



COMODO
CYBERSECURITY



Comodo Secure Email Gateway Enterprise

Software Version 6.7

Admin Guide

Guide Version 6.7.010620

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1	Introduction to Comodo Secure Email Gateway - Enterprise	5
1.1	Login to the Secure Email Gateway Module	7
1.2	Get Started	8
1.2.1	Cloud Customers	8
1.2.2	On-premise Customers	8
1.3	The Main Interface	20
2	The Dashboard	21
2.1	System Usage Graphics	22
2.2	About Software	23
3	System Configurations	28
3.1	Services	28
3.2	License	30
3.3	Configure System Settings	34
3.3.1	System General Settings	34
3.3.2	Cache Settings	35
3.3.3	Session Settings	35
3.3.4	GUI Customization	36
3.3.5	System Backup	36
3.3.6	System Restore	38
3.3.7	Log Upload Settings	39
3.3.8	Postmaster Settings	39
3.3.9	Web UI SSL	40
3.3.10	SMTP TLS Settings	41
3.3.11	Update Database	43
3.3.12	Syslog Server	44
3.4	Logs	44
3.4.1	Log Files	45
3.4.2	Purge Files	46
3.5	Tools	47
3.5.1	Check Connectivity	48
3.5.2	Clear SMTP Queue	52
3.6	Session Reports	53
3.7	System Usage Statistics	53
4	SMTP Configuration	61
4.1	SMTP (Send E-Mail Protocol) Settings	62
4.1.1	General Settings	62
4.1.2	Advanced Settings	63
4.1.3	Outbound Delivery Queue	65
4.2	Manage Domains	68
4.2.1	Manage Domain Names	69
4.2.2	Manage Domain Routes	75

4.2.3	Manage Smart Hosts.....	81
4.2.4	Default Domain Routing.....	85
4.3	Secure Email Gateway SMTP AUTH Connector.....	86
4.3.1	SMTP Authentication Settings.....	86
4.3.2	Block Users.....	89
4.3.3	Anomaly Detection.....	95
4.4	LDAP/Local DB/My SQL User Database.....	96
4.4.1	LDAP Profile.....	96
4.4.2	Local DB Users.....	100
4.4.3	My SQL User Database.....	106
4.5	Greylist.....	109
4.5.1	Greylist Ignored IP Addresses/Domains.....	110
4.6	Manage RBL Servers.....	113
4.7	Disclaimer.....	116
4.8	SMTP Relay.....	117
4.9	DomainKeys Identified Mail (DKIM).....	118
4.10	Outgoing SMTP Limits.....	122
4.11	Incoming SMTP Limits.....	130
5	Modules.....	135
5.1	Anti-spam.....	135
5.1.1	Anti-spam General Settings.....	136
5.1.2	Authorized Trainers.....	138
5.1.3	Advanced Anti-spam Settings.....	139
5.1.4	Bayesian Training.....	139
5.1.5	Content Filter.....	141
5.1.6	Signature Whitelist.....	143
5.1.7	Attachment Filter.....	145
5.2	Anti-Virus.....	145
5.2.1	Anti-Virus General Settings.....	146
5.2.2	Advanced Anti-Virus Settings.....	147
5.3	Korunami Reputation Network (KRN).....	149
5.4	Anti-Spoofing.....	151
5.5	SMTP IPS/FW.....	155
5.5.1	SMTP IPS General Settings.....	156
5.5.2	Whitelist IP Addresses.....	158
5.5.3	Blocked IP Addresses.....	160
5.5.4	Rate Control.....	163
5.6	Auto Whitelist.....	164
5.7	Containment System.....	166
5.8	Data Leak Prevention (DLP).....	166
5.9	Attachment Verdict System.....	167
6	Profile Management.....	168
6.1	Add and Configure a New Profile.....	170

6.1.1 Edit a Profile.....	201
6.1.2 Delete a Profile.....	202
7 Reports.....	204
7.1 Mail Logs Report.....	204
7.2 SMTP Queue Report.....	213
7.3 Delivery Logs Report.....	215
7.4 SMTP-AUTH Logs Report.....	216
7.5 Summary Reports.....	218
7.6 Domain Reports.....	224
7.7 Attachment Verdict Reports.....	228
7.8 Original Mail Request.....	229
8 Quarantine & Archive.....	231
8.1 Quarantine & Archive Settings.....	232
8.1.1 Quarantine & Archive General Settings.....	232
8.1.2 Email Reports Settings.....	233
8.1.3 Admin E-mail Reports Settings.....	235
8.2 Quarantine Logs.....	237
8.3 Archived Mails.....	245
About Comodo Security Solutions.....	254

1 Introduction to Comodo Secure Email Gateway - Enterprise

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

Key Features

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

Guide Structure

This guide is intended to take you through the installation, configuration and use of Comodo Secure Email Gateway

- **Introduction to Secure Email Gateway**
 - **Logging-in to the Secure Email Gateway**
 - **Get Started**
 - **The Main Interface**
- **The Dashboard**
 - **System Usage Graphics**
 - **About Software**
- **System Configurations**
 - **Services**
 - **License**
 - **Configure System Settings**
 - **Logs**
 - **Tools**
 - **Session Reports**
 - **System Usage Statistics**
- **SMTP Configuration**

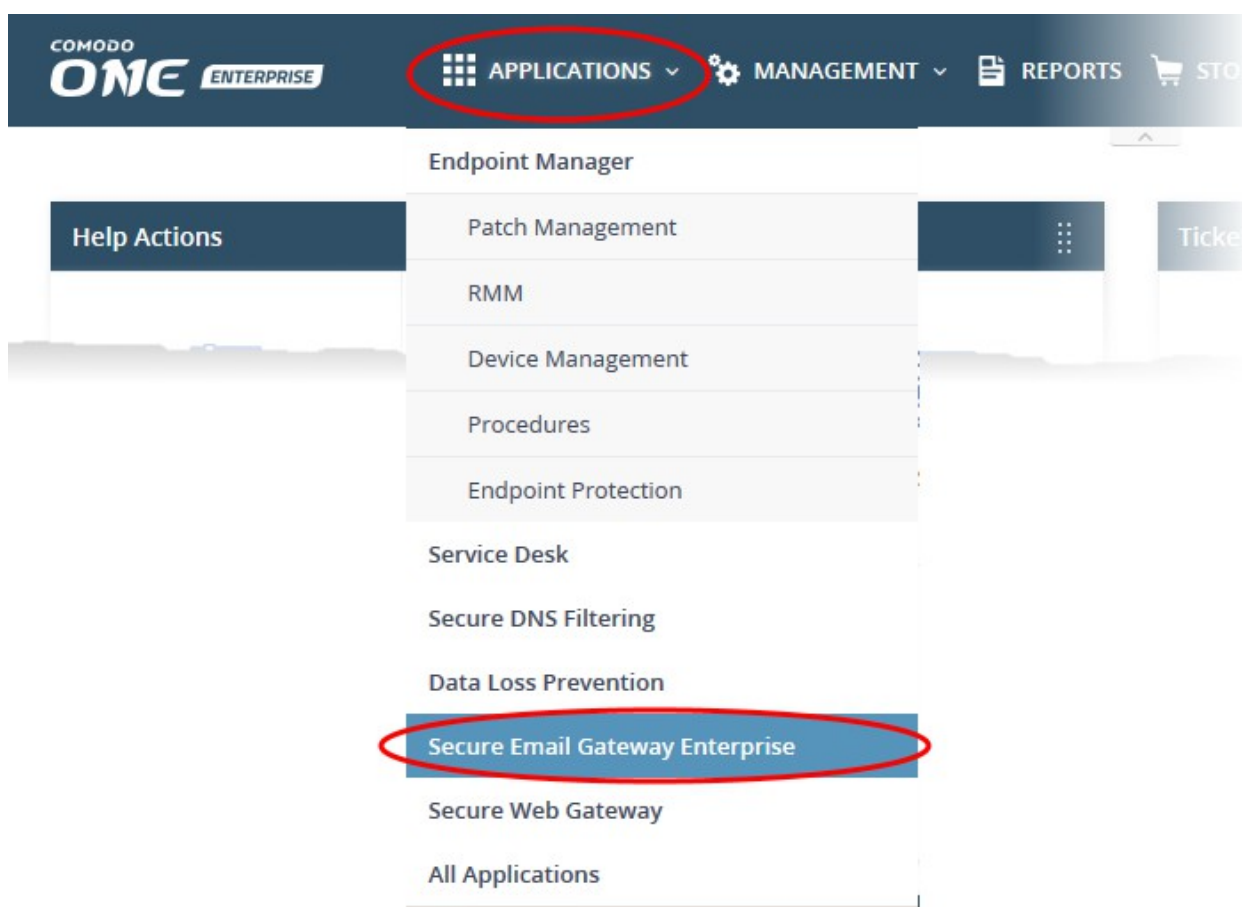
- **SMTP (Send E-Mail Protocol) Settings**
- **Manage Domains**
- **Secure Email Gateway SMTP AUTH Connector**
- **LDAP/Local DB/My SQL User Database**
- **Greylist**
- **Manage RBL Servers**
- **Disclaimer**
- **SMTP Relay**
- **DomainKeys Identified Mail (DKIM)**
- **Outgoing SMTP Limits**
- **Incoming SMTP Limits**
- **Modules**
 - **Anti-spam**
 - **Anti-Virus**
 - **Reputation Network (KRN)**
 - **Anti-Spoofing**
 - **SMTP IPS/FW**
 - **Auto Whitelist**
 - **Containment System**
 - **Data Leak Prevention (DLP)**
 - **Attachment Verdict System**
- **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**
 - **Original Mail Request**
- **Quarantine & Archive**
 - **Quarantine & Archive General Settings**
 - **Quarantine Logs**
 - **Archived Mails**

1.1 Login to the Secure Email Gateway Module

- **Cloud Customers**
- **On-premise Customers**

Cloud Customers

- Login to your **Comodo One** / **Comodo Dragon** / **ITarian** account (Comodo One portal is shown below as an example)
- Comodo One portal opens at the dashboard.
- Click 'Applications' then 'Secure Email Gateway Enterprise'



Secure Email Gateway Enterprise will open at the dashboard.

On-premise Customers

- You can login to Secure Email Gateway (SEG) after deployment on your premises. **Click here** for help to deploy SEG on your network.
- Enter the IP address of your instance that was configured during SEG deployment on any web-browser. For example:
https://ip-address: 8443
- Default credentials:
 - Username: admin
 - Password: admin

1.2 Get Started

There are two ways to get started with Secure Email Gateway based on the type of customers.

- **Cloud Customers**
- **On-premise Customers**

1.2.1 Cloud Customers

After creating your account, the first step is to configure your mail server to work with the Secure Email Gateway service.

Incoming Filter Configuration

- Comodo will set up your antispam instance. After this is done, you will receive a mail that contains your account and service URL details. If you think there is a delay in this process, contact Comodo support at domesupport@comodo.com
- Change your incoming mail server domain MX records to point to Secure Email Gateway. Mail will be directed to your domain after passing through antispam filtering.
- Enter routing details in 'SMTP' > 'Domains' > 'Routes'. See '**Manage Domains**' to find out how to add domain names and their corresponding routing types. If no routing is configured then the default domain routing applies.

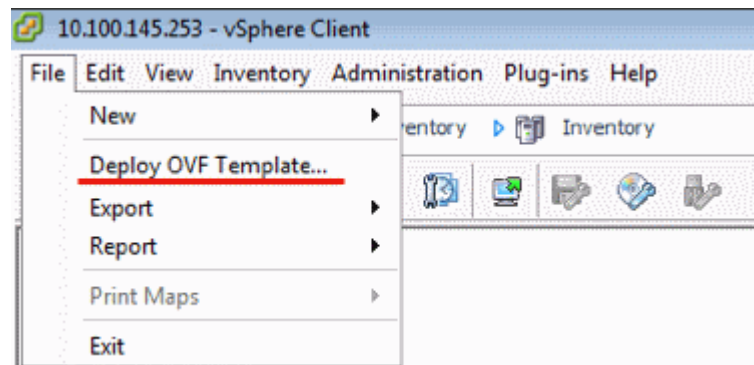
Outgoing Filter Configuration

- The outgoing filter checks mail that is sent from your network. You can enable the feature by routing your outgoing traffic to your Secure Email Gateway service URL.
- This service URL is same as used for incoming filtering. This URL is sent to you after Comodo finish provisioning your instance. If you have any questions or need assistance, do not hesitate to contact domesupport@comodo.com

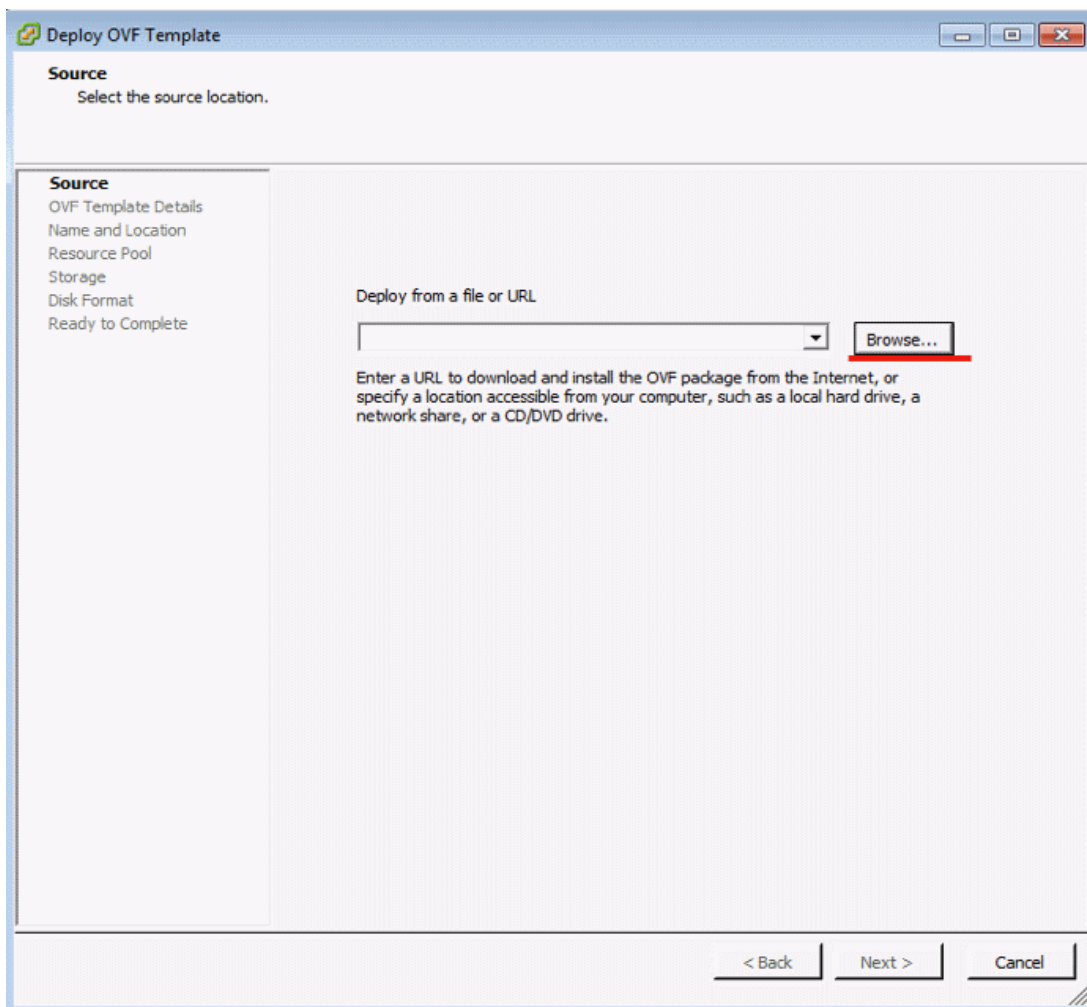
1.2.2 On-premise Customers

Secure Email Gateway is deployed as a VMware image. Please follow the steps below to install the product.

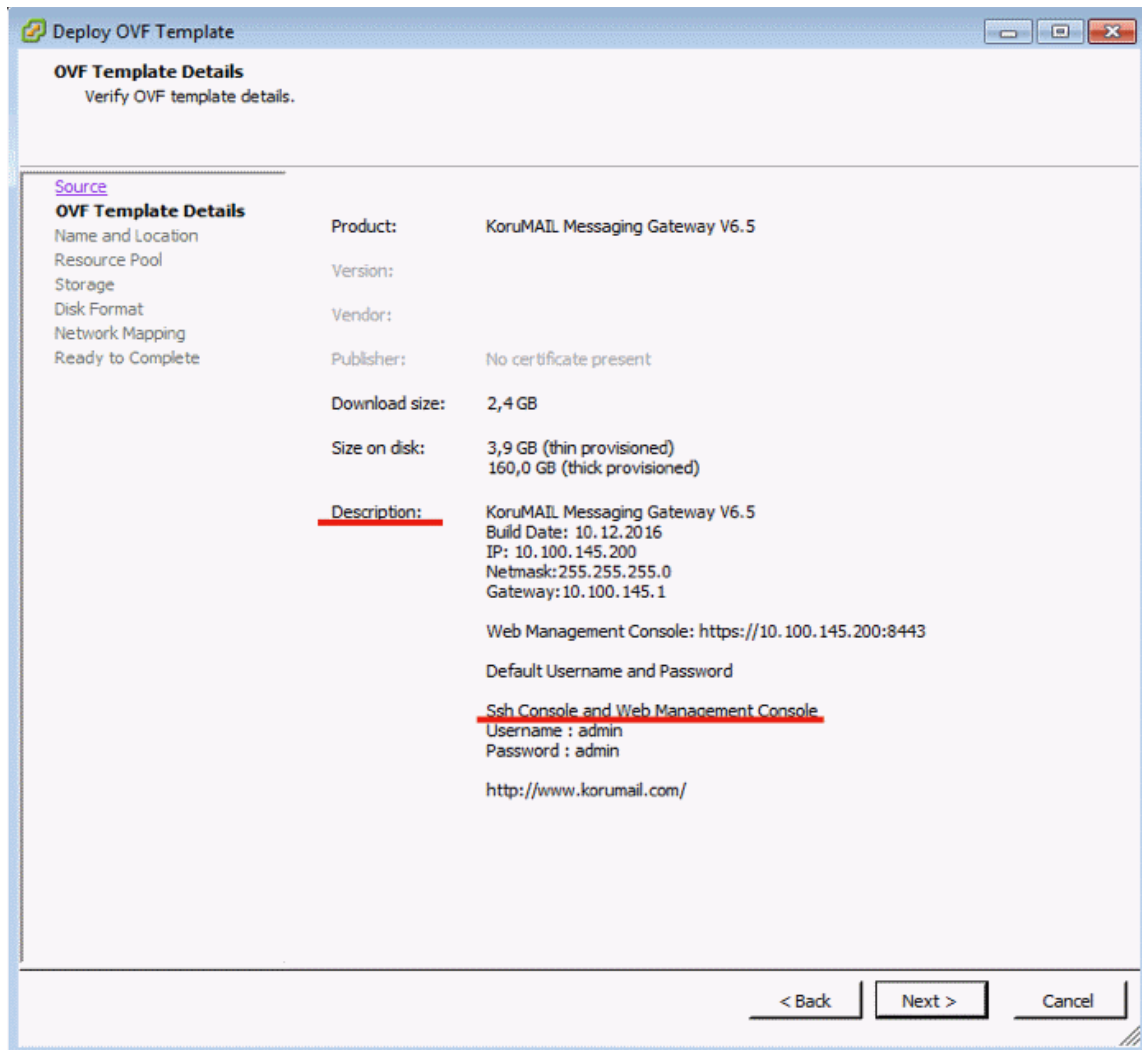
1. Download the virtual machine image:
 - HyperV Template - https://download.comodo.com/domeasg/DomeASG_hyperv.rarOr
 - ESX Template - https://download.comodo.com/domeasg/DomeASG_esx.rar
2. Extract the contents of the .rar file using Winrar or 7zip.
3. Open the VMware Vsphere client and login to the ESXi server.
4. Follow the steps below to deploy SEG (Korumail) to your ESX server:
 - Click 'File' > 'Deploy OVF Template'



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



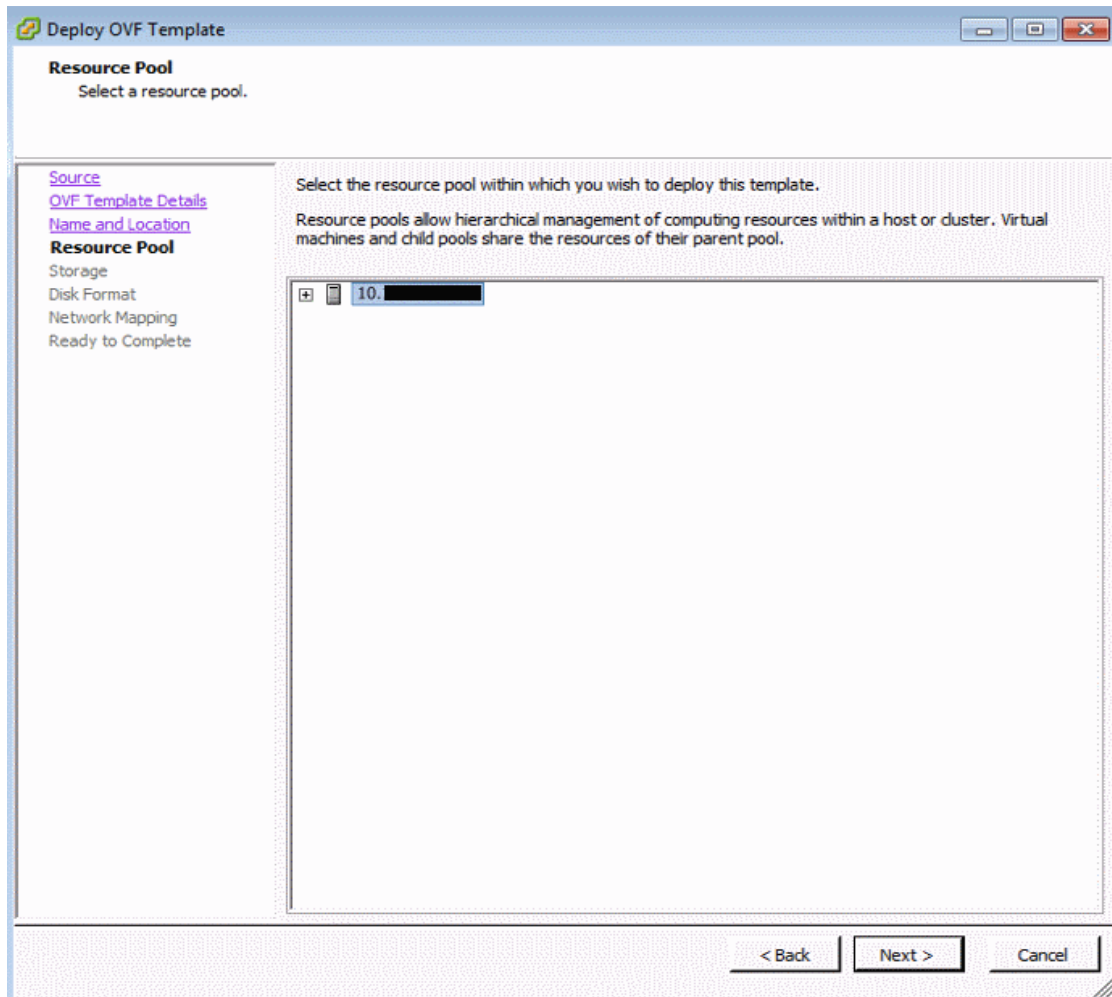
- Review the information in the details screen, especially the default username/password, then click 'Next':



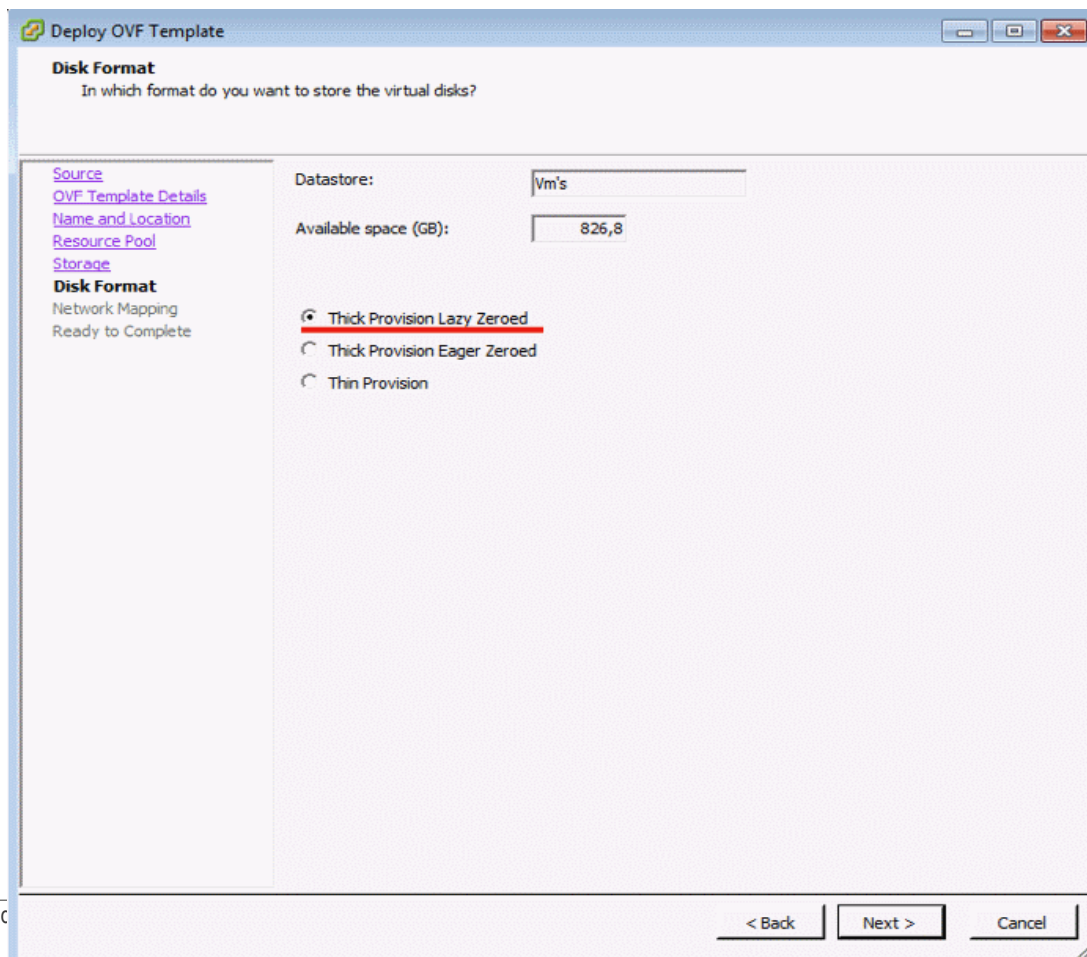
- Specify a name for the server, or leave it at the default:

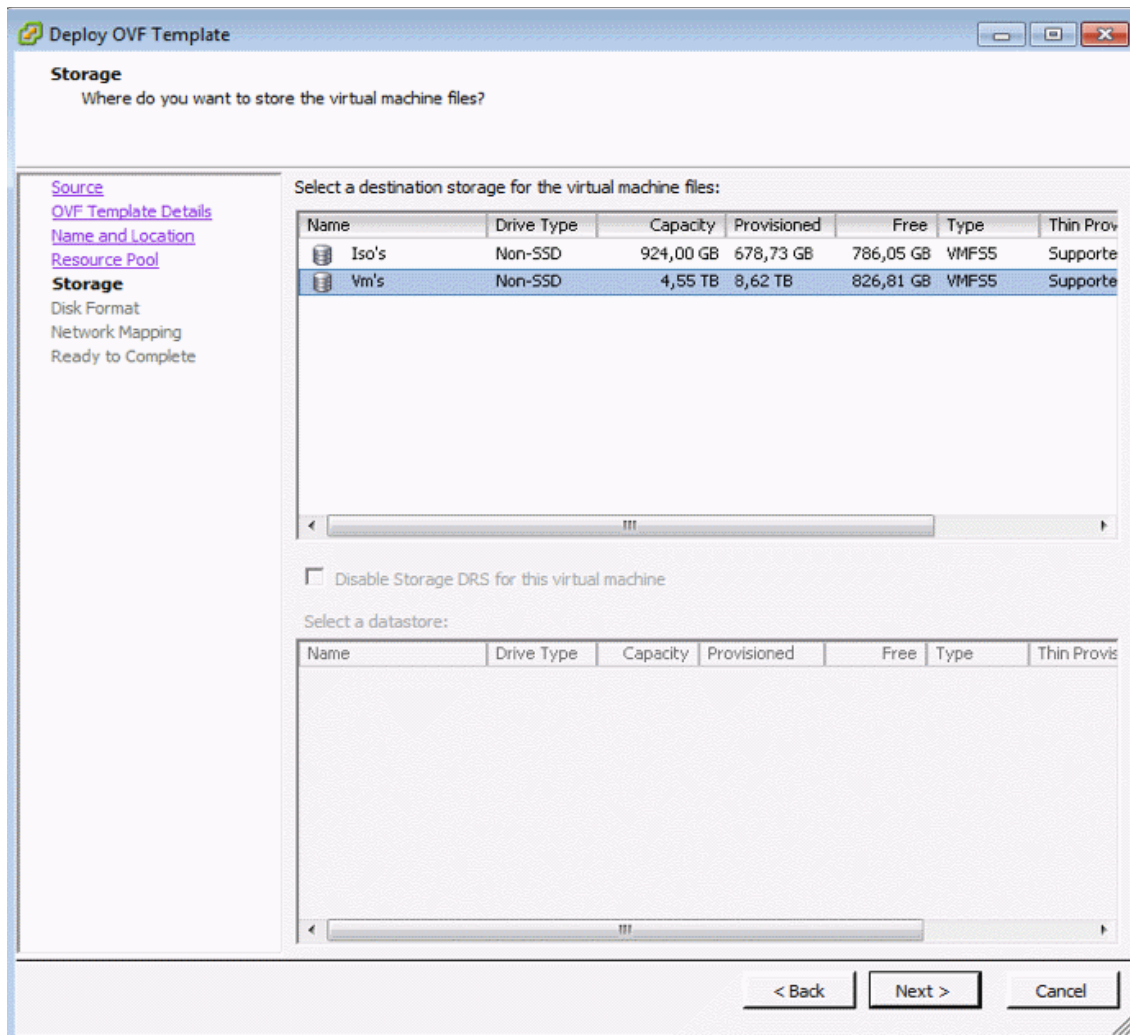
The screenshot shows a window titled "Deploy OVF Template" with a sub-header "Name and Location" and the instruction "Specify a name and location for the deployed template". On the left, a navigation pane lists steps: "Source", "OVF Template Details", "Name and Location" (which is selected), "Resource Pool", "Storage", "Disk Format", "Network Mapping", and "Ready to Complete". The main area has a "Name:" label and a text input field containing "koruMAIL Messaging Gateway V6.5". Below the input field, a note states: "The name can contain up to 80 characters and it must be unique within the inventory folder." At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

