

KoruMail Reputation Network® Server	Description	Enabled
srn.surgate.net	KoruMail Reputation Network	Yes

Below the table, there is a copyright notice: 'Copyright© 2006-2016 Comodo Group, Inc. All rights reserved. KoruMail name and logo are trademarks of Comodo Group, Inc. Release: 6.4.3.04cf1ea'.

The interface 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.

This is a close-up of the 'KRN® Servers' table from the previous screenshot. It shows the table structure with columns for the server name, description, and an 'Enabled' column containing a 'Yes' link.

KoruMail Reputation Network® Server	Description	Enabled
srn.surgate.net	KoruMail Reputation Network	Yes

KRN Settings

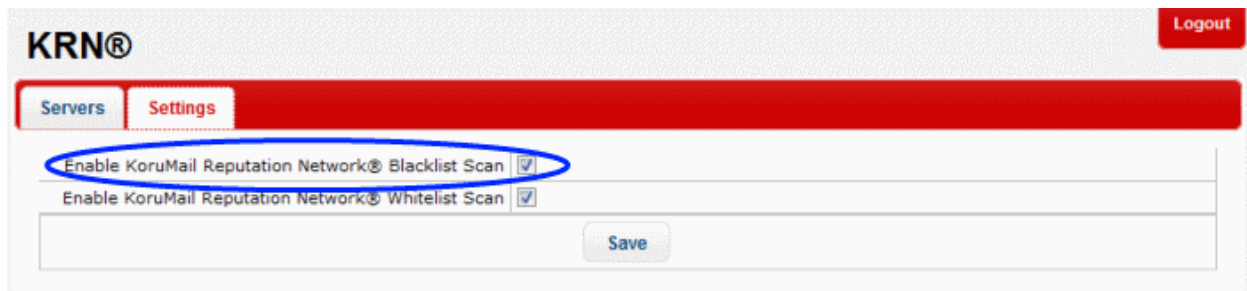
The KRN settings interface allows administrators to enable / disable KRN Blacklist and Whitelist scan. The KRN Blacklist and Whitelist scan in the KRN module must be enabled in order to activate the KRN scan parameters specified in profile settings. Refer to the '**Profile Management**' section for more 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

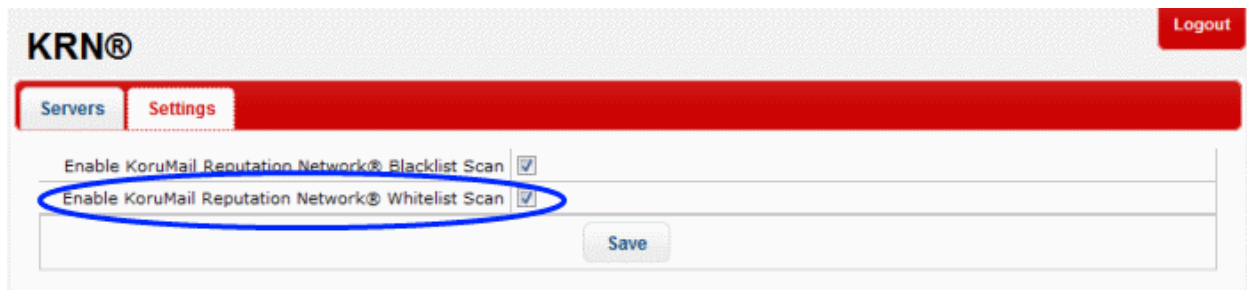
- Click the 'Settings' tab in the KRN® interface



- Select / deselect the 'Enable KoruMail Reputation Network® Blacklist Scan' check box to activate or deactivate the KRN blacklist scan
- Click the 'Save' button to apply your changes.

To enable / disable KRM whitelist scan

- Click the 'Settings' tab in the KRN® interface

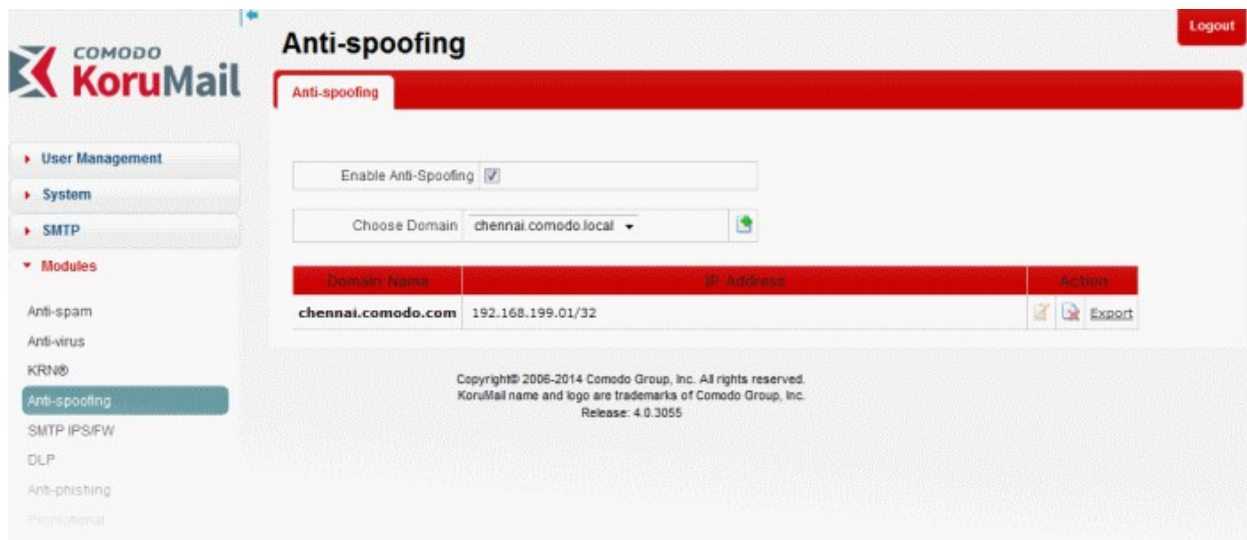


- Select / deselect the 'Enable KoruMail Reputation Network® Whitelist Scan' check box to activate or deactivate the KRN whitelist scan
- Click the 'Save' button to apply your changes.



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'.



- 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 Logout

Anti-spoofing

Enable Anti-Spoofing ☒

Choose Domain chennai.comodo.com +

- chennai.comodo.com
- chennai.comodo.local
- chennai.comodo.net
- example.com
- example.domain.com
- ve.comodo.local

Domain Name	IPs	Action
Th		Records.

- Click the button

The 'Anti-spoofing Edit' screen will be displayed.

Anti-spoofing Edit

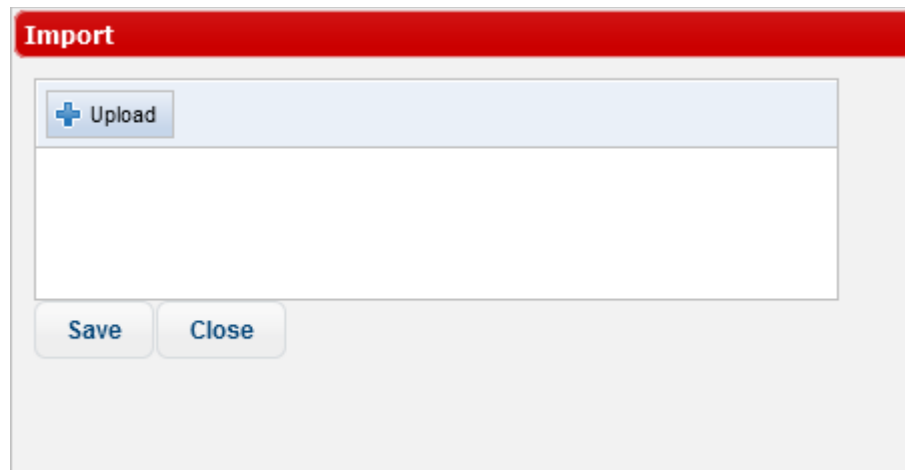
chennai.comodo.com

Write IP addresses which properly below example.

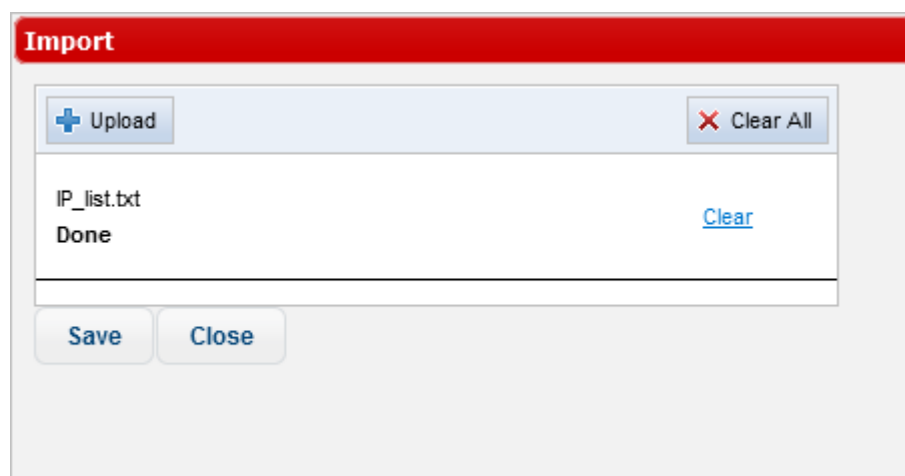
Import Save Delete all Cancel

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 the 'Clear' link beside it.
- To remove all the files, click the 'Clear All' button at the top.
- Click the 'Save' button.

Anti-spoofing Edit

Write IP addresses which properly below example.


192.168.200.1/32
192.168.199.1/32

[Import](#) [Save](#) [Delete all](#) [Cancel](#)

Example:
1.2.3.4
1.2.3.4/5
1:2:3:4
1:2:3:4/5

- 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

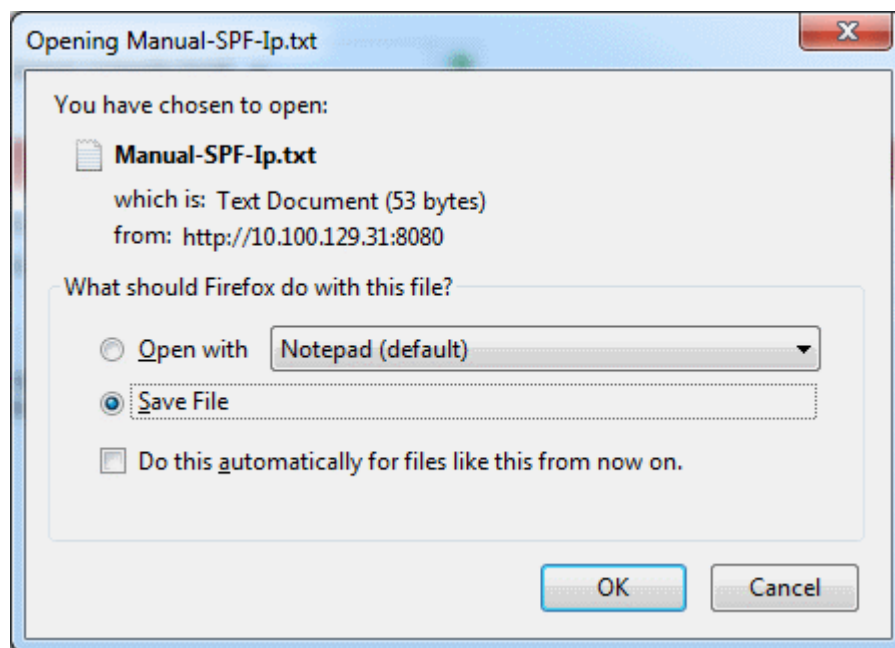
- To delete a domain name from the list, click the  button under the 'Action' column and confirm it in the confirmation screen.

To export the list of IP addresses for a domain

- Click the 'Export' link under the 'Action' column



- Click 'OK' to download and save the SPF IP list as a text file to your system.



8.5 SMTP IPS/FW

KoruMail's SMTP Intrusion Prevention System (IPS) and Firewall (FW) module provides protection against Denial of Service (DoS) and SYN attacks. To deal with SYN attacks, KoruMail uses SYN Cookies and SYN Cache features. To manage DoS attacks, it uses various usage limitations. For example, KoruMail is able to limit the number of connections for a specified period. The SMTP IPS/FW module blocks fake IPs that want make connections more than the specified number in a selected security profile.

The module also allows administrators to define Whitelist and Blocked rules to better control the spam mails. The Rate Control feature, a subset of DoS protection system, allows 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'.



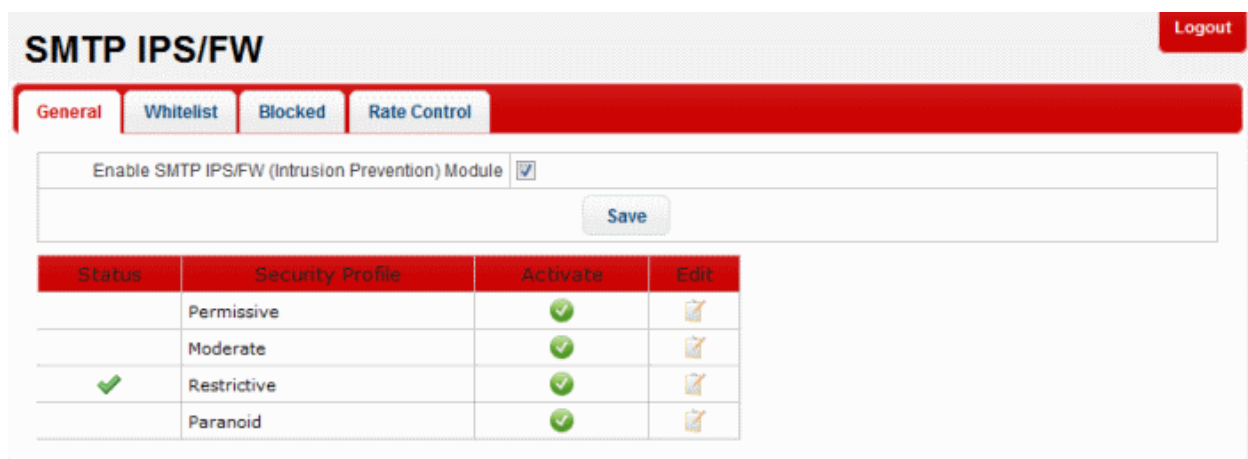
Refer to the following sections for more details.

- [SMTP IPS General Settings](#)
- [Whitelist IP Addresses](#)
- [Blocked IP Addresses](#)
- [Rate Control](#)

8.5.1 SMTP IPS General Settings

The 'General' tab in the SMTP IPS/FW module allows administrators to enable/disable the Intrusion Prevention System (IPS) and configure a security profile for KoruMail. The IPS allows KoruMail to control the number and rate 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 (Intrusion Prevention) Module: Select the check box to activate the module so as to apply the security profile.

The module has a set of predefined security profiles with different setting levels for each of the profile. The predefined profile can be edited as per the organization's requirement.


IPS General Settings – Table of Column Descriptions	
Column Header	Description
Status	Indicates whether the security profile is activated

Security Profile	The name of the security profile. The name cannot be edited. There are four security profiles - 'Permissive', 'Moderate', 'Restrictive' and 'Paranoid'. Each one has default settings provided according to their respective security levels.	
Activate	Click this button to enable a profile. Please note that only one security profile can be active at a time.	
Edit		Allows administrators to edit the parameters of a security 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.

The 'Edit IPS profile' screen will be displayed.

Logout

Edit IPS profile

Security profile	Permissive
Number of connections threshold to return SMTP 451 message	<input type="text" value="10"/>
Number of connections threshold to block remote IP	<input type="text" value="100"/>
Limit simultaneous connections	<input type="checkbox"/>
Maximum number of simultaneous sessions from a single IP address	<input type="text" value="0"/>
Limit the rate of new SMTP connections	<input type="checkbox"/>
New SMTP connection interval (seconds)	<input type="text" value="0"/>
New SMTP connection rate per interval	<input type="text" value="0"/>

Save

Restore Defaults

Cancel

IPS Profile - Table of Parameters

Parameter	Description
Security profile	The name of the predefined profile
Number of connections threshold to return SMTP 451 message	<ul style="list-style-type: none"> • Maximum number of SMTP connections before KoruMail will refuse further connections and will send out a 451 'bounce-back' email to the sender. If you wish to unblock this sender, please contact support@comodo.com to whitelist or unblock the IP.
Number of connections threshold to block remote	Maximum number of remote connections allowed before KoruMail's built in firewall



IP	blocks the exceeding connections.
Limit simultaneous connections	If enabled, instant SMTP connections are limited from a single IP as per the maximum number of simultaneous sessions allowed.
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 the 'Save' button to apply your changes.
- Click the 'Restore Defaults' button to restore the parameters to factory setting.

8.5.2 Whitelist IP Addresses

KoruMail allows administrators to add trusted network addresses to the 'Whitelist' so they will not be filtered by the SMTP IPS module.


- To open the 'Whitelist' interface, click the 'Whitelist' tab in the SMTP IPS/FW module.

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.

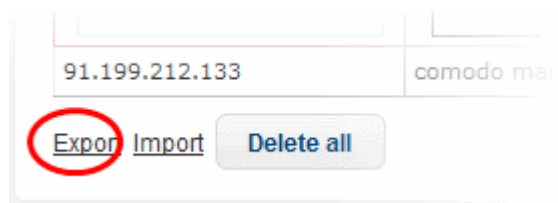
The address will be added and listed as whitelisted.

To delete a whitelisted network or IP address from the list

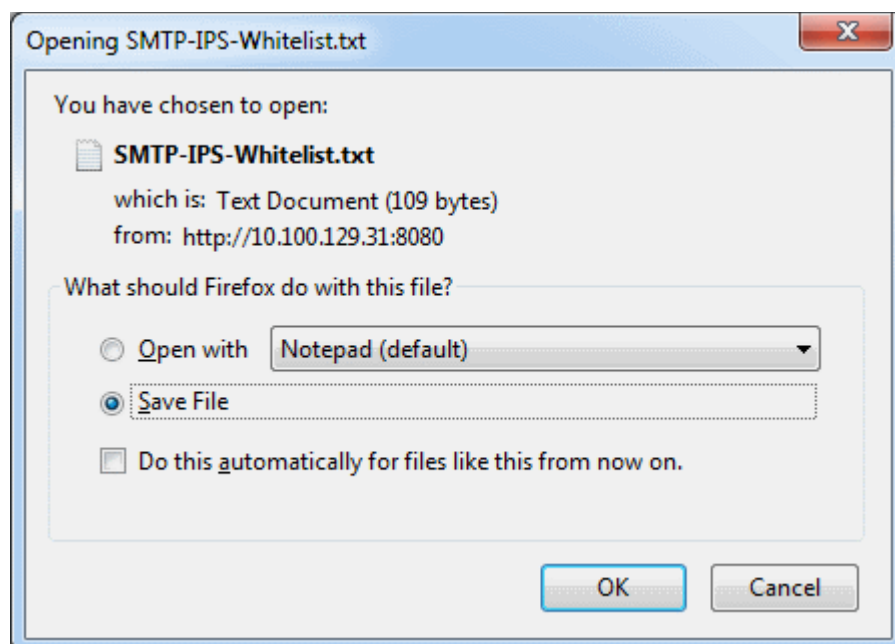
- Click the  button beside an address that you want to delete and click 'OK' in the confirmation screen
- Click the 'Delete all' button below to remove all the whitelisted addresses from the list and click 'OK' in the confirmation screen.

To export the whitelisted network or IP address details

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

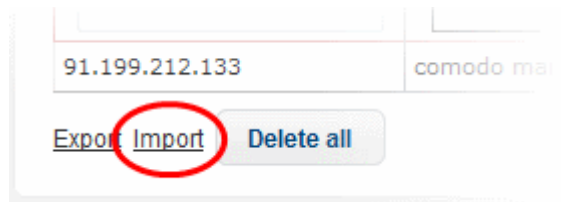


- Click 'OK' to download and save the list as a text file to your system.

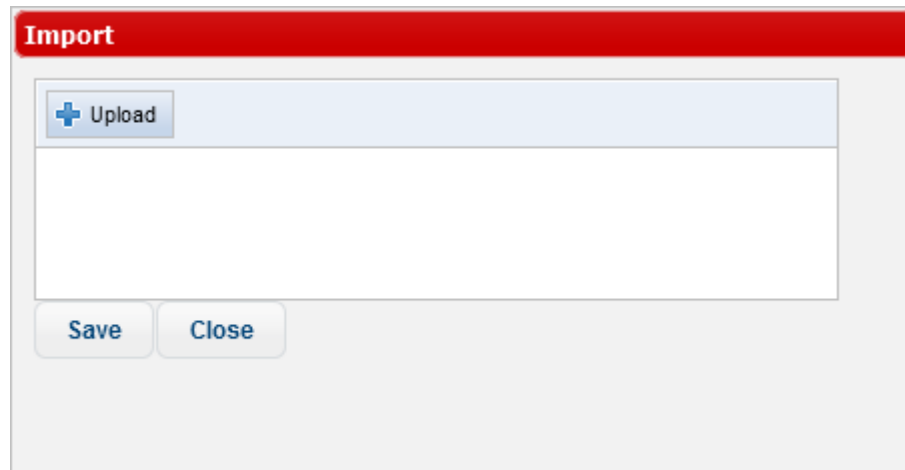


To import lists of whitelisted network or IP addresses from files

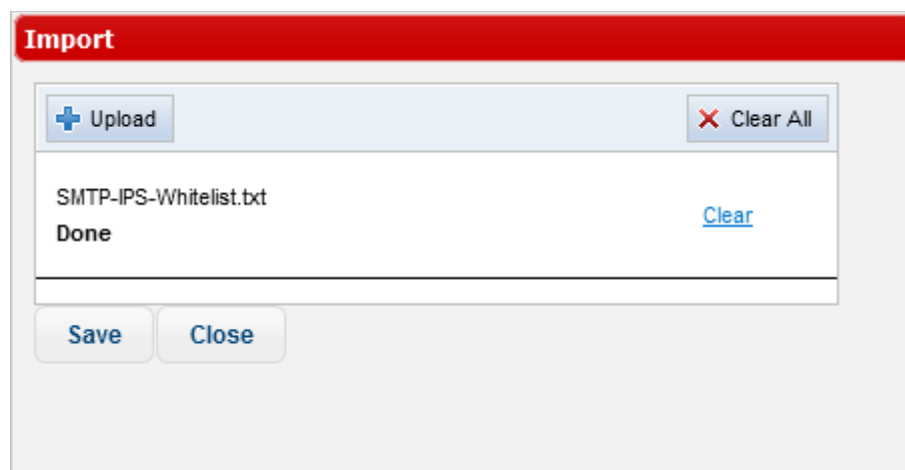
- Click the 'Import' link at the bottom of the screen



- 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.



- 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

KoruMail allows administrators to add IP addresses to blacklist so that mails from these sources never reach the SMTP level for processing. In addition to manually including the IPs to be blocked, the IPs detected by SMTP IPS module as probable spamming addresses are also added automatically and listed separately below the interface. Administrators can unblock the IP addresses by simply deleting the entry in the respective table.

- To open the 'Blocked' interface, click the 'Blocked' tab in the SMTP IPS/FW module.

SMTP IPS/FW Logout

General **Whitelist** **Blocked** **Rate Control**

User-defined block rules

IP or Network Address	Description	Action
<input type="text"/>	<input type="text"/>	
90.168.1.1/32	Probable spam	

[Export](#) [Import](#) [Delete all](#)

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)	

[Delete all](#)

The table at the top of the interface displays the details of the blocked IPs manually and the table below provides the details of IPs that were blocked automatically by SMTP IP sensor.

The interface allows administrators 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.

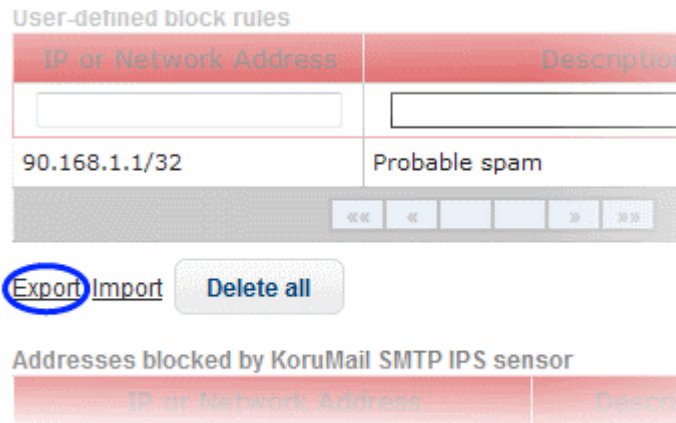
The address will be added and listed.

To delete a blocked network or IP address from the list

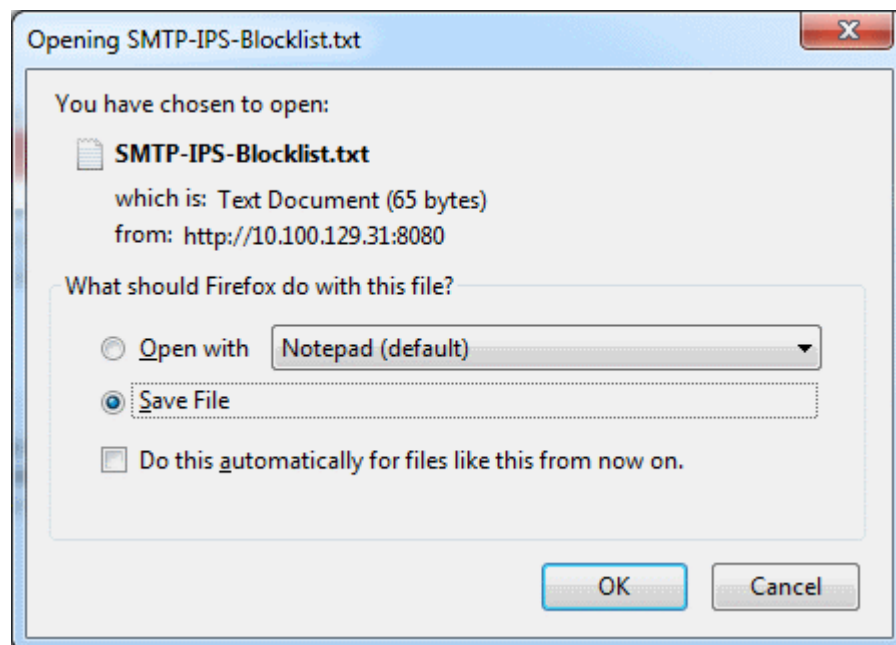
- Click the button beside an address that you want to delete and click 'OK' in the confirmation screen
- Click the 'Delete all' button below to remove all the blocked addresses from the list and click 'OK' in the confirmation screen.

To export the blocked network or IP address details

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

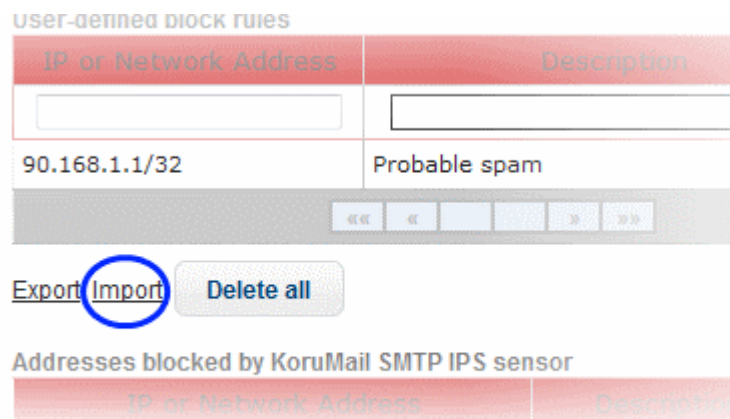


- Click 'OK' to download and save the list as a text file to your system.



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 the 'Save' button.

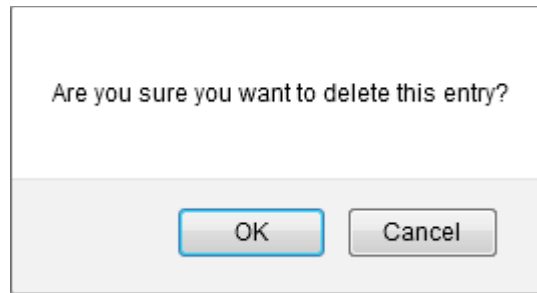
To delete an automatically blocked network or IP address by SMTP IPS sensor from the list

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.

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



8.5.4 Rate Control

The 'Rate Control' feature is a Firewall component of KoruMail that protects an Organization from spammers that send huge amounts of emails to the server in a small amount of time. The 'Rate Control' mechanism in KoruMail counts the specified number of mails categorized as Spam, Virus, LDAP and Relay originating from a source for a specified amount of time and if the value exceeds the specified threshold percentage, then the IP addresses are automatically added to blacklist.

- To open the 'Rate Control' interface, click the 'Rate Control' tab in the SMTP IPS/FW module.

The screenshot shows the 'SMTP IPS/FW' configuration page with the 'Rate Control' tab selected. The page has a 'Logout' button in the top right corner. Below the tabs, there is a table with the following columns: 'Enable', 'Number of mail', 'Check interval (in hours)', and 'Threshold (percentage)'. The table contains five rows of settings for different mail categories. A 'Save' button is located at the bottom of the table.

	Enable	Number of mail	Check interval (in hours)	Threshold (percentage)
SPAM	<input checked="" type="checkbox"/>	40	1	50
LDAP	<input type="checkbox"/>	40	1	50
RELAY	<input checked="" type="checkbox"/>	50	1	50
CERTAINLY SPAM	<input checked="" type="checkbox"/>	40	1	50
VIRUS	<input checked="" type="checkbox"/>	40	1	20

Save

Rate Control Settings – Table of Column Descriptions

Column Header	Description
Category	<p>SPAM – Mails that are categorized as spam</p> <p>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</p> <p>RELAY – IPs from which mails can be sent by users who are not available on the mail server.</p> <p>CERTAINLY SPAM – Mails that are categorized as definite spam.</p> <p>VIRUS – Mails that are categorized as with virus</p>
Enable	Activate or disable the Rate Control for a mail category
Number of mail	Enter the number of mails for a category that will be checked for the specified time in

	'Check interval' column.
Check interval (in hours)	Enter the time in hours for the specified number of mails to be checked for a category.
Threshold (percentage)	Enter or use the slider to set the threshold percentage for the 'Rate Control' to be applied for a 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 the 'Save' button to apply your changes.

8.6 Auto Whitelist

Koremail 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 the profile settings. Refer to the '**Profile Management**' section for more details about profile settings.

Auto Whitelist Settings:

- To open the 'Auto Whitelist' interface, click the 'Modules' tab on the left, then click 'Auto Whitelist'.

Auto Whitelist

Settings Auto Whitelist

Successfully Saved.

Enable Autowhitelisting	<input checked="" type="checkbox"/>
Auto Whitelist Threshold	<input type="text" value="4"/>
Auto Whitelist Maximum Day Count	<input type="text" value="31"/>

Save


- **Enable Autowhitelisting:** Enable to allow whitelisting of incoming and outgoing emails
- **Auto Whitelist Threshold:** The number of mails to sender that will be whitelisted
- Click 'Save' to apply your changes.

Please note that you can manually whitelist emails from the 'Mail logs' interface.

Auto Whitelist details

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 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. Refer to the '**Profile Management**' section for more details about profile settings.

- To open the 'DLP' interface, click the 'Modules' tab on the left, then click 'DLP'.

- 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

- **Maximum Archive Extracting Level:** 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.

Refer to the '**Profile Management**' section for more details about profile settings.

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

8.8 Promotional

KoruMail has the ability to block promotional emails sent to users on your network. If the promotional module is enabled, KoruMail will quarantine incoming mails that contain 'unsubscribe' links or contain URLs redirect to different websites.

- To open the 'Promotional' interface, click the 'Modules' tab on the left, then click 'Promotional'.

Promotional		Logout
General Settings		
Enable Promotional Module	<input checked="" type="checkbox"/>	
Host Name or IP Address *	<input type="text" value="aslab.comodo.com"/>	
Timeout *	<input type="text" value="3"/>	
Enable URL Analyser	<input type="checkbox"/>	
Save		

- **Enable Promotional Module:** Select this check box to activate this module. KoruMail will block all promotional emails from various sources if the module is activated.
- **Host Name or IP Address:** Host name or IP of the server which will check email content to determine whether a mail is promotional or not.
- **Timeout:** Time limit in seconds for checking incoming mails with the promo filter. If the time limit is exceeded, the promotional filter will not be applied.
- **Enable URL Analyser:** Will check the links in a mail to see if the target web page contains promotional or malicious content
- Click the 'Save' button 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.

[Logout](#)

Attachment Verdict System

General Settings

Successfully Saved.

Enable Attachment Verdict System	<input checked="" type="checkbox"/>
CAM Key *	<div style="background-color: #ccc; border: 1px solid #000; width: 150px; height: 20px;"></div>
Hostname *	<div style="border: 1px solid #000; padding: 2px;">valkyrie.comodo.com</div>
Malware Probability Value *	<div style="display: flex; align-items: center;"> <div style="flex: 1;"> <div style="display: flex; justify-content: space-between; padding: 0 10px;">0100</div> <div style="border: 1px solid #000; width: 100%; height: 15px; position: relative;"> <div style="background-color: #007bff; width: 46%;"></div> </div> </div> <div style="border: 1px solid #000; width: 40px; text-align: center; margin-left: 5px;">46</div> </div>
Do not analyze attachments coming from whitelisted domains	<input checked="" type="checkbox"/>
Do not analyze attachments coming from whitelisted IPs	<input checked="" type="checkbox"/>
Send files that not found in File Verdict System	<input checked="" type="checkbox"/>
Auto submission in-queue waiting time *	<div style="display: flex; align-items: center;"> <div style="flex: 1;"> <div style="display: flex; justify-content: space-between; padding: 0 10px;">15300</div> <div style="border: 1px solid #000; width: 100%; height: 15px; position: relative;"> <div style="background-color: #007bff; width: 15%;"></div> </div> </div> <div style="border: 1px solid #000; width: 40px; text-align: center; margin-left: 5px;">15</div> </div> <div style="margin-top: 5px;">s</div>
<div style="background-color: #007bff; color: white; padding: 5px 15px; border-radius: 3px; display: inline-block;">Save</div>	

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.
Malware Probability Value	<p>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.</p> <p>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.</p>

	Raising the value in this slider means KoruMail is more tolerant/less likely to class attachments as malware.
Do not analyze attachments coming from whitelisted domains	If enabled, Korumail will not analyze attachments coming from white-listed domains
Do not analyze attachments coming from whitelisted IPs	If enabled, Korumail will not analyze attachments coming from white-listed IPs
Send files that not found in File Verdict System	If enabled, Korumail will upload files rated 'Unknown', to the attachment 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.

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. To view reports of attachment verdict system, refer to **Attachment Verdict Reports**.

9 Profile Management

Profiles are collections of settings for KoruMail features such as 'Anti-virus', 'Anti-spam', 'Black List' and White List' which can be applied to added domains and/or users. There are two kinds of profiles that can be created in KoruMail – 'Incoming E-mail' and 'Outgoing E-mail'. This allows administrators the flexibility to apply different profiles for incoming mails and outgoing mails. KoruMail ships with a set of default incoming and outgoing profiles that can be only edited and cannot be deleted.

To open the 'Profiles' interface, click the 'Profile Management' tab on the left, then click 'Profiles'



Profiles

[+ Add profile](#) [Profile Membership Search](#)

Profiles for user admin

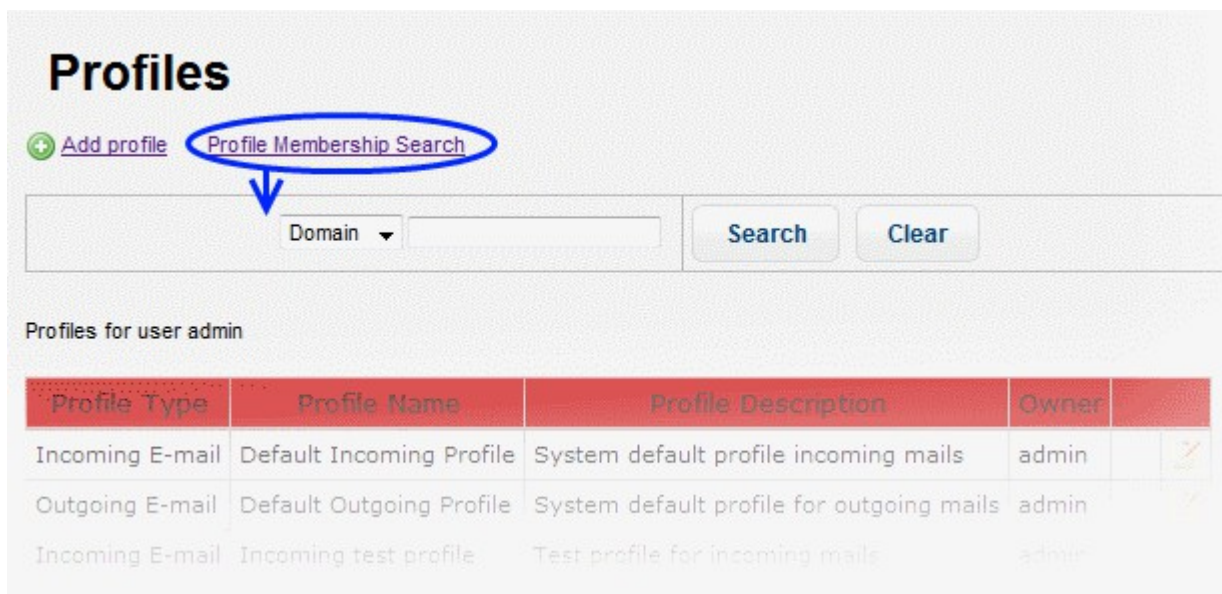
Profile Type	Profile Name	Profile Description	Owner	
Incoming E-mail	Default Incoming Profile	System default profile incoming mails	admin	
Outgoing E-mail	Default Outgoing Profile	System default profile for outgoing mails	admin	
Incoming E-mail	Incoming test 1	Test	admin	

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 will apply to the domains and / or users belonging 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

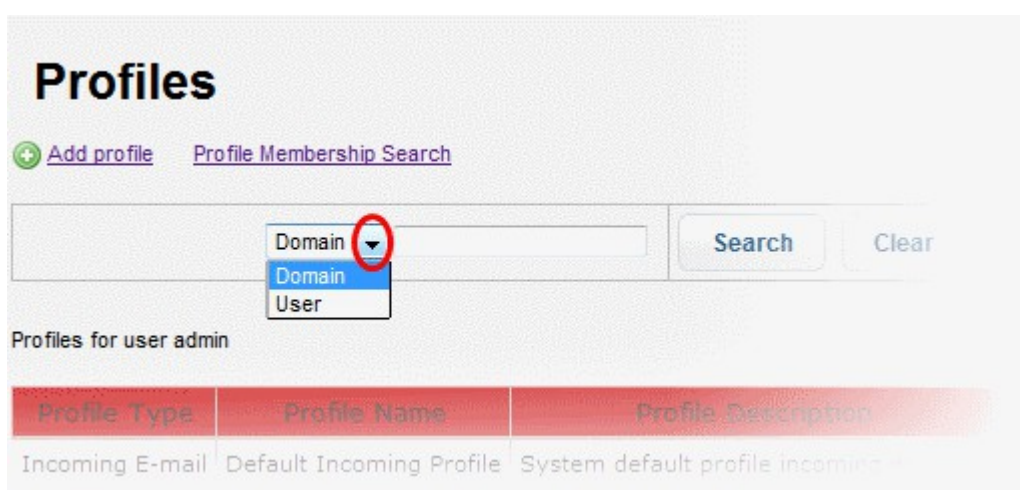
[+ Add profile](#) [Profile Membership Search](#)

Domain

Profiles for user admin

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	Incoming test profile	Test profile for incoming mails	admin	

- Select 'Domain' or 'User' from the drop-down for which you want to search the profile



Profiles

[+ Add profile](#) [Profile Membership Search](#)

Domain

Profiles for user admin

Profile Type	Profile Name	Profile Description
Incoming E-mail	Default Incoming Profile	System default profile incoming

- Enter the domain or user details and click the the 'Search' button.