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



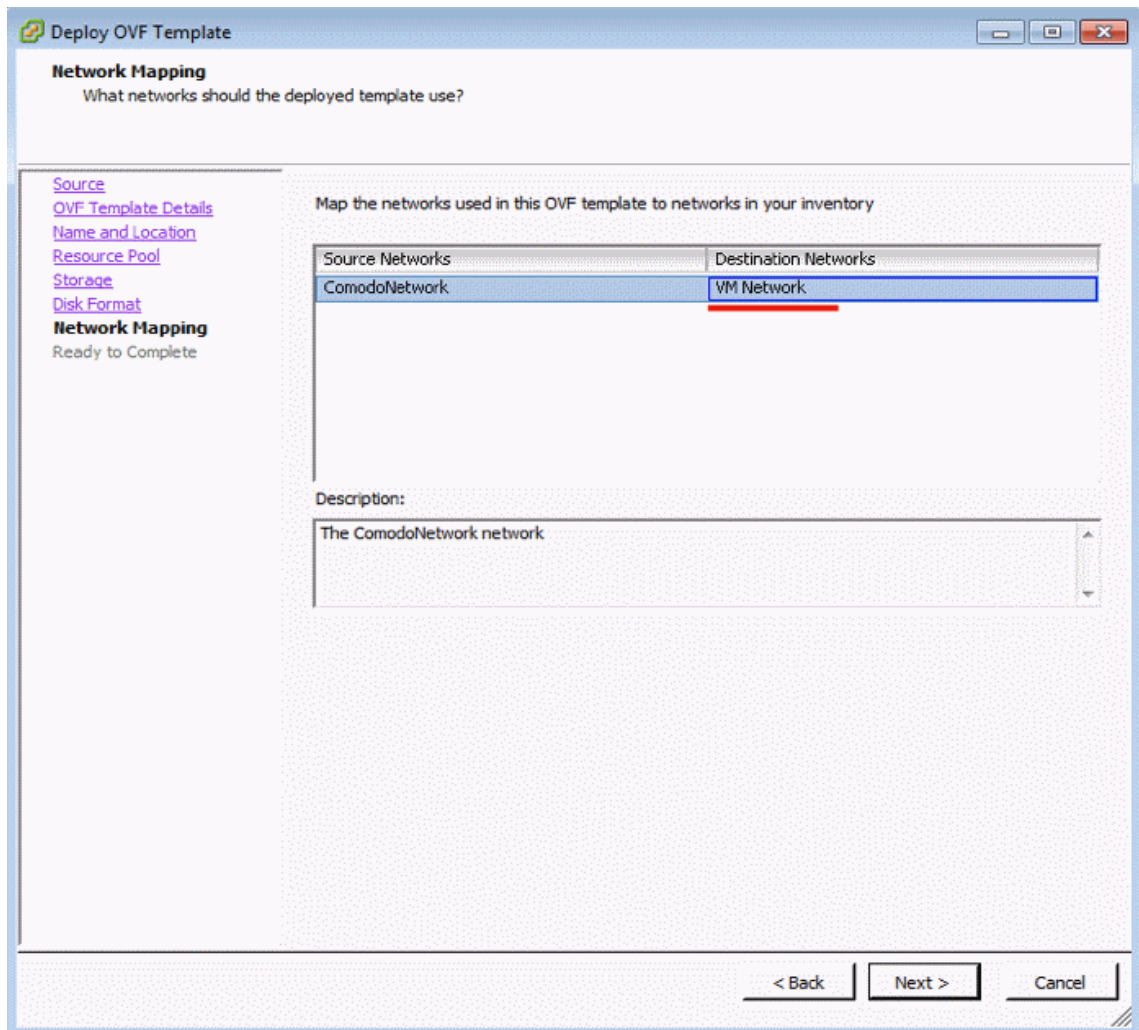
- Choose which storage area your virtual machine image should be copied to. SEG (Korumail) requires 160 Gb of disk space. Click 'Next' when done.



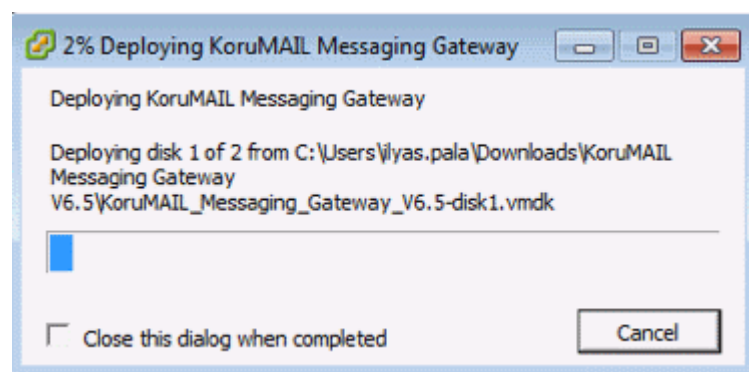
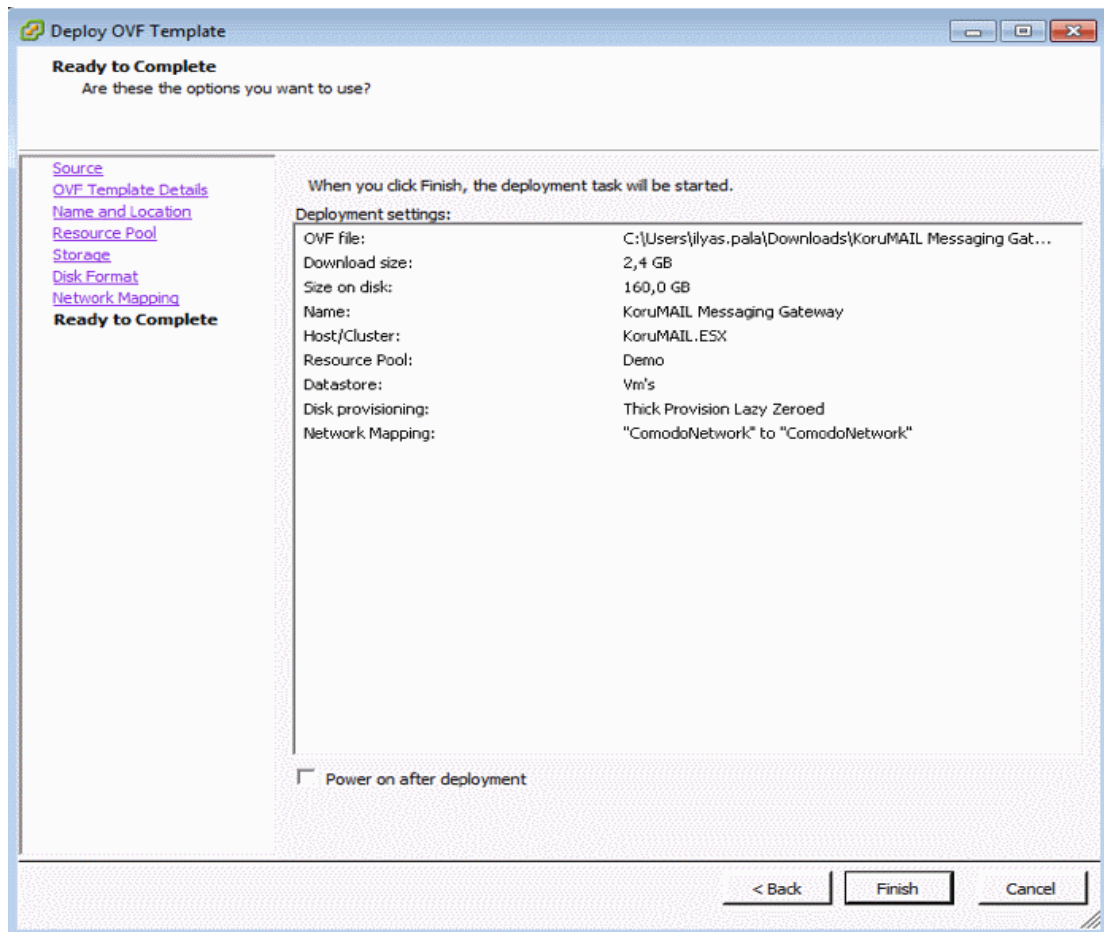


- Select 'Thick Provision' as 'Disk Format' and click 'Next':

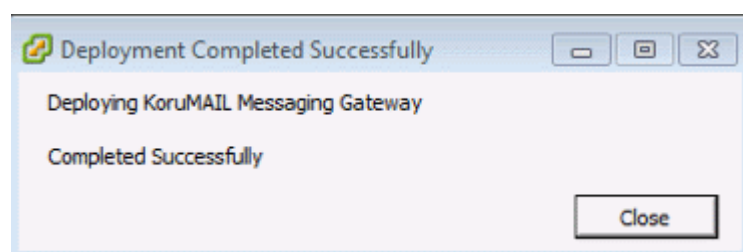
- Select a network with an active internet connection:



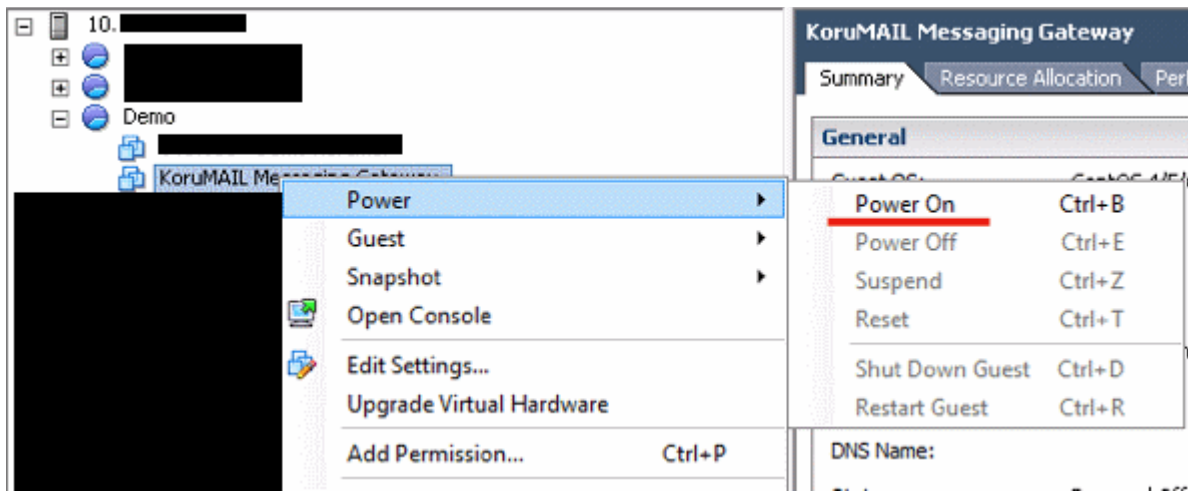
- Review the setup details then click 'Finish' to begin installation:



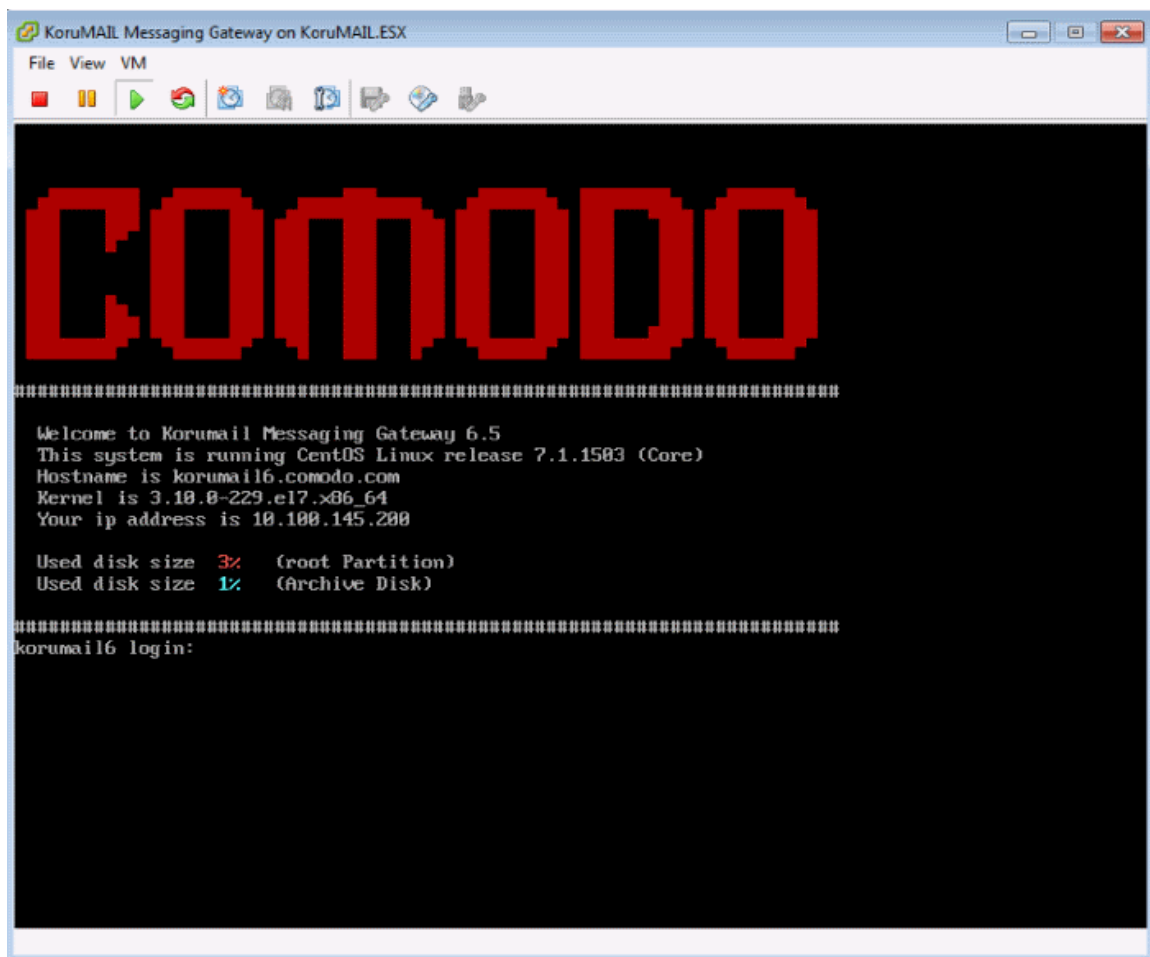
- The deployment process takes a few minutes to complete.



- Select the SEG (Korumaail) server, right-click then select 'Power On':

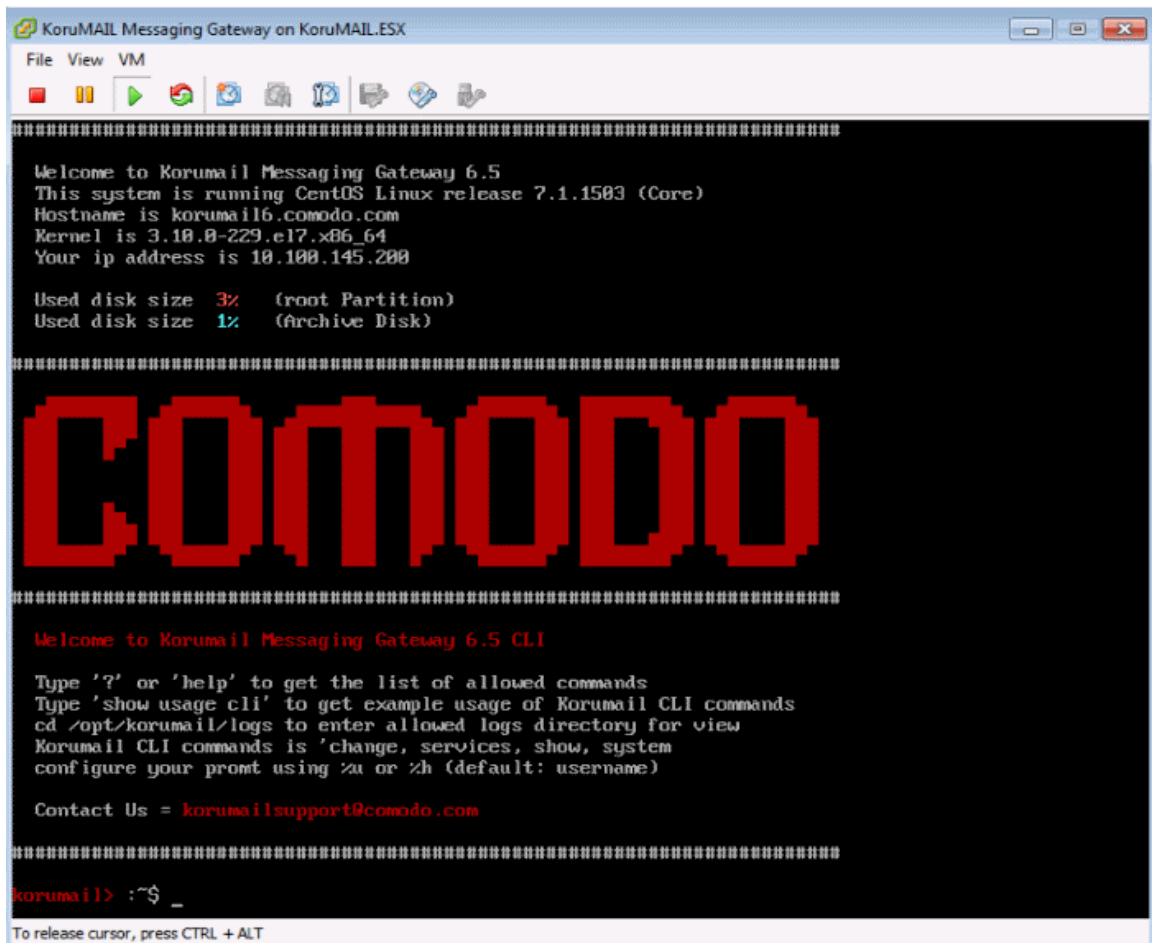


- Wait for the server to boot-up.



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

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



The screenshot shows a terminal window titled "KoruMAIL Messaging Gateway on KoruMAIL.ESX". The terminal displays the following text:

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

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

COMODO
=====

Welcome to Korumail Messaging Gateway 6.5 CLI

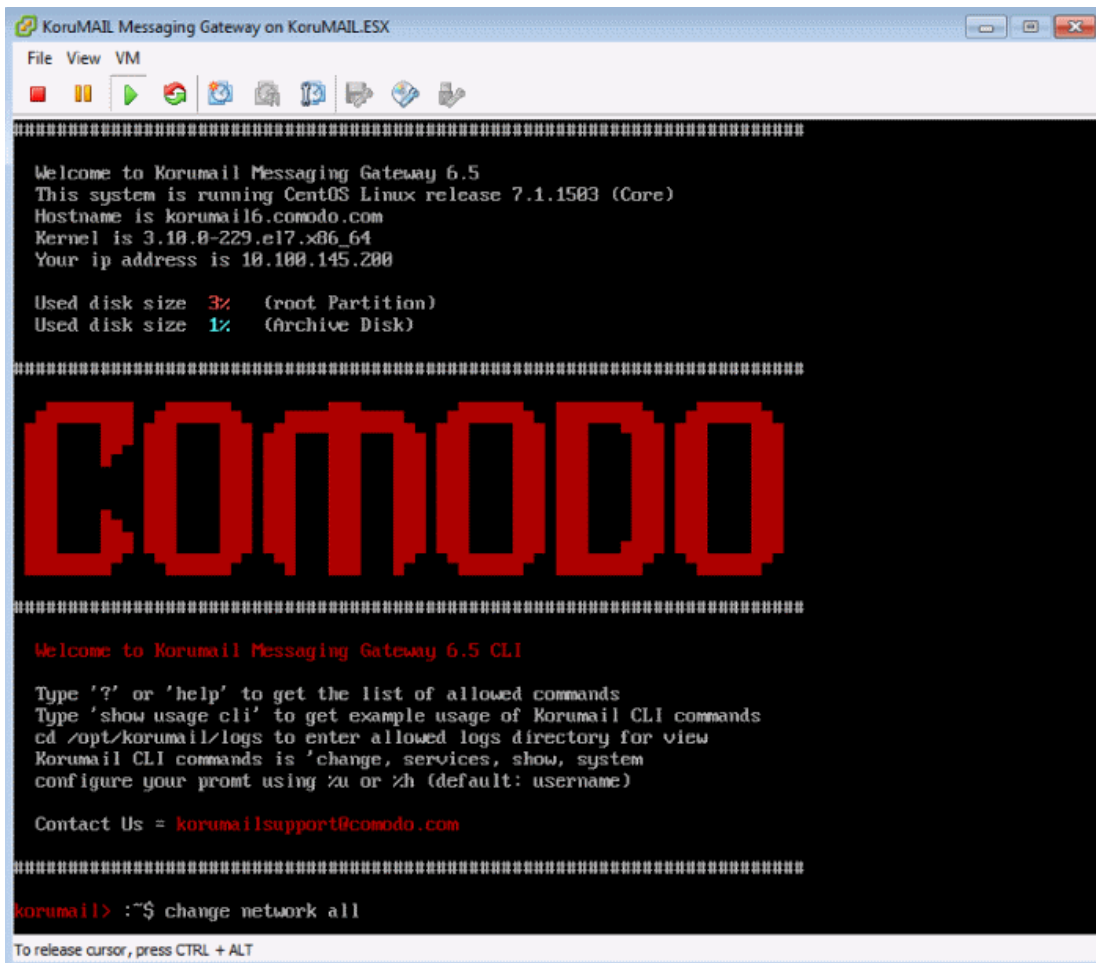
Type '?' or 'help' to get the list of allowed commands
Type 'show usage cli' to get example usage of Korumail CLI commands
cd /opt/korumail/logs to enter allowed logs directory for view
Korumail CLI commands is 'change, services, show, system
configure your prompt using %u or %h (default: username)

Contact Us = korumailsupport@comodo.com
=====

korumail> :~$ _

To release cursor, press CTRL + ALT
```

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



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

```

korumail> :~$ change network all
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!! Making changes here will restart system immediately!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
    