The profile applied for the entered details will be displayed.

Profiles

[+ Add profile](#) [Profile Membership Search](#)

Domain

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 Configure a New Profile**
- **Edit a Profile**
- **Delete a Profile**

9.1 Adding and Configuring a New Profile

Profiles allow administrators to determine how KoruMail's anti-spam, anti-virus engine and other filtering mechanisms should behave for incoming/outgoing mails belonging to protected domains and/or users. 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).

- To add a new profile, click the 'Add profile' link in the 'Profiles' screen:

Profiles

[+ Add profile](#) [Profile Membership Search](#)

Profiles for user admin

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	Incoming test profile	Test profile for incoming mails	admin
Incoming E-mail	Test Incoming		admin
Outgoing E-mail	Test outgoing		

The 'Add New Profile' screen will be displayed:

Default Incoming Profile - Parameters

Members
Anti-virus
Anti-spam
Black List
White List
SMTP
Attachment Filter
Header Filter
Archive And Quarantine
Rules
RBL
DLP

Profile Type * Incoming E-mail
Profile Name * Incoming test 1
Description Test
Username* admin

Domain Members
You can only select domains that are not member of any profile.

Copy all
Copy
Remove
Remove All

mail.postmanllc.net
www.mail.yahoo.com

E-mail Members
You can enter any e-mail address here.

Import

Save Cancel

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 the 'Save' button

The profile will be saved and the tabs for configuring other parameters will be displayed.

Profiles

[+ Add profile](#)
[Profile Membership Search](#)

Profiles for user admin

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	Incoming test 1	Test	admin	

The interface allows administrators to configure profile parameters for:

- **Anti-virus**
- **Anti-spam**
- **Black List**
- **White List**
- **SMTP**
- **Attachment Filter**
- **Header Filter**
- **Archive and Quarantine**
- **Rules**
- **Realtime Blackhole List (RBL)**
- **Data Leak Prevention (DLP)**

Anti-virus

- Click the 'Anti-virus' tab

[Logout](#)

Add New Profile

Incoming test 1 - Parameters

Members Anti-virus Anti-spam Black List White List SMTP Attachment Filter Header Filter

Archive And Quarantine Rules RBL DLP

Settings saved successfully

Enable Anti Virus	<input checked="" type="checkbox"/>
Quarantine mails containing virus	<input checked="" type="checkbox"/>

Save
Cancel

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

Anti-spam

- Click the 'Anti-spam' tab.

[Logout](#)

Add New Profile

Incoming test 1 - Parameters

Members Anti-virus Anti-spam Black List White List SMTP Attachment Filter Header Filter

Archive And Quarantine Rules RBL DLP

Settings saved successfully

Enable Anti SPAM	<input checked="" type="checkbox"/>
Use a dedicated bayesian database for this profile	<input type="checkbox"/>
Maximum number of bytes that an e-mail enters spam filtering	<input type="text" value="1228800"/>
Certainly spam points	<input type="text" value="100"/>
Spam points	<input type="text" value="50"/>
Probable spam points	<input type="text" value="40"/>
Certainly spam action	<input type="text" value="Discard"/>
Certainly spam tag	<input type="text" value="[!] CERTAINLY SPA"/>
Spam Action	<input type="text" value="Tag"/>
Spam tag	<input type="text" value="[!] SPAM"/>
Probable spam action	<input type="text" value="Tag"/>
Probable spam tag	<input type="text" value="[!] PROBABLE SPA"/>
Spam mailbox	<input type="text" value="spam@korumail.com"/>
Quarantine mails matching policies	<input checked="" type="checkbox"/>
Quarantine Certainly SPAM Mails	<input checked="" type="checkbox"/>
Quarantine SPAM Mails	<input checked="" type="checkbox"/>
Quarantine Probable SPAM Mails	<input checked="" type="checkbox"/>

Save
Cancel

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 number of bytes 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	<p>Select the action that has to be taken for emails that are categorized as definitely spam. The options available are:</p> <ul style="list-style-type: none"> 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	<p>Select the action that has to be taken for emails that are categorized as spam. The options available are:</p> <ul style="list-style-type: none"> 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	<p>Select the action that has to be taken for emails that are categorized as probable spam. The options available are:</p> <ul style="list-style-type: none"> • 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 the 'Save' button to apply your changes.

Black List

- Click the 'Black List' tab.

Add New Profile

Logout

Incoming test 1 - Parameters

Members
Anti-virus
Anti-spam
Black List
White List
SMTP
Attachment Filter
Header Filter



Archive And Quarantine
Rules
RBL
DLP

Settings saved successfully

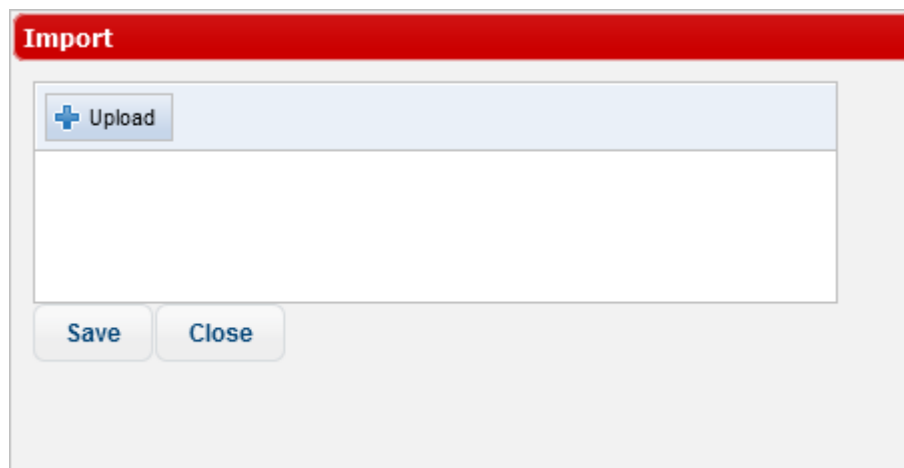
Blacklist Type	Blacklist Value	Comment	Action
IPv4 Address	0 . 0 . 0 . 0		

There are no available records.

[Export](#)
[Import](#)
[Delete all](#)
[Cancel](#)

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: <ul style="list-style-type: none"> • 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



The image shows a dialog box titled "Import" with a red header bar. Inside the dialog, there is a light blue button with a plus icon and the text "Upload". Below this button is a large, empty white rectangular area for file selection. At the bottom of the dialog, there are two buttons: "Save" and "Close".

- 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 from the files, click the 'Save' button.
- To delete a blacklist type from the list, click the  button 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 the 'White List' tab.

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: <ul style="list-style-type: none"> • IPv4 Address • IPv6 Address • E-mail

	<ul style="list-style-type: none"> • 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

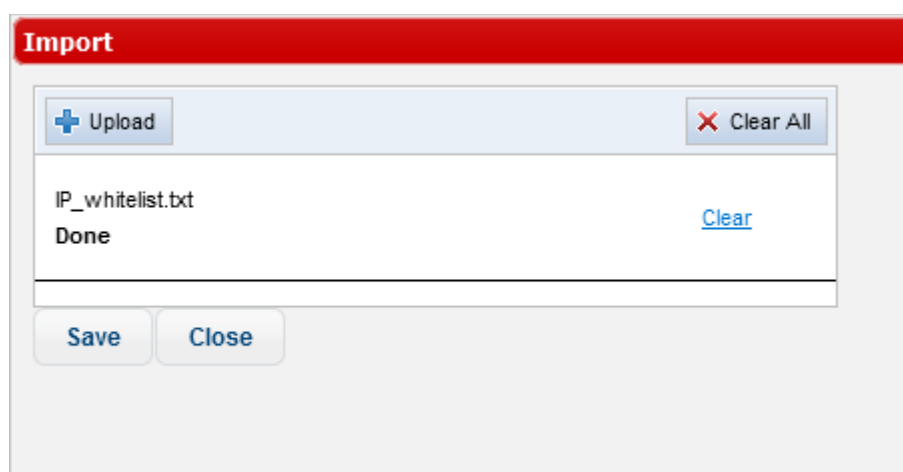
- To save the list of whitelisted sources, click the 'Export' link and save it to your system.
- To import a list of sources to be whitelisted, click the 'Import' link



The 'Import' dialog box has a red header bar with the word 'Import' in white. Below the header is a light blue bar containing a '+ Upload' button. Underneath is a large white text area. At the bottom are two buttons: 'Save' and 'Close'.


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

The file will be added.



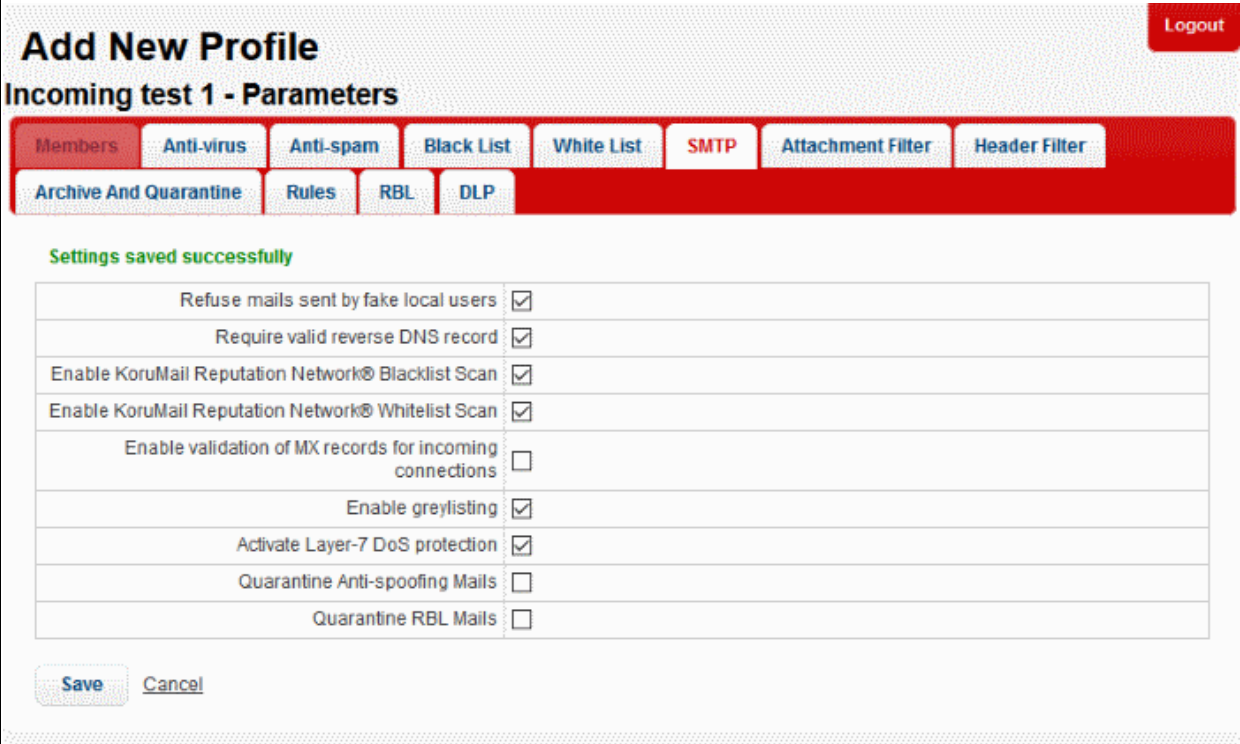
The 'Import' dialog box now shows the file 'IP_whitelist.txt' has been added. The text 'Done' appears below the filename. A 'Clear' link is visible to the right of 'Done'. The '+ Upload' button remains, and a new 'X Clear All' button has appeared in the top right corner of the file list area. The 'Save' and 'Close' buttons are still at the bottom.

- 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 the 'Save' button.
- To delete a whitelist type from the list, click the  button 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

- Click the 'SMTP' tab



Add New Profile Logout

Incoming test 1 - Parameters

Members Anti-virus Anti-spam Black List White List **SMTP** Attachment Filter Header Filter

Archive And Quarantine Rules RBL DLP

Settings saved successfully

Refuse mails sent by fake local users	<input checked="" type="checkbox"/>
Require valid reverse DNS record	<input checked="" type="checkbox"/>
Enable KoruMail Reputation Network® Blacklist Scan	<input checked="" type="checkbox"/>
Enable KoruMail Reputation Network® Whitelist Scan	<input checked="" type="checkbox"/>
Enable validation of MX records for incoming connections	<input type="checkbox"/>
Enable greylisting	<input checked="" type="checkbox"/>
Activate Layer-7 DoS protection	<input checked="" type="checkbox"/>
Quarantine Anti-spoofing Mails	<input type="checkbox"/>
Quarantine RBL Mails	<input type="checkbox"/>

[Save](#) [Cancel](#)

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 Antispoofing Mails	If enabled, the spoofing mails will be Quarantined.
Quarantine RBL Mails	If enables, the RBL mails will be Quarantined.

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

Attachment Filter

- Click the 'Attachment Filter' tab

Logout

Add New Profile

Incoming test 1 - Parameters

Members

Anti-virus

Anti-spam

Black List

White List

SMTP

Attachment Filter

Header Filter

Archive And Quarantine

Rules

RBL

DLP



Settings saved successfully

Addition		Action	
<input type="text"/>	Contains	Reject	

There are no available records.

[Export](#) [Import](#) [Delete all](#) [Cancel](#)

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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Reject – The mail will be rejected and a reject response will be sent to the sender's mail server. 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

		<p>Quarantined Email web interface.</p> <ul style="list-style-type: none"> 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




The 'Import' dialog box has a red header with the title 'Import'. Below the header is a light blue bar containing a '+ Upload' button. Underneath is a large white text area for file content. At the bottom left are 'Save' and 'Close' buttons.

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

The file will be added.



The 'Import' dialog box now shows the file 'attachment_filters.txt' added to the list. The word 'Done' appears below the filename. A 'Clear' link is visible to the right of the filename. A 'Clear All' button with a red 'X' icon is now present in the top right corner of the file list area. The '+ Upload' button remains on the left. 'Save' and 'Close' buttons are at the bottom.

- 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 the 'Save' button.
- 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 the 'Header Filter' tab

Add New Profile Logout

Incoming test 1 - Parameters

Members Anti-virus Anti-spam Black List White List SMTP Attachment Filter **Header Filter**

Archive And Quarantine Rules RBL DLP

Settings saved successfully


Header	Value	Type	Action	Action
-Choose-		Contains	Reject	

There are no available records.

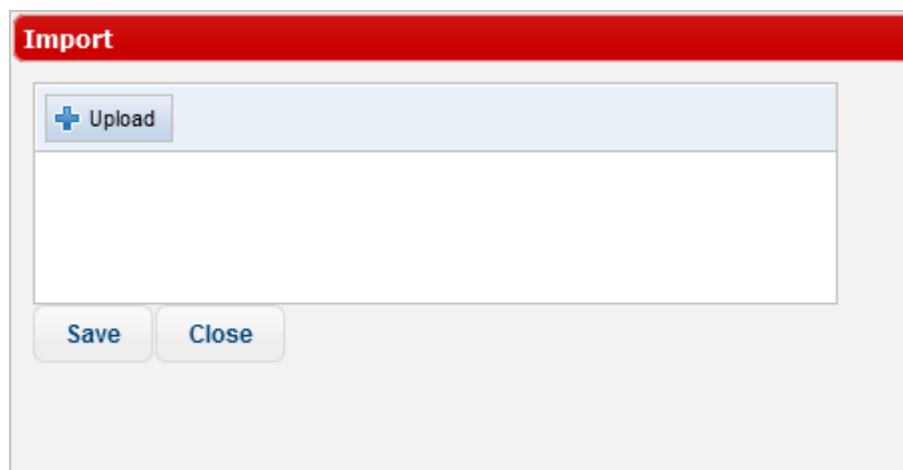
[Export](#) [Import](#) [Delete all](#) [Cancel](#)

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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Reject – The mail will be rejected and a reject command will be sent to the sender mail server. 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.
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




The 'Import' dialog box has a red header bar with the word 'Import' in white. Below the header is a light blue bar containing a '+ Upload' button. Underneath is a large white rectangular area for file selection. At the bottom of the dialog are two buttons: 'Save' and 'Close'.

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

The file will be added.



The 'Import' dialog box now shows the file 'headerrules.txt' has been added. The file name is listed in the central white area, with the word 'Done' below it. To the right of the file name is a blue 'Clear' link. In the top right corner of the file list area is a 'Clear All' button with a red 'X' icon. The '+ Upload' button remains in the top left, and 'Save' and 'Close' buttons are at the bottom.

- 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 the 'Save' button.
- 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 Logout

Incoming test 1 - Parameters

Members Anti-virus Anti-spam Black List White List SMTP Attachment Filter Header Filter

Archive And Quarantine Rules RBL DLP

Settings saved successfully

Archive method: Disk

Archive mailbox: spam@comodo.ordabirbat

Send daily quarantine report to recipients: ☐

Archive Flags

Mails with CLEAN content	<input checked="" type="checkbox"/>
Mails with CERTAINLY SPAM content	<input checked="" type="checkbox"/>
Mails with SPAM content	<input checked="" type="checkbox"/>
Mails with PROBABLE SPAM content	<input checked="" type="checkbox"/>
Mails matched by CONTENT FILTER rules	<input checked="" type="checkbox"/>
Mails containing VIRUS	<input checked="" type="checkbox"/>

[Save](#) [Cancel](#)

Profiles: Archive and Quarantine Settings - Table of Parameters

Parameter	Description
Archive method	<p>Select how the mails should be archived from the drop-down. The options available are:</p> <ul style="list-style-type: none"> 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' <p>Please note the archived and quarantined mails are removed from the disk as per the configuration done in the 'Quarantine & Archive Settings' interface.</p>
Archive mailbox	<p>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.</p>
Send daily quarantine report to recipients	<p>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.</p>
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 the 'Save' button to apply your changes.

Rules

- Click the 'Rules' tab

Add New Profile

Logout

Incoming test 1 - Parameters

Members Anti-virus Anti-spam Black List White List SMTP Attachment Filter Header Filter

Archive And Quarantine Rules RBL DLP

Settings saved successfully

Promotional Tag	<input type="text" value="[PROMO]"/>
Promotional Action	<input type="text" value="OK+TAG"/>
Enable Phishing Check	<input checked="" type="checkbox"/>
Phishing Action	<input type="text" value="Reject"/>
Phishing Tag	<input type="text" value="[PHISHING]"/>
Quarantine Phishing Mails	<input checked="" type="checkbox"/>

Rules Settings - Table of Parameters	
Parameter	Description
Promotion Tag	Promotional emails will be sent to the recipient with the a tag as entered in this field.
Promotional Action	Select the action to be performed when the condition is met for a 'Rules' setting in a promotional mail. The options available are: <ul style="list-style-type: none"> OK + TAG – The tagged mail will be sent to the recipient. Reject – The mail will be rejected and a reject response will be sent to the

	<p>sender mail server.</p> <ul style="list-style-type: none"> 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.
Enable Phishing Check	If enabled, checks for phishing emails.
Phishing Action	<p>Select the action to be performed when the condition is met for a 'Rules' setting in a phishing mail. The options available are:</p> <ul style="list-style-type: none"> OK + TAG – 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. 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.
Phishing Tag	Phishing emails will be sent to the recipient with the a tag as entered in this field.
Quarantine Phishing Emails	If enabled, phishing mails will be Quarantined.