```

This option will change network settings
Do you want to proceed [y/n] (Default is NO) ? > Y

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

The following changes will be made to network configuration

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

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

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

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

1.3 The Main Interface

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

The screenshot shows the main interface of the Comodo Secure Email Gateway Admin Console. It features a left-hand navigation menu, a central dashboard area, and an 'About' section on the right. Callouts provide detailed information about these sections:

- Configuration Tabs:** View and configure various settings.
- The Dashboard Area:** View graphical summary of system unsafe, system messages and About system and details.
- About:** View appliance model number, software version, change password, update license and run setup wizard.

The interface includes a 'System Messages' section with a warning: 'No valid system administrator e-mail address defined. Click for new update details.' The 'System Usage Graphics' section shows a bar chart for 'SMTP Connection' with tabs for Hourly, Daily, Weekly, Monthly, and Yearly. The 'About' section contains a table with system information:

System Date	06/04/2017 06:52 UTC
Uptime	20 hours 25 minutes
Online Users	1
IP Address	172.31.22.243
Spam Signature Last Update Time	Thu Apr 6 06:30:02 UTC 2017
Spam Signature Count	488968
Virus Signature Last Update Time	Thu Apr 6 05:30:03 UTC 2017
Virus Signature Count	6204187
Run The Setup Wizard	
Details	

Configuration Tabs

The menu on the left allows you to add new domains for filtering, add users, user groups, configure various settings, view reports and more.

- System:** Configure network settings, add NTP servers, enable or disable services, view license information and more. See '**System Configuration**' for more details.
- SMTP:** Configure SMTP settings, add domains, add new LDAP profiles, create IP/domain greylists, set outgoing limits and more. See '**System Configuration**' for more details.
- Modules:** Enable or disable anti-spam, anti-virus, anti-spoofing, anti-phishing and configure settings for anti-spam training and content filter. See **Modules** for more details.
- Profile Management:** Configure various settings such as anti-virus, anti-spam, blacklist and more for default incoming and outgoing profile. See '**Profile Management**' for more details.
- Reports:** View and generate log reports for incoming and outgoing mails and a summary of mails categorized as spam, RBL, phishing and more. See '**Reports**' for more details.
- Quarantine & Archive:** Enables to configure Quarantine and Archive settings, view quarantined mail logs and archived mails. See '**Quarantine & Archive**' for more details.

Dashboard

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

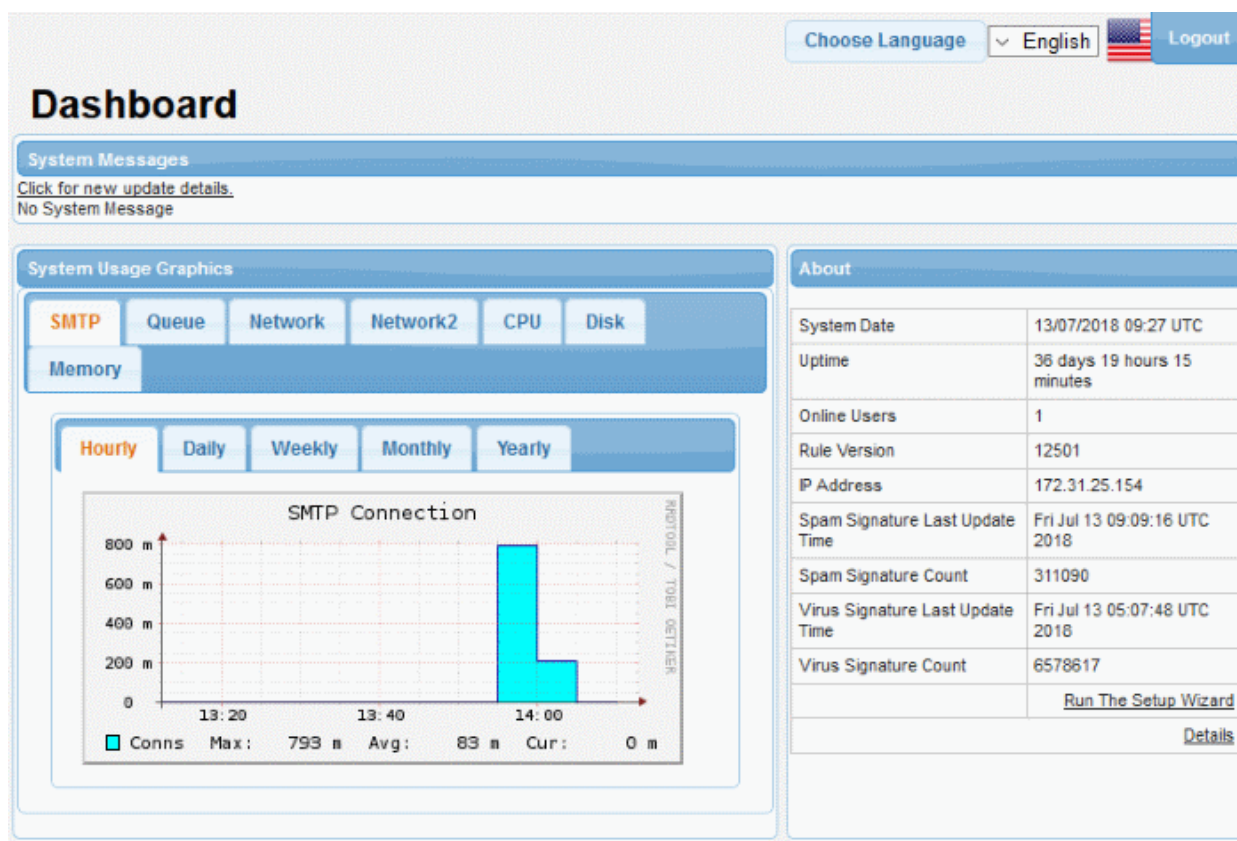
- **System Messages:** Displays error messages or important notifications that might affect the performance of the messaging gateway.
- **System Usage Graphics:** Provides a graphical representation of the system usage such as SMTP connection rate in hourly, daily, weekly, monthly or yearly basis, utilization of network, CPU, disk and memory. See '**System Usage Graphics**' for more details.
- **About:** Allows you to change your current password, view software details and manage the license. See **About Software**.
- **Run the Setup Wizard:** Enables administrators to quickly configure the Secure Email Gateway system.

You can change the theme from the settings interface. [Click here](#) to know how.

2 The Dashboard

The dashboard displays statistics about your mail traffic and provides overall system details. You can also view important system messages and update the license.

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



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

You can change the theme from the settings interface. [Click here](#) to know how.

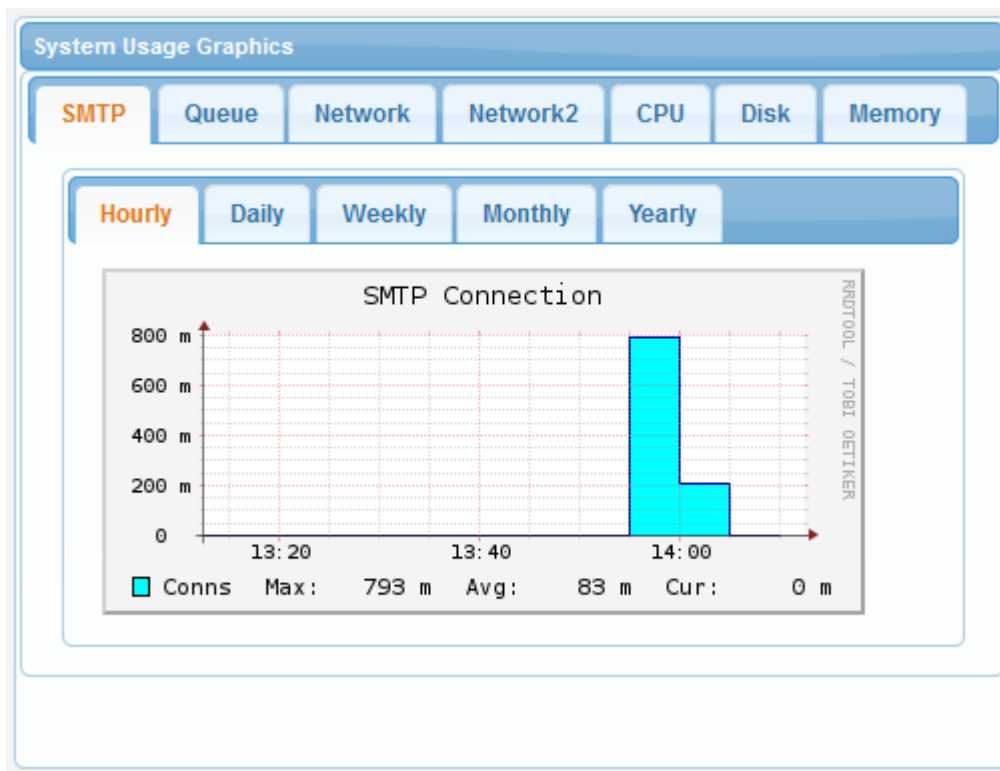
Click the following links for more details about other areas in the dashboard:

- **System Usage Graphics**

- **About Software**

2.1 System Usage Graphics

The 'System Usage Graphics' area displays a graphical summary of SMTP connections, the number of queued mails, network utilization rate, CPU utilization rate, disk usage and system memory usage. 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 Secure Email Gateway 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.

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

2.2 About Software

The 'About' section in the 'Dashboard' area displays hardware, software and virus update details.

About	
System Date	23/12/2019 08:03 UTC
Uptime	229 days 19 hours 13 minutes
Online Users	1
Rule Version	13575
IP Address	172.31.19.251
Spam Signature Last Update Time	Mon Dec 23 07:30:02 UTC 2019
Spam Signature Count	187863
Virus Signature Last Update Time	Sun Dec 22 10:30:03 UTC 2019
Virus Signature Count	6639252
	Run The Setup Wizard
	Details

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

About	
<div style="display: flex; justify-content: space-between;"> About System Admin </div>	
Engine Version	Koromail SMTP Filter Engine Koromail 6.7.8
User Interface Version	Release 6.7.8 - Build 5225ada
Patch Level	6708
Spam Signature Last Update Time	Mon Dec 23 08:07:17 UTC 2019
Spam Signature Count	188079
Virus Signature Last Update Time	Sun Dec 22 10:30:03 UTC 2019
Virus Signature Count	6639252

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

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

About

About
System Admin

System Admin Name:	<input type="text" value="SEC"/>
System Admin Surname:	<input type="text" value="Demo"/>
System Admin Tel. No.:	<input type="text"/>
System Admin E-mail *	<input type="text" value="ilyas.pala@comodo.cc"/>

- When the SMTP IPS module blocks IP addresses, a list of the blocked IP's will be sent to the e-mail address shown in this interface.
- If the field 'System Admin E-mail' is left blank then an error message will be displayed in 'System Messages' in the dashboard.
- Click 'Save' after completing all fields.

Run 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 setup wizard screen will be displayed. This allows you to choose the SSL certificate you wish to use on your console, as well as system admin details, LDAP profiles, 'Managed Domains', 'Routes' and 'Relay' details.


The screenshot shows the main dashboard with a 'Run The Setup Wizard' link circled in red. Below it, the 'Setup Wizard Certificate Entrance' screen is displayed, featuring a 'Certificate File' upload field, a 'Password' field, and a 'Next' button.

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

- Upload a certificate you have on file. Ideally, this will be a certificate which you have obtained from a trusted certificate authority. Using such a certificate means you will not see browser error messages when you access the admin console. Note: The certificate should be for the domain that Comodo has setup for your Secure Email Gateway console on the AWS instance. Details of your Secure Email Gateway domain will have been sent to your registered email after you signed up for the account.
- Use the default, self-signed certificate. Secure Email Gateway will automatically install a self-signed certificate on your console. Your connection to the console will be just as secure as above, but your

browser will show error messages as the certificate is not signed by a trusted certificate authority. You can bypass these errors and create an exception in your browser to avoid these messages in future.

- You can also upload SSL certificate from the setting interface. [Click here](#) for details.
- Click next to enter admin details such as 'System Admin Name', 'System Admin Surname', 'System Admin Tel. No' and 'System Admin E-mail'.

[Choose Language](#) | English  [Logout](#)

Setup Wizard


System Admin

Default Certificate will be used.

System Admin Name	<input type="text" value="Dome AS"/>
System Admin Surname	<input type="text" value="Demo"/>
System Admin Tel. No.	<input type="text" value="123456789"/>
System Admin E-mail *	<input type="text" value="domersa@yopmail.com"/>

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






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

[Choose Language](#) | English  [Logout](#)

Setup Wizard

LDAP

[+ Add LDAP profile](#)

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

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

See the **LDAP** section for more details.

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

Choose Language v English Logout

Setup Wizard

Managed Domains

Managed Domain Name	Generate Report	Owner	Action
<input type="text"/>	<input type="checkbox"/>		
arda.com	<input checked="" type="checkbox"/>	admin	
office365domain.com	<input checked="" type="checkbox"/>	admin	
outlook.com	<input checked="" type="checkbox"/>	admin	
pala.com	<input checked="" type="checkbox"/>	admin	
steven.com	<input type="checkbox"/>	admin	
	<input type="checkbox"/>	admin	
	<input checked="" type="checkbox"/>	admin	
test.com	<input checked="" type="checkbox"/>	admin	
testcustomer.com	<input type="checkbox"/>	admin	
testdomain.com	<input checked="" type="checkbox"/>	admin	
testtest.com	<input type="checkbox"/>	admin	
yahoo.com	<input checked="" type="checkbox"/>	admin	
yandex.com	<input checked="" type="checkbox"/>	admin	
yeni.com	<input type="checkbox"/>	admin	
yopmail.com	<input type="checkbox"/>	admin	

See the **Manage Domains** section for more details.

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

Choose Language v English Logout


Setup Wizard

Routes

Managed Domain Name	Routing Type	SMTP Server	Port Number	User Verification	LDAP/DB Profile	Action
-Choose-	IPv4	<input type="text"/>	<input type="text" value="25"/>	None	None	
bilisim.ml	IPv4	217.79.179.102	25	None	-None-	
bulut.ml	IPv4	78.31.65.172	25	None	-None-	
comodo.ordabirbahce.com	IPv4	213.14.70.194	25	None	-None-	
example.com	IPv4	192.168.199.31	25	None	-None-	
steven.com	IPv6 or HOSTNAME	mail.steven.com	25	LDAP	company LDAP	
test.com	LDAP			LDAP	Default OpenLDAP	
testcustomer.com	IPv4	213.168.32.78	25	None	-None-	
yahoo.com	IPv6 or HOSTNAME	smtp.mail.yahoo.com	25	LocalUserDB	LocalUserDB	
yopmail.com	MX RECORD			MySQL		





See the **Routes** section for more details.

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

Choose Language English  Logout

Setup Wizard

Relay

IP Range	
<input type="text"/>	
192.168.2.1	
192.168.	
192.168.1.1	

Range Examples

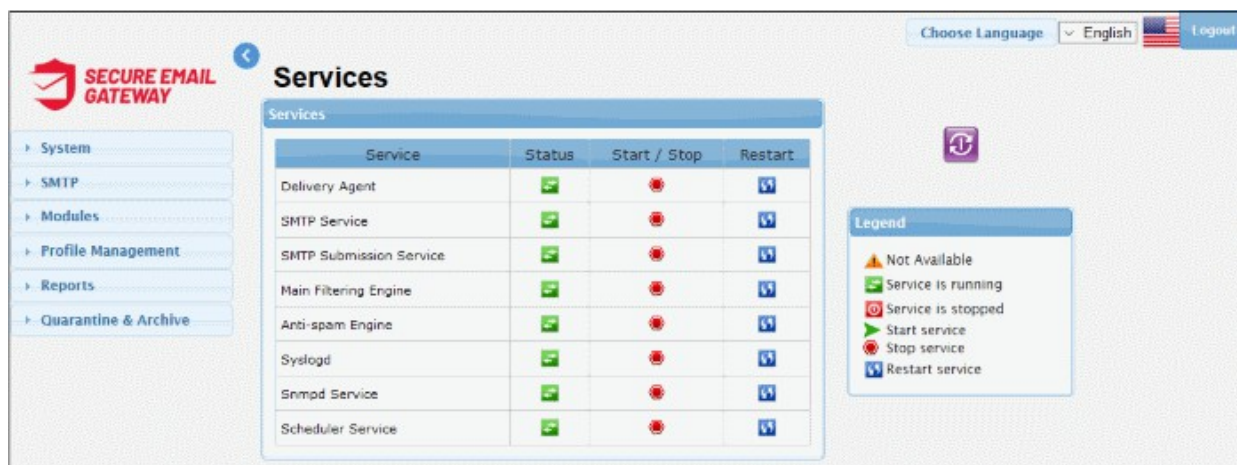
192.168.2.1 (only one IP address)
192.168.2.2-5 (IP addresses in the range 192.168.2.2 to 192.168.2.5)
192.168.2. (whole 192.168.2.0/24 C class)
192.168. (whole 192.168.0.0/16 B class)

Prev End

See the **Relay** section for more details.

3 System Configurations

The 'System' link in the left menu allows you to configure important parameters after initial configuration



- **Services:** Allows you to start or stop various services such as delivery agent, SMTP, Snmpd, scheduler and more. See '**Services**' for more details.
- **License:** View and update Secure Email Gateway licenses from this interface. See '**License**' for more details.
- **Settings:** Configure various system settings such as Cache, Session, Backup and more. See '**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. See '**Logs**' for more details.
- **Tools:** Allows admin users to check connectivity such as SMTP, Ping, Nslookup, Telnet as well as clear SMTP queue. See '**Tools**' for more details.
- **Session Reports:** Enables you to view the details of last login and last activity performed on the user interface. See '**Session Reports**' for more details
- **Statistics:** View the graphical summary of system usage. See '**System Usage Statistics**' for more details.

3.1 Services

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





- To view and configure Secure Email Gateway services, click the 'System' tab on the left then 'Services':




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

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

Description of the Services	
Column Header	Description
Delivery Agent	The service forwards the emails processed by Secure Email Gateway to target email server.
SMTP Service	The service that filters emails on hosted domain names on Secure Email Gateway. 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 - Secure Email Gateway 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.
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 Secure Email Gateway Delivery Agent.
Anti-spam Engine	Secure Email Gateway 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.
Syslogd	The daemon service that stores system logs in rsyslog format.
Snmpd Service	It is a Simple Network Management Protocol (SNMP) agent which binds to port and acts on SNMP management application's requests and sends the requested information to the requester.
Scheduler Service	This service organizes the programs that runs periodically. This feature in Secure Email Gateway creates periodic reports and graphics about system usage.

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

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

- To restart a service, click on the  button under the 'Restart' column. If the service is running, it will stop and restart again. If the service is stopped, then it will restart.
- To shutdown the Secure Email Gateway, click on the  button.
- To reboot the Secure Email Gateway, click on the  button.

3.2 License

The 'License' screen allows you to view current license details as well as to create a license requests and install a new license. Secure Email Gateway 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 Secure Email Gateway license, click the 'System' tab on the left menu then 'License'

License

Licenses
License Activation
End User License Agreement

Automatic Renewal	No
Users	100
Current Users Count	<div style="width: 10px; height: 10px; background-color: green; display: inline-block;"></div>
Activation Date	2017-10-12 00:00:00
License Expiration Date	2020-04-26 23:59:59
Remaining Days	125
Current CAM Activation Key	XXXXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
Status	<div style="width: 10px; height: 10px; background-color: green; display: inline-block;"></div>
Click here to get CAM license key	

From here you can:

- View the details of your current license**

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 Secure Email Gateway license purchase procedure.

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

Activate your license

- Click the 'License Activation' tab.

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 'Save'.

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.

Choose Language English Logout

License

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

END USER LICENSE AGREEMENT COMODO DOME ANTISPAM

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THIS AGREEMENT CAREFULLY BEFORE ACCEPTING ITS TERMS AND CONDITIONS

IMPORTANT – PLEASE READ THESE TERMS CAREFULLY BEFORE USING THE PRODUCT. THE “PRODUCT” MEANS COMODO’S DOME ANTISPAM, INCLUDING ALL OF THE ELECTRONIC FILES, DOCUMENTATION, AND SOFTWARE PROVIDED THEREIN, EXCEPT AS EXPRESSLY STATED HEREIN. BY USING THE PRODUCT, OR BY CLICKING ON “I ACCEPT” BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS HEREIN, DO NOT USE THE PRODUCT, SUBSCRIBE TO OR USE THE SERVICES, OR CLICK ON “I ACCEPT”.

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 DAMAGE.

ACCEPTANCE

10
EULA – Comodo Dome Antispam (20161031)

BY CLICKING “I ACCEPT” BELOW, SUBSCRIBER AGREES THAT IT HAS READ AND UNDERSTANDS THIS AGREEMENT AND THAT IT WILL BE BOUND BY AND COMPLY WITH ALL OF ITS TERMS. DO NOT CLICK THE “I ACCEPT” BUTTON IF SUBSCRIBER DOES NOT AGREE TO THE TERMS OF THIS AGREEMENT.

[Download As PDF](#)

- Read the EULA fully.

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

- To download the PDF, click 'Download Ad PDF' link at the bottom left corner of the interface.

...distribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. * Redistribution provided with the distribution. * The names of its contributors may not be used to endorse or promote products derived from this software v

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

ACCEPTANCE

10
EULA – Comodo Dome Antispam (20161031)

BY CLICKING “I ACCEPT” BELOW, SUBSCRIBER AGREES THAT IT HAS READ AND UNDERSTANDS THIS AGREEMENT AND THAT IT WILL THIS AGREEMENT.

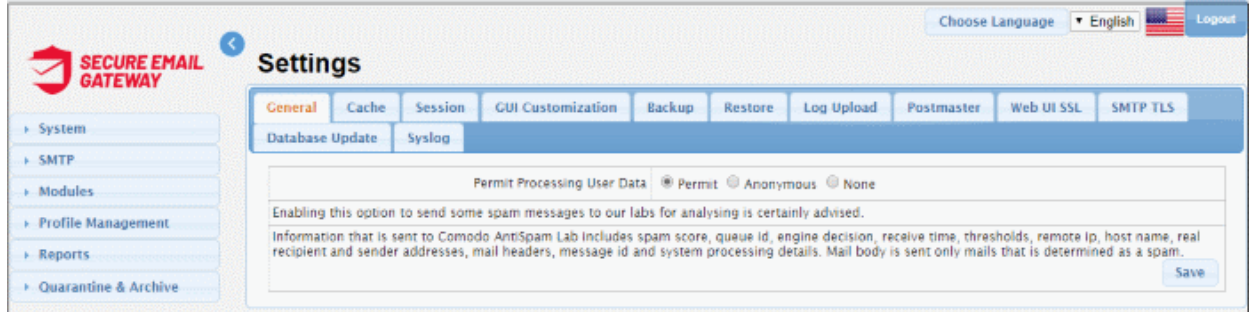
[Download As PDF](#)

The pdf will be downloaded.

3.3 Configure System Settings

The 'Settings' interface lets you configure all aspects of Secure Email Gateway.

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



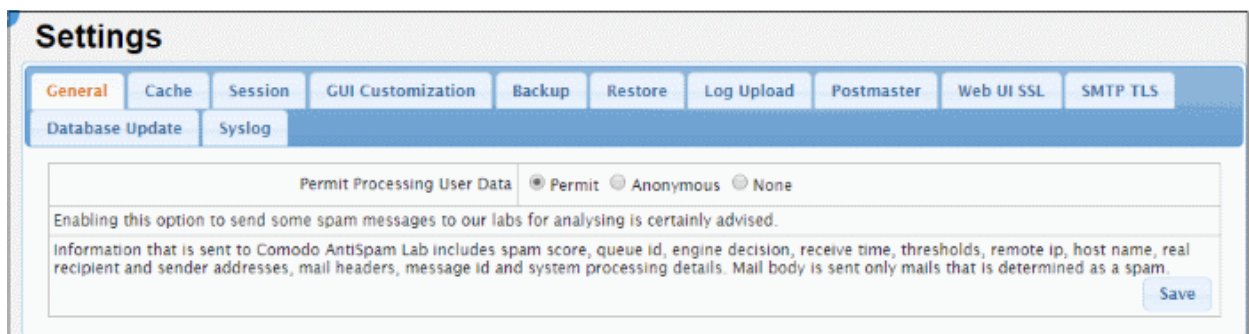
Click the following links for more details:

- [General](#)
- [Cache](#)
- [Session](#)
- [GUI Customization](#)
- [Backup](#)
- [Restore](#)
- [Log Upload](#)
- [Postmaster](#)
- [Web UI SSL Certificate](#)
- [SMTP TLS](#)
- [Update Database](#)
- [Syslog](#)

3.3.1 System General Settings

The 'General' settings tab lets you enable or disable automatic upload of selected spam messages to Comodo for analysis.

- To open the interface, click 'System' on the left then 'Settings' > 'General'.



- **Permit Processing User Data:**
 - Permit - Selected spam messages will be uploaded to Comodo labs for analysis.
 - Anonymous - Selected spam messages will be uploaded anonymously, without data which links them to your company or users.
 - None - Spam messages will not be uploaded to Comodo.
- Click 'Save' to apply your changes.

3.3.2 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.

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

- **Greylist IP Cache expire time:** Secure Email Gateway 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 Secure Email Gateway does not query the LDAP server.
- Click the 'Clear Now' beside an item to clear the cache immediately.
- Click 'Save' to apply your changes.

3.3.3 Session Settings

The 'Session' tab lets you configure the session timeout period and to limit the number of times an admin can log into the console before the password has to be changed.

- To open the interface, click 'System' on the left then 'Settings' > 'Session'.

Settings

General Cache **Session** GUI Customization Backup Restore Log Upload Postmaster Web UI SSL SMTP TLS

Database Update Syslog

Session Timeout Duration: 30 minutes

Login Limit: 100

Save

- **Session Timeout Duration:** Determines how many minutes of inactivity should be allowed before all users are automatically logged out.
- **Login Limit:** Enter the maximum amount of users that can login to the portal at the same time.
- Click 'Save' to apply your changes.

3.3.4 GUI Customization

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

- To open the interface, click 'System' on the left then 'Settings' > 'GUI Customization'

Settings

General Cache Session **GUI Customization** Backup Restore Log Upload Postmaster Web UI SSL SMTP TLS

Database Update Syslog

Company: Dome Antispam

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

Theme: Redmond

Save

- **Company:** Type the name of the company to be shown in the interface.
- **Logo:** Upload your company logo. The logo will be shown in the interface to all users. Images should be in .png format and no larger than 150 px L x 100 px H.
 - Click 'Upload', choose file then again click 'Upload'
 - To remove the logo, click the 'Clear' link.
 - Click 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 'Save' to apply your changes.

3.3.5 System Backup

The 'Backup' tab allows you store copies of all configurations and logs. You can also automate the backup process by scheduling the backup dates and time. You can restore your antispam configuration from your backup at any time.

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

Instant Backup

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

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

The screenshot shows the 'Settings' page with the 'Backup' tab selected. The 'Backup Password' field is filled with dots. Below it, the 'Create Backup' button is circled in red. A blue progress bar is visible, and below it, the link 'Click here to download backup' is also circled in red. The 'Enable Auto Backup' checkbox is unchecked. A 'Save' button is at the bottom.

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

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

Scheduled Backup

You can automate the backup process by scheduling the jobs.

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

The screenshot shows the 'Settings' page with the 'Backup' tab selected. The 'Enable Auto Backup' checkbox is checked. Below it, the 'Host' field contains '10.108.51.100', 'User' contains 'John', and 'Password' fields are filled with dots. The 'Remote Path' field is empty. The 'Backup type' dropdown is set to 'FTP'. The 'Days to backup' section has 'Monday' checked. The 'Backup hour' dropdown is set to '07:00'. A 'Save' button is at the bottom.

- Host:** The name or IP of the system where the data should be backed up.
- User:** The user name of the system
- Password:** Enter the password to access the system
- Remote Path:** Enter the remote path of the system including the folder name. Leaving the field blank means the backup will be uploaded to the default FTP folder.
- Backup type:** Select the backup type from the drop-down. Currently only FTP option is available.

- **Days to backup:** Schedule the backup day(s) from the options.
- **Backup hour:** Select the hour when the scheduled backup should run on the selected backup day(s)
- Click 'Save'. The scheduled job will be saved. To change the schedule or the backup location, edit the settings accordingly and click 'Save'.

3.3.6 System Restore

The 'Restore' feature allows you to revert your Secure Email Gateway configuration and logs to a previous system state. The console will need to be rebooted in order to complete a restore operation.

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

Settings

General Cache Session GUI Customization Backup **Restore** Log Upload Postmaster Web UI SSL SMTP TLS

Database Update Syslog

Backup File:

Backup Password:

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

File Upload - Google Chrome

demo-das.cdome.net:8443/fileUploader.xhtml

File Upload

No file chosen

Installed Files:

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

- Click 'Restore'

Settings

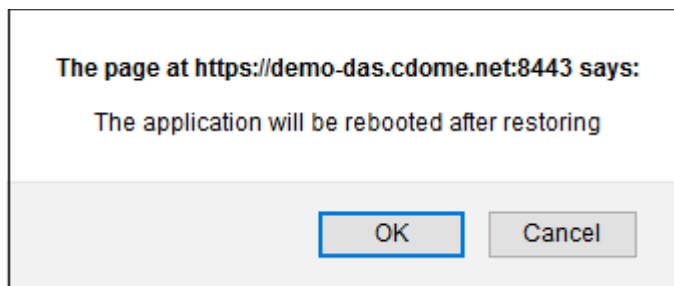
General Cache Session GUI Customization Backup **Restore** Log Upload Postmaster Web UI SSL SMTP TLS

Database Update Syslog

Backup File:

Backup Password:

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

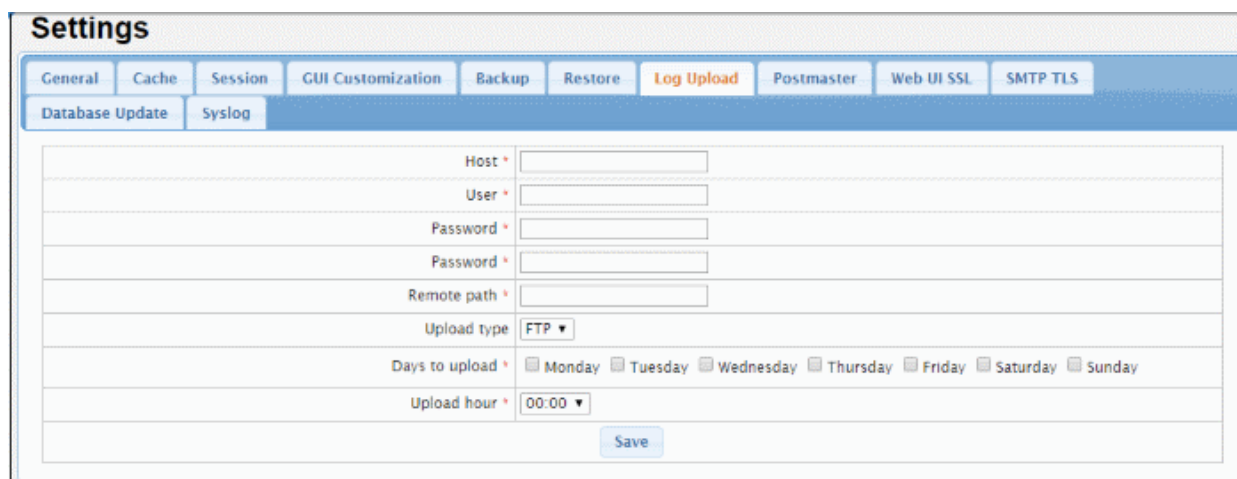


- Click 'OK' to confirm.

3.3.7 Log Upload Settings

The 'Log Upload' tab allows you to configure the automated upload of various types of Secure Email Gateway logs.

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



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

3.3.8 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. Secure Email Gateway allow administrators to forward these to other addresses and /or reject emails sent to these addresses.

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

Settings

General Cache Session GUI Customization Backup Restore Log Upload **Postmaster** Web UI SSL SMTP TLS

Database Update Syslog

Postmaster Forwarding Address Discard incoming mails

MAILER-DAEMON Forwarding Address Discard incoming mails

Save

- **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 'Save'.

3.3.9 Web UI SSL

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

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

Settings

General Cache Session GUI Customization Backup Restore Log Upload Postmaster **Web UI SSL** SMTP TLS

Database Update Syslog

Certificate Entrance

Use Default Certificate

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

Password

Save