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

Realtime Blackhole List (RBL)

- Click the 'RBL' tab

Add New Profile Logout

Incoming test 1 - Parameters

Members Anti-virus Anti-spam Black List White List SMTP Attachment Filter Header Filter

Archive And Quarantine Rules **RBL** DLP

Server Host Address	Description	Type	Enable
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
zen.spamhaus.org	spamhaus	RBL	Yes

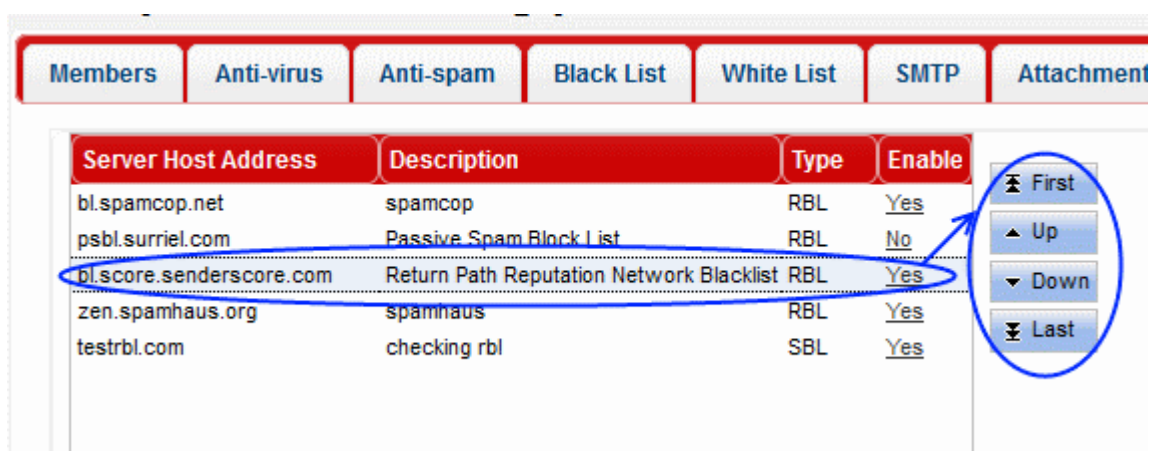
First Up Down Last

The screen displays the RBL servers that are available by default and added manually. Refer to the section '[Managing 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.



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. Refer to the section '[Data Leak Prevention](#)' for more details.

- Click the 'DLP' tab

Add New Profile Logout

Incoming test 1 - Parameters

Members Anti-virus Anti-spam Black List White List SMTP Attachment Filter Header Filter

Archive And Quarantine Rules RBL **DLP**

General Attachment List DLP Body Filter

Settings saved successfully

DLP Action	Reject
Enable DLP Quarantine	<input checked="" type="checkbox"/>
Enable DLP Notify	<input checked="" type="checkbox"/>

DLP Action

These settings determine what action should be taken if KoruMail detects a message that could present a data leak.

Add New Profile Logout

Incoming test 1 - Parameters

Members Anti-virus Anti-spam Black List White List SMTP Attachment Filter Header Filter

Archive And Quarantine Rules RBL **DLP**

General Attachment List DLP Body Filter

Settings saved successfully

DLP Action	Reject
Enable DLP Quarantine	<input checked="" type="checkbox"/>
Enable DLP Notify	<input checked="" type="checkbox"/>

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.

DLP Quarantine

- Click the 'DLP Quarantine' bar
- Select the check box beside 'Enable DLP Quarantine' to quarantine mails with data leak. Please note the setting in 'DLP Action' should be 'Discard' for mails to quarantined.

DLP Notify

- Click the 'DLP Notify' bar
- **Enable DLP Notify** – Select the check box to keep the system admin informed about DLP breaches.

Attachment List

- Click the 'Attachment List' bar

Logout

Add New Profile

Incoming test 1 - Parameters

Members
Anti-virus
Anti-spam
Black List
White List
SMTP
Attachment Filter
Header Filter

Archive And Quarantine
Rules
RBL
DLP

General
Attachment List
DLP Body Filter

Settings saved successfully

Enable Attachment List	<input checked="" type="checkbox"/>
Scan Archive Files	<input checked="" type="checkbox"/>

Enable Attachment List

Choose File Class	<div style="border: 1px solid #ccc; padding: 2px;">-Choose-</div>
<input type="checkbox"/>	File Types
<div style="background-color: #ccc; padding: 2px 10px; border-radius: 3px;">Add</div>	

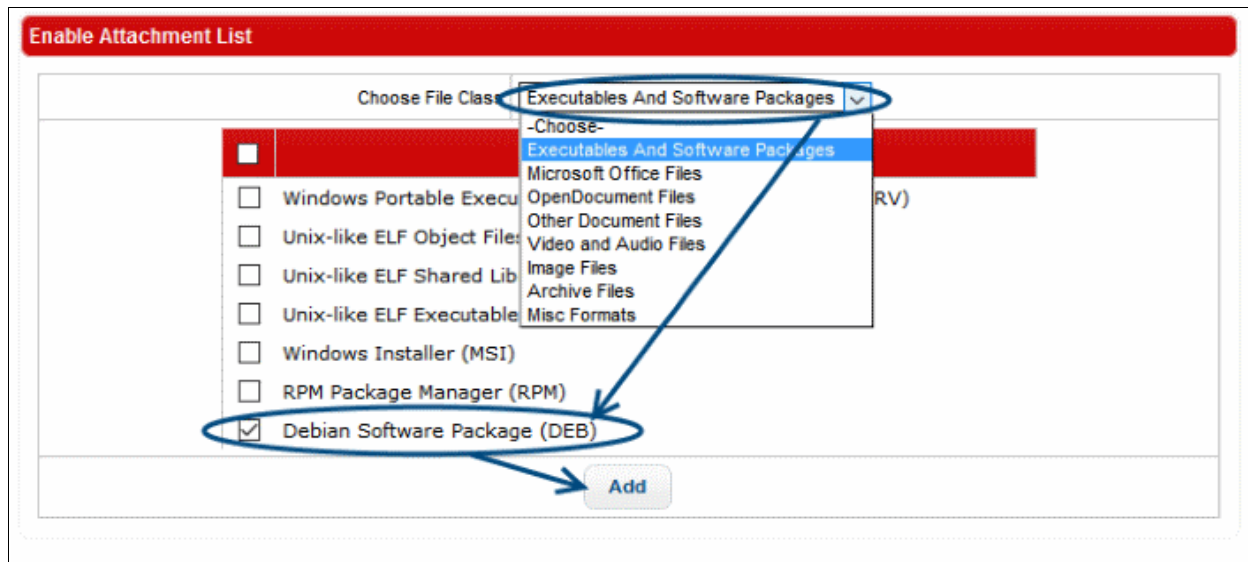
<input type="checkbox"/>	File Class Name	File Types	Status
There are no available records.			

Delete

- 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



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.

<input type="checkbox"/>	File Class Name	File Types	Status
<input type="checkbox"/>	Executables And Software Packages	Debian Software Package (DEB)	Active
<input type="checkbox"/>	Executables And Software Packages	RPM Package Manager (RPM)	Active
<input type="checkbox"/>	Executables And Software Packages	Windows Installer (MSI)	Active
Delete			




- 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

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

Add New Profile

Logout

Incoming test 1 - Parameters

Members
Anti-virus
Anti-spam
Black List
White List
SMTP
Attachment Filter
Header Filter
Archive And Quarantine
Rules
RBL
DLP










General
Attachment List
DLP Body Filter

Settings saved successfully

☐ Enable DLP Body Filter

Policy










Add

Status	Enable DLP Body Filter	Action
<input type="checkbox"/>	Credit Card	  
<input type="checkbox"/>	Email Address	  
<input type="checkbox"/>	Turkish Identity Number	  

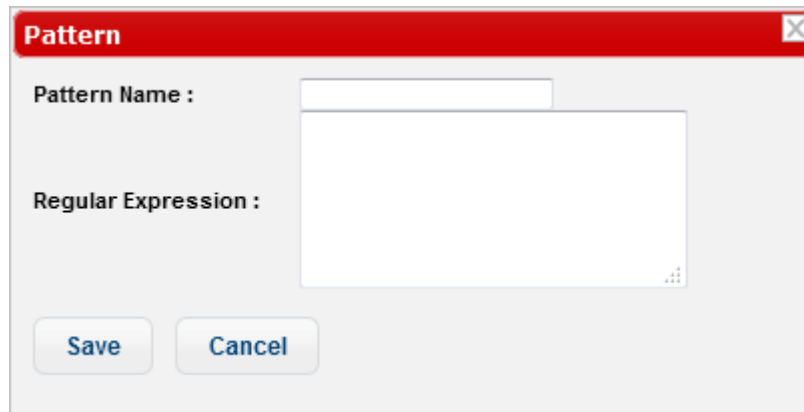
To add a new DLP body filter

- Click the 'Add' button at the top of the table

Add

Status	Enable DLP Body Filter	Action
<input type="checkbox"/>	Credit Card	  
<input type="checkbox"/>	Email Address	  
<input type="checkbox"/>	Turkish Identity Number	  

The filter 'Pattern' screen will be displayed.



A dialog box titled "Pattern" with a red header bar and a close button (X) in the top right corner. It contains two input fields: "Pattern Name :" and "Regular Expression :". Below these fields are two buttons: "Save" and "Cancel".

- **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, refer to 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

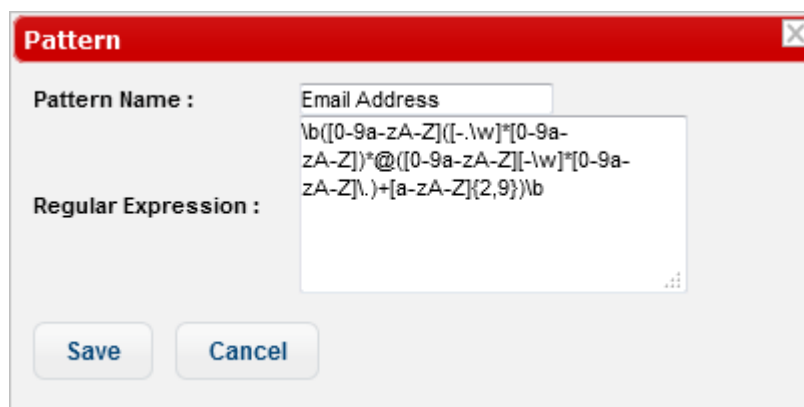


A dialog box titled "Pattern" with a red header bar and a close button (X) in the top right corner. It contains two input fields: "Pattern Name :" and "Regular Expression :". The "Pattern Name" field contains the text "Email Address". The "Regular Expression" field contains the text: `\b([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])*\b@([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])\b|.+[a-zA-Z]{2,9})\b`. Below these fields is a "Cancel" button.

- 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

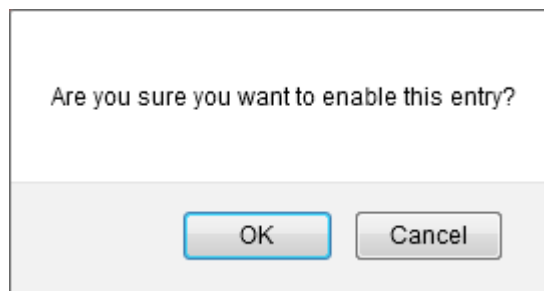


A dialog box titled "Pattern" with a red header bar and a close button (X) in the top right corner. It contains two input fields: "Pattern Name :" and "Regular Expression :". The "Pattern Name" field contains the text "Email Address". The "Regular Expression" field contains the text: `\b([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])*\b@([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])\b|.+[a-zA-Z]{2,9})\b`. Below these fields are two buttons: "Save" and "Cancel".

- 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



- Click 'OK' to confirm the deletion.





9.2 Editing a Profile

- Click the  icon beside a profile in the 'Profiles' screen that you want to edit the details

Profiles

[Add profile](#)
[Profile Membership Search](#)

Profiles for user admin

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	Incoming test 1	Test	admin	 

The 'Edit Profile' screen will be displayed.

Edit profile: Incoming test 1

Logout

Members
Anti-virus
Anti-spam
Black List
White List
SMTP
Attachment Filter
Header Filter

Archive And Quarantine
Rules
RBL
DLP

Profile Type * Incoming E-mail ▾

Profile Name * Incoming test 1

Description Test

Username * admin ▾

Domain Members

You can only select domains that are not member of any profile.

Copy all

Copy

Remove

Remove All

mail.postmanllc.net
www.mail.yahoo.com

E-mail Members

You can enter any e-mail address here.


Import

Save

Cancel

- Edit the parameters as required. The procedure is similar to adding a new profile. Refer to the section **'Adding and Configuring a New Profile'** for more details.

9.3 Deleting a Profile

- Click the  icon beside a profile in the 'Profiles' screen that you want to delete from the list.




Comodo KoruMail – Admin Guide | © 2017 Comodo Security Solutions Inc. | All rights reserved.

237

Profiles

[Add profile](#) [Profile Membership Search](#)

Profiles for user admin

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	Incoming test 1	Test	admin	

- Click 'OK' to confirm the deletion.

Are you sure you want to delete this entry?

OK Cancel

Please note if an incoming or outgoing profile is deleted, the respective default profile will apply for the domains and users.

10 Reports

The 'Reports' section in KoruMail provides comprehensive details of all mails for protected domains that were routed via KoruMail. The section is divided into six subsections, Mail Logs, SMTP Queue, Delivery Logs, SMTP-AUTH Logs, Summary Reports, Domain Reports and Attachment Verdict Reports. Each section provides a detailed report of each item, for example, the 'Mail Logs' section displays the details of mails that are categorized as Spam, Blacklisted and so on.

- 239

Mail Logs

Logout

Search

Clear

Advanced search

Subject

Sender

Recipients

IP

Result

↓

EQUALS

↓

CERTAINLY SPAM

↓

+

Search

Clear

Actions

↓

Do!

First

Previous

Page 1

1 / 250

Records per page

Next

Last

Subject	Result	Received	Sender	Recipient(s)	IP	Details
[1] CERTAINLY SPAM]Why do att	CSPAM	10.11.2016 20:21:57	bianna.monroe@lucapuncelli.com	faith@mail.postmanic.net	199.229.249.201	Score: 129.0
[1] CERTAINLY SPAM]MAJOR -SER	CSPAM	10.11.2016 09:04:31	jefferybuchana77@gmail.com	anthony@mail.postmanic.net	52.86.0.96	Koruma! global spam signature detected
[1] CERTAINLY SPAM]i- k-6821010101	CSPAM	07.11.2016 10:18:26	info@fin-neo.com	chishant@mail.postmanic.net	175.184.27.174	Koruma! global spam signature detected
[1] CERTAINLY SPAM]Acne can r	CSPAM	07.11.2016 10:01:01	chloe.blackwell@hyperionelcinc.com	faith@mail.postmanic.net	172.245.211.197	Koruma! global spam signature detected
[1] CERTAINLY SPAM]Acne can r	CSPAM	07.11.2016 09:56:50	chloe.blackwell@hyperionelcinc.com	faith@mail.postmanic.net	172.245.211.197	Koruma! global spam signature detected
[1] CERTAINLY SPAM]RE: PRIZE	CSPAM	07.11.2016 01:09:23	sanchezperezcozo@gmail.com	dorothy@mail.postmanic.net	188.40.111.74	Koruma! global spam signature detected
[1] CERTAINLY SPAM]SYRIAN REF	CSPAM	06.11.2016 09:08:00	johndmed1012@gmail.com	harry@mail.postmanic.net	52.86.0.96	Score: 167.0
[1] CERTAINLY SPAM]RE: PRIZE	CSPAM	06.11.2016 07:55:52	sanchezperezcozo@gmail.com	dorothy@mail.postmanic.net	199.254.123.22	Koruma! global spam signature detected
[1] CERTAINLY SPAM](Spam?) RE	CSPAM	06.11.2016 01:52:31	amenchan@saalem.hic	harry@mail.postmanic.net	118.140.177.62	Koruma! global spam signature detected
[1] CERTAINLY SPAM](Spam?) RE	CSPAM	05.11.2016 17:08:02	amenchan@saalem.hic	dorothy@mail.postmanic.net	118.140.177.62	Koruma! global spam signature detected
[1] CERTAINLY SPAM]SYRIAN REF	CSPAM	05.11.2016 15:58:49	johndmed1012@gmail.com	dorothy@mail.postmanic.net	52.86.0.96	Score: 179.0
[1] CERTAINLY SPAM]SYRIAN REF	CSPAM	05.11.2016 08:28:43	johndmed1012@gmail.com	bridget@mail.postmanic.net	52.86.0.96	Score: 204.0
[1] CERTAINLY SPAM]SYRIAN REF	CSPAM	04.11.2016 23:35:08	johndmed1012@gmail.com	barbara@mail.postmanic.net	52.86.0.96	Score: 173.0
[1] CERTAINLY SPAM]Reply	CSPAM	04.11.2016 22:57:32	kwamemenaah@ecobankgh.com	jessica@mail.postmanic.net	93.187.162.98	Koruma! global spam signature detected
[1] CERTAINLY SPAM]Reply	CSPAM	04.11.2016 21:22:44	kwamemenaah@ecobankgh.com	dorothy@mail.postmanic.net	93.187.162.98	Koruma! global spam signature detected
[1] CERTAINLY SPAM]SYRIAN REF	CSPAM	04.11.2016 18:35:14	johndmed1012@gmail.com	anthony@mail.postmanic.net	52.86.0.96	Score: 179.0
[1] CERTAINLY SPAM]这串200个国	CSPAM	04.11.2016 14:31:04	bts@ajyou.com	carol@mail.postmanic.net	42.51.216.11	Score: 120.0
[1] CERTAINLY SPAM]Bad Acne c	CSPAM	04.11.2016 13:40:51	maggie.medina@ningtech.com	faith@mail.postmanic.net	38.99.252.11	Koruma! global spam signature detected
[1] CERTAINLY SPAM]Bad Acne c	CSPAM	04.11.2016 13:40:51	maggie.medina@ningtech.com	faith@mail.postmanic.net	38.99.252.11	Koruma! global spam signature detected
[1] CERTAINLY SPAM]\$ Charity	CSPAM	04.11.2016 08:24:33	sarahhwool@test.com	harry@mail.postmanic.net	75.131.133.237	Koruma! global spam signature detected
[1] CERTAINLY SPAM]OFFICIAL N	CSPAM	04.11.2016 02:52:05	award@googlemail.com	dorothy@mail.postmanic.net	117.52.99.146	Koruma! global spam signature detected
[1] CERTAINLY SPAM]RE: CONGRA	CSPAM	03.11.2016 17:28:02	amenchan@saalem.hic	harry@mail.postmanic.net	220.241.212.155	Koruma! global spam signature detected
[1] CERTAINLY SPAM]ACCOUNTS:	CSPAM	03.11.2016 17:21:05	chongzhuat.com	dorothy@mail.postmanic.net	89.253.252.22	Koruma! global spam signature detected
[1] CERTAINLY SPAM]Simply the	CSPAM	03.11.2016 17:15:43	amberhobbs@fashionfestivalbd.com	faith@mail.postmanic.net	198.8.81.11	Score: 118.0
[1] CERTAINLY SPAM]Simply the	CSPAM	03.11.2016 17:15:43	amberhobbs@fashionfestivalbd.com	faith@mail.postmanic.net	198.8.81.11	Score: 118.0

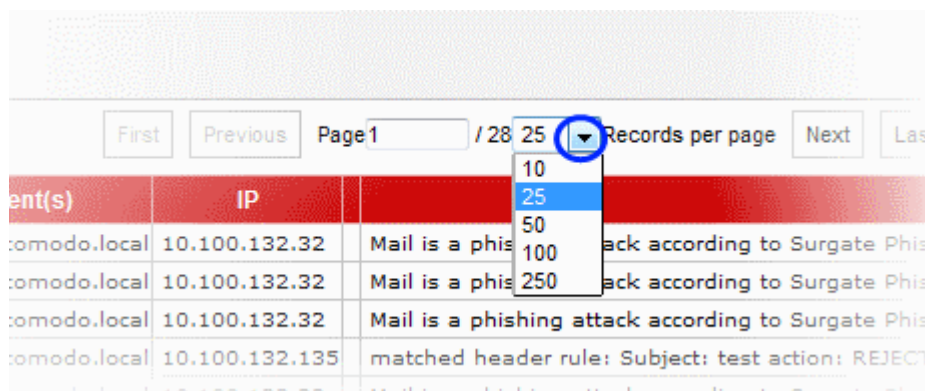
Mail Logs Report – Table of Column Descriptions

Column Header	Description
Icon	<p>Indicates the status of the mail after the filtering process. Placing your mouse cursor over an icon will show a description of the action.</p> <p> - Relayed: Indicates the mail has successfully passed the filtering process and user verified.</p> <p> - Rejected: Indicates the mail is rejected by KoruMail after the filtering process and reject message sent to the sender mail server.</p> <p> - Discarded: Indicates the mail is quarantined</p> <p> - Delayed: Indicates the source is greylisted.</p>
Subject	The content in the 'Subject' line of the mails
Result	The result for a mail after the filtering process.
Received	Date and time of email received by KoruMail
Sender	Domain details of the email sender
Recipient(s)	Domain details of the recipient(s)
IP	The IP address of the system from where the mail was sent. The next column displays the flag of the originating country.
Details	Provides the reasons why a mail is rejected, delayed and so on.

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

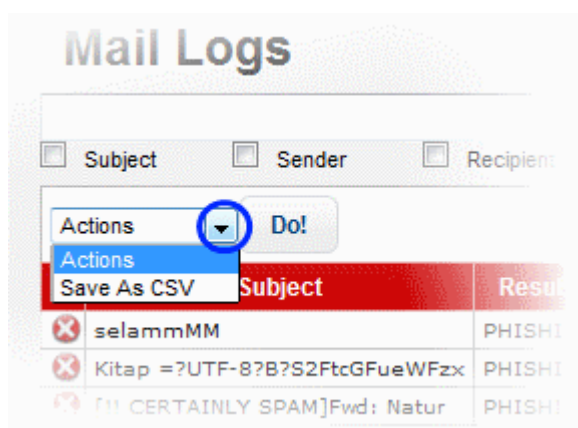
- Click the 'Records per page' drop-down



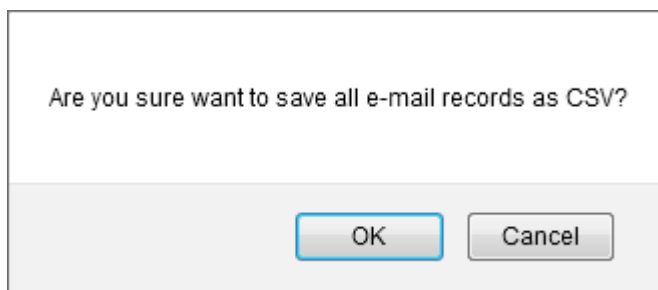
- Select the number of records per page to be displayed from the options.
- Click the 'First', 'Previous', 'Next' and 'Last' buttons to navigate to the respective pages.

To export the report to a CSV file

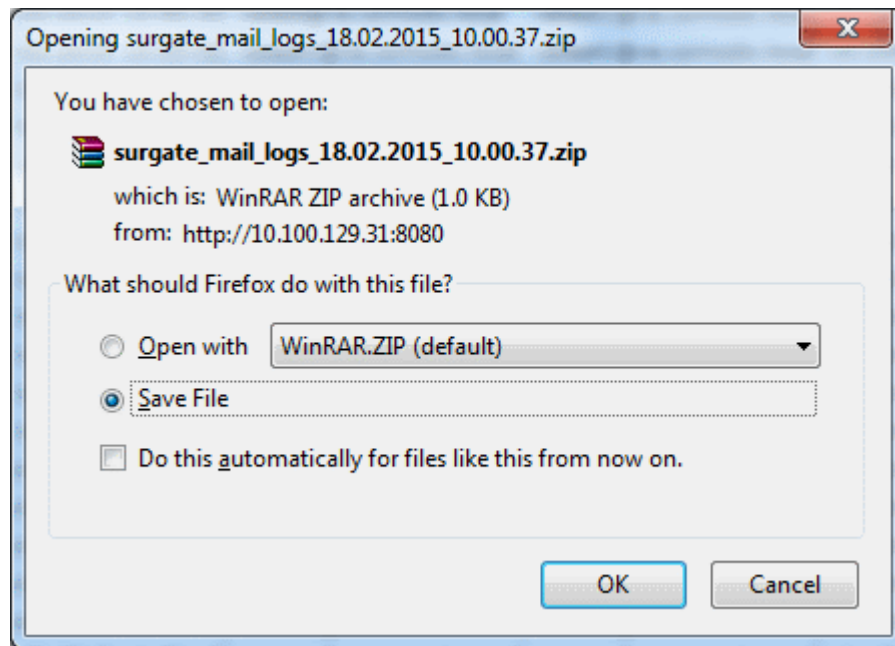
- Click the 'Actions' drop-down



- Select 'Save As CSV' and click the 'Do!' button



- Click 'OK' in the confirmation dialog.



- Click 'OK' to save the report in your system.

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

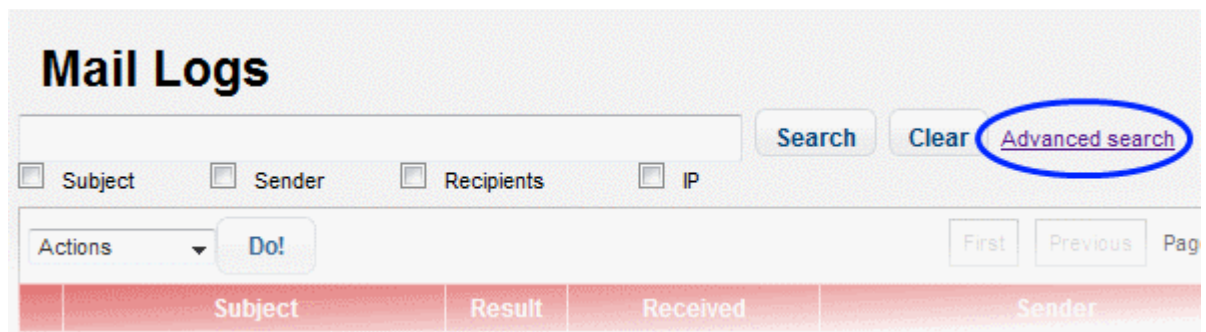
The simple search options allows you to search for a particular record or records based on 'Subject', 'Sender', 'Recipients' and / or 'IP' details only.

- 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

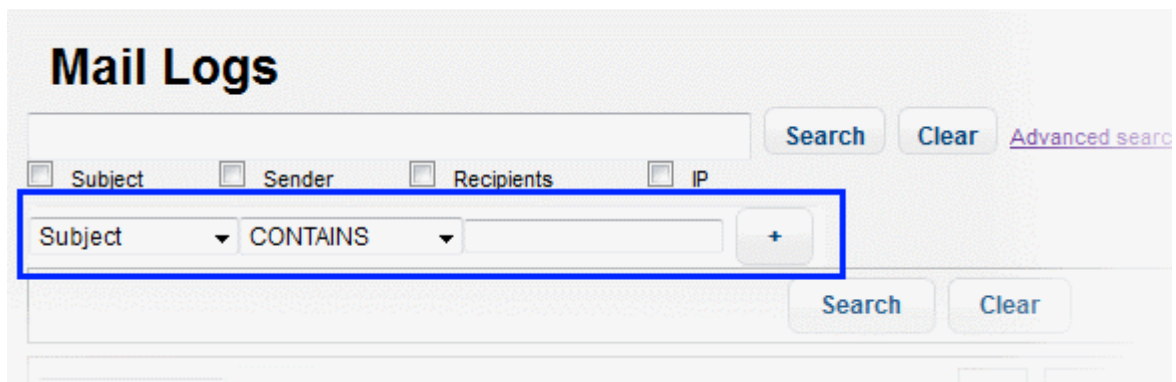
The 'Advanced Search' option allows you a more granular search by including rules and filters.

- Click the 'Advanced Search' link at the top of the screen.



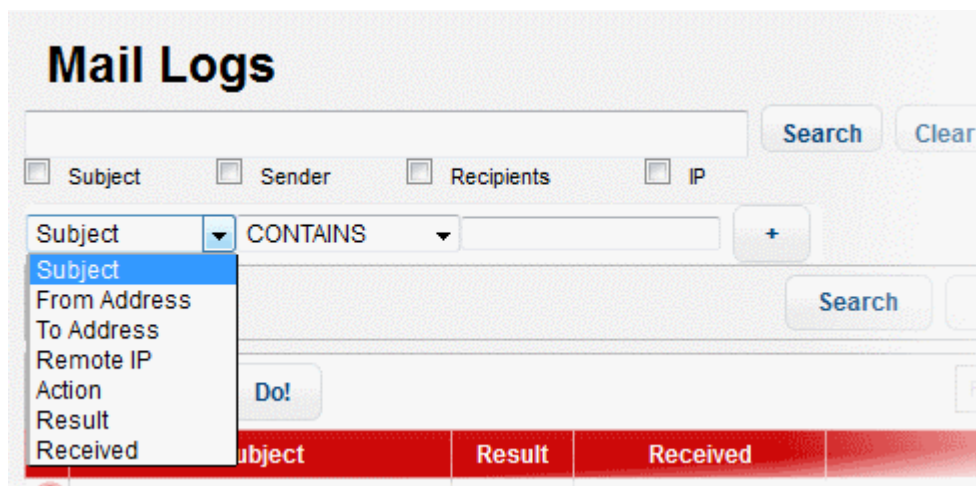
The screenshot shows the 'Mail Logs' interface. At the top, there is a search bar with a 'Search' button and a 'Clear' button. To the right of the 'Clear' button is a link labeled 'Advanced search', which is circled in blue. Below the search bar, there are checkboxes for 'Subject', 'Sender', 'Recipients', and 'IP'. Below these checkboxes is a row with a dropdown menu labeled 'Actions', a 'Do!' button, and buttons for 'First', 'Previous', and 'Page'. At the bottom, there is a table with columns labeled 'Subject', 'Result', 'Received', and 'Sender'.

The 'Advanced Search' option will be displayed.



The screenshot shows the 'Mail Logs' interface with the 'Advanced search' form. A blue box highlights the first dropdown menu, which contains the column headers 'Subject', 'Sender', 'Recipients', and 'IP'. The second dropdown menu is labeled 'CONTAINS'. There is a text input field and a '+' button next to it. Below the form, there are 'Search' and 'Clear' buttons. At the bottom, there is a table with columns labeled 'Subject', 'Result', 'Received', and 'Sender'.

The first drop-down contains the column headers that can be selected for an advanced search.



The screenshot shows the 'Mail Logs' interface with the 'Advanced search' form. The first dropdown menu is open, displaying a list of column headers: 'Subject', 'From Address', 'To Address', 'Remote IP', 'Action', 'Result', and 'Received'. The second dropdown menu is labeled 'CONTAINS'. There is a text input field and a '+' button next to it. Below the form, there are 'Search' and 'Clear' buttons. At the bottom, there is a table with columns labeled 'Subject', 'Result', 'Received', and 'Sender'.

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 screenshot shows the 'Mail Logs' search interface. At the top, there are checkboxes for 'Subject', 'Sender', 'Recipients', and 'IP'. Below these, a search bar is visible with a 'Search' button. A dropdown menu is open for the 'Subject' column, showing options: 'CONTAINS' (selected), 'EQUALS', 'NOTEQUALS', and 'NOTCONTAINS'. There is also a 'Do!' button and a '+' icon for adding more criteria.

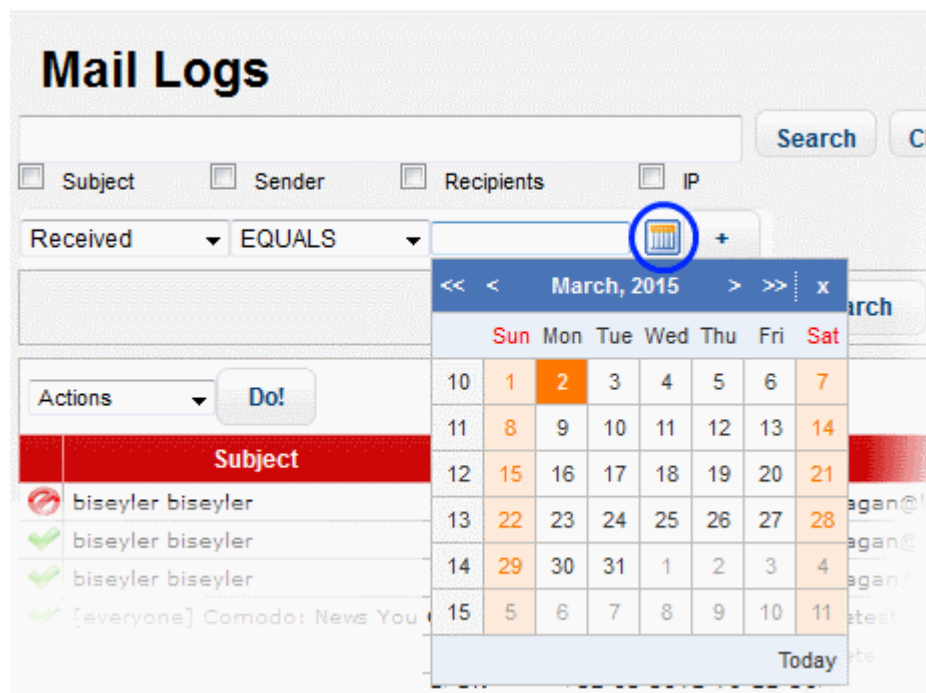
The third column allows you to enter the text/number or select from the options depending on the selection in the first column. For example, choosing 'Subject', 'From Address' or 'Remote IP' allows you to enter the text in the third column

This screenshot shows the 'Mail Logs' search interface with 'Subject' selected in the first column and 'CONTAINS' chosen in the second column. The third column contains the text 'Important'. There are 'Search' and 'Clear' buttons, and a link for 'Advanced Search'.

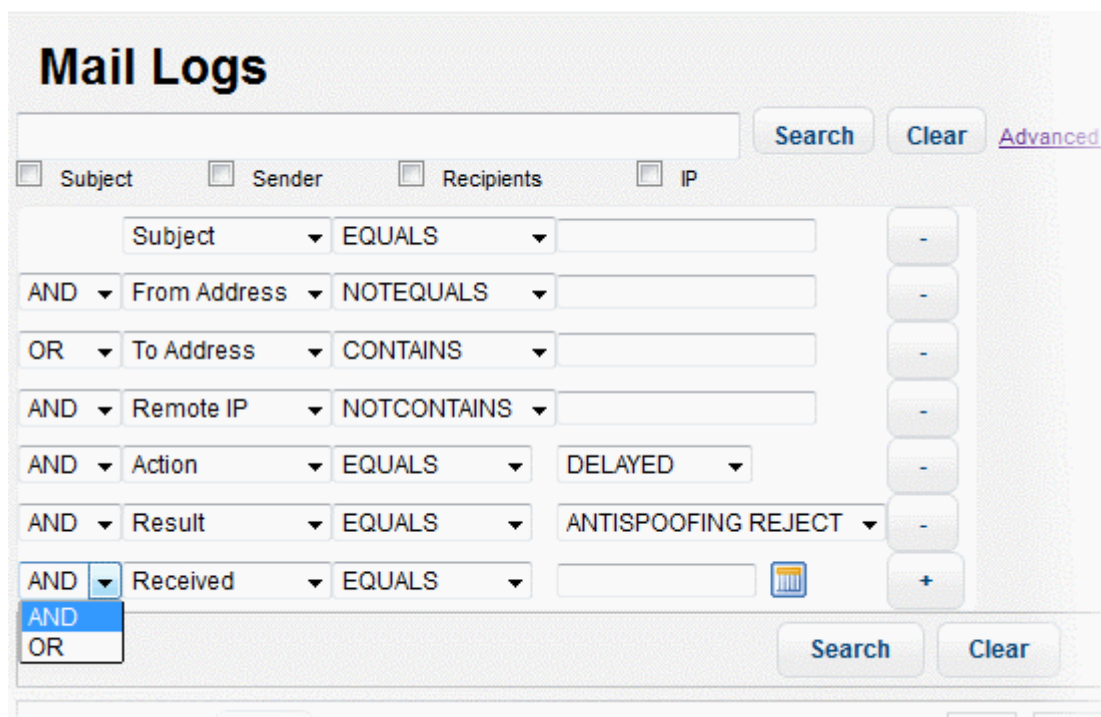
If you select 'Action' or 'Result' in the first column, then further options can be selected from the third column.

This screenshot shows the 'Mail Logs' search interface with two criteria. The first criterion has 'Action' selected in the first column, 'EQUALS' in the second, and 'DELAYED' in the third. The second criterion has 'AND' selected in the first column, 'Received' in the second, and 'EQUALS' in the third. A dropdown menu is open for the third column of the second criterion, showing options: 'DELAYED' (selected), 'DISCARDED', 'PASSED', and 'REJECTED'. There are 'Search' and 'Clear' buttons, and a link for 'Advanced Search'.

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.



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 the 'Clear' button to remove the advanced search rules.
- Click the 'Search' button 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

Not spam



Close

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.


Description

- 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.

Description

- 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.

10.2 SMTP Queue Report

The 'SMTP Queue' report provides details of mails that are queued for delivery.

- To open the queue report interface, click 'Reports' then click 'SMTP Queue'.

SMTP Queue

Search: ID equals to [] Search Clear

Re-process queue

Page 1 / 100 Records per page [] [First] [Previous] [Next] [Last]

ID	From	To	Subject	Date	Size
787108	mailer-daemon@10.108.51.98	postmaster@10.108.51.98	failure notice	13 Nov 2016 17:00:05 -0000	7.87 KB
785107	mailer-daemon@10.108.51.98	bounce-mc.us9_36021329.2006057-faith@mail.postmanllc.net@mail161.suw18.rsgsv.net	failure notice	14 Nov 2016 01:00:18 -0000	63.67 KB
785112	mailer-daemon@10.108.51.98	thepaucitypaths@gmail.com	failure notice	14 Nov 2016 01:17:23 -0000	3.77 KB
787241	mailer-daemon@10.108.51.98	info@agc.com	failure notice	13 Nov 2016 13:38:03 -0000	14.00 KB
785106	mailer-daemon@10.108.51.98	root@10.108.51.98	failure notice	14 Nov 2016 04:00:03 -0000	22.79 KB
787130	mailer-daemon@10.108.51.98	postmaster@10.108.51.98	failure notice	14 Nov 2016 05:00:04 -0000	17.56 KB
787154	mailer-daemon@10.108.51.98	gordon.jackson65@gmail.com	failure notice	13 Nov 2016 13:27:28 -0000	5.63 KB
787248	mailer-daemon@10.108.51.98	root@10.108.51.98	failure notice	13 Nov 2016 16:00:04 -0000	14.35 KB

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	Subject of the email in SMTP queue
Date	Date and time that the mail was sent
Size	Size of the email in 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.

To configure the number of records to be displayed per page

- Click the 'Records per page' drop-down

First Previous Page 1 / 100 Records per page [100] Next Last

10
25
50
100
250
500

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.

Message Statuses in SMTP Queue

- **Total messages:** Displays the total number of messages in the SMTP queue.
- **Messages with local recipients:** Displays the number of messages with the local recipients.
- **Messages with remote recipients:** Displays the number of messages with the remote recipients.
- **Messages with bounces:** Displays the number of mails that are bounced.
- **Messages with in preprocess:** Displays the number of mails with in preprocess

10.3 Delivery Logs Report

While 'Mails Logs' provide a report of all incoming and outgoing mails irrespective of whether mails are accepted by mail servers or not, 'Delivery Logs' provide a report of all incoming and outgoing mails that are only accepted by mail servers.