- **Use Default Certificate** – This is an SEG self-signed certificate. Secure Email Gateway will automatically install a self-signed certificate on your console. Your connection to the console will be just as secure as above, but your browser will show error messages as the certificate is not signed by a trusted certificate authority. You can bypass these errors and create an exception in your browser to avoid these messages in future.
- **Certificate File** - Upload a certificate you have on file. Ideally, this will be a certificate which you have obtained from a trusted certificate authority. Using such a certificate means you will not see browser error messages when you access the admin console. Note: The certificate should be for the domain that Comodo has setup for your Secure Email Gateway console on the AWS instance. Details of your Secure Email Gateway domain will have been sent to your registered email after you signed up for the account.
 - Click 'Upload'



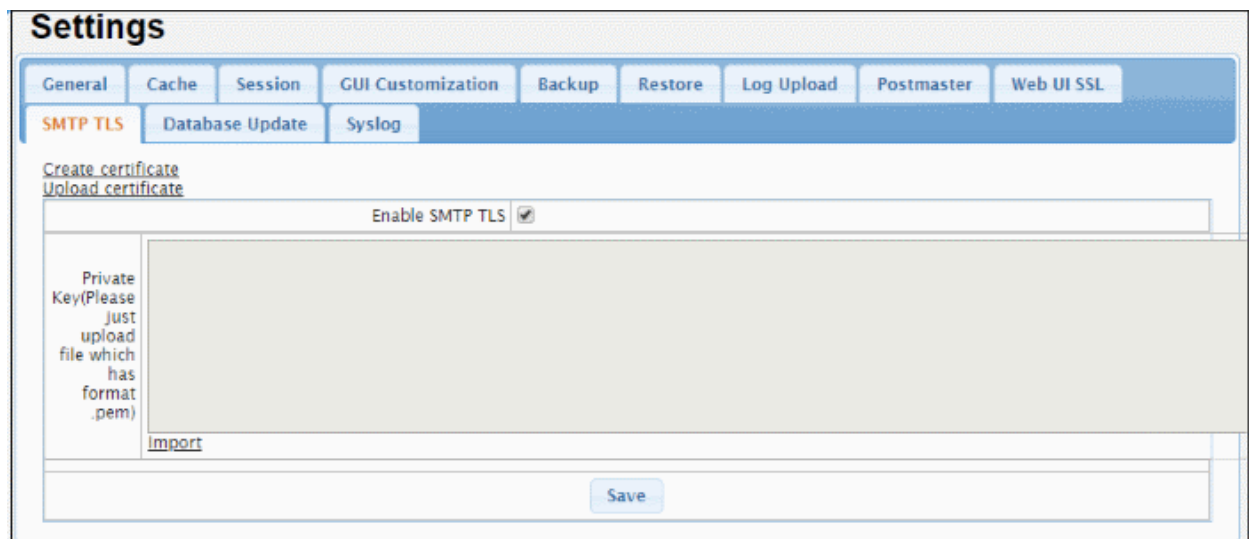
- Click 'Choose File' then select the cert file and click 'Upload'
- Enter the certificate password in the SEG interface
- Click 'Save'

3.3.10 SMTP TLS Settings

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

Open the 'SMTP TLS' settings interface

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



- Enable SMTP TLS – Select to activate SMTP TLS

Create a certificate

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

Settings

General Cache Session GUI Customization Backup Restore Log Upload Postmaster Web UI SSL

SMTP TLS Database Update Syslog

Create certificate
Upload certificate

Enable SMTP TLS

The number of days of validity of certificate * 360

Country * -- ▾

State *

City *

Department *

Host Name or IP Address *

E-mail *

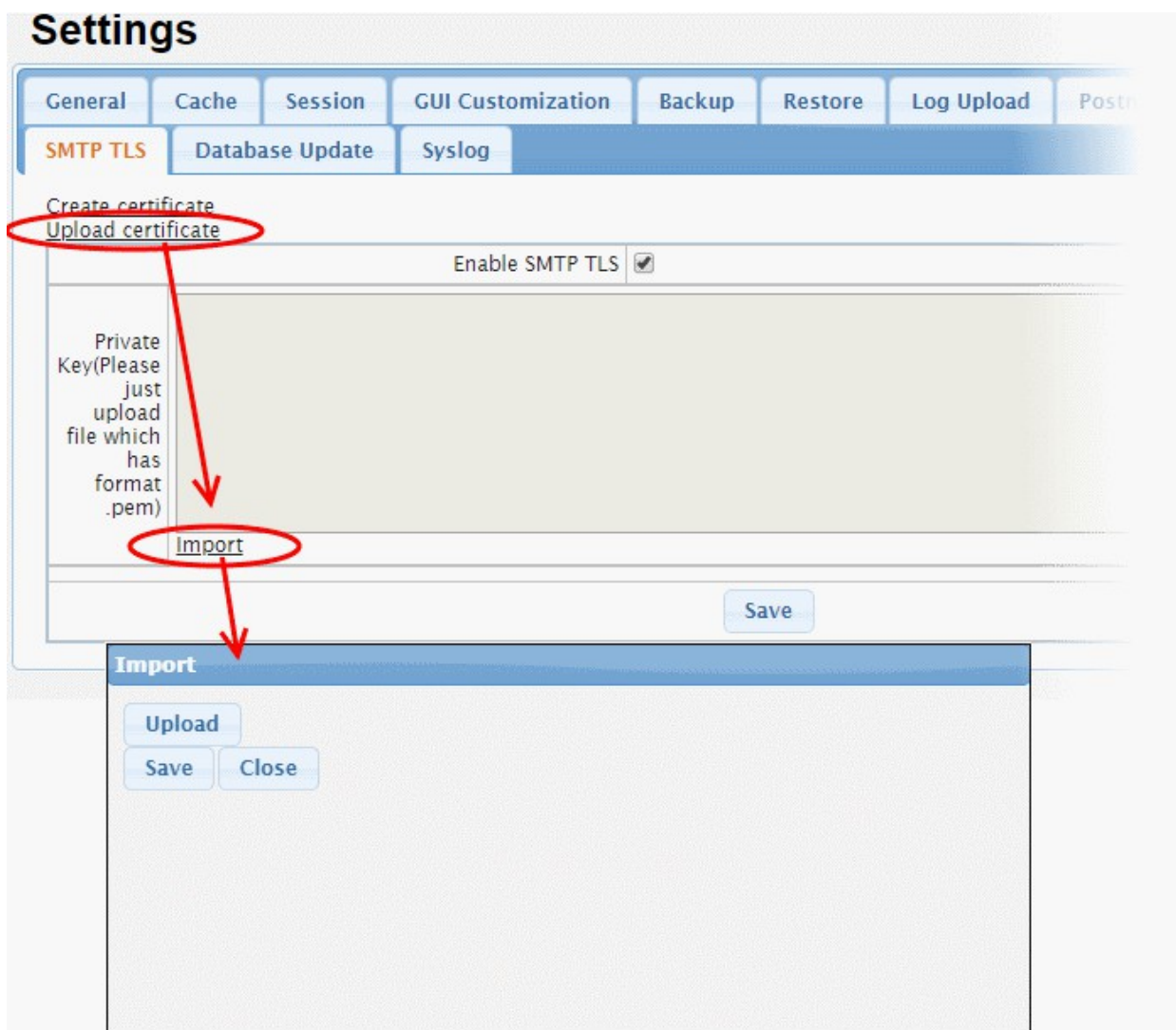
Created Date

Save

- Validity - Specify the term length of the certificate in days. Note - certificates for public-facing websites have a maximum term length of 720 days.
- Country - Select the two-character code for your country.
- State - Two character code of the state/province in which your organization is located.
- City/Locality - The name of the city in which your organization is located
- E-mail - Your contact email address
- Department – Name of the department
- Host or IP address - Type the domain, hostname or IP address of the server you want to secure
- Click 'Save' to create the certificate.

Upload a certificate

- Click 'Upload certificate' then click 'Import'

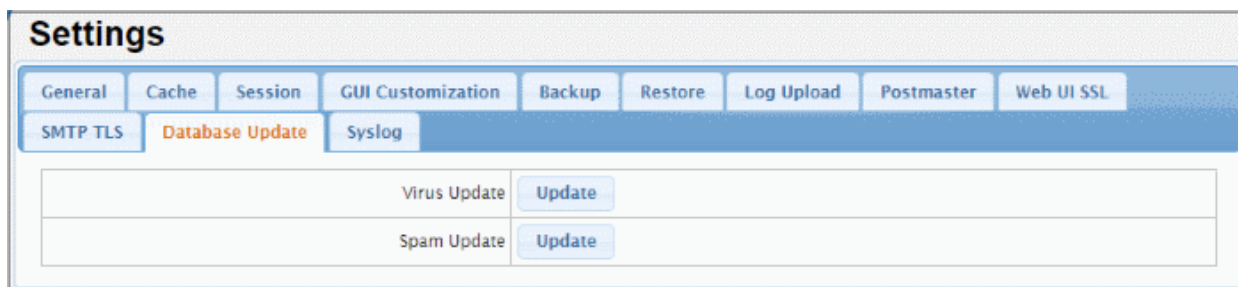


- Click the upload button to browse for the certificate you wish to import
- Click 'Save'.

3.3.11 Update Database

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

- Click 'System' > 'Settings' > 'Database Update'.



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

3.3.12 Syslog Server

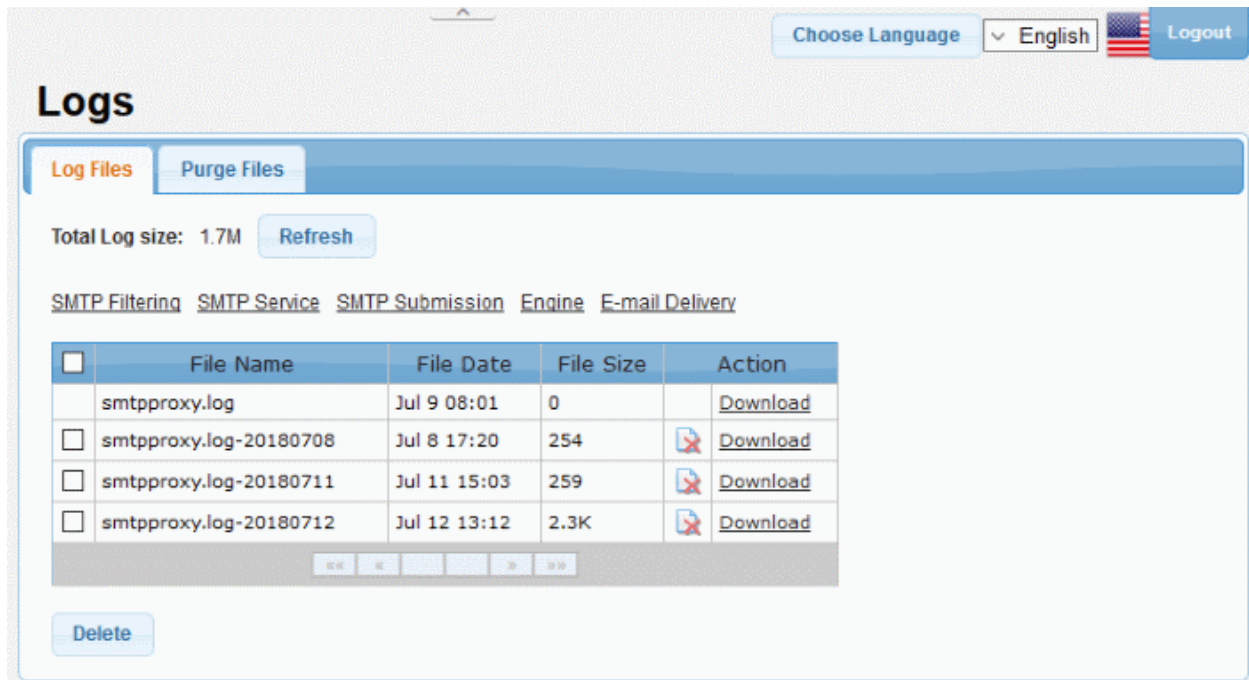
Secure Email Gateway has the ability to forward logs pertaining to various operations and configuration changes to a remote Syslog server.

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

- **Enable Syslog Server:** Enable this to store logs on your remote server. Enter your Syslog server details in the fields provided:
- **Host Name or IP Address:** Enter the host name or the IP address of the remote logging server to which the logs should be passed.
- **Port:** Enter the port number through which the server receives the logs. Default is 514.
- **Level:** Specify the types of logs by severity level that you want to forward to the remote logging server.
- Click 'Save'

3.4 Logs

- Secure Email Gateway 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. Logged details include mail subject, sender domain and receiver domain and more.
- Click 'System' > 'Log Files' to open this interface



The 'Logs' interface has the following tabs:

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

3.4.1 Log Files

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

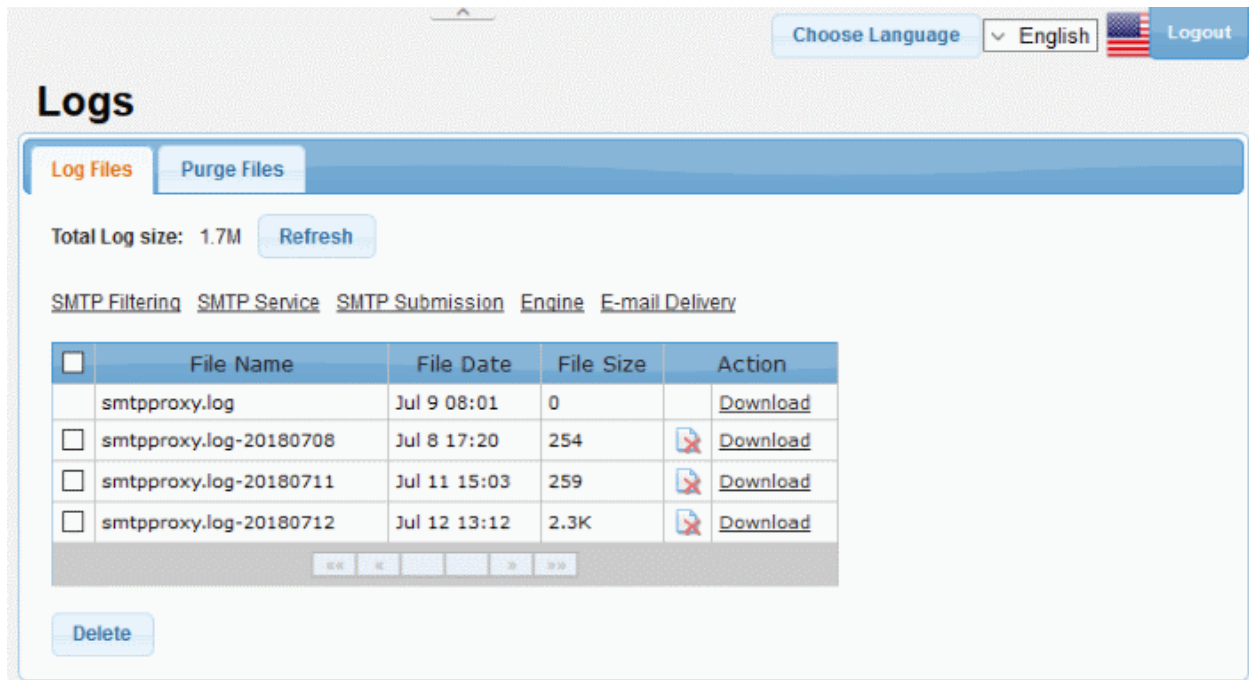
- SMTP Filtering
- SMTP Services
- SMTP Submission
- Engine Activities
- E-mail Delivery

Admins can download or delete logs as required.


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

Open the log files interface

- Click 'System' > 'Logs' > 'Log Files' in the left-hand menu



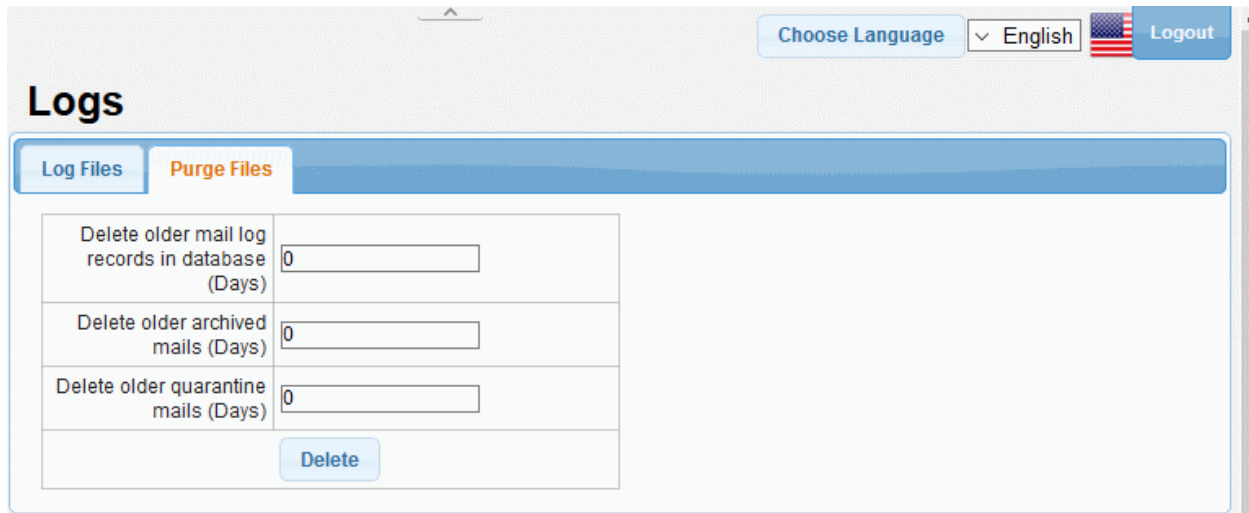
- The interface lists all available log files along with the size and date
- Use the links above the table to view a specific category of logs
- Click 'Refresh' to reload the list with the latest logs.

Log Files - Table of Column Descriptions	
Column Header	Description
File Name	Log label
File Date	Date and time the file was created
File Size	Size of the log file
Actions	 Delete selected logs.
	Download Save a copy of a log.

3.4.2 Purge Files

The 'Purge Files' interface allows you to configure the time limit for preserving log files, archived mails and quarantine mails. Items that are older than the period specified in this interface will be automatically removed.

- Click 'System' on the left then 'Logs'
- Click the 'Purge Files' tab

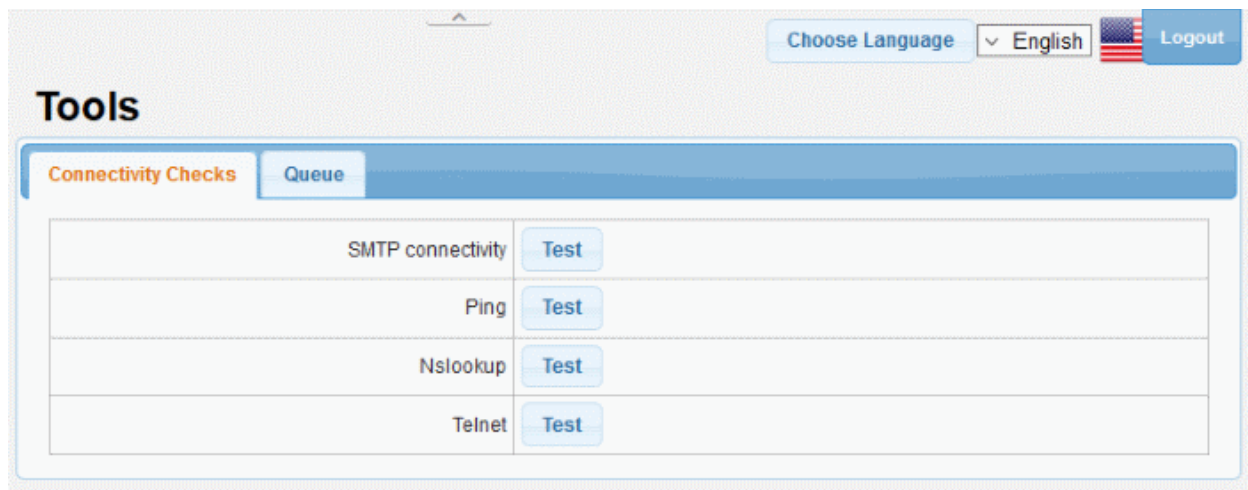


- Delete older mail log records in database (Days) - Specify the number of days to store the log files. The log files older than the days specified here will be automatically deleted.
- Delete older archived mails (Days) - Specify the number of days for which the quarantined mails are to be retained 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.
- Click 'Delete' to run the remove operation.

3.5 Tools

Secure Email Gateway 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.

- Click 'System' on the left then 'Tools'



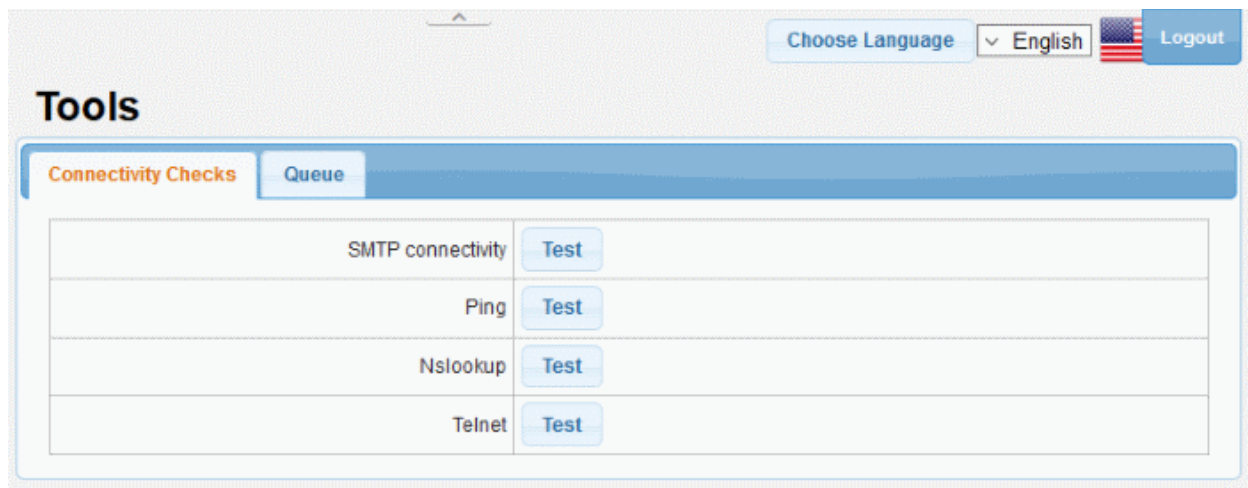
The tools interface has two tabs:

- **Connectivity Checks**
- **SMTP Queue**

3.5.1 Check Connectivity

The 'Connectivity Checks' tab allows you to test Secure Email Gateway's connectivity to external mail servers and clients

- Click 'System' on the left then 'Tools'
- Click 'Connectivity Checks' tab if not already open



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**

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 Secure Email Gateway Enterprise Admin Guide. The 'Connectivity Checks' tab is selected, and the 'Test' button next to 'SMTP connectivity' is circled in red. A red arrow points from this button to the 'Check remote SMTP Connectivity' dialog box. The dialog box contains the following fields:

Host Name or IP Address *	<input type="text"/>
Port	<input type="text" value="25"/>
Sender *	<input type="text"/>
Recipient *	<input type="text"/>
Result	<div style="border: 1px solid gray; height: 100px;"></div>

At the bottom of the dialog box, there are 'Send' and 'Close' buttons.

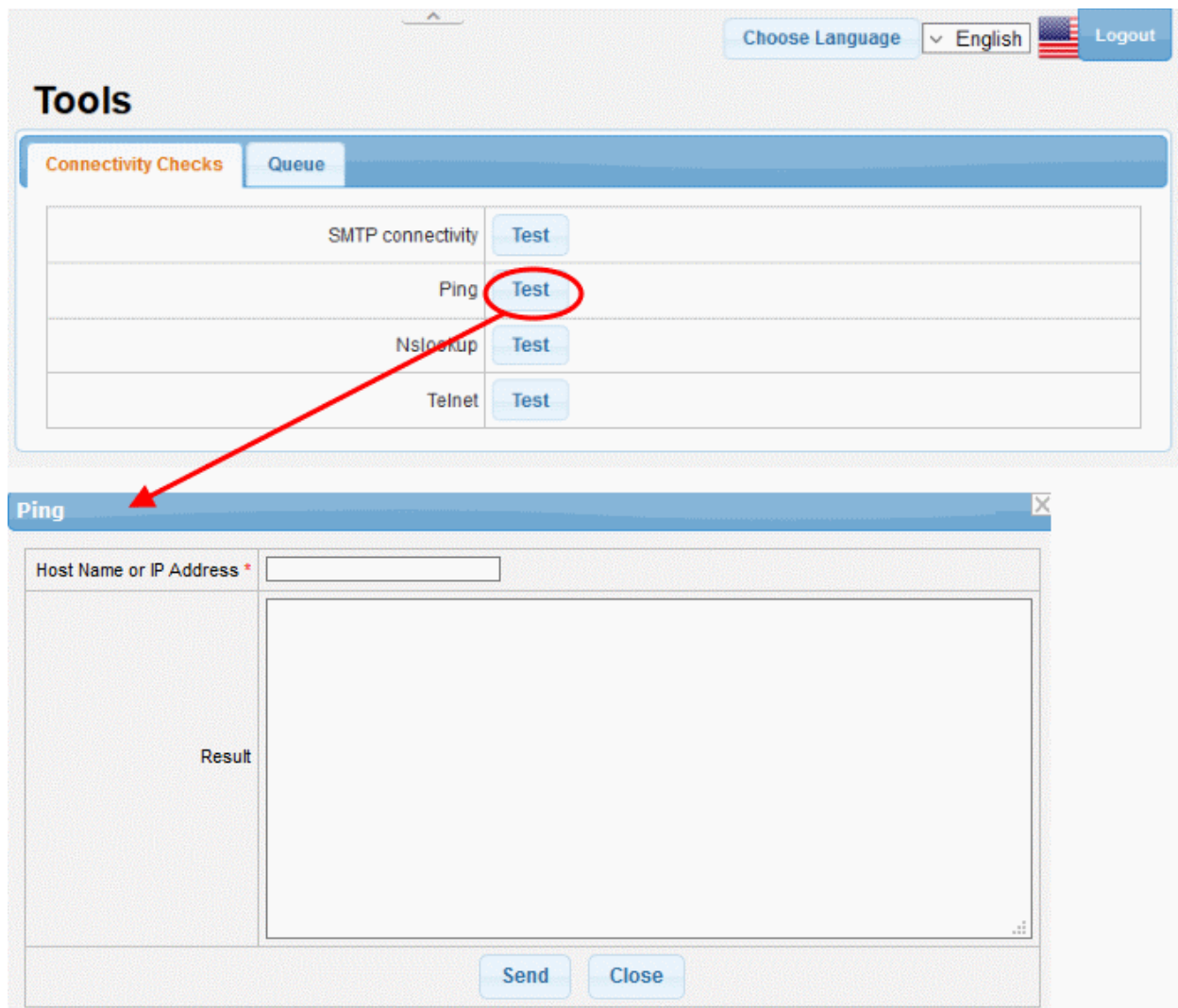
The 'Check remote SMTP Connectivity' interface will appear.

- 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'

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

Check connectivity to a remote host

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



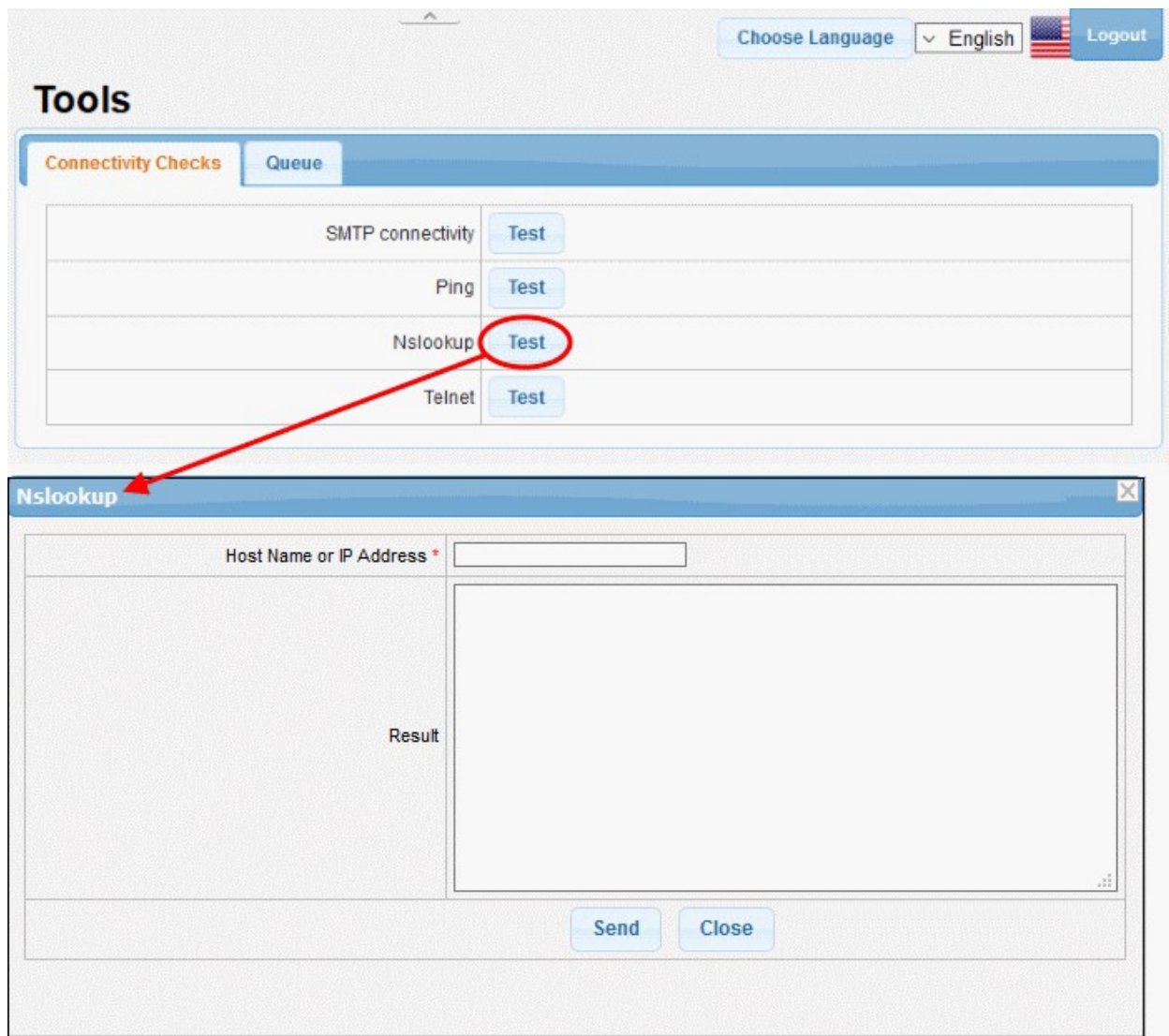
The 'Ping' interface will appear.

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

Secure Email Gateway will ping the remote host and display the results in the 'Result' field.

Lookup name server for a remote host

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



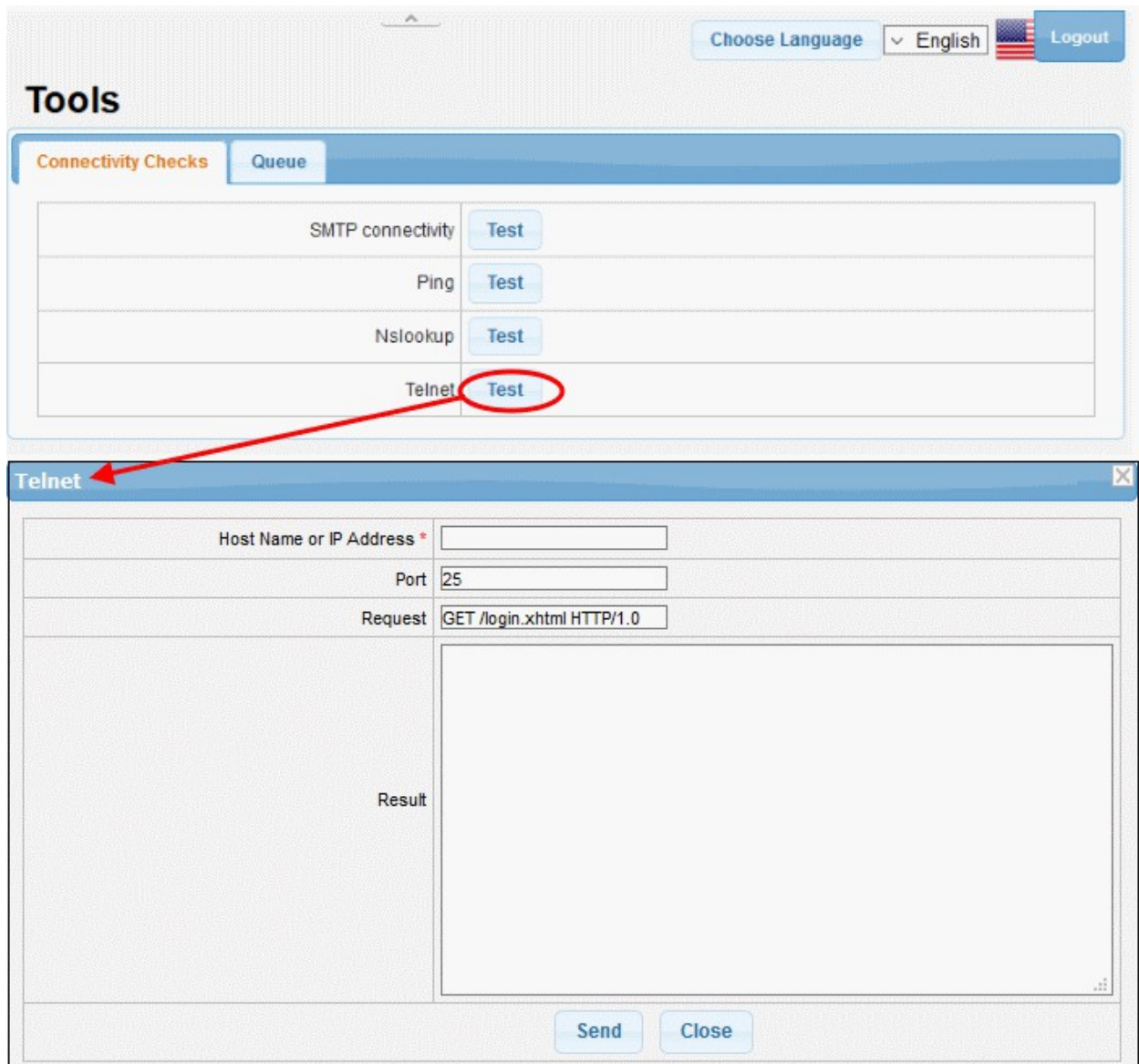
The 'Nslookup' interface will appear.

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

Secure Email Gateway 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.

Check Telnet connectivity to a remote host

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



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).
- Secure Email Gateway 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'

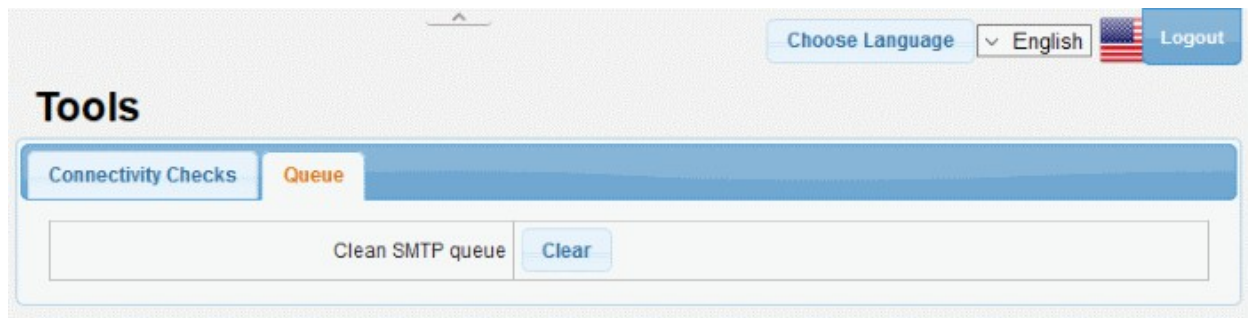
Secure Email Gateway will send the request to the remote host for checking the Telnet connectivity and display the results in the 'Result' field.

3.5.2 Clear SMTP Queue

The 'Queue' tab under the 'Tools' interface allows admins to remove mails that have been queued for SMTP forwarding.

Clear the SMTP queue

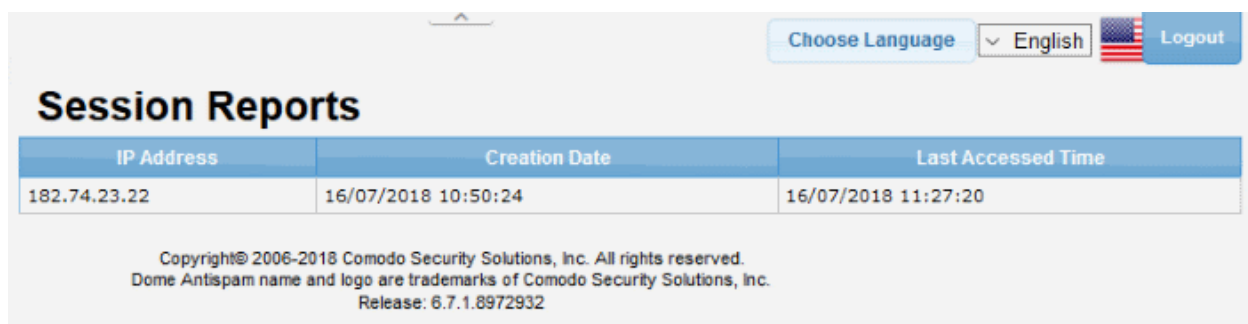
- Click the 'System' tab from the left, then 'Tools' and 'Queue' tab.



- Click the Clear button beside CLEAN SMTP queue.

3.6 Session Reports

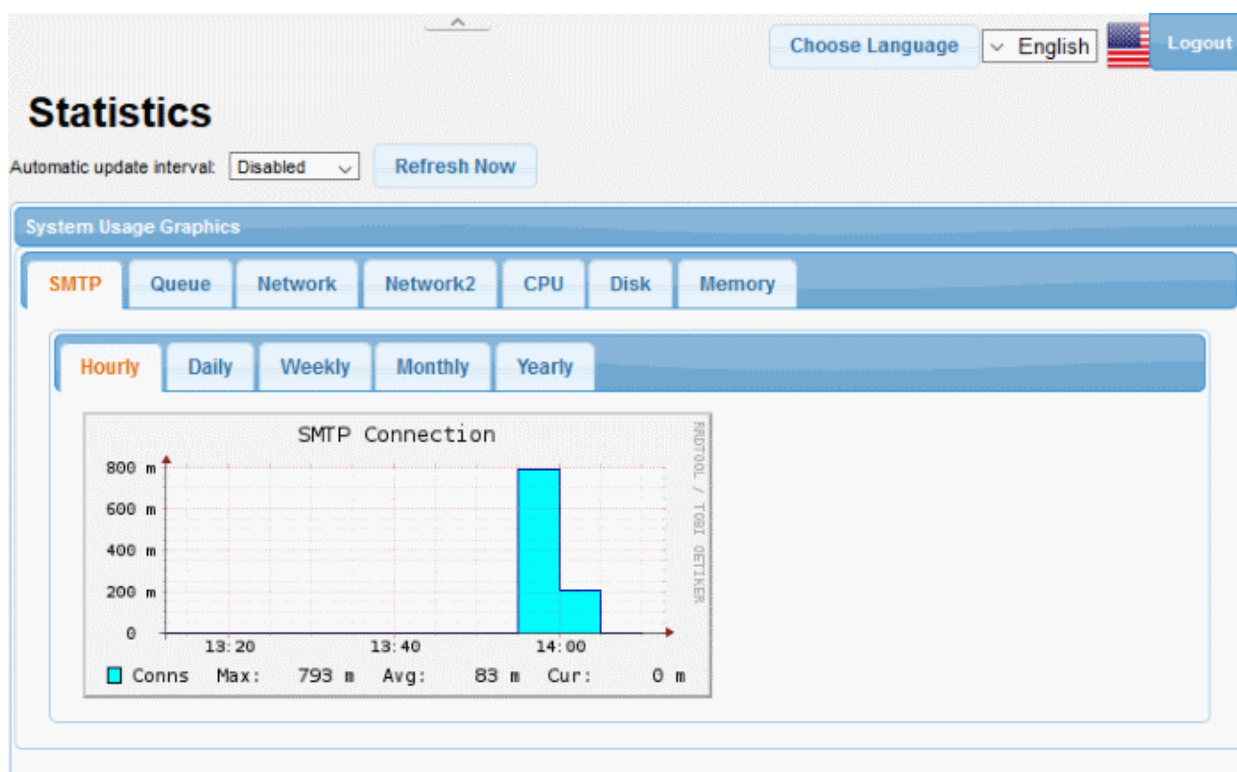
- Click the 'System' tab from the left, then click 'Session Reports'.
- Session reports show all currently active logins.
- Details include the IP address of the user, the last login time and the details of last activity performed on the user interface.



3.7 System Usage Statistics

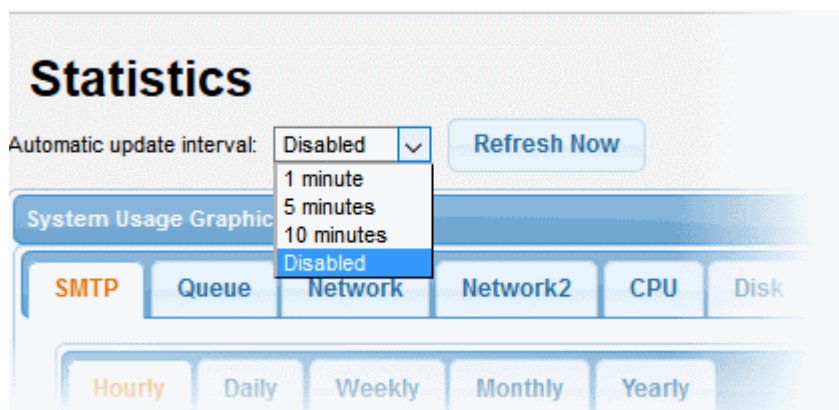
Secure Email Gateway displays SMTP connection statistics, mail statistics and utilization statistics of hardware and software resources like network, CPU, hard disks and system memory as graphs in the 'Statistics' interface.

- Click 'System' on the left then 'Statistics'



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.



- Click 'Refresh Now' to instantly update the statistics

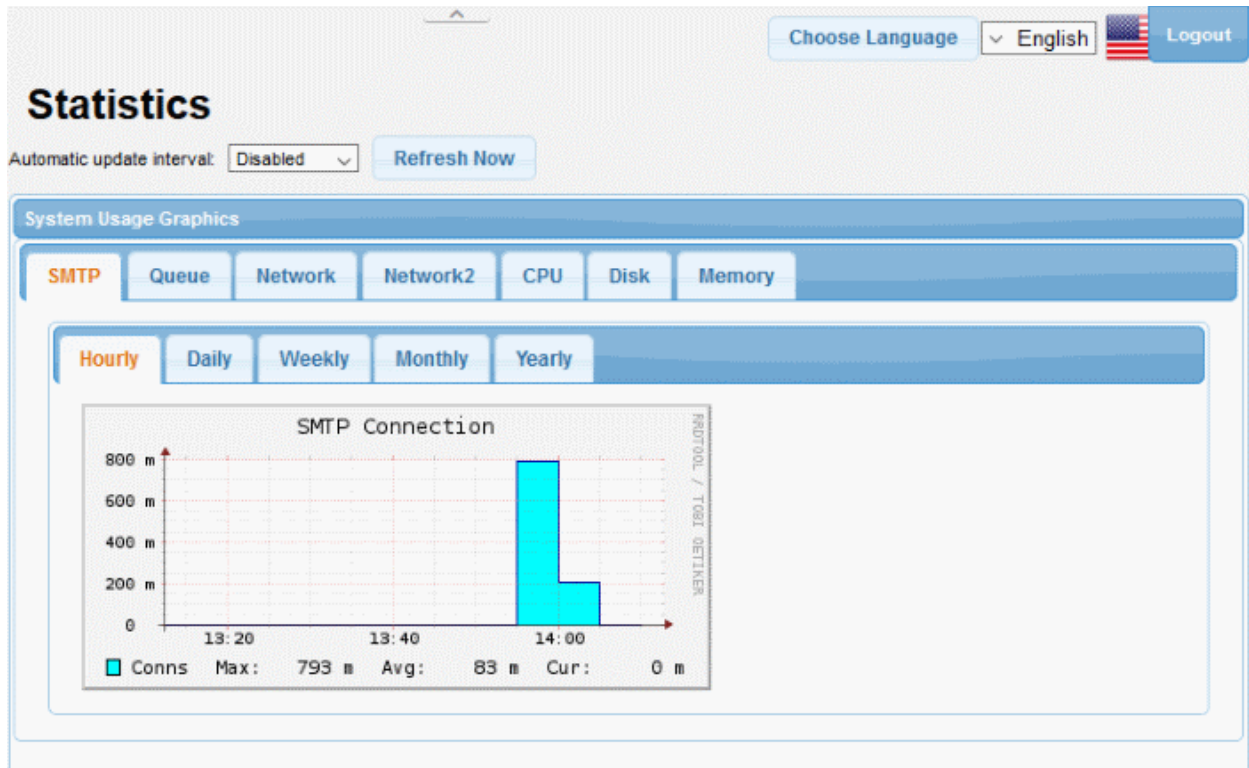
The 'System Usage Graphics' area displays the connection and usage statistics graphs under the following tabs:

- SMTP:** A graphical representation of the number of SMTP connections between Secure Email Gateway 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 Secure Email Gateway 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:

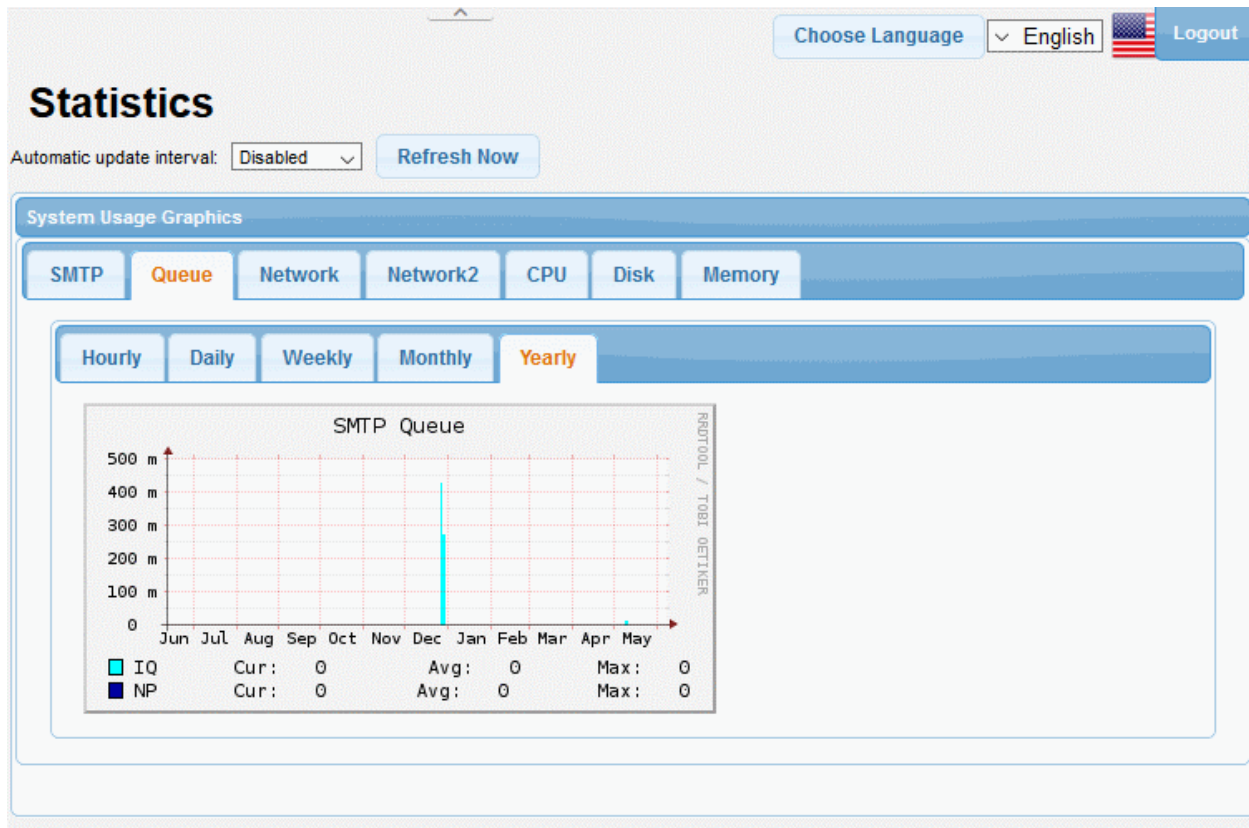


- Hourly - Shows the log of connections for the past one hour
- Daily - Shows the log of connections for the past 24 hours
- Weekly - Shows the log of connections for the past seven days
- Monthly - Shows the log of connections for the past four weeks
- Yearly - Shows the log of connections for the past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

Secure Email Gateway 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.

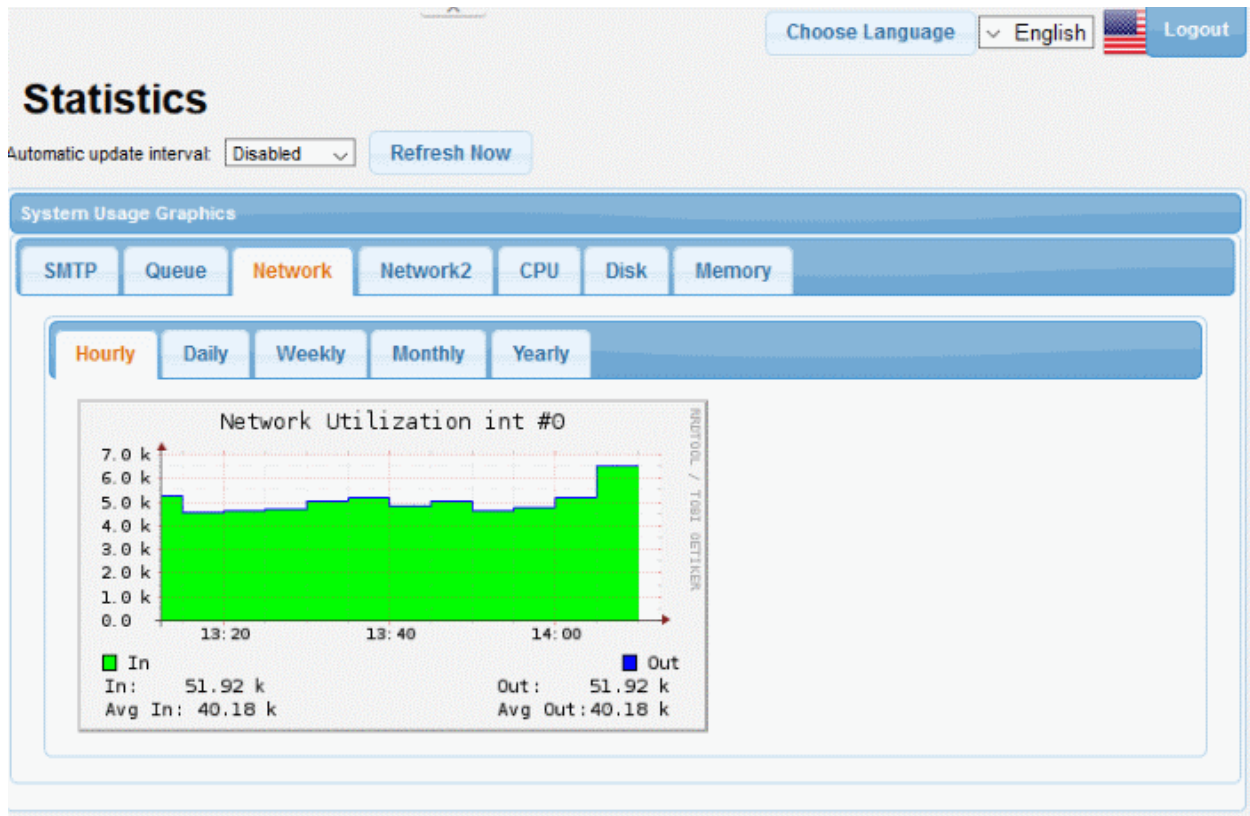


You can choose the time period for which you wish to see the logs from the sub tabs:

- 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

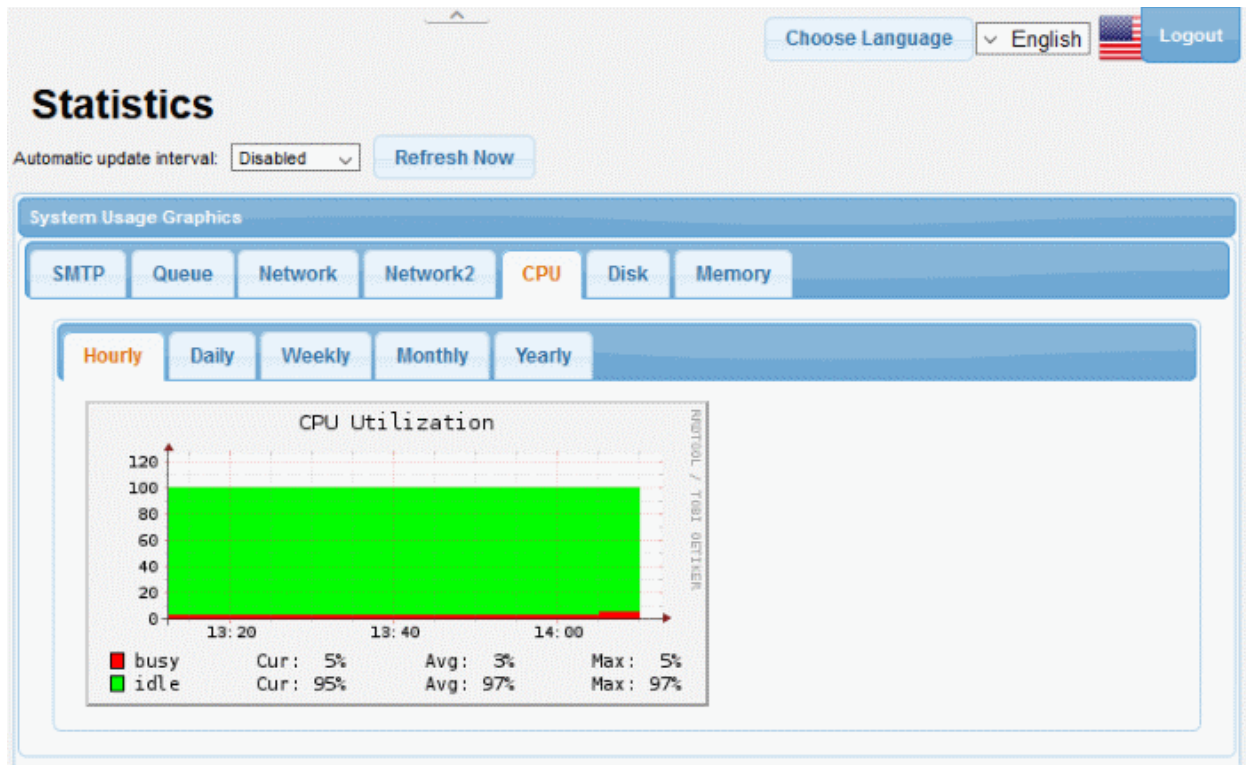
The incoming and outgoing traffic are represented with different colors in the graph.

- 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 Secure Email Gateway 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

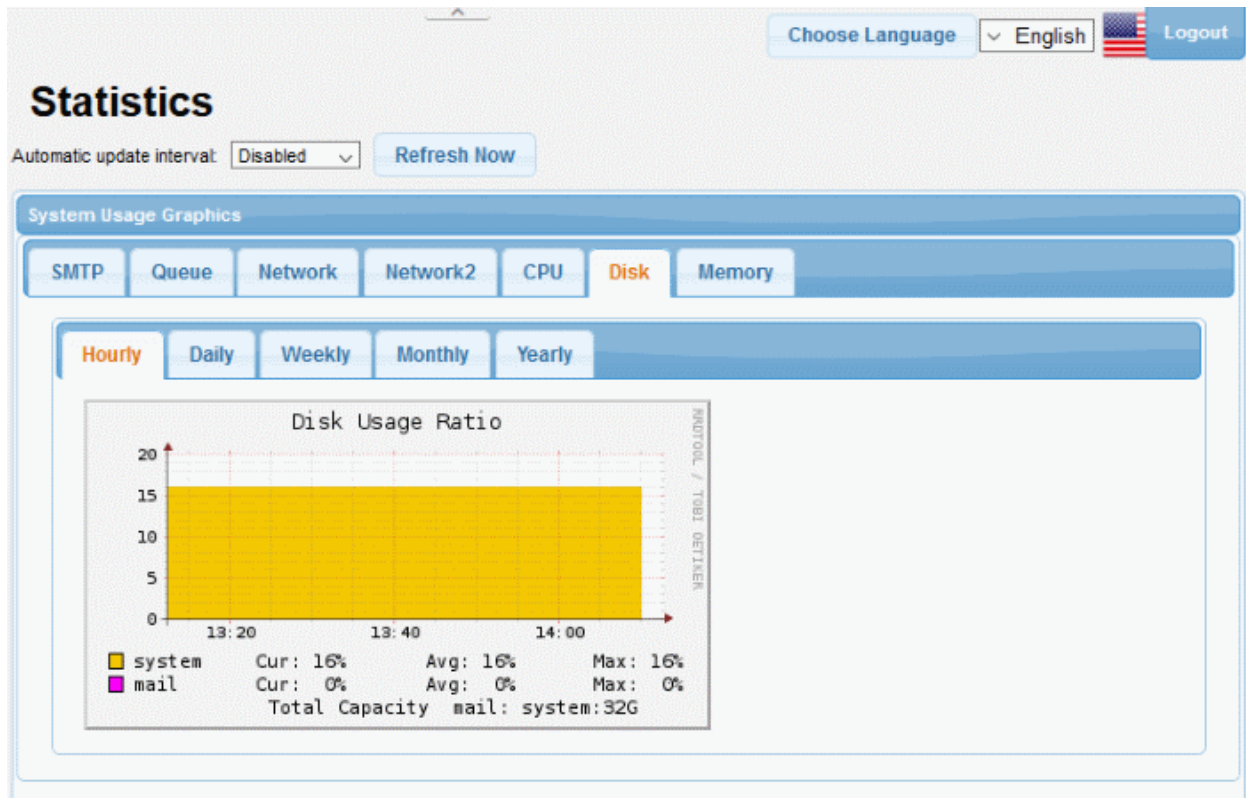
The processes that are responsible for CPU usage are indicated with different colors.

- 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 Secure Email Gateway, 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 Secure Email Gateway, for the period chosen from the sub-tabs.

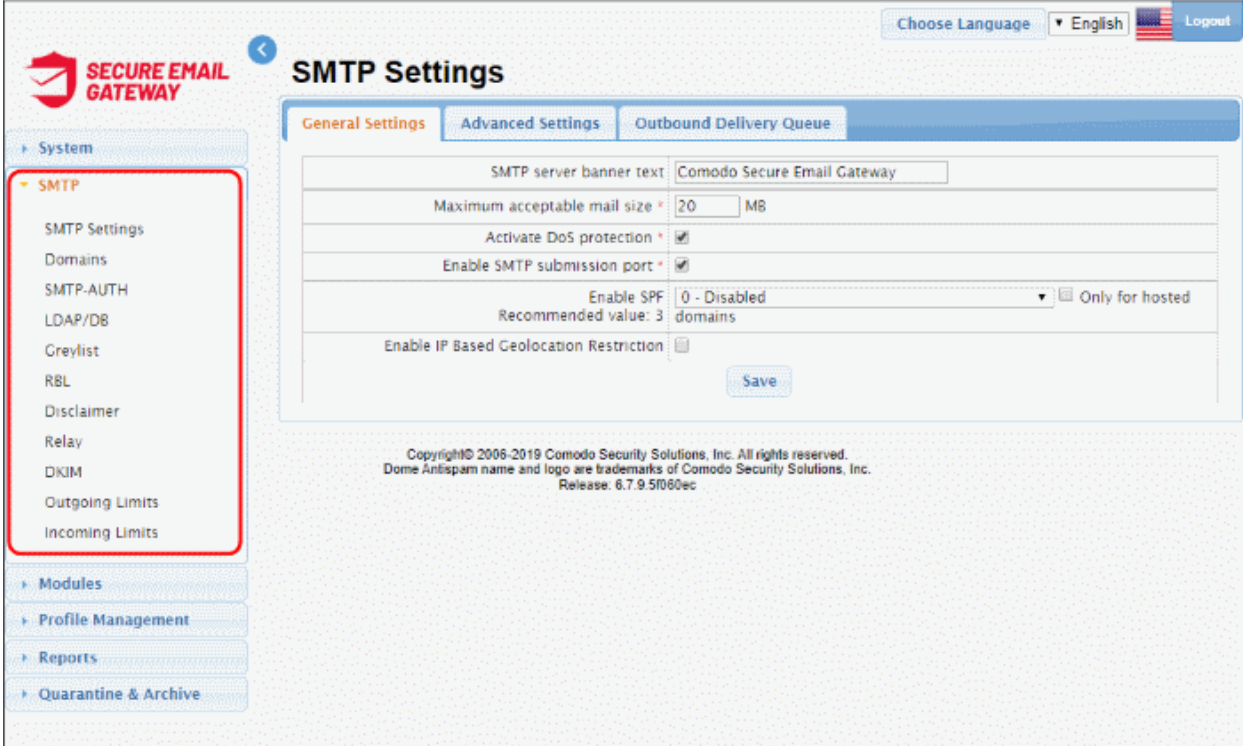


- Hourly - Shows the memory usage for the past one hour
- Daily - Shows the memory usage for the past 24 hours
- Weekly - Shows the memory usage for the past seven days
- Monthly - Shows the memory usage for the past four weeks
- Yearly - Shows the memory usage for the past twelve months

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

4 SMTP Configuration

The 'SMTP' area allows you to configure settings for outgoing mails. This includes settings such as maximum file size, denial-of-service protection, outgoing/incoming limits and more.



The screenshot displays the 'SMTP Settings' page in the Comodo Secure Email Gateway Admin Panel. The page is divided into three tabs: 'General Settings', 'Advanced Settings', and 'Outbound Delivery Queue'. The 'General Settings' tab is active, showing the following configuration options:

SMTP server banner text	Comodo 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	0 - Disabled <input type="checkbox"/> Only for hosted domains
Enable IP Based Geolocation Restriction	<input type="checkbox"/>

A 'Save' button is located at the bottom right of the configuration area. The left sidebar shows a navigation menu with 'SMTP' highlighted in red. Below the main configuration area, there is a copyright notice: 'Copyright© 2006-2019 Comodo Security Solutions, Inc. All rights reserved. Dome Antispam name and logo are trademarks of Comodo Security Solutions, Inc. Release: 6.7.9.51060ec'.