- To open the 'Delivery Logs' interface, click 'Reports' and then click 'Delivery Logs'

Delivery Logs						Logout
<input type="checkbox"/> Sender <input type="checkbox"/> Recipients <input type="checkbox"/> IP		Search	Clear	Advanced search		
<div> First Previous Page 1 / 65 25 Records per page Next Last </div>						
Result	Received	Sender	Recipient(s)	IP	Details	
✓	18.02.2015 13:59:23	ozcan.ilhan@comodo.com	vetest1@ve.comodo.local	10.100.129.54	250 ok 1424260762 qp 23974 by mail.surmail.com	
✓	18.02.2015 13:55:38	ozcan.ilhan@comodo.com	vetest1@ve.comodo.local	10.100.129.54	250 ok 1424260537 qp 22856 by mail.surmail.com	
✓	18.02.2015 13:50:09	ozcan.ilhan@comodo.com	vetest1@ve.comodo.local	10.100.129.54	250 ok 1424260208 qp 21040 by mail.surmail.com	
✗	18.02.2015 13:44:06	anonymous@surgategw.comodo.com	fiatliena@gmail.com		Sorry, I couldn't find any host by that name. (#4.1.2)	
✓	18.02.2015 13:42:14	ozcan.ilhan@comodo.com	vetest1@ve.comodo.local	10.100.129.54	250 ok 1424259733 qp 18327 by mail.surmail.com	
✗	18.02.2015 13:41:13	anonymous@surgategw.comodo.com	fiatliena@gmail.com		Sorry, I couldn't find any host by that name. (#4.1.2)	
✗	18.02.2015 13:40:06	anonymous@surgategw.comodo.com	fiatliena@gmail.com		Sorry, I couldn't find any host by that name. (#4.1.2)	
✓	18.02.2015 13:29:50	vetest1@ve.comodo.local	vetest1@ve.comodo.local	10.100.129.54	250 ok 1424258989 qp 14128 by mail.surmail.com	
✓	18.02.2015 13:29:09	vetest1@ve.comodo.local	vetest1@ve.comodo.local	10.100.129.54	250 ok 1424258948 qp 13924 by mail.surmail.com	
✓	18.02.2015 13:28:03	vetest1@ve.comodo.local	vetest1@ve.comodo.local	10.100.129.54	250 ok 1424258882 qp 13590 by mail.surmail.com	
✗	18.02.2015 13:20:06	anonymous@surgategw.comodo.com	fiatliena@gmail.com		Sorry, I couldn't find any host by that name. (#4.1.2)	
✗	18.02.2015 13:13:26	anonymous@surgategw.comodo.com	fiatliena@gmail.com		Sorry, I couldn't find any host by that name. (#4.1.2)	
✓	06.02.2015 11:06:25	fatih.erhan@comodo.com	vetest1@ve.comodo.local	10.100.129.54	250 ok 1423213584 qp 30370 by mail.surmail.com	
✗	06.02.2015 11:06:25	fatih.erhan@comodo.com	vetest1@ve.comodo.local	10.100.129.54	250 ok 1423213584 qp 30371 by mail.surmail.com	
✗	06.02.2015 04:09:26	anonymous@surgategw.comodo.com	anonymous@surgategw.comodo.com	127.0.0.1	554 too many hops, this message is looping (#5.4.6)	
✓	06.02.2015 04:09:23	anonymous@surgategw.comodo.com	anonymous@surgategw.comodo.com	127.0.0.1	250 OK 1423188563 queuepid 38117	
✗	06.02.2015 04:02:18	anonymous@surgategw.comodo.com	anonymous@surgategw.comodo.com	127.0.0.1	451 temporary failure while processing your mail, please try again	
✓	06.02.2015 04:02:15	anonymous@surgategw.comodo.com	anonymous@surgategw.comodo.com	127.0.0.1	250 OK 1423188135 queuepid 36632	
✗	06.02.2015 03:55:07	anonymous@surgategw.comodo.com	anonymous@surgategw.comodo.com	127.0.0.1	451 temporary failure while processing your mail, please try again	
✓	06.02.2015 03:54:56	anonymous@surgategw.comodo.com	anonymous@surgategw.comodo.com	127.0.0.1	250 OK 1423187696 queuepid 34813	
✓	06.02.2015 03:54:44	anonymous@surgategw.comodo.com	anonymous@surgategw.comodo.com	127.0.0.1	250 OK 1423187684 queuepid 34803	
✗	06.02.2015 03:21:16	anonymous@surgategw.comodo.com	anonymous@surgategw.comodo.com		Sorry, I couldn't find any host by that name. (#4.1.2)	
✗	06.02.2015 03:01:03	anonymous@surgategw.comodo.com	anonymous@surgategw.comodo.com	127.0.0.1	451 temporary failure while processing your mail, please try again	
✗	06.02.2015 02:54:24	anonymous@surgategw.comodo.com	anonymous@surgategw.comodo.com	127.0.0.1	451 temporary failure while processing your mail, please try again	
✓	06.02.2015 02:54:13	anonymous@surgategw.comodo.com	anonymous@surgategw.comodo.com	127.0.0.1	250 OK 1423184053 queuepid 21653	
<div> First Previous Page 1 / 65 25 Records per page Next Last </div>						

Delivery Logs Report – Table of Column Descriptions

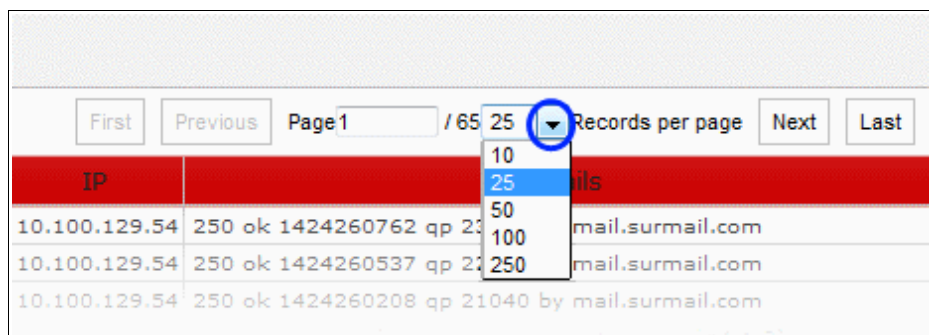
Column Header	Description
Result	<p>Indicates the status of the mail processed by mail server. The tool tip on hovering the mouse cursor over an icon displays the action.</p> <p>✓ - Success: Indicates the mail has been successfully delivered to the recipient.</p> <p>✗ - Permanent Error: Indicates the mail server failed to deliver the mail to the recipient.</p>

	🔔 - Temporary: Indicates it is temporary error and the server will try again to deliver.
Received	Date and time of email received by KoruMail
Sender	Domain details of the email sender
Recipient(s)	Domain details of the recipient(s)
IP	The details of the recipient's IP address
Details	Provides details 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



- 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-AUTHLogs 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:
 Search Clear

Page 1 / 38 100 Records per page Next Last

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 IP address of the SMTP mail client
Date	The date and time of the log in event

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

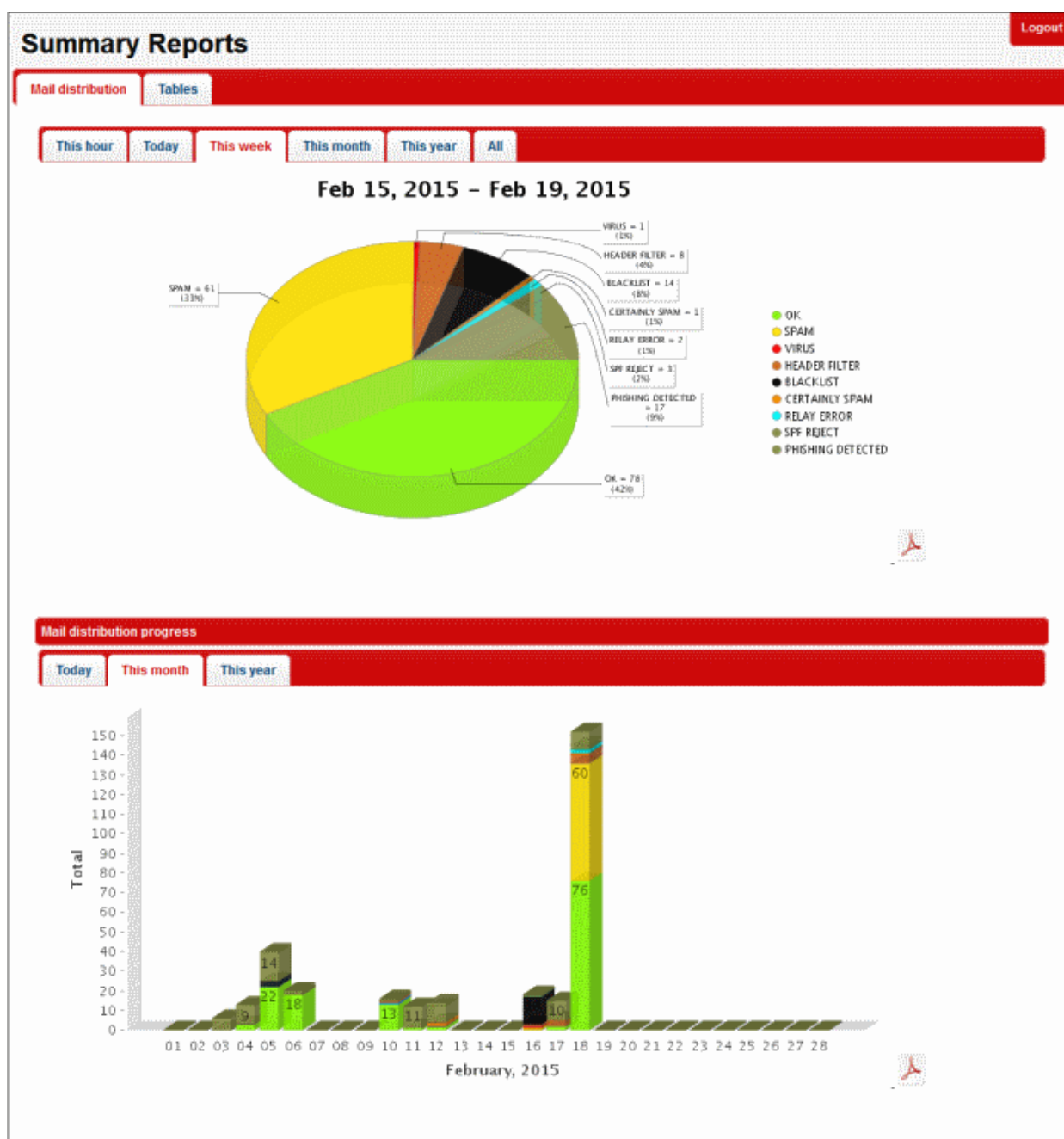
User:
 IP:
 Date From:
 Date To:
 Result:
 Search Clear

- 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**

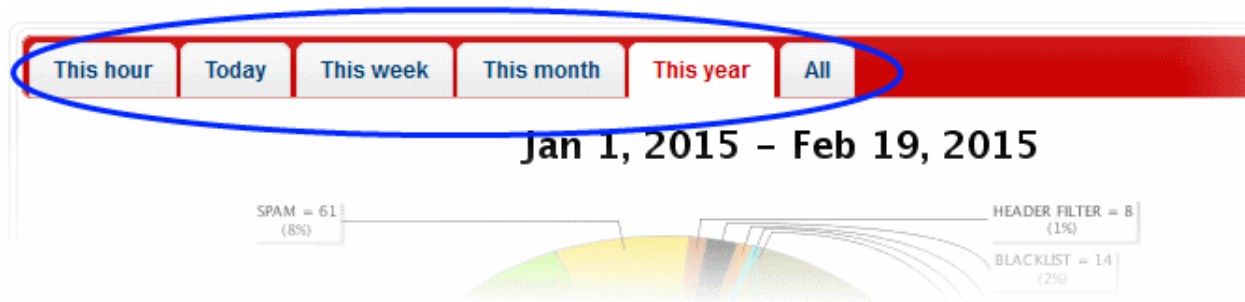
To view and download the report in graphical format

- Click the 'Mail Distribution' tab at the top

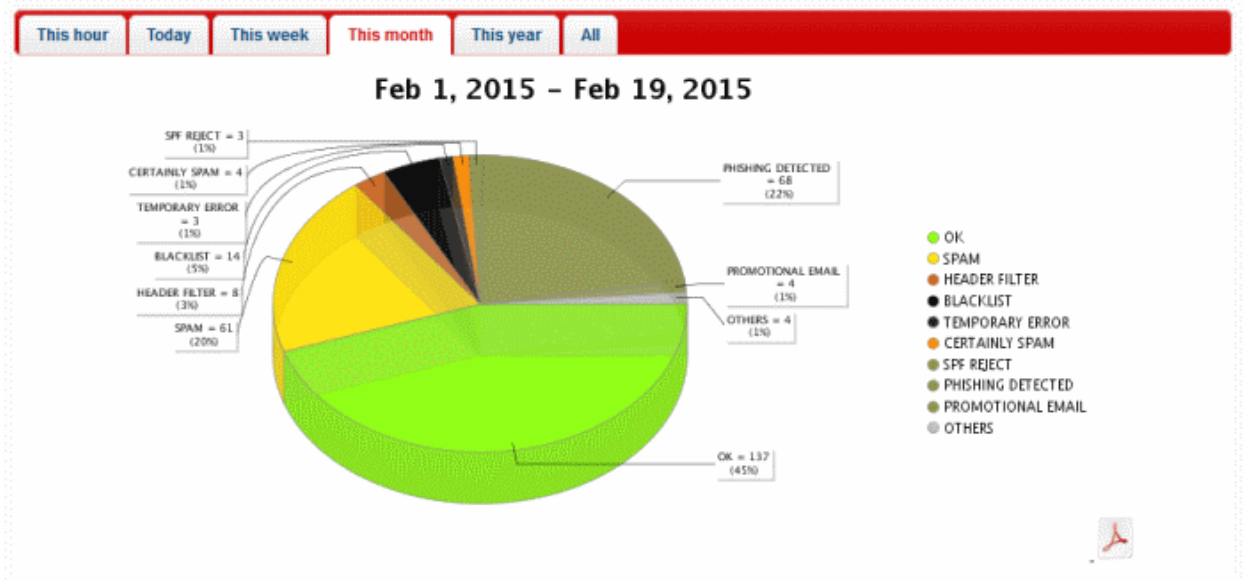
The results in **pie chart** format at the top and **bar chart** format at the bottom will be displayed.

- To view the results for a particular period, click the relevant tabs at the top.

Pie Chart

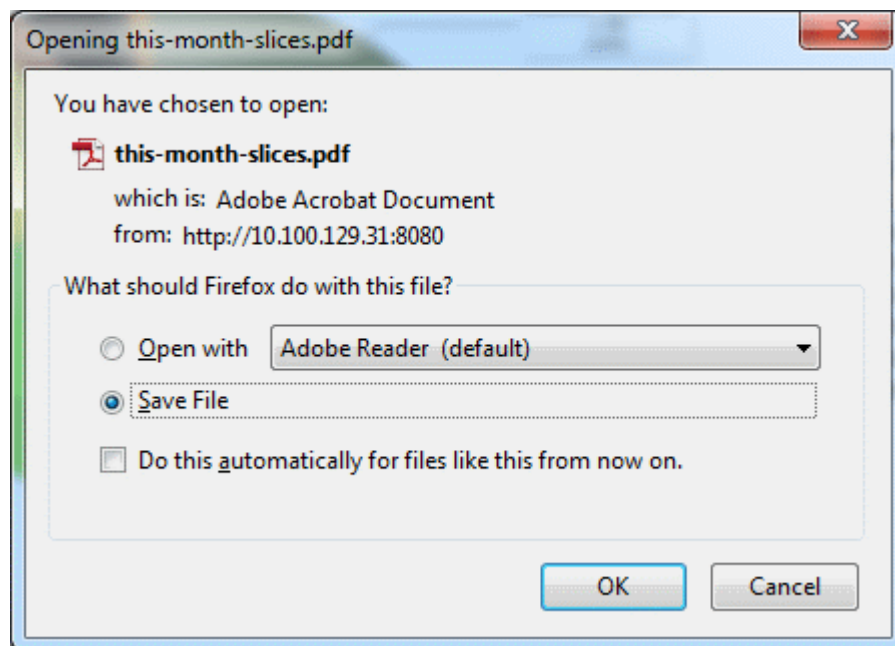


- Click the desired period for which you want to view and download the report. The available periods are hourly, daily, weekly, monthly, yearly and from the time of KoruMail installation.



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 



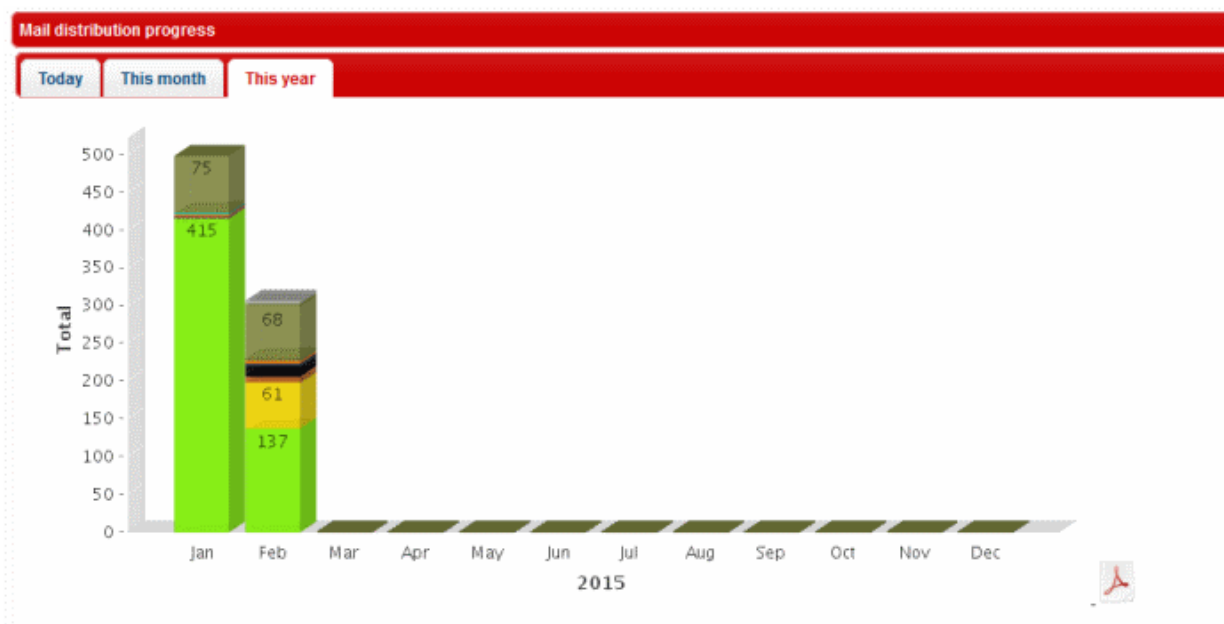
- Click 'OK' to download the report in PDF format.

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.

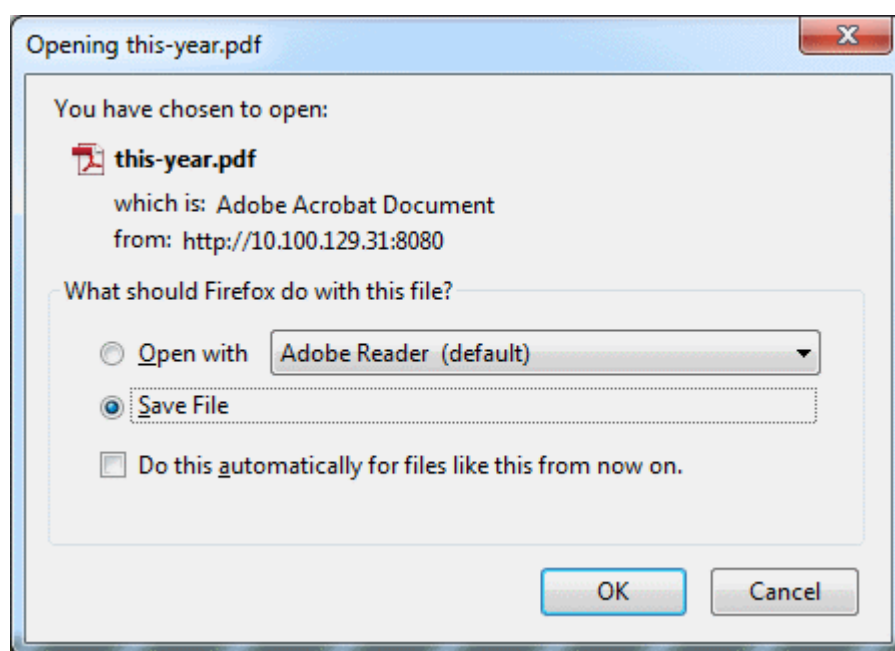


The report for the selected period will be displayed.



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



- Click 'OK' to download the report in PDF format.

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.

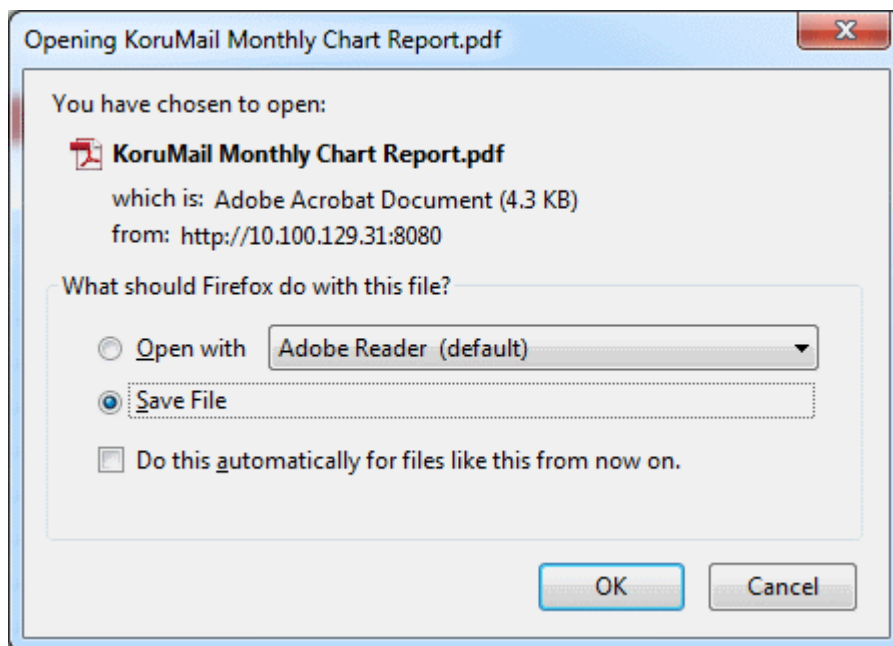
The screenshot shows the 'Summary Reports' section with the 'Tables' tab selected. The 'This month' button is highlighted. Below the buttons, there is a 'Refresh' button and two icons for downloading the report: a PDF icon and a CSV icon. A table is displayed with three columns: 'Category', 'Count', and 'Percent(%)'. The table contains data for various mail categories.

Category	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.

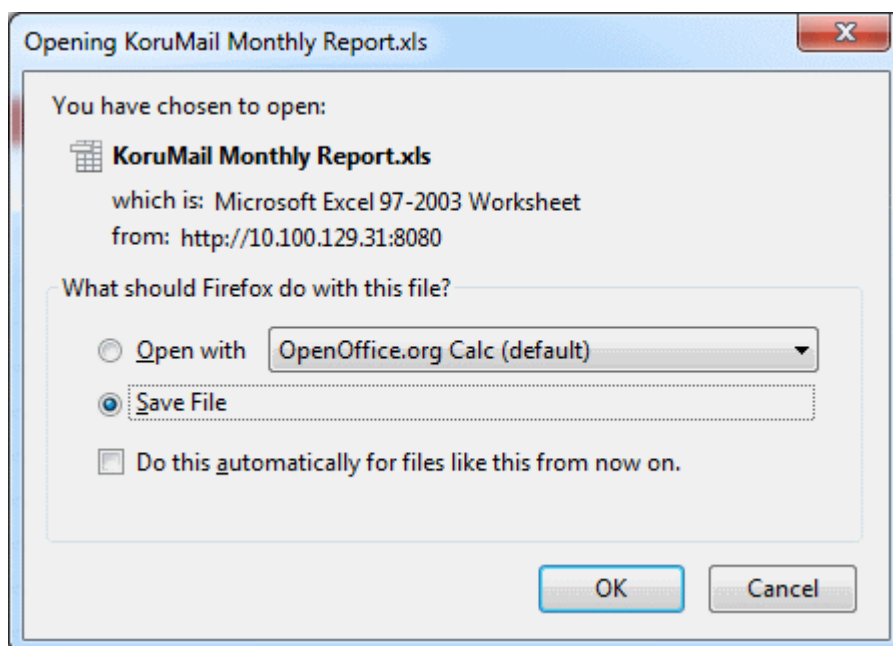
- To download the report in PDF format, click the PDF icon





- Click 'OK' to download the report in PDF format.

- To download the report in XLS (spreadsheet) format, click the XLS icon



- Click 'OK' to download the report in XLS format.

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.



Summary Reports Logout

Mail distribution **Tables**

This hour **Today** **This week** **This month** **This year** **All** **Custom Reports**

Show records between selected dates

  **Show**

Count	Percent(%)
There are no available records.	



- Click on the fields or calendar icon and select the period from the calendar.

Summary Reports

Mail distribution **Tables**

This hour **Today** **This week** **This month** **This year** **All** **Custom**

Show records between selected dates

  **Show**

<< < February, 2015 > >> x


Sun	Mon	Tue	Wed	Thu	Fri	Sat
6	1	2	3	4	5	7
7	8	9	10	11	12	14
8	15	16	17	18	19	21
9	22	23	24	25	26	28
10	1	2	3	4	5	7
11	8	9	10	11	12	14
Today						


Count	Percent(%)
There are no available records.	

- Click the 'Show' button after selecting the custom period.



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.

Mail distribution

Tables

This hour

Today

This week

This month

This year

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
2	4	5	6	7	8	9
3	11	12	13	14	15	16
4	18	19	20	21	22	23
5	25	26	27	28	29	30
6	1	2	3	4	5	6
2015-01-01	2015-01-02	2015-01-03	2015-01-04	2015-01-05	2015-01-06	2015-01-07

Clean

Today

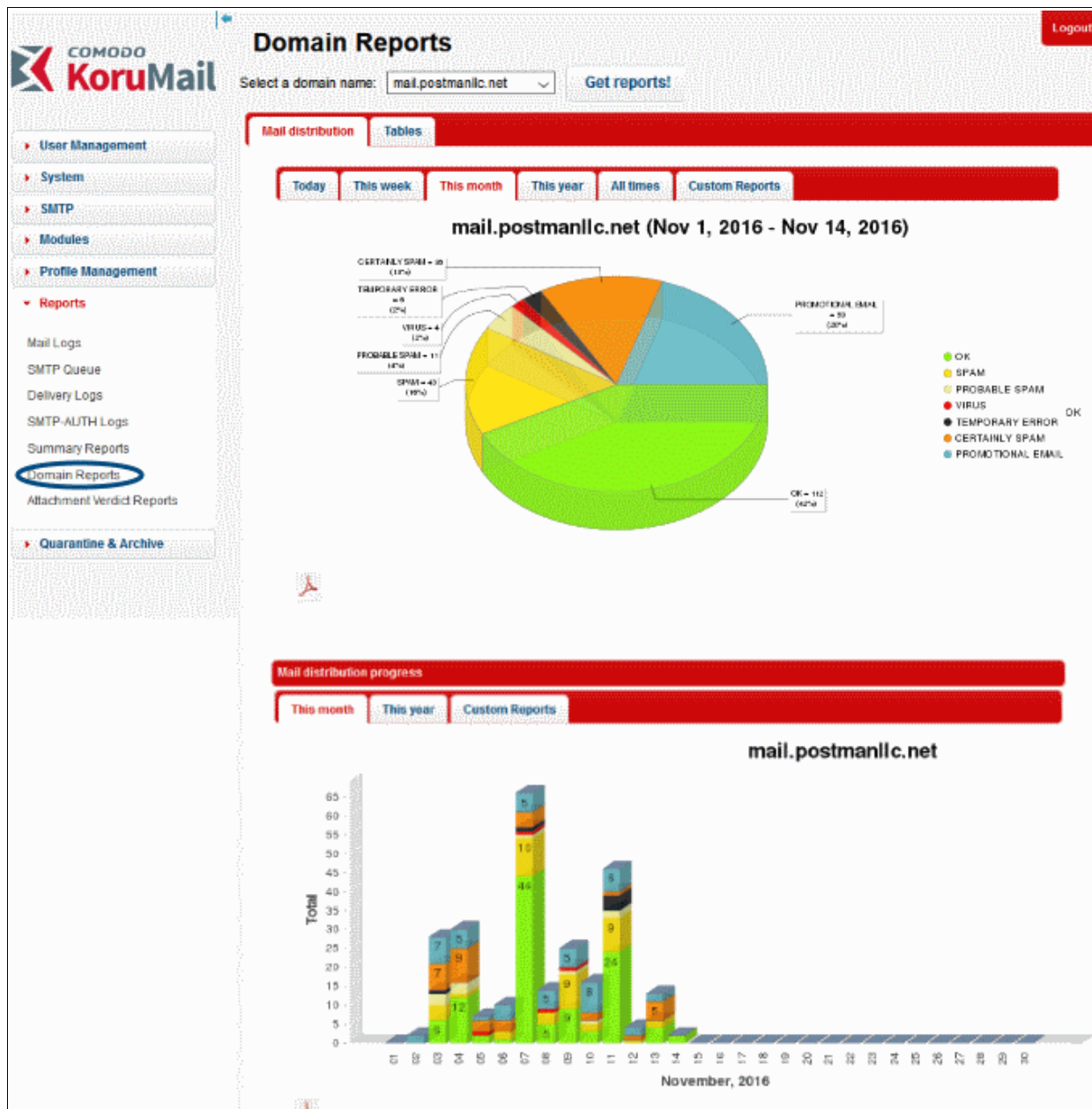
Count
552
143
61
14
8
7

CSPAM

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':



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:

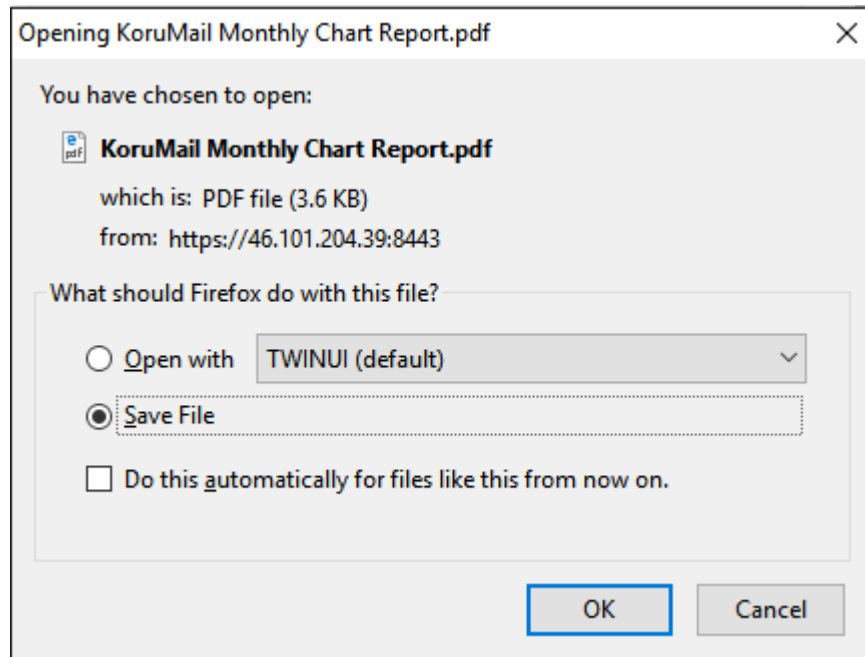
The 'Mail Distribution' chart categorizes mails sent/received on the specified domain according to mail category. Categories include 'OK', 'Spam', 'Probable Spam', 'Virus' etc. Use the tabs above the chart to change the time-period

covered by the chart. Choices include 'Today', 'This Week', 'This Month', 'This Year' and 'All Time'.

Mail Distribution Progress:

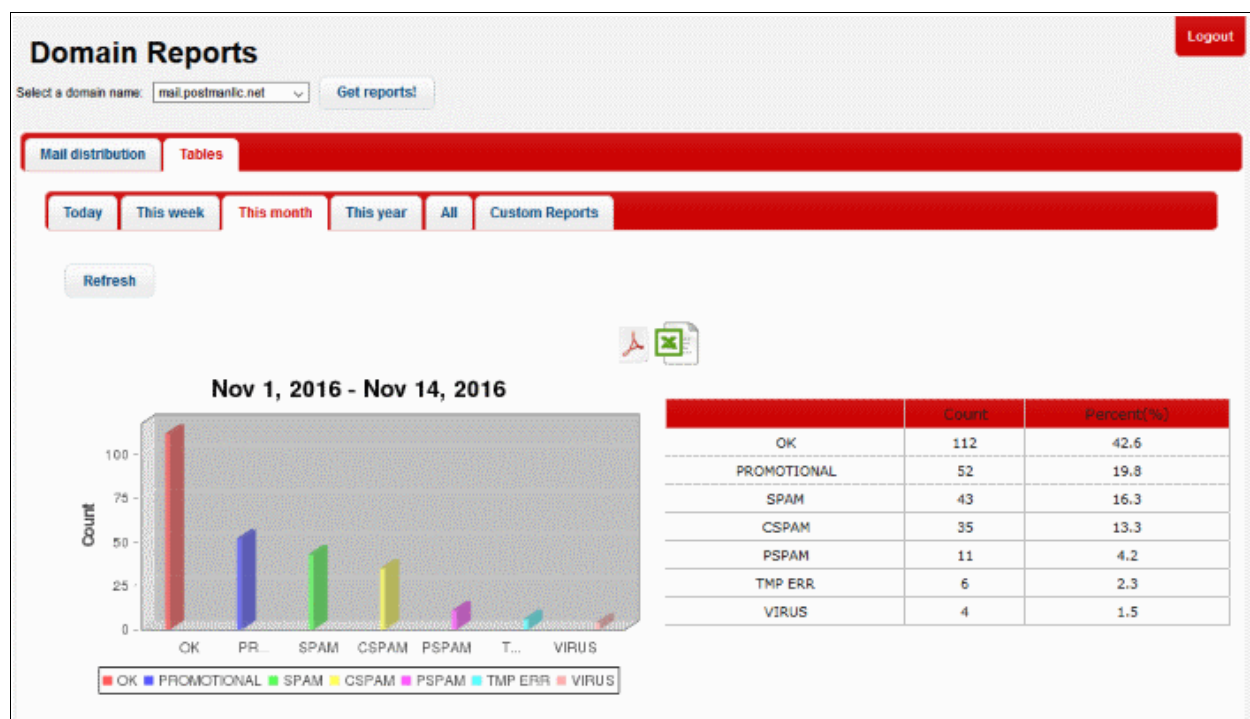
The 'Mail Distribution Progress' bar chart shows how many mails of each category were sent/received on each day over a period of a month or a year.

- 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.



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 distribution **Tables**

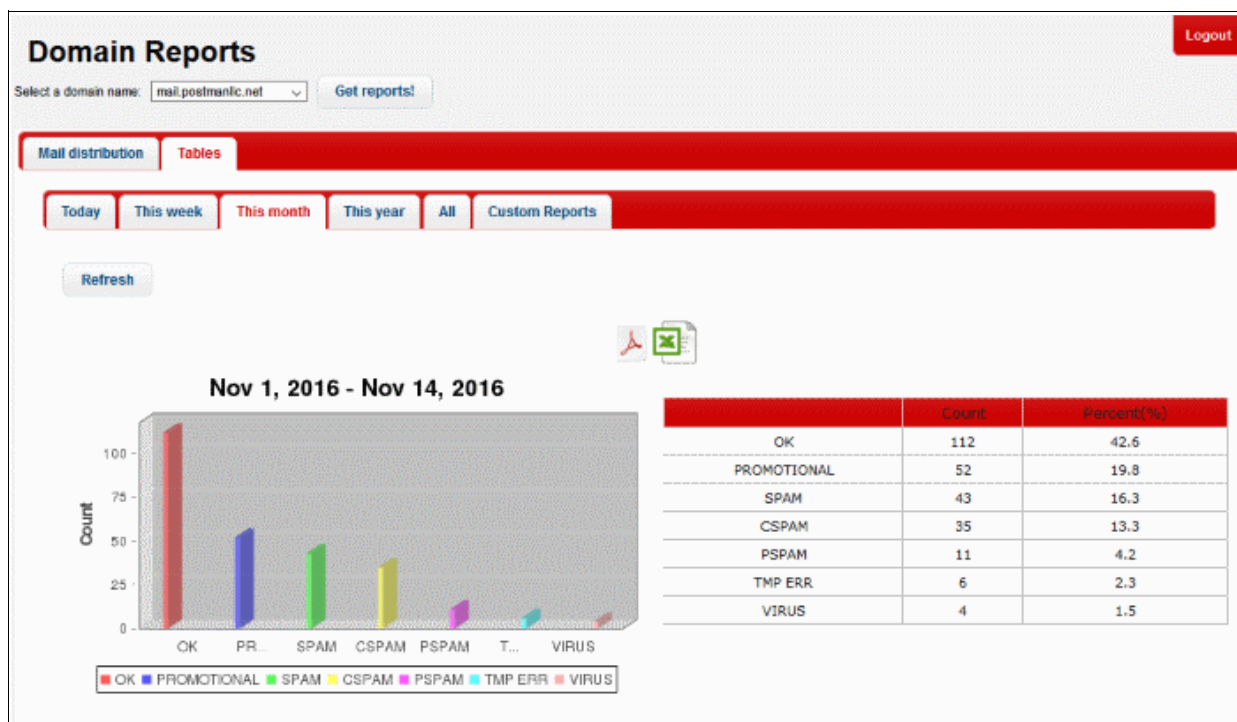
Today **This week** **This month** **This year** **All** **Custom Reports**

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							

8 0.5 -

- Click on the fields or calendar icon and select the period from the calendar.
- Click the 'Show' button after selecting the custom period.



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.

The screenshot shows the 'Mail distribution' interface. At the top, there are tabs for 'Mail distribution' and 'Tables'. Below these are filters for 'This hour', 'Today', 'This week', 'This month', and 'This year'. A section titled 'Show records between selected dates' contains date pickers for '2015-01-01' and '2015-02-19'. A calendar for January 2015 is displayed, with the 'Clean' button circled in blue. To the right of the calendar is a table with a 'Count' column.

	Count
1	552
2	143
3	61
4	14
5	8
6	7

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'.

The screenshot shows the 'Attachment Verdict Reports' interface. At the top right is a 'Logout' button. Below it is a search bar with 'Search' and 'Clear' buttons. There are radio buttons for 'File Name', 'Subject', 'Sender', and 'Recipient(s)'. Below the search bar is a table with columns: 'Received', 'Subject', 'Sender', 'Recipient(s)', 'File Name', and 'Action'. The table has pagination controls at the bottom.

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	Domain details of the email sender.
Recipient(s)	Domain details of the recipient(s).
File Name	Name of the file that is given a verdict.

Action	Action taken for verdict given.
--------	---------------------------------

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. 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'.

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.

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'

Click the following links for more details:

- [Quarantine & Archive General Settings](#)
- [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 also can set the method of user authentication for users that access their quarantined emails at 'Quarantined Webmail' interface.

- To open the interface, click the 'General' tab in the 'Quarantine & Archive' screen

Quarantine & Archive Settings Logout

General **E-mail Reports**

E-mail Logs Deleted Time (max to 729 days) * 60

Archive remove interval (max. 729 days) * 3

Attachment Verdict System record remove interval (Max 729 days) * 60

Quarantine remove interval (max. 30 days) * 3

Quarantine Webmail authentication type Local DB

Save

Quarantine & Archive General Settings - Table of Parameters

Parameter	Description
E-mail Logs Deleted Time	Enter the number of days for which the email logs will be retained. The maximum period is 729 days. Refer to the section ' 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. Refer to the section ' 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. Refer to section ' 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. Refer to the section ' Quarantine Logs ' for more details.
Quarantine Webmail authentication type	Select the user authentication type from the option for users that access the Webmail interface to check their quarantined mails.

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

11.1.2 Email Reports Settings

KoruMail allow users to access their quarantined emails via a separate web based quarantine page that contains all their quarantined messages. The 'Email Report' section allows administrators 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 that is applied to the users.