Click the following links for more details:

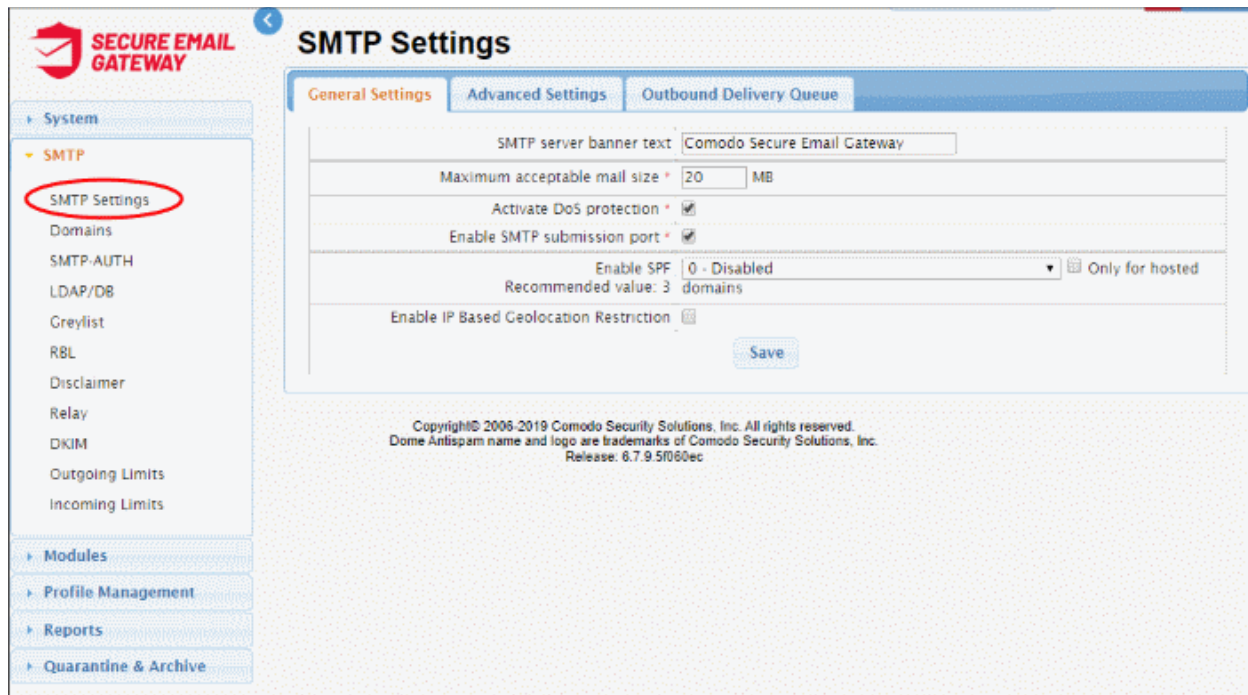
- [SMTP Settings](#)
- [Manage Domains](#)
- [Secure Email Gateway SMTP AUTH Connector](#)
- [LDAP/Local DB/My SQL User Database](#)
- [Greylist](#)
- [Managing RBL Servers](#)
- [Disclaimer](#)
- [SMTP Relay](#)
- [DomainKeys Identified Mail \(DKIM\)](#)
- [Outgoing SMTP Limits](#)
- [Incoming SMTP Limits](#)

4.1 SMTP (Send E-Mail Protocol) Settings

The 'SMTP' settings area allows you to configure the SMTP connection response message, activate DoS protection, and configure the maximum number of processes that the filtering engine can use. The area also lets you set the number of mails that can be queued and sent at a time for a particular domain.

Open the SMTP screen:

- Click 'SMTP' > 'SMTP Settings' in the left-hand menu



Click the following links for more details:

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

4.1.1 General Settings

'General Settings' allow you to configure banner text, the maximum size of outgoing mails, denial of service protection and more.

- Click the 'SMTP' > 'SMTP Settings' on the left menu
- Click the 'General Settings' tab if not already open

SMTP Settings

General Settings
Advanced Settings
Outbound Delivery Queue

SMTP server banner text	<input type="text" value="Comodo Secure Email Gateway"/>
Maximum acceptable mail size *	<input type="text" value="20"/> MB
Activate DoS protection *	<input checked="" type="checkbox"/>
Enable SMTP submission port *	<input checked="" type="checkbox"/>
Enable SPF Recommended value: 3	<input type="text" value="0 - Disabled"/> <input type="checkbox"/> Only for hosted domains
Enable IP Based Geolocation Restriction	<input type="checkbox"/>

SMTP Settings - General Settings Table of Parameters	
Parameter	Description
SMTP server banner text	The welcome message displayed on the SMTP server when connection to Secure Email Gateway port 25 is established.
Maximum acceptable mail size (MB)	The maximum permitted size of a single email + attachments. The default value is 20 MB.
Activate DoS protection	A DoS (Denial of Service) attack occurs when a malicious sender attempts to overload your mail server by bombarding it with unsolicited mail. DoS protection implements limits to help ensure your servers are not stopped or brought to a standstill by such attacks.
Enable SMTP submission port	If enabled, Secure Email Gateway will not 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"> 1. Just add received-SPF header 2. Return temporary failure in DNS query error 3. If SPF result fails (ban) then reject it (recommended) 4. If SPF result is softfail then reject it 5. If SPF result is neutral then reject it 6. If SPF result is not passed then reject it <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 'Save' to apply your changes.

4.1.2 Advanced Settings

- 'Advanced Settings' let you configure the max/min number of processors that the filtering engine should

use. More processors will improve the performance of Secure Email Gateway

- You can also specify the maximum number of recipients per SMTP transaction.

Open the advanced settings screen

- Click 'SMTP' >'SMTP Settings' in the left menu
- Click the 'Advanced Settings' tab

SMTP Settings

General Settings
Advanced Settings
Outbound Delivery Queue

Minimum number of filter processors *	<input type="text" value="10"/>
Maximum number of filter processors *	<input type="text" value="50"/>
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 * <small>Maximum: 500</small>	<input type="text" value="200"/>
Maximum number of concurrent mail delivery *	<input type="text" value="500"/>
Main Filter engine log level	<input type="text" value="Info"/>

SMTP Settings - Advanced Settings Table of Parameters	
Parameter	Description
Minimum number of filter processors	Minimum amount of filter processes that the filtering engine should use. Filter processors are threads used to scan and handle mail. <ul style="list-style-type: none"> • Fewer processors = Lower resource overhead / slower performance
Maximum number of filter processors	Maximum amount of filter processes that the filtering engine should use. Filter processors are threads used to scan and handle mail. <ul style="list-style-type: none"> • More processors = Higher resource overhead / better performance
Maximum number of recipients per SMTP transaction	Maximum number of recipients for each incoming SMTP request that comes to Secure Email Gateway.
Incoming SMTP session timeout (seconds)	Timeout duration of each SMTP session.

RBL Timeout (seconds)	If this time is exceeded, the RBL query is canceled and next filter is applied to the e-mail.
Early talker drop time (seconds)	The SMTP server has a waiting time before sending a first greeting message after which the client replies 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.
Tarbit count	Tarpitting will become active if the number of recipients exceeds the Tarbit count.
Tarbit 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 'Notice' will log all the levels.

- Click 'Save' to apply your changes.



4.1.3 Outbound Delivery Queue

- Click 'SMTP' > 'SMTP Settings' in the left menu then the 'Outbound Delivery Queue' tab
- The 'Outbound Delivery Queue' lets you restrict how many emails can be delivered simultaneously from a source domain.
- Secure Email Gateway has three preset queues with 50, 100 and 150 concurrent mails. You can add multiple domains to any of these queues.
- You can also change the concurrent mail numbers if required
- Queuing mail ensures only a certain number of mails are delivered at once, preventing outbound spam and protecting your mail server from overload.



SMTP Settings

General Settings
Advanced Settings
Outbound Delivery Queue



Queue 1

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

Queue 2

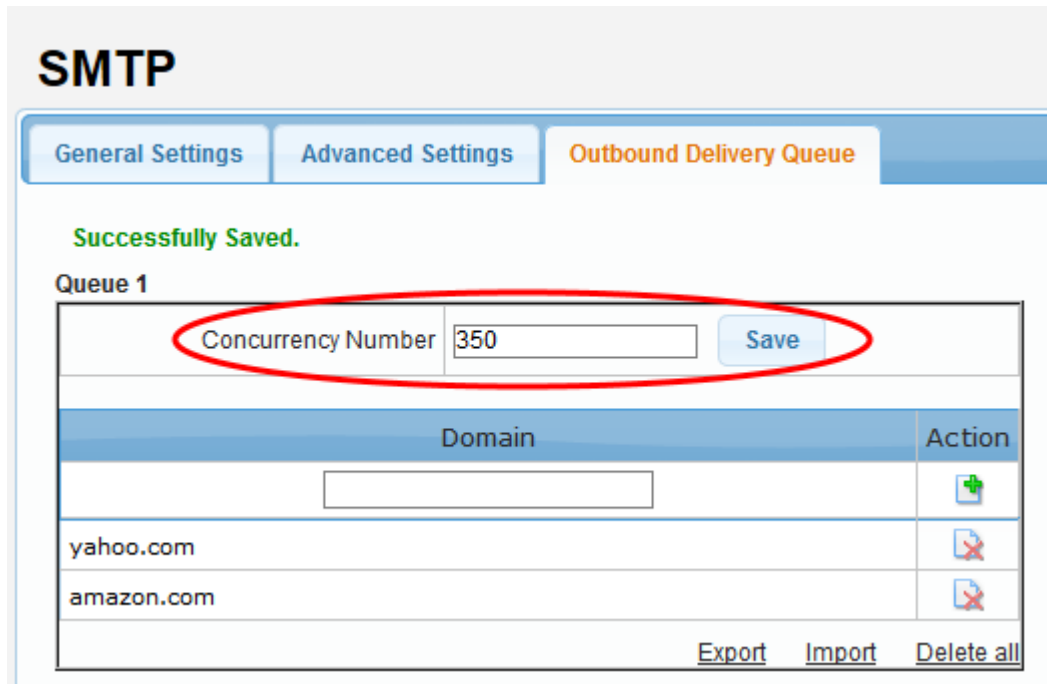
Concurrency Number	<input type="text" value="100"/>	Save
<hr/>		
Domain	Action	
<input type="text"/>		
aol.com		
Export Import Delete all		

Queue 3

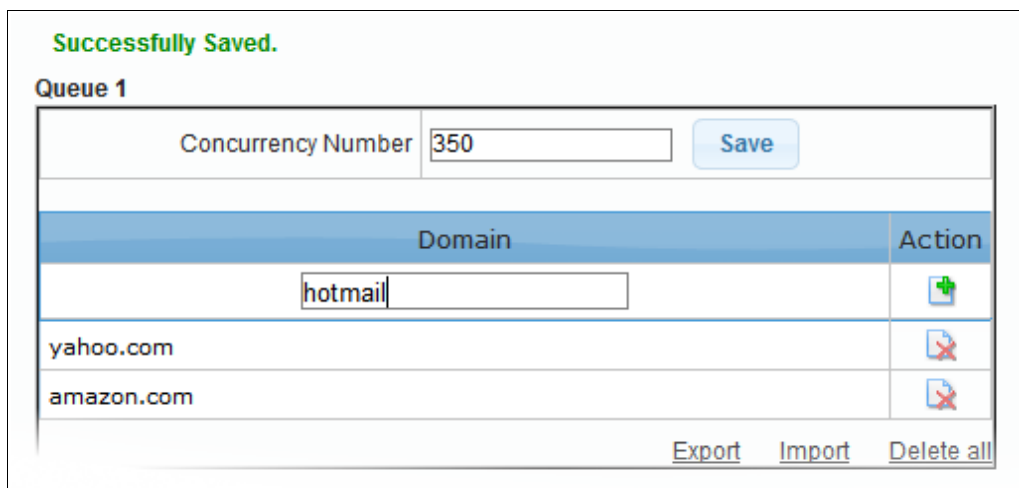
Concurrency Number	<input type="text" value="150"/>	Save
<hr/>		
Domain	Action	
<input type="text"/>		
att.net		
Export Import Delete all		


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.

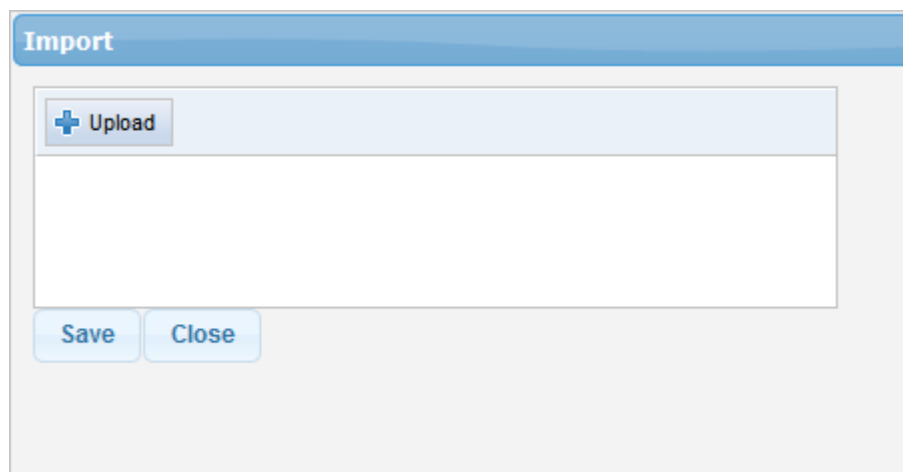
- To set the number of emails that can be sent at a time, enter the number in the 'Concurrency Number' field and click the 'Save' button.



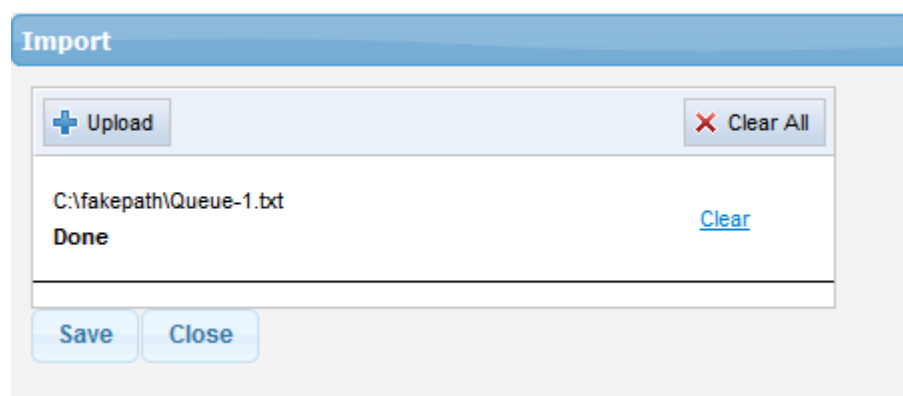
- Add a domain to a queue by typing the domain name in the field then clicking the '+' button



- 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.

4.2 Manage Domains

- The 'Manage Domains' area lets you add, edit and view the domains you wish to filter.
- You can also configure routes and domain 'Smart Hosts', whereby mail is routed to an intermediate/relay server instead of direct to the recipient server.

Open the domains screen

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

SECURE EMAIL GATEWAY

Choose Language: English | Logout

Domains

Managed Domains | Routes | Smart Hosts

Total: 3 domain(s)

[Bulk Add](#)

All None	Managed Domain Name	Generate Report	Owner	Action
	<input type="text"/>			
	bulut.ml		admin	
	ilyespa.ml		admin	
	korumail.tk		admin	

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

Copyright© 2006-2019 Comodo Security Solutions, Inc. All rights reserved.
Dome Antispam name and logo are trademarks of Comodo Security Solutions, Inc.
Release: 6.7.9.5f060ec

Click the following the links for more details:

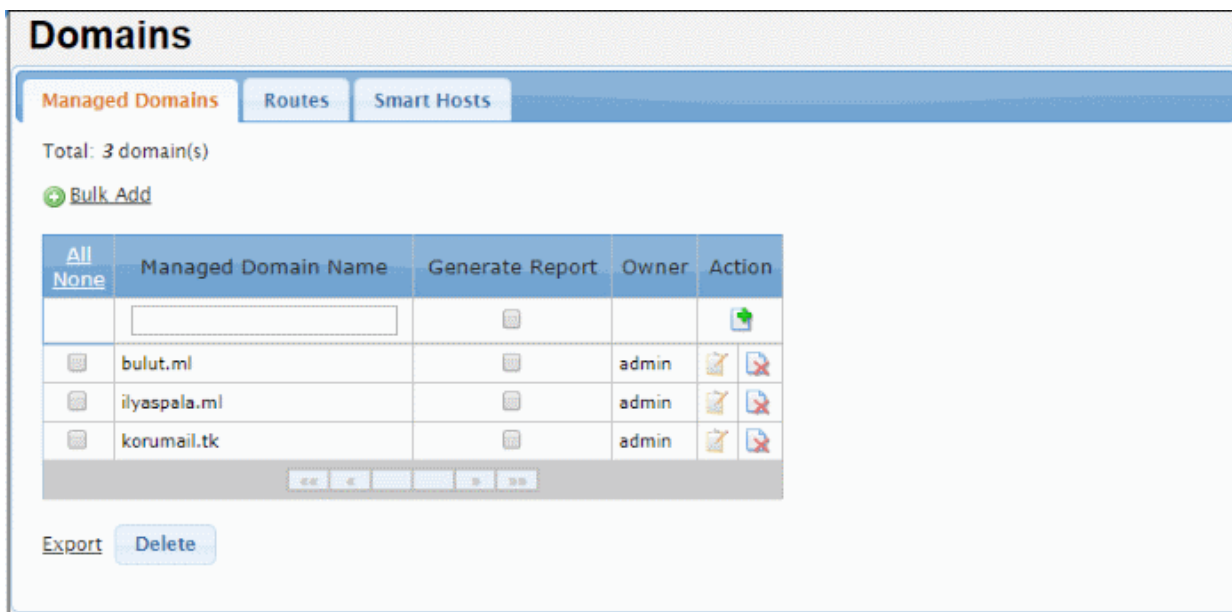
- [Manage Domain Names](#)
- [Manage Domain Routes](#)
- [Manage Smart Hosts](#)
- [Default Domain Routing](#)

4.2.1 Manage Domain Names

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

Open the managed domains screen:

- Click 'SMTP' > 'Domains' in the left menu
- Click the 'Managed Domains' tab if not already open



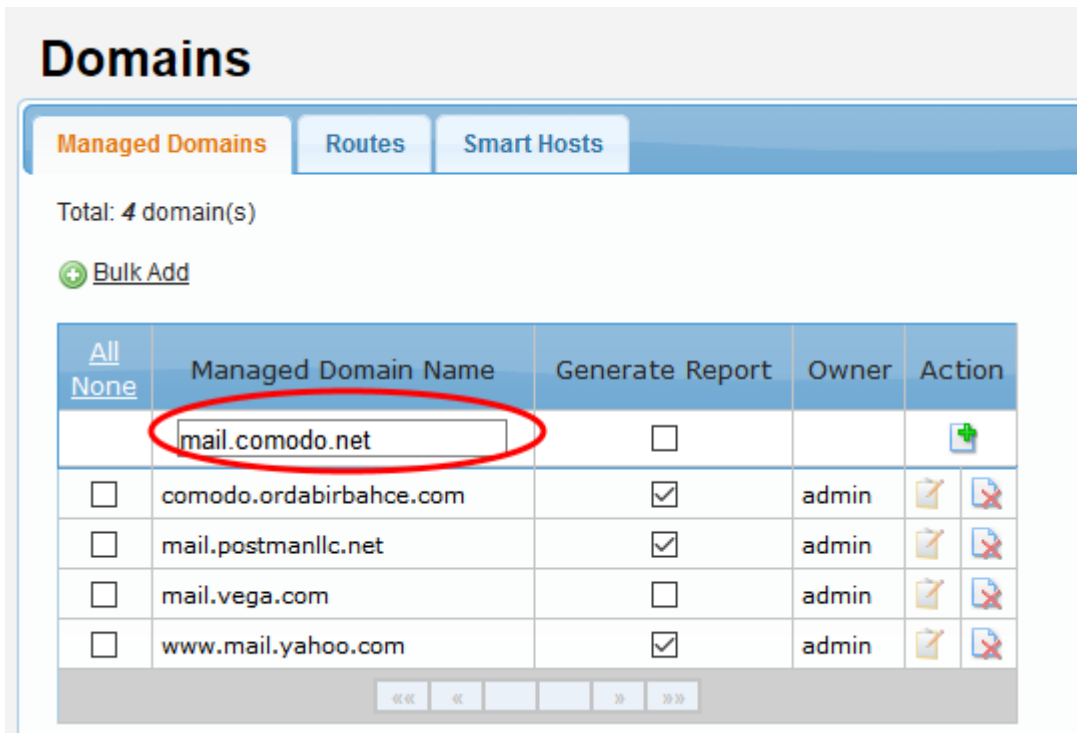
Managed Domains - Table of Column Descriptions	
Column Header	Description
Managed Domain Name	The FQDN of the protected domain
Generate Report	<ul style="list-style-type: none"> Will create a report containing email statistics for the domain. The report will be available in 'Domain Reports' Click 'Reports' > 'Domain Reports' to open this interface.
Owner	The name of the admin who added the domain.
Actions	<ul style="list-style-type: none"> Type the domain you wish to add in the field under the 'Managed Domain Name' column header. Next, click this button to add the domain to the list.
	Delete a domain.
	Edit domain details.

The interface allows you to:

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

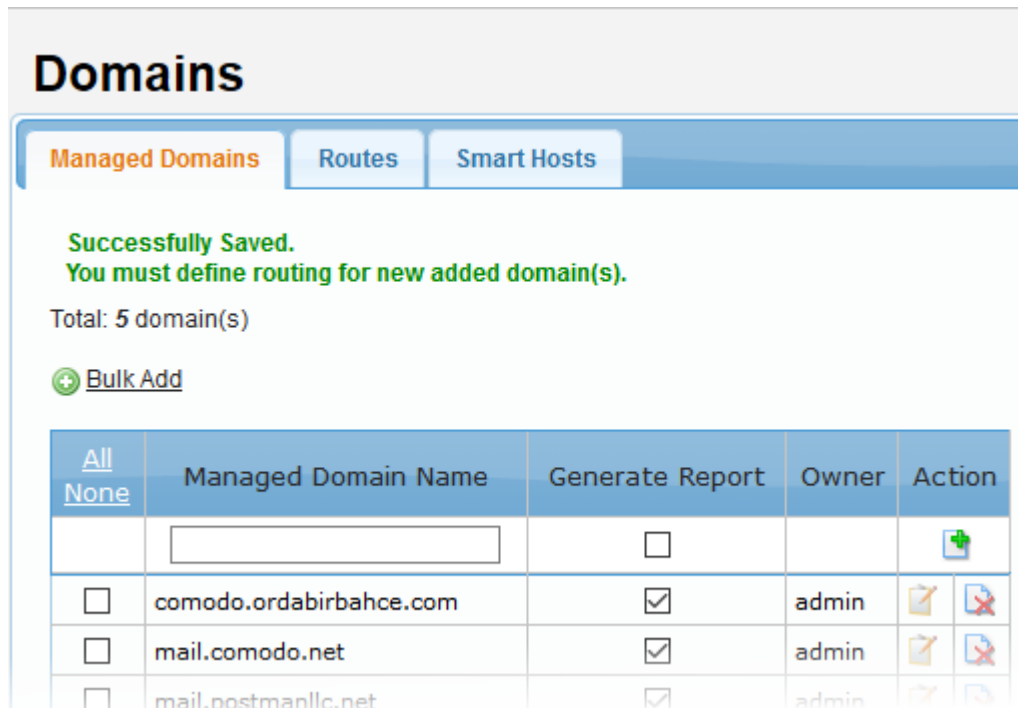
Add a domain name

- Click 'SMTP' > 'Domains' in the left menu
- Click the 'Managed Domains' tab
- Enter the domain name in the field under 'Managed Domain Name' column



- Select 'Generate Report' if you want to record email statistics for the domain in 'Domain Reports'. Click 'Reports' > 'Domain Reports' to view this interface.
- 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.



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

Add multiple domain names

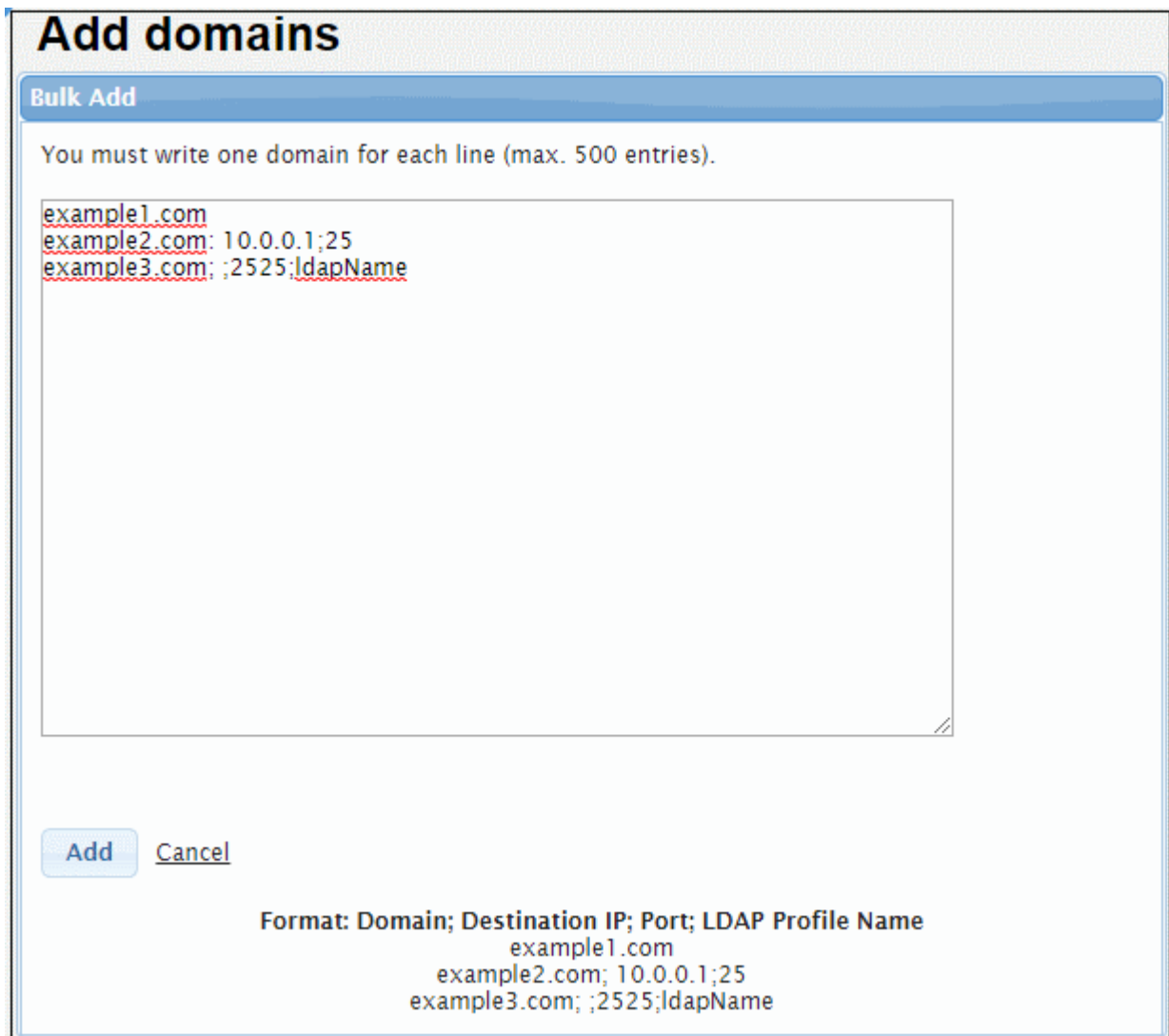
The most significant feature of this menu is when you add the domain name you can route the domain name at the

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

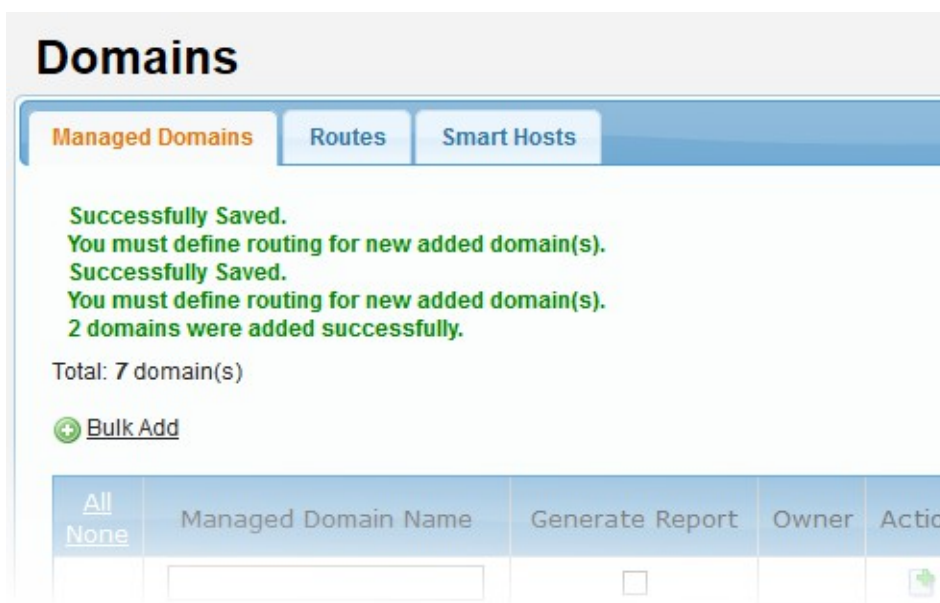


The 'Bulk Add' screen will be displayed.



- 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 'Add'.

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.

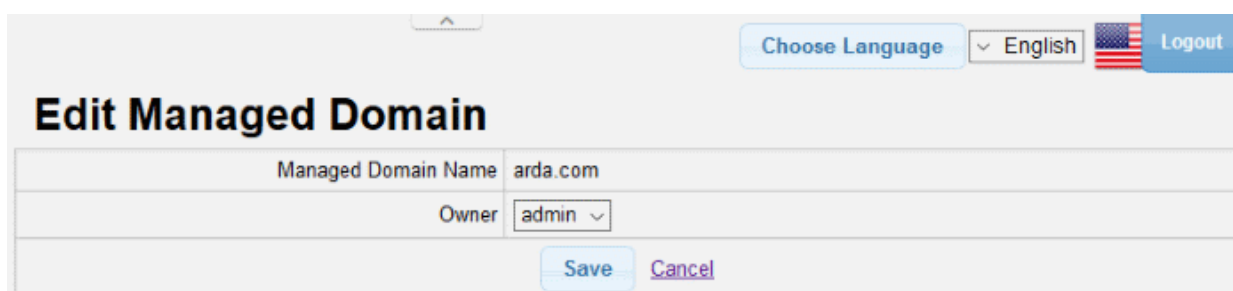


Edit a domain owner

When you add a domain name, your 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.



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

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 'Delete' at the bottom.

Choose Language English Logout

Domains

Managed Domains | Routes | Smart Hosts

Filter: Filter! Clear Total: 21 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"/>	arda.com	<input checked="" type="checkbox"/>	admin	
<input checked="" type="checkbox"/>	bilisim.ml	<input checked="" type="checkbox"/>	admin	
<input checked="" type="checkbox"/>	bulut.ml	<input checked="" type="checkbox"/>	admin	
<input checked="" type="checkbox"/>	yandex.com	<input checked="" type="checkbox"/>	admin	
<input checked="" type="checkbox"/>	yeni.com	<input type="checkbox"/>	admin	
<input checked="" type="checkbox"/>	yopmail.com	<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

Export the domain names to a file

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

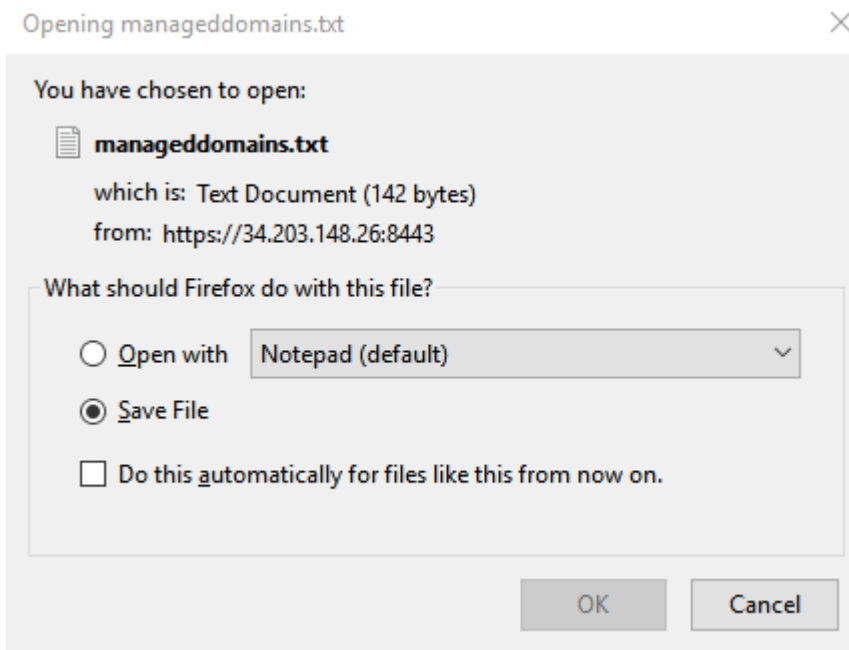
Total: 7 domain(s)

[Bulk Add](#)

All None	Managed Domain Name	Generate Report	Owner	Action
	<input type="text"/>	<input type="checkbox"/>		
<input type="checkbox"/>	comodo.ordabirbahce.com	<input checked="" type="checkbox"/>	admin	
<input type="checkbox"/>	mail.comodo.net	<input checked="" type="checkbox"/>	admin	
<input type="checkbox"/>	mail.postmanllc.net	<input checked="" type="checkbox"/>	admin	
<input type="checkbox"/>	mail.vega.com	<input type="checkbox"/>	admin	
<input type="checkbox"/>	www.gmail.com	<input type="checkbox"/>	admin	
<input type="checkbox"/>	www.google.com	<input type="checkbox"/>	admin	
<input type="checkbox"/>	www.mail.yahoo.com	<input checked="" type="checkbox"/>	admin	

Export Delete

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



4.2.2 Manage Domain Routes

- Click 'SMTP' > 'Domains' > 'Routes' to open this interface.
- A domain route is the path that a domain should use to deliver mail after it has been filtered.
- If no route is defined then the default domain route is applied. See **Default Domain Routing** for more info.
 - Note. You must already have added a domain before you can configure its route.
 - Click 'SMTP' > 'Domains' > 'Managed Domains' to add new domains. **Click here** if you need more help.

Choose Language English Logout

Domains





Managed Domains
Routes
Smart Hosts

All None	Managed Domain Name	Routing Type	SMTP Server	Port Number	User Verification	LDAP/DB Profile	Action
<input type="checkbox"/>	-Choose-	IPv4		25	None	None	
<input type="checkbox"/>	bilisim.ml	IPv4	217.79.179.102	25	None	-None-	
<input type="checkbox"/>	bulut.ml	IPv4	78.31.65.172	25	None	-None-	
<input type="checkbox"/>	comodo.ordabirbahce.com	IPv4	213.14.70.194	25	None	-None-	
<input type="checkbox"/>	example.com	IPv4	192.168.199.31	25	None	-None-	
<input type="checkbox"/>	steven.com	IPv6 or HOSTNAME	mail.steven.com	25	LDAP	company LDAP	
<input type="checkbox"/>	test.com	LDAP			LDAP	Default OpenLDAP	
<input type="checkbox"/>	testcustomer.com	IPv4	213.168.32.78	25	None	-None-	
<input type="checkbox"/>	yahoo.com	IPv6 or HOSTNAME	smtp.mail.yahoo.com	25	LocalUserDB	LocalUserDB	
<input type="checkbox"/>	yopmail.com	MX RECORD			MySQL		

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

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

Domain Route - Table of Column Descriptions	
Column Header	Description
Managed Domain Name	The FQDN of the protected domain
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 Secure Email Gateway should forward the mail
User Verification	The type of user authentication that Secure Email Gateway 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.

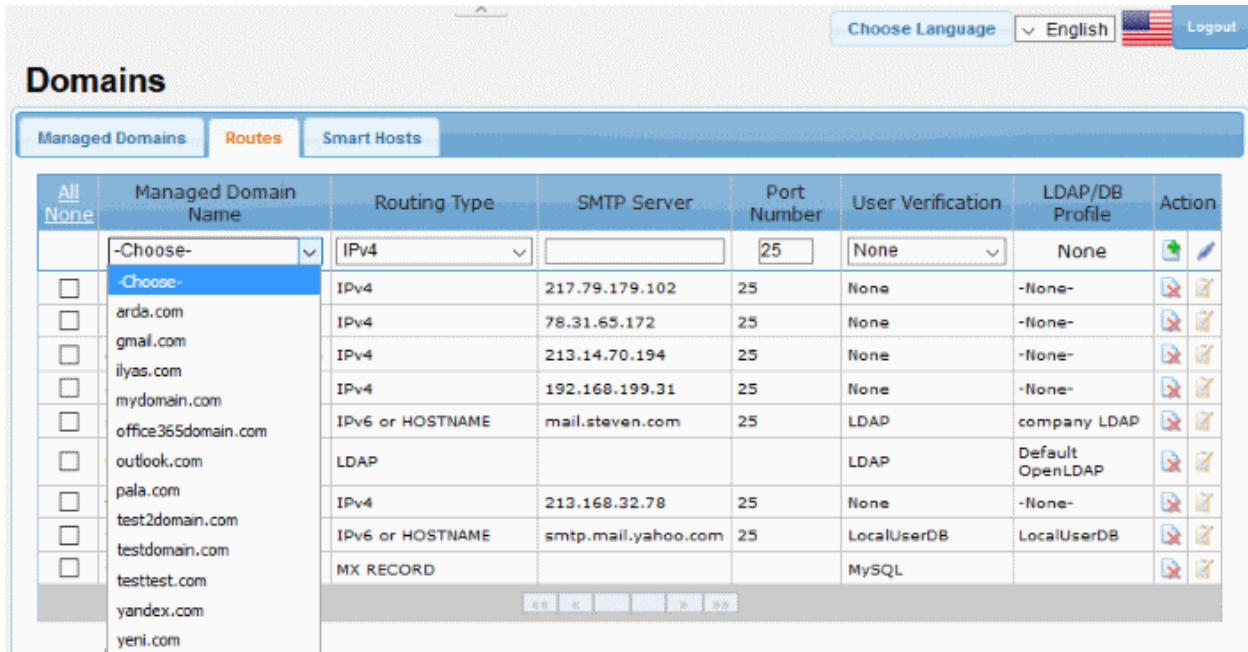
Action		After completing all routing details, click this button to save the domain route.
		Check connectivity between Secure Email Gateway and the SMTP server.
		Delete a domain route from the list.
		Edit a domain route.

The interface allows you to:

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

Configure a domain route

- Click 'SMTP' > 'Domains' > 'Routes'
- Click the 'Choose' drop-down
- Select the **domain** for which you want to configure a route.
 - Click the 'Managed Domains' tab if you still need to add a domain



The screenshot shows the 'Domains' configuration page with the 'Routes' tab selected. A table lists domain routes with columns for Managed Domain Name, Routing Type, SMTP Server, Port Number, User Verification, LDAP/DB Profile, and Action. A dropdown menu is open for the 'Managed Domain Name' column, showing a list of domains including arda.com, gmail.com, and others. The 'Routing Type' is set to IPv4, the 'SMTP Server' is 217.79.179.102, and the 'Port Number' is 25.

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

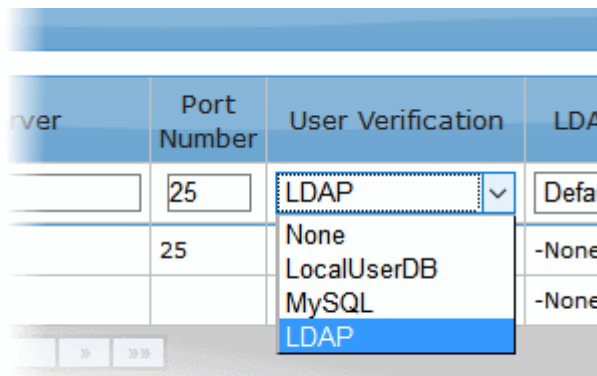
Choose Language English Logout

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"/>	bilisim.ml	IPv4	217.79.179.102	25	None	-None-	
<input type="checkbox"/>	bulut.ml	IPv4	78.31.65.172	25	None	-None-	
<input type="checkbox"/>	comodo.ordabirbahce.com	IPv6 or HOSTNAME	213.14.70.194	25	None	-None-	
<input type="checkbox"/>	example.com	MX RECORD	192.168.199.31	25	None	-None-	
<input type="checkbox"/>	steven.com	LDAP	mail.steven.com	25	LDAP	company LDAP	
<input type="checkbox"/>	test.com	LDAP			LDAP	Default OpenLDAP	

- 'SMTP Server' field - Enter the hostname or IP of the SMTP server to which SEG should forward mails after filtering
 - Enter the server port number in the next column
- 'User verification' drop-down – Choose the type of authentication that Secure Email Gateway should use to verify the recipient.
 - The options available are: 'None', 'Local User DB', 'My SQL' and 'LDAP'.
 - SEG will only forward mails after successful verification. Unless you choose 'None', of course.
 - The verification database can be configured in the **LDAP/DB** section. Click 'SMTP' > 'LDAP/DB' to open this interface.
- Depending on the 'User Verification' type chosen, the 'LDAP/DB Profile' column will be populated. If 'LDAP' is chosen as 'User Verification' then the LDAP profiles added in **LDAP/DB** section will be displayed from the drop-down. Select the LDAP profile from the options.



- To check the connectivity between Secure Email Gateway 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.

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.

Choose Language English Logout

Edit domain route

Domain	comodo.ordabirbahce.com
Routing Type	IPv4
SMTP Server	213.14.70.194
Port Number	25
User Verification	None
LDAP/DB Profile	None

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

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.

Choose Language English Logout

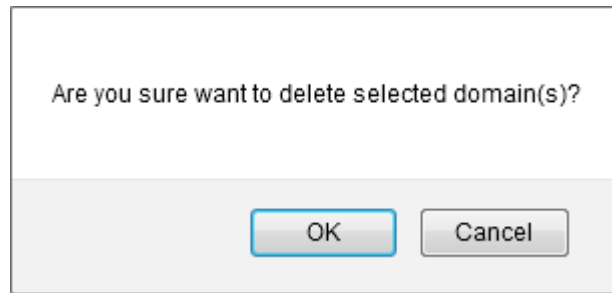
Domains

Managed Domains **Routes** Smart Hosts

All None	Managed Domain Name	Routing Type	SMTP Server	Port Number	User Verification	LDAP/DB Profile	Action
<input type="checkbox"/>	-Choose-	IPv4		25	None	None	
<input checked="" type="checkbox"/>	bilisim.ml	IPv4	217.79.179.102	25	None	-None-	
<input type="checkbox"/>	bulut.ml	IPv4	78.31.65.172	25	None	-None-	
<input type="checkbox"/>	comodo.ordabirbahce.com	IPv4	213.14.70.194	25	None	-None-	
<input type="checkbox"/>	example.com	IPv4	192.168.199.31	25	None	-None-	
<input type="checkbox"/>	steven.com	IPv6 or HOSTNAME	mail.steven.com	25	LDAP	company LDAP	
<input type="checkbox"/>	test.com	LDAP			LDAP	Default OpenLDAP	
<input type="checkbox"/>	testcustomer.com	IPv4	213.168.32.78	25	None	-None-	
<input type="checkbox"/>	yahoo.com	IPv6 or HOSTNAME	smtp.mail.yahoo.com	25	LocalUserDB	LocalUserDB	
<input type="checkbox"/>	youmail.com	MX RECORD			MySQL		

Smtip server examples;
IPV4 :192.168.199.31 (IPV4 address only)
IPV6 or HOSTNAME :smtp.mail.example.com (FV6 address or Hostname only)
MX RECORD :(Mail Exchanger Record, no need to input any server address)
LDAP :(Lightweight Directory Access Protocol, no need to input any server address)

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



To export the domain routes to a file

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

Domains

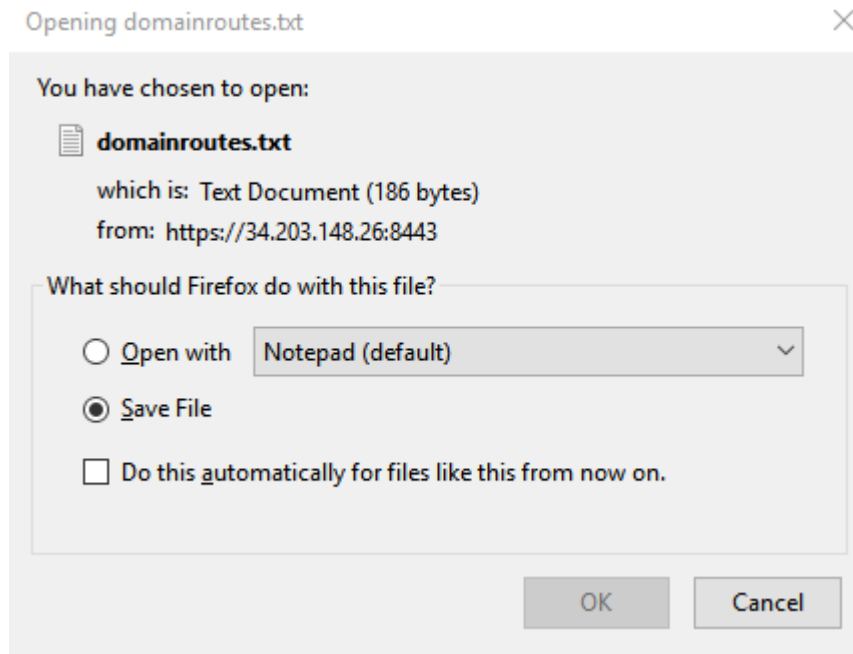
Managed Domains **Routes** Smart Hosts

All None	Managed Domain Name	Routing Type	SMTP Server	Port Number	User V
	-Choose-	IPv4		25	None
<input checked="" type="checkbox"/>	bilisim.ml	IPv4	217.79.179.102	25	None
<input type="checkbox"/>	bulut.ml	IPv6 or HOSTNAME	78.31.65.172	25	None
<input type="checkbox"/>	comodo.ordabirbahce.com	MX RECORD	213.14.70.194	25	None
<input type="checkbox"/>	example.com	LDAP	192.168.199.31	25	None
<input type="checkbox"/>	yopmail.com	IPv4			MySQL
		MX RECORD			

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

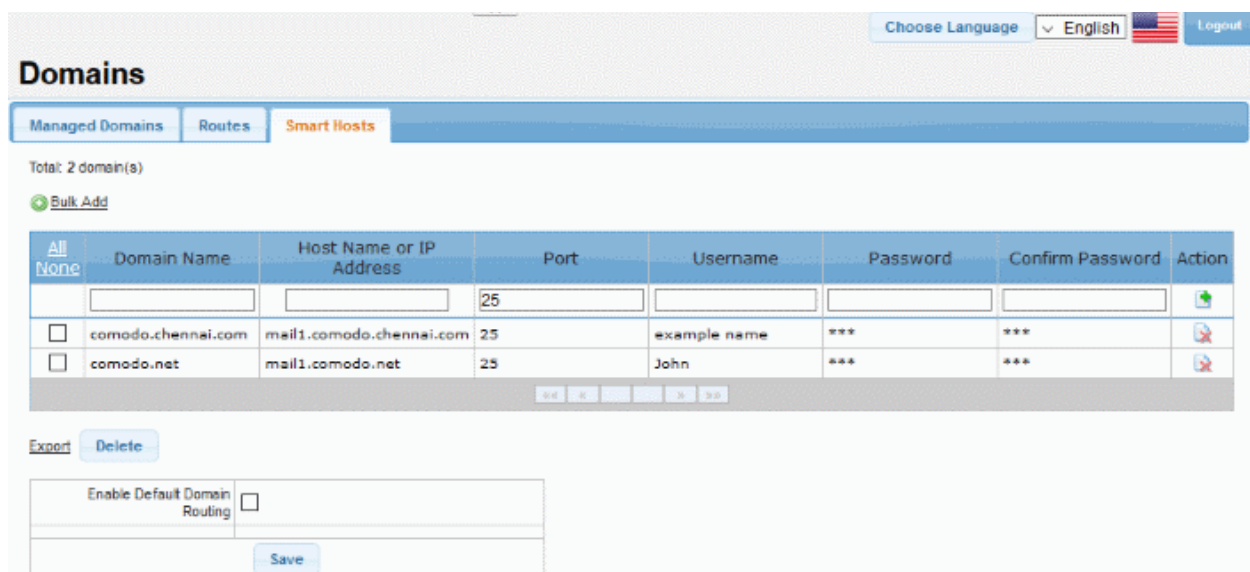
Export Delete



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



4.2.3 Manage Smart Hosts

- Click 'SMTP' > 'Domains' > 'Smart Hosts' to open the smart hosts screen.
- Smart hosts are intermediate servers that receive mail and, after applying their own policy, forward them to end user mail boxes.
- Smart hosts require sender-authentication to verify that they have permission to send mails.
- This is different to an open mail relay that will forward mails directly to the recipient server without authentication.
- Please note that a domain added to 'Managed Domains' cannot be used for smart host routing.
- The interface also allows you to configure default domain routing. This applies to 'Managed Domains' whose routing has not been configured. See '**Default Domain Routing**' for more details.




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

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 Secure Email Gateway should forward the mail
- To add the 'Smart Host' route to the list, click the  button under the 'Action' column header.

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: 2 domain(s)

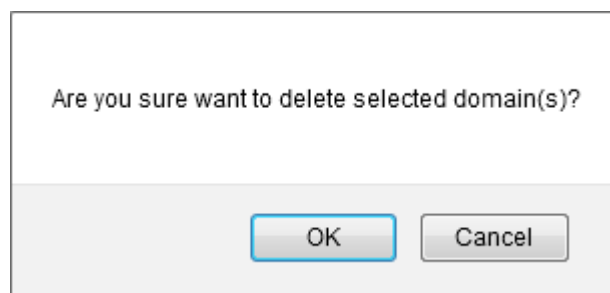
+ [Bulk Add](#)

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

Export Delete

Enable Default Domain Routing
Save

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



Export smart host routes list for domains

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

Domains

Managed Domains Routes **Smart Hosts**

Total: 2 domain(s)

[+ Bulk Add](#)

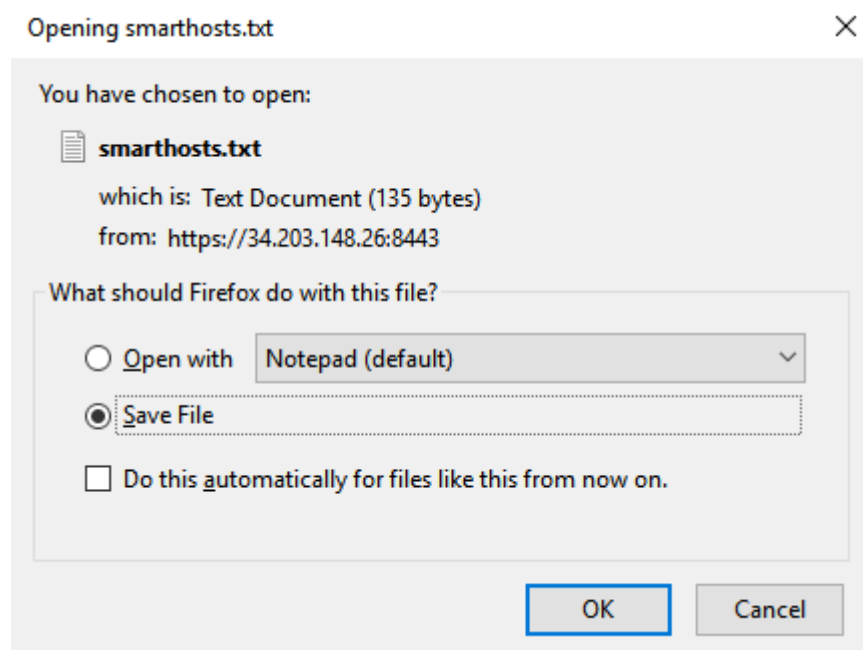
All None	Domain Name	Host Name or IP Address	Port
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="25"/>
<input checked="" type="checkbox"/>	comodo.chennai.com	mail1.comodo.chennai.com	25
<input checked="" type="checkbox"/>	comodo.net	mail1.comodo.net	25

Export Delete

Enable Default Domain Routing

Save

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



4.2.4 Default Domain Routing

- Secure Email Gateway lets you configure routing for **Managed Domains** that are protected by its filtering engine. See **'Manage Domain Routes'** to find out how to configure routing for managed domains.
- If no routing is configured, then the default domain routing will be applied. This default route can be configured in the 'Smart Hosts' section.
- Click 'SMTP' > 'Domains' > 'Smart Hosts' to open this interface.

Domains

Managed Domains | Routes | **Smart Hosts**

Total: 2 domain(s)

[Bulk Add](#)

All None	Domain Name	Host Name or IP Address	Port	Username	Password	Confirm Password	Action
<input type="checkbox"/>	comodo.chennai.com	mail1.comodo.chennai.com	25	example name	***	***	
<input type="checkbox"/>	comodo.net	mail1.comodo.net	25	John	***	***	

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

Enable Default Domain Routing

[Save](#)

- Select the 'Enable Default Domain Routing' check box
- The will open the route configuration section:

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

Enable Default Domain Routing	<input checked="" type="checkbox"/>
SMTP Server	<input type="text"/>
SMTP Port	25
LDAP Profile	-None-

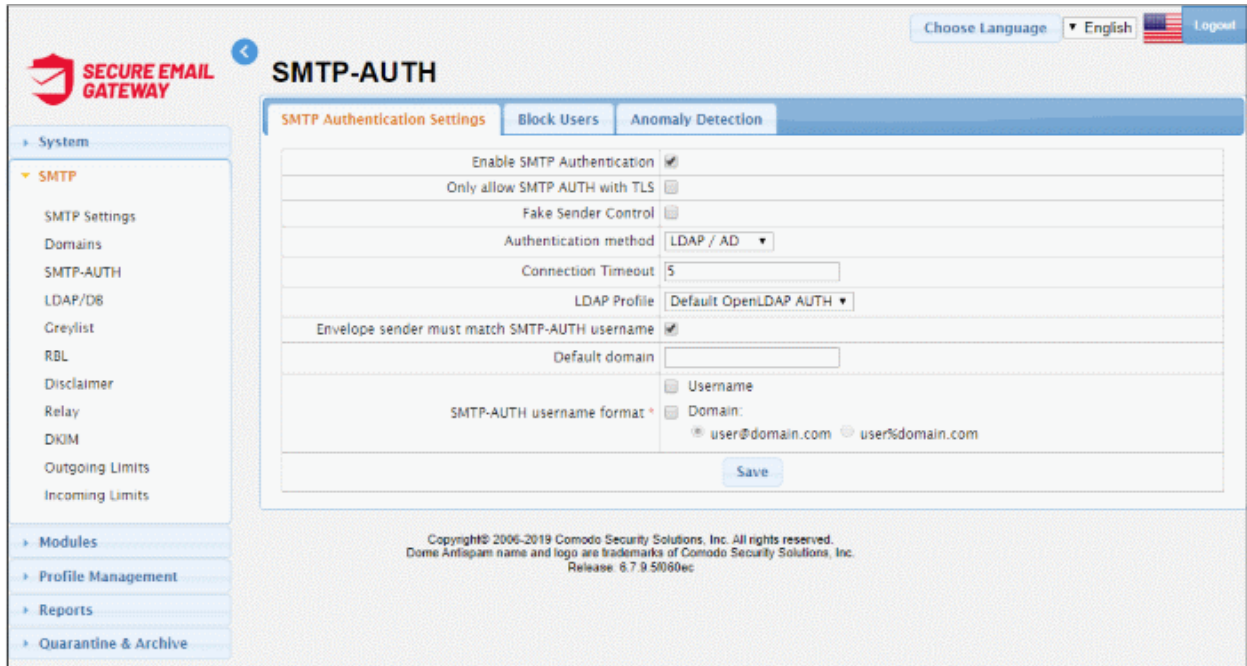
[Save](#)

- SMTP Server:** Enter the host name or IP address of the SMTP server to which SEG should forward email.
- SMTP Port:** Enter the port number to which SEG should forward mail.
- LDAP Profile:** Select the LDAP profile that SEG should use to verify users before forwarding mail. LDAP Profiles are configured in the **LDAP/DB** section.
- Click 'Save' to apply your changes.

4.3 Secure Email Gateway SMTP AUTH Connector

The 'SMTP-AUTH' section lets you configure authentication settings for outgoing mails, to block users, and to configure 'Anomaly Detection'. Anomaly detection lets you track the IP addresses used to send mail for an email address.

- Click 'SMTP' > 'SMTP-AUTH' to open this interface.



Click the following links for more details:

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

4.3.1 SMTP Authentication Settings




- This area lets you choose the method of user authentication that SEG should use on outgoing mail.
- User authentication verifies that the sender is entitled to send mail from a specific domain.
- Click 'SMTP' > 'SMTP-AUTH' > 'SMTP Authentication Settings' to open this interface

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	5
LDAP Profile	Default OpenLDAP AUTH ▼
Envelope sender must match SMTP-AUTH username	<input checked="" type="checkbox"/>
Default domain	
SMTP-AUTH username format *	<input type="checkbox"/> Username <input type="checkbox"/> Domain: <input checked="" type="radio"/> user@domain.com <input type="radio"/> user%domain.com


SMTP Authentication Settings - Table of Parameters			
Parameter	Description		
Enable SMTP Authentication	If enabled, admins can configure an SMTP authentication method for senders. This option is disabled by default.		
Only allow SMTP AUTH with TLS	If enabled, authentication must be conducted over a secure TLS connection.		
Fake Sender Control	Will prevent outgoing mails that have a spoofed 'from' address. By default this option is disabled		
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. See ' POP3/IMAP Authentication Method ' and ' LDAP Authentication Method ' for details on the respective settings.		
Connection Timeout	Enter the time in seconds during which authentication between the client and the POP3/IMAP/LDAP server must be completed. The user will be prompted to enter credentials again if the time elapses.		
Envelope sender must match SMTP-AUTH username	SEG checks whether the envelope sender name and username is same. SEG authenticates the users via the servers added in the SMTP-AUTH server list. If enabled, you have to select any of the authentication type below: SMTP-AUTH username format: <ul style="list-style-type: none"> Username – Enter the domain in the default domain field. SEG appends the domain to the username and checks in the SMTP auth servers. Domain – Select the domain format. SEG checks the usernames for all domains in the SMTP auth servers. 		