- To open the 'E-mail Reports' interface, click the 'E-mail Reports' tab in the 'Quarantine & Archive' screen.

[Logout](#)

Quarantine & Archive Settings

General
E-mail Reports

Mail Subject	E-mail Quarantine Rep
Mail From	surgate@surgategw.co
Base URL	http://surgategw.comod
Mail Template	<pre> <!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 \${mail}, <p>Karantinadaki tüm e-postalarnızın bulunduğu web tabanlı karantina </pre>
Days To Send	<input checked="" type="checkbox"/> Monday <input checked="" type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday <input checked="" type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday <input checked="" type="checkbox"/> Saturday <input checked="" type="checkbox"/> Sunday
Send Hour	<div style="border: 1px solid #ccc; padding: 5px;"> 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 </div>

Save
Defaults
Preview

Quarantine & Archive – E-mail Reports Settings - Table of Parameters

Parameter	Description
Mail Subject	Enter the 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) to send the email notifications

Send Hour	Select the hour of the day to send the email notifications for the selected days.

- Click the 'Default' button to restore the settings to default values.
- Click the 'Preview' button to view the mail that will be sent to users

Merhaba user@domain.com,
Karantinadaki tüm e-postalarınızın bulunduğu web tabanlı karantina sayfanıza ulaşmak için [buraya](#) tıklayınız.
Hello user@domain.com,
[Click here](#) to access the web based quarantine page which contains your all quarantine messages.

Action / Eylem	Date / Tarih	From / Gönderici	Subject / Konu	Status / Durum
Release / B?rak	Fri, Feb 27 10:41 EET 2015	user@domain.com	Preview subject	CERTAINLY SPAM
Release / B?rak	Fri, Feb 27 10:41 EET 2015	user@domain.com	Second subject	CERTAINLY SPAM

KoruMail Messaging Gateway

Test

Recipient

[Send](#)




[Close](#)

- To test if the mails are delivered successfully, enter the user's email address in the 'Recipient' field and click the 'Send' button
- Click the 'Close' button to return to the 'E-mail Reports' interface.
- Click the 'Save' button to apply your changes.

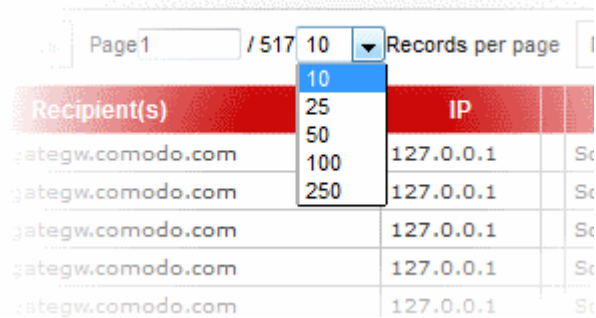
11.2 Quarantine Logs

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' then 'Quarantine Logs'

Quarantine Logs – Table of Column Descriptions	
Column Header	Description
Icon	<p>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.</p> <p> - Relayed: Indicates the mail has successfully passed the filtering process and user verified.</p> <p> - Rejected: Indicates the mail is rejected by KoruMail after the filtering process and reject message sent to the sender mail server.</p> <p> - Discarded: Indicates the mail is quarantined</p>
Subject	The content in the 'Subject' line of the mails
Result	The result for a mail after the filtering process.
Received	Date and time of email received by KoruMail
Sender	Domain details of the email sender
Recipient(s)	Domain details of the recipient(s)
IP	The IP address of the system from where the mail was sent.
Details	Provides the reasons why a mail is quarantined and spam score if it is marked as spam.

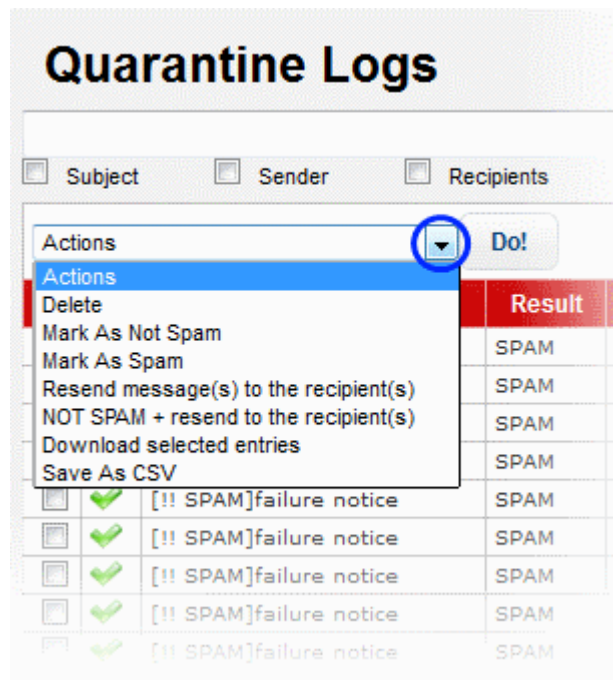
- Click the 'Records per page' drop-down



- 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



- 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.

The screenshot shows the 'Quarantine Logs' interface. At the top, there is a search bar with a 'Search' button and a 'Clear' button. Below the search bar, there are four checkboxes: 'Subject', 'Sender', 'Recipients', and 'IP'. To the right of these checkboxes is a link for 'Advanced search'. Below the checkboxes, there is a dropdown menu labeled 'Actions' and a 'Do!' button. At the bottom right, there are buttons for 'First', 'Previous', and 'Page 1'. The interface is designed for filtering and searching through quarantine logs.

- 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 '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.

This screenshot is similar to the previous one, but the 'Advanced search' link is circled in blue, indicating it is the next step in the process. The interface remains the same, with search filters and buttons.

The 'Advanced Search' option will be displayed.

This screenshot shows the 'Advanced Search' interface. It features a dropdown menu for selecting a column header (currently set to 'Subject') and a dropdown menu for selecting a filter (currently set to 'CONTAINS'). A blue box highlights these two dropdown menus. Below the dropdowns, there is a text input field and a '+' button. At the bottom, there are 'Search' and 'Clear' buttons. The interface is designed for creating specific search rules.

The first drop-down contains the column headers that can be selected for an advanced search.

The screenshot shows the 'Quarantine Logs' interface. At the top, there are checkboxes for 'Subject', 'Sender', 'Recipients', and 'IP'. Below these, a search filter is set to 'Subject' with a dropdown menu open showing options: 'Subject', 'From Address', 'To Address', 'Remote IP', 'Action', 'Result', and 'Received'. The 'CONTAINS' operator is selected. A table below shows a log entry with columns: Subject, Result, Received, and Sender. The entry for 'biseyler biseyler' has a result of 'PHISHING' and a received time of '27.02.2015 17:45:59'.

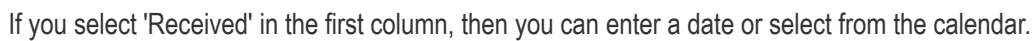
The second column contains the condition for a search, which depends on the item selected in the first column and text/number entered or options selected in the third column.

This screenshot shows the search filter dropdown menu expanded, displaying operators: 'CONTAINS', 'EQUALS', 'NOTEQUALS', 'CONTAINS', and 'NOTCONTAINS'. The 'CONTAINS' operator is highlighted. The interface also shows a 'Do!' button and a table with columns: Subject, Result, Received, and Sender.

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

The screenshot shows the 'Quarantine Logs' interface with the search filter set to 'Subject' and the operator 'CONTAINS'. The third column contains the text 'Important'. The interface includes a 'Search' button and a table with columns: Subject, Result, Received, and Sender.

If you select 'Action' or 'Result' in the first column, then further options can be selected from the third column.



The screenshot shows the 'Quarantine Logs' interface. At the top, there are checkboxes for 'Subject', 'Sender', 'Recipients', and 'IP'. Below these are several filter rules. Each rule consists of a logical operator (AND/OR), a field (Subject, From Address, To Address, Remote IP, Action, Result, Received), a comparison operator (EQUALS, NOTEQUALS, CONTAINS), and a value. For example, the first rule is 'Subject EQUALS important'. To the right of each rule is a button with a minus sign (-) to remove the rule. At the bottom of the filter section, there are buttons for 'Search' and 'Clear', and a link for 'Advanced search'. Below the filter section, there is a dropdown for 'Actions' and a 'Do!' button. At the very bottom, there are 'First' and 'Previous' buttons.

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 the 'Clear' button to remove the advanced search rules.
- Click the 'Search' button 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.

The screenshot shows a row of radio buttons for filtering results by month. The options are: 'Last Month' (selected), 'Last 2 Months', 'Last 3 Months', 'Last 6 Months', and '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.

Mail Logs

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)	fiatlina@gmail.com	
RFC2822 Sender	surgate@surgategw.an.office.comodo.net	
RFC2822 Recipient(s)	fiatlina@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	

[Download](#)
[Forward](#)
[Resend](#)
[Resend as attachment](#)
[Spam](#)
[Close](#)

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.



E-mail Forward

E-mail :

Send

Close

- 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.


Description

- 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.

Description

- 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'

Icon	Subject	Result	Received	Sender	Recipient(s)	IP	Details
OK	[?] SPAM? cure for balding.	SPAM	15.11.2016 04:33:04	savanmah.ataron@qpsathartech.com	faith@mail.postmanic.net	67.222.134.121	Score: 54.0
OK	A cure for balding, at a cell	OK	15.11.2016 04:33:09	savanmah.ataron@qpsathartech.com	faith@mail.postmanic.net	67.222.134.121	
OK	[?] SPAM?	SPAM	15.11.2016 04:46:51	dylan.brander@qpsathartech.com	faith@mail.postmanic.net	67.222.134.122	Score: 96.0
OK	Rebel from the mopping jet	OK	15.11.2016 04:53:25	josh.cornford@bighthorsten.com	faith@mail.postmanic.net	67.222.134.126	
OK	A resolution in ear cleaning.	OK	15.11.2016 04:14:42	stephanie.marquez@bahrhotel.com	faith@mail.postmanic.net	67.222.134.114	
OK	[?] SPAM?New model 2017 SUVs	SPAM	15.11.2016 04:04:10	offers.rufina@mailmmex.com	faith@mail.postmanic.net	67.222.134.103	Score: 94.0
OK	[?] SPAM?New model 2017 SUVs	SPAM	15.11.2016 04:03:24	offers.rufina@mailmmex.com	faith@mail.postmanic.net	67.222.134.103	Score: 65.0
OK	[?] PROBABLE SPAM?Staying in	SPAM	15.11.2016 02:46:47	dylan.cornel@peggyvirens.com	faith@mail.postmanic.net	67.222.134.112	Score: 47.0
OK	[?] PROBABLE SPAM?Staying in	SPAM	15.11.2016 03:48:16	dylan.cornel@peggyvirens.com	faith@mail.postmanic.net	67.222.134.112	Score: 47.0
OK	[?] PROBABLE SPAM?Cub heater	SPAM	15.11.2016 03:37:30	eric.morid@vmmotorco.com	faith@mail.postmanic.net	67.222.134.123	Score: 46.0
OK	[?] PROBABLE SPAM?Cub heater	SPAM	15.11.2016 03:36:29	eric.morid@vmmotorco.com	faith@mail.postmanic.net	67.222.134.123	Score: 46.0
OK	With the holidays coming up.	OK	15.11.2016 03:20:44	alexa.petel@actualmovie.com	faith@mail.postmanic.net	67.222.134.123	
OK	With the holidays coming up.	OK	15.11.2016 03:20:51	alexa.petel@actualmovie.com	faith@mail.postmanic.net	67.222.134.123	
OK	[?] SPAM?You have got to see	SPAM	15.11.2016 03:17:03	brittany.hench@yorklinnews Herald.com	faith@mail.postmanic.net	67.222.134.119	Score: 71.0
OK	Now you can have a flat belly	OK	15.11.2016 02:00:22	danielle.reedward@uofolinsnews Herald.com	faith@mail.postmanic.net	67.222.134.117	
OK	Now you can have a flat belly	OK	15.11.2016 02:00:25	danielle.reedward@uofolinsnews Herald.com	faith@mail.postmanic.net	67.222.134.117	
OK	Yes, even the top laundry list	OK	15.11.2016 02:02:10	kathryn.hughes@indianave.com	faith@mail.postmanic.net	67.222.134.103	
OK	You're simply not going to it	OK	15.11.2016 02:08:17	richelle.vicathens@paulabunken.com	faith@mail.postmanic.net	67.222.134.114	
OK	Pinet's the brightest. Pears	OK	15.11.2016 02:25:33	zach.shang@nodes.com	faith@mail.postmanic.net	67.222.134.131	
OK	[?] PROBABLE SPAM?Business or	SPAM	15.11.2016 02:13:50	camartha.brownand@webcyclo.com	faith@mail.postmanic.net	67.222.134.119	Score: 42.0
OK	Business or otherwise, private	OK	15.11.2016 02:13:04	camartha.brownand@webcyclo.com	faith@mail.postmanic.net	67.222.134.119	
OK	A professional network by usm	OK	15.11.2016 02:03:50	vanessa.burgess@musicaadnet.com	faith@mail.postmanic.net	67.222.134.123	Score: 40.0
OK	[?] PROBABLE SPAM?A professional	SPAM	15.11.2016 02:03:08	vanessa.burgess@musicaadnet.com	faith@mail.postmanic.net	67.222.134.123	Score: 40.0
OK	Need to college, or planning a	OK	15.11.2016 01:49:21	andrey.nabers@vhtech.com	faith@mail.postmanic.net	67.222.134.120	
OK	Need to college, or planning a	OK	15.11.2016 01:48:22	andrey.nabers@vhtech.com	faith@mail.postmanic.net	67.222.134.120	
OK	[?] CERTAINLY SPAM?Stop overp	SPAM	15.11.2016 01:35:16	lathemna.powers@aleocephus.com	faith@mail.postmanic.net	67.222.134.118	KoruMail global spam signature detected
OK	[?] CERTAINLY SPAM?Stop overp	SPAM	15.11.2016 01:35:16	lathemna.powers@aleocephus.com	faith@mail.postmanic.net	67.222.134.118	KoruMail global spam signature detected

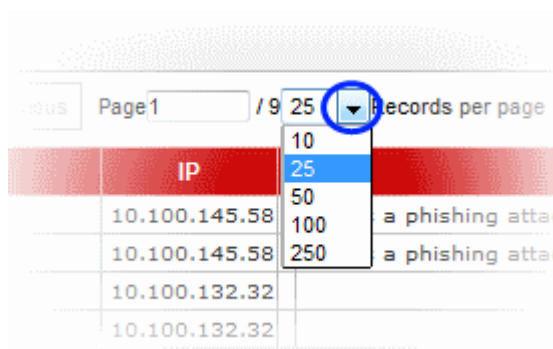
Archived Mails – Table of Column Descriptions

Column Header	Description
Icon	<p>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.</p> <p>✔ - Relayed: Indicates the mail has successfully passed the filtering process and user verified.</p> <p>✖ - Rejected: Indicates the mail is rejected by KoruMail after the filtering process and reject message sent to the sender mail server.</p> <p>✖ - Discarded: Indicates the mail is quarantined</p>
Subject	The content in the 'Subject' line of the mails
Result	The result for a mail after the filtering process.
Received	Date and time of email received by KoruMail
Sender	Domain details of the email sender
Recipient(s)	Domain details of the recipient(s)
IP	The IP address of the system from where the mail was sent.
Details	Provides the reasons 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

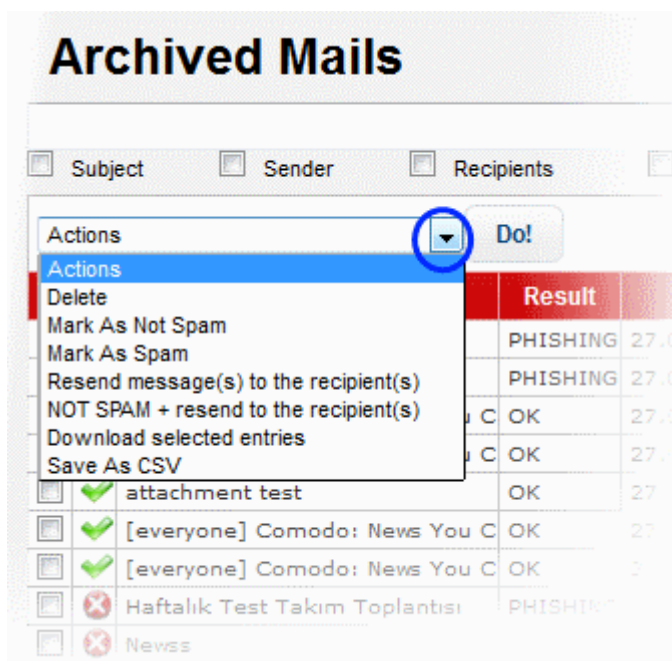
- Click the 'Records per page' drop-down



- 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



- 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.

The screenshot shows the 'Archived Mails' search interface. At the top, there's a search bar with a 'Search' button and a 'Clear' button. Below the search bar, there are four checkboxes: 'Subject', 'Sender', 'Recipients', and 'IP'. To the right of these checkboxes is a 'Do!' button. Below the 'Do!' button, there are 'First', 'Previous', and 'Page 1' links. At the bottom, there's a table with columns: 'Subject', 'Result', 'Received', and 'Sender'.

- 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 screenshot shows the 'Archived Mails' search interface. The 'Advanced search' link is highlighted with a blue circle. The interface is the same as the previous screenshot, but with the 'Advanced search' link being the focus.

The 'Advanced Search' option will be displayed.

The screenshot shows the 'Archived Mails' advanced search interface. A blue box highlights the first drop-down menu, which contains the column headers 'Subject', 'Sender', 'Recipients', and 'IP'. The second drop-down menu shows the operator 'CONTAINS'. There is a text input field for the search criteria and a '+' button to add more filters. Below the highlighted area, there are 'Search' and 'Clear' buttons.

The first drop-down contains the column headers that can be selected for an advanced search.

Archived Mails

☐ Subject ☐ Sender ☐ Recipients

Subject CONTAINS

☐ Subject
☐ From Address
☐ To Address
☐ Remote IP
☐ Action
☐ Result
☐ Received

	Subject	Result
<input type="checkbox"/>	✓ biseyler biseyler	PHISHING
<input type="checkbox"/>	✓ biseyler biseyler	PHISHING
<input type="checkbox"/>	✓ [everyone] Comodo: New	

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.

Archived Mails

☐ Subject ☐ Sender ☐ Recipients ☐ IP

Subject CONTAINS

☐ EQUALS
☐ NOTEQUALS
☐ CONTAINS
☐ NOTCONTAINS

Actions

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

Archived Mails

☐ Subject ☐ Sender ☐ Recipients ☐ IP [Advanced search](#)

Subject CONTAINS important

Actions

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

[Advanced search](#)

☐ 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

 Received

 EQUALS

AND

 OR

Mail Logs

[Advanced search](#)

☐ 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

 Received

 EQUALS

 18/2/15

AND

 OR

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 the 'Clear' button to remove the advanced search rules.
- Click the 'Search' button 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

[Download](#)
[Forward](#)
[Resend](#)
[Resend as attachment](#)
[Spam](#)
[Close](#)

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.

E-mail Forward

E-mail :

Send

Close

- 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.

Score	0.0
Sender	vetest1@ve.comodo.local
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

- Select the category from the options that you want to add the email and click the  button beside it.

Description

Save


Close

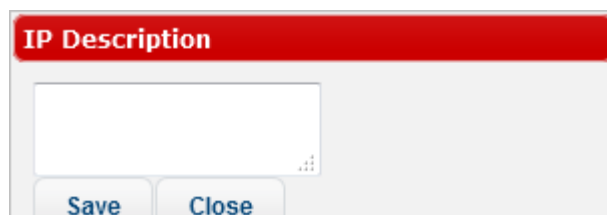
- Enter the reason for changing the category and click the 'Save' button.

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
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.

A small dialog box titled "IP Description" with a red header bar. It contains a large white text input area. At the bottom, there are two buttons: "Save" and "Close".

- 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.

About Comodo

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information.

With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ, 07013

United States

Email: EnterpriseSolutions@Comodo.com

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road, Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

For additional information on Comodo - visit <http://www.comodo.com>.