POP3/IMAP Authentication Method			
SMTP-AUTH server list	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%; padding: 2px;">Authenticati on method</td> <td style="padding: 2px;">Select authentication method - either POP3 or IMAP.</td> </tr> </table>	Authenticati on method	Select authentication method - either POP3 or IMAP.
Authenticati on method	Select authentication method - either POP3 or IMAP.		






	Connection type	Select the type of connection (clear text or encrypted SSL/TLS).
	Hostname	Enter the server name or IP address of the SMTP-AUTH server.
	Port	Enter the port of the server to which Secure Email Gateway should connect to.
	Enabled	Activate or disable the server.
	Action	
		Allows you to delete an auth server from the list.
		Allows you to edit the parameters of an auth server.
LDAP/AD Authentication Method		
LDAP Profile	Select the type of LDAP profile from the drop-down. The profiles available are configured in LDAP/DB section.	


Configure SMTP authentication settings

- Select the 'Enable SMTP Authentication' check box
- Select the 'Only allow SMTP AUTH with TLS' check box to allow only encrypted SMTP AUTH sessions
- Select the 'Fake Sender Control' to block fake sender email address in the SMTP Server.
- Select the type of authentication method from the 'Authentication method' drop-down. The options available are POP3 / IMAP and LDAP. See '**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 Secure Email Gateway should connect.
- Click the  button to add the server to the list.
- Repeat the process to add more auth servers.

	Authentication method	Connection type	Hostname	Port	Enabled	Action
SMTP-AUTH server list Drag and drop to change server order.	POP3 ▾	Plain ▾	<input type="text"/>	<input type="text" value="0"/>		
	POP3	Plain	192.168.199.31	25	Yes	 
	IMAP	Plain	192.168.199.30	25	Yes	 

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

Authentication method	POP3
Connection type	SSL
Hostname *	192.168.199.31
Port *	25
Save	

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

Choose Language English Logout

SMTP-AUTH

SMTP Authentication Settings | Block Users | Anomaly Detection

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

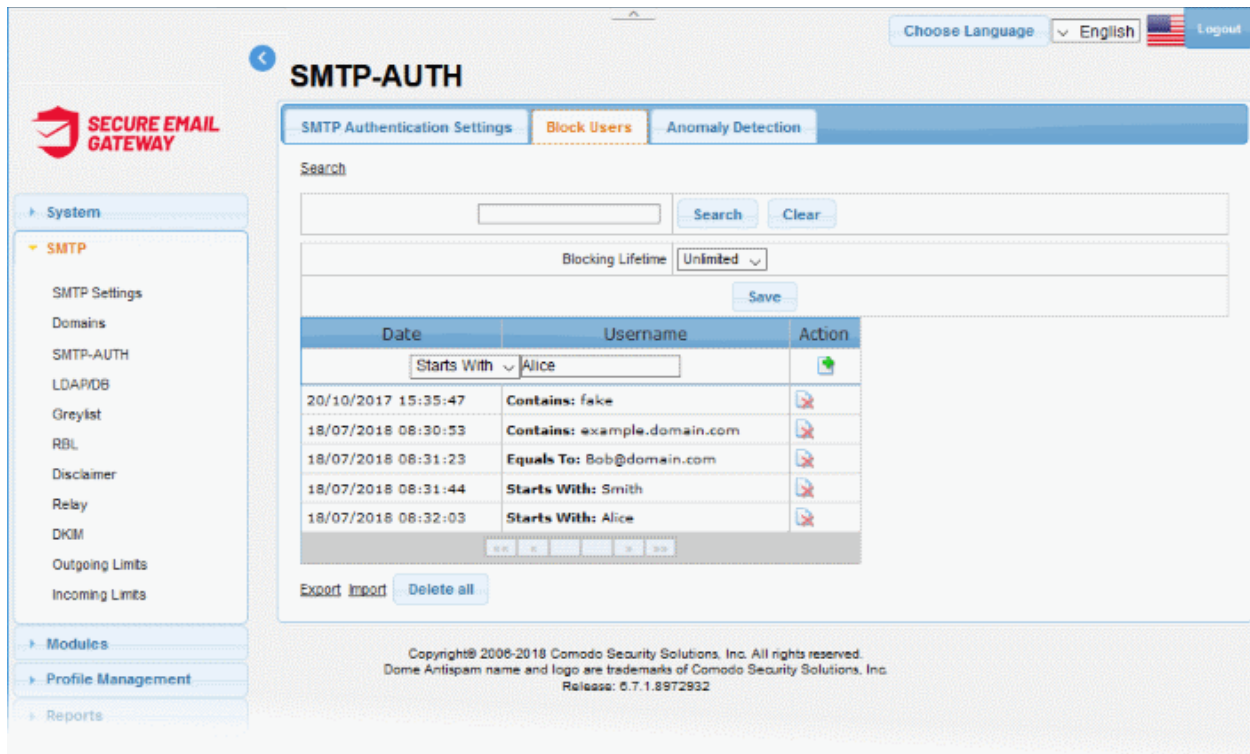
Default AD
Default OpenLDAP
Default OpenLDAP AUTH
Default AD AUTH
company LDAP

Copyright© 2006-2018 Comodo Security So
Dome Antispam name and logo are trademarks
Release: 6.7.1.897

- Click 'Save' to apply your changes.

4.3.2 Block Users

- The 'Block Users' area lets you block outgoing mail that is routed through Secure Email Gateway. You can block individual users or entire domains.
- The interface lets you view existing blocks, add new block rules, and search users by name and domain.
- Click 'SMTP' > 'SMTP-AUTH' > 'Block Users' to open the interface



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**

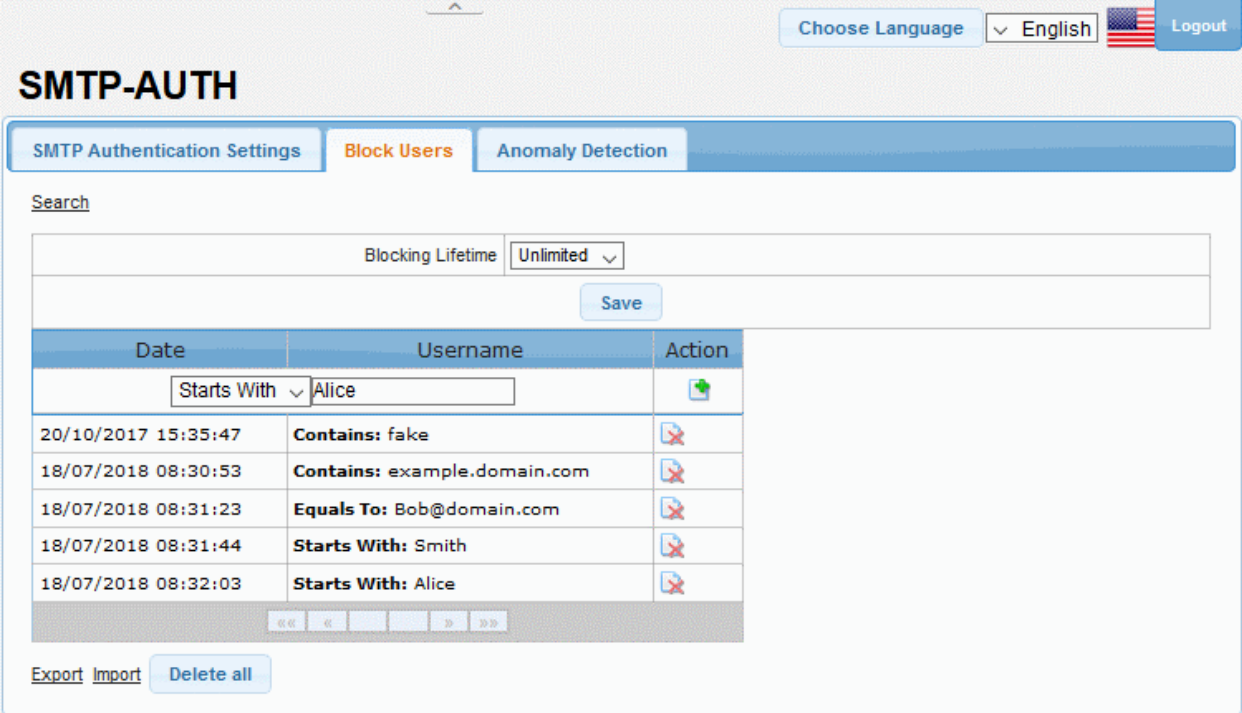
To Add a Blocked User

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
	Contains example.domain.com	
13.04.2017 10:17:10	Starts With: Alice	
13.04.2017 10:17:10	Starts With: Smith	
13.04.2017 10:17:10	Equals To: Bob@eample.com	
13.04.2017 10:17:25	Contains: example.domain.com	

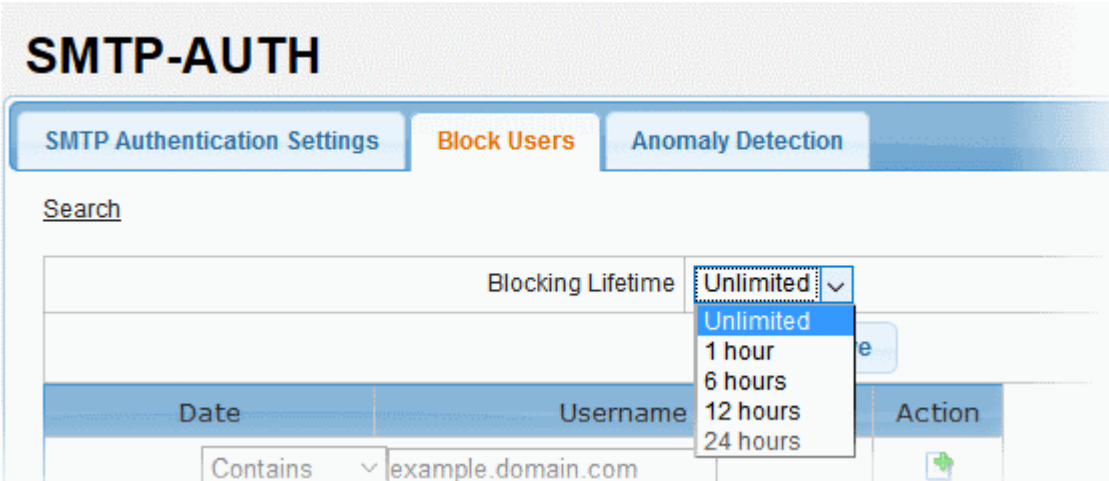
- Click the 'Add' button  to apply your choice. The item will be added to the list with the category type displaying on the left side.



The screenshot shows the 'SMTP-AUTH' admin interface. At the top right, there are options for 'Choose Language' (set to English) and a 'Logout' button. Below the title, there are three tabs: 'SMTP Authentication Settings', 'Block Users' (active), and 'Anomaly Detection'. A search bar is present above a table. The table has columns for 'Date', 'Username', and 'Action'. A 'Blocking Lifetime' dropdown is set to 'Unlimited'. A 'Save' button is located above the table. The table contains several entries with details like 'Contains: fake', 'Contains: example.domain.com', 'Equals To: Bob@domain.com', and 'Starts With: Alice'. Each entry has a delete icon in the 'Action' column. At the bottom, there are 'Export', 'Import', and 'Delete all' buttons.

Blocking Lifetime

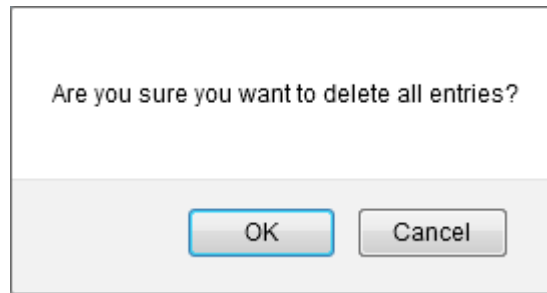
The 'Blocking lifetime' refers to the number of hours the email address will remain blocked at the SMTP Server. The available intervals are 'Unlimited', '1 hour', '6 hours', '12 hours' and '24 hours'.



This screenshot shows the 'SMTP-AUTH' admin interface with the 'Blocking Lifetime' dropdown menu open. The menu lists the following options: 'Unlimited', '1 hour', '6 hours', '12 hours', and '24 hours'. The 'Unlimited' option is currently selected. The background shows the 'Block Users' tab and a search bar with 'example.domain.com' entered.

To remove users from the blocked list

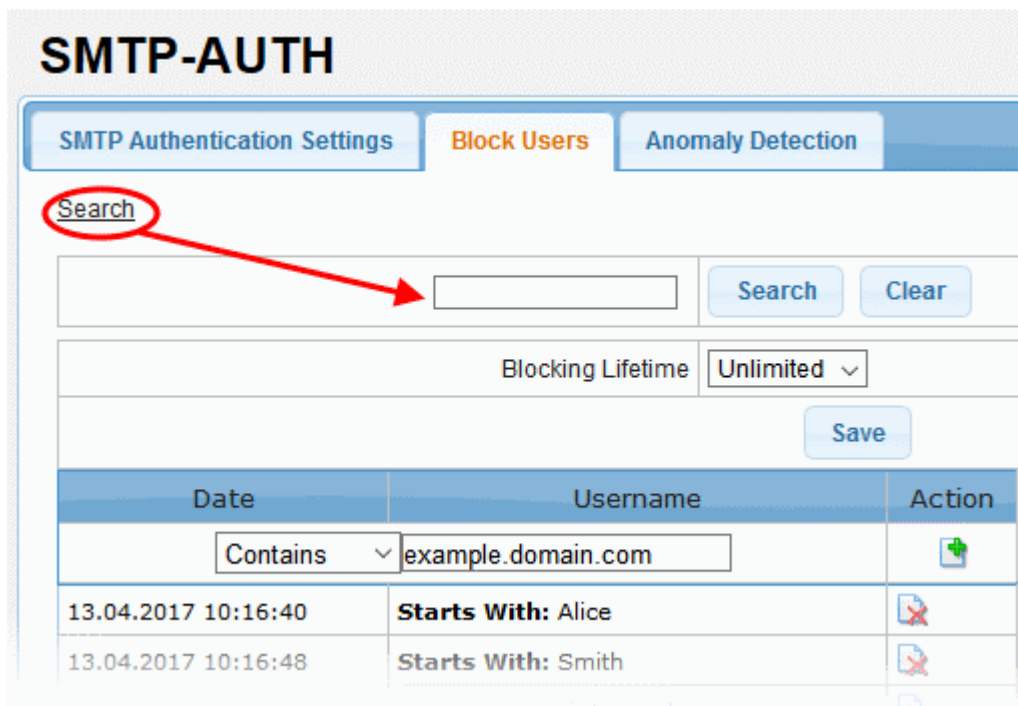
- To remove users one at a time, click the  button under the 'Action' column header and confirm the deletion in the 'Confirmation' dialog.
- To delete all the blocked users in the list, click the 'Delete all' button at the bottom.



- 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



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

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

The screenshot shows the 'SMTP-AUTH' configuration page. At the top right, there are links for 'Choose Language', a language dropdown set to 'English', an American flag icon, and a 'Logout' button. Below this is a navigation bar with three tabs: 'SMTP Authentication Settings' (active), 'Block Users', and 'Anomaly Detection'. A search bar contains the text 'example' with 'Search' and 'Clear' buttons. Below the search bar, there is a 'Blocking Lifetime' dropdown menu set to 'Unlimited' and a 'Save' button. A table displays blocked users with columns for 'Date', 'Username', and 'Action'. The table has one row with the date '18/07/2018 08:30:53' and the username 'Contains: example.domain.com'. Below the table are 'Export', 'Import', and 'Delete all' buttons.

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

This screenshot is similar to the previous one but shows a list of blocked users. The table has five rows:

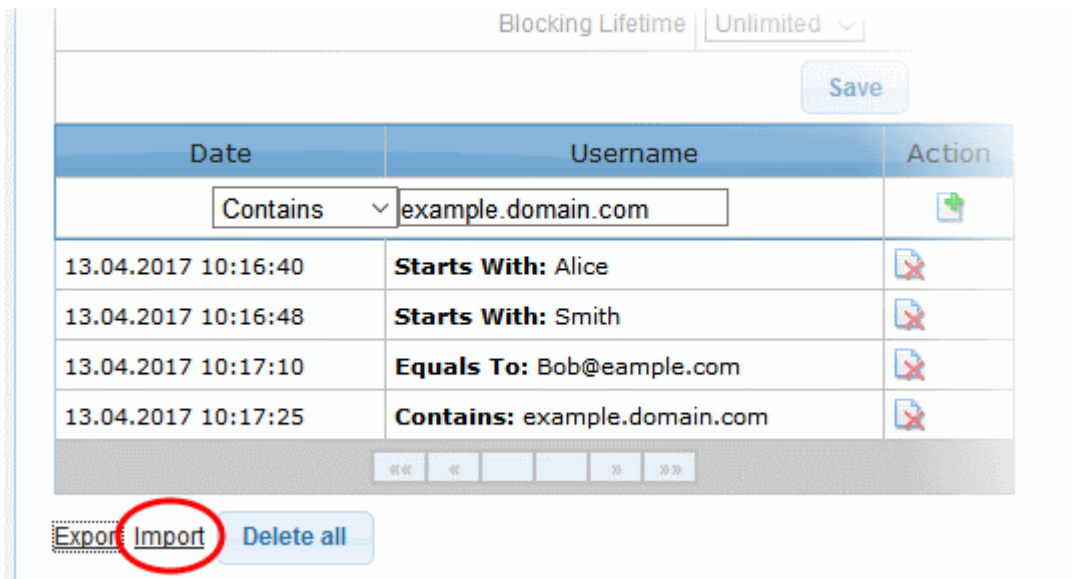
Date	Username	Action
	Starts With Alice	
20/10/2017 15:35:47	Contains: fake	
18/07/2018 08:30:53	Contains: example.domain.com	
18/07/2018 08:31:23	Equals To: Bob@domain.com	
18/07/2018 08:31:44	Starts With: Smith	
18/07/2018 08:32:03	Starts With: Alice	

 The 'Export' button at the bottom left is circled in red.

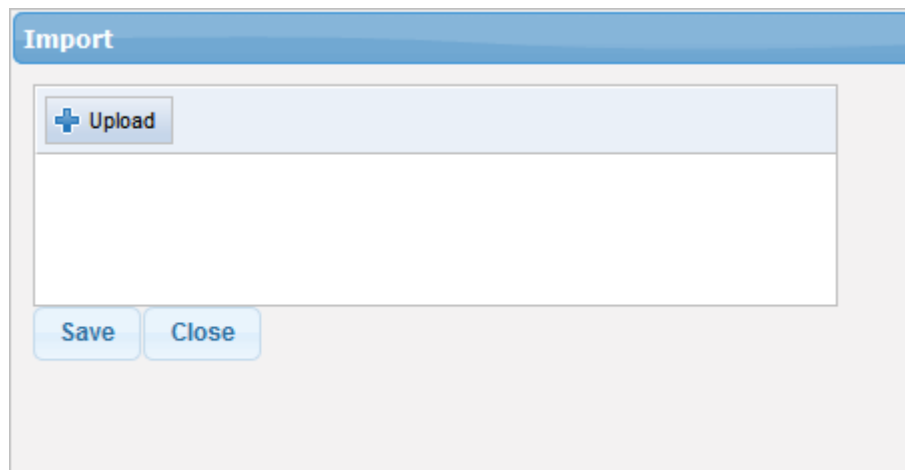
- The user list will be exported as a .txt file. Save the file as required.

To import blocked users from file

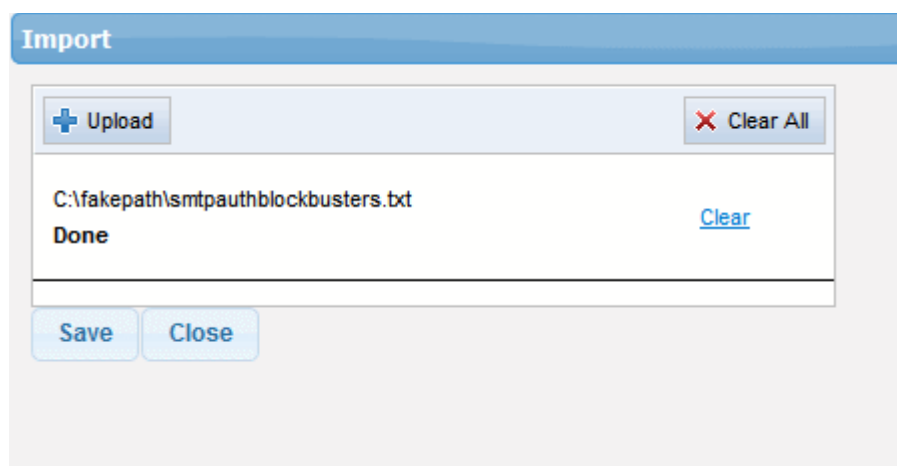
- Click the 'Import' link at the bottom of the screen



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 'Clear All' at top right.

- To finalize the import, click 'Save'.

4.3.3 Anomaly Detection

- 'Anomaly Detection' will alert you if a user has sent messages from multiple IP addresses within a set time period.
- You can choose to block these users if the outgoing mail IP addresses exceed the number set in this tab.
 - This value cannot be '0'. Set a value between 1 and 10,000 to block users, IP addresses or SMTP auth requests.
- Click 'SMTP' > 'SMTP-AUTH' > 'Anomaly Detection' to open this area.

Anomaly Detection Settings - Table of Parameters

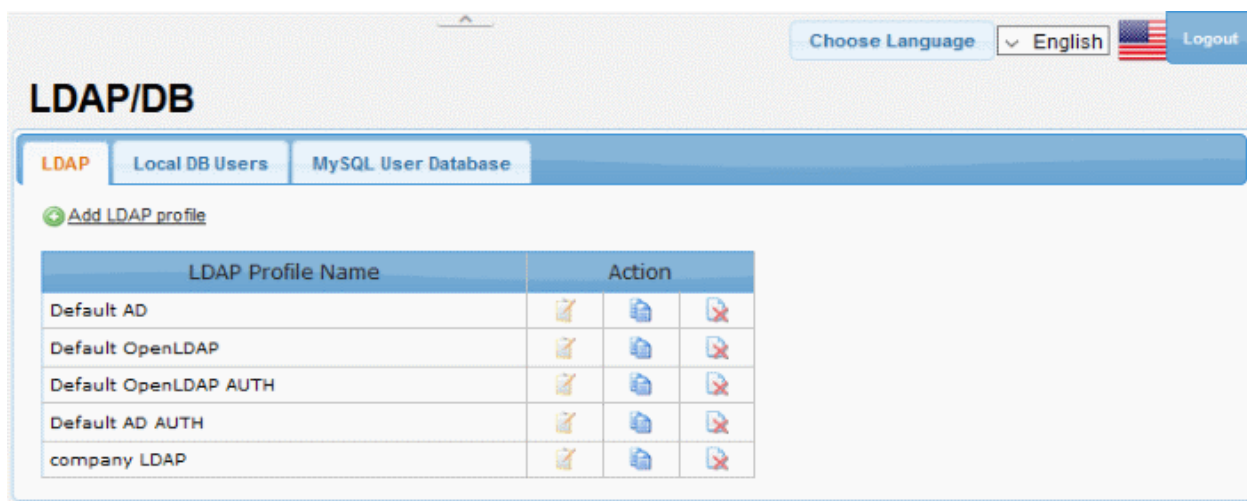
Parameter	Description
Enable Anomaly Detection	Enable the feature with the parameters listed directly below this setting. Anomaly detection is disabled by default.
Enable monitoring mode	If enabled, the SMTP-AUTH controller monitors authorization requests from the specified IP addresses. By default this setting is disabled.
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	The minimum number of different IP addresses that can make successful SMTP-AUTH

addresses that makes successful SMTP-AUTH requests with same username	requests with the same username. Any request beyond the threshold set will not be processed
---	---

- Click 'Save' to apply your changes.

4.4 LDAP/Local DB/My SQL User Database

- Secure Email Gateway can be configured to check the validity of a recipient before filtering begins. This helps ensure resources are not wasted on invalid recipients.
- If the email servers behind Secure Email Gateway are integrated with LDAP, Local DB or MY SQL Database, then Secure Email Gateway will check the validity of recipients. If they are not valid then it will reject the emails at the SMTP level.
- To open the 'LDAP/DB' screen, click the 'SMTP' tab on the left menu and click 'LDAP/DB'.

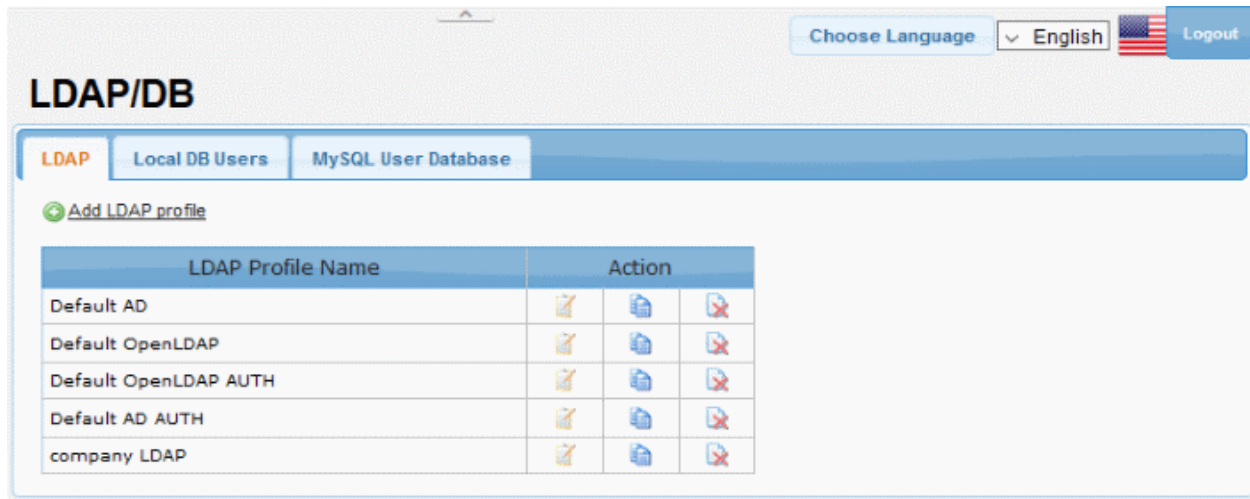





See the following sections for more details:

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

4.4.1 LDAP Profile

- The lightweight directory access protocol (LDAP) is a protocol for querying and modifying data using directory services running over TCP/IP.
- If you integrate LDAP database with Secure Email Gateway then the service can check whether a recipient is a valid
 - If the recipient is not a valid user then the email is rejected.
- This avoids wasting resources by filtering mail for invalid recipients. The LDAP profiles added here are available for selection in interfaces such as **'Manage Domains' > 'Routes'** and **'SMTP AUTH > SMTP Authentication Settings'**.
- Click 'SMTP' > 'LDAP/DB' > 'LDAP', to open the configuration screen.



LDAP Profile - Table of Column Descriptions	
Column Header	Description
LDAP Profile Name	The label provided for the custom LDAP policy. Each profile contains connection information and search settings to query the database.
Action	 Edit the details of a profile
	 Copy a profile so it can be used as the basis for a new profile.
	 Delete the 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

Choose Language English Logout

New LDAP Profile

Profile Name *	<input type="text"/>
Connection type	Plain <input type="button" value="v"/>
Host Name or IP Address *	<input type="text"/>
Port *	389 <input type="text"/>
Host Name or IP Address (Secondary)	<input type="text"/>
Port (Secondary)	0 <input type="text"/>
Search Type	Realtime <input type="button" value="v"/>
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 *	<input type="text" value="(mail=%m)"/>
<small>%u = "user" for "user@domain.com" %d = "domain.com" for "user@domain.com" %m = Whole e-mail address</small>	
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 Secure Email Gateway 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. Secure Email Gateway 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: <ul style="list-style-type: none"> 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 Secure Email Gateway 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 'Verify' to check the entered parameters and connectivity are correct. If verification fails, the error message will be displayed.
- Click 'Save' to apply your changes.

To edit a LDAP profile

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

Choose Language English Logout

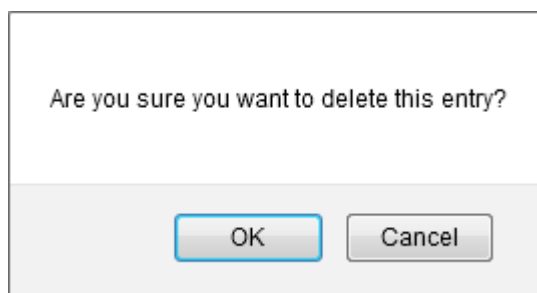
Edit LDAP profile

Profile Name *	<input type="text" value="Comodo Open LDAP"/>
Connection type	<input type="text" value="Plain"/>
Host Name or IP Address *	<input type="text" value="192.168.193.31"/>
Port *	<input type="text" value="389"/>
Host Name or IP Address (Secondary)	<input type="text"/>
Port (Secondary)	<input type="text" value="0"/>
Search Type	<input type="text" value="Realtime"/>
Cache Time (minutes) *	<input type="text" value="0"/>
Anonymous Access	<input type="checkbox"/>
Login DN *	<input type="text" value="comodo"/>
Password *	<input type="password" value="*****"/>
Enable catch-all for this profile	<input checked="" type="checkbox"/>
Search Base *	<input type="text" value="Support dc=comodo"/>
Search Pattern * <small>%u = "user" for "user@domain.com" %d = "domain.com" for "user@domain.com" %m = Whole e-mail address</small>	<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"/>	

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

To delete a LDAP profile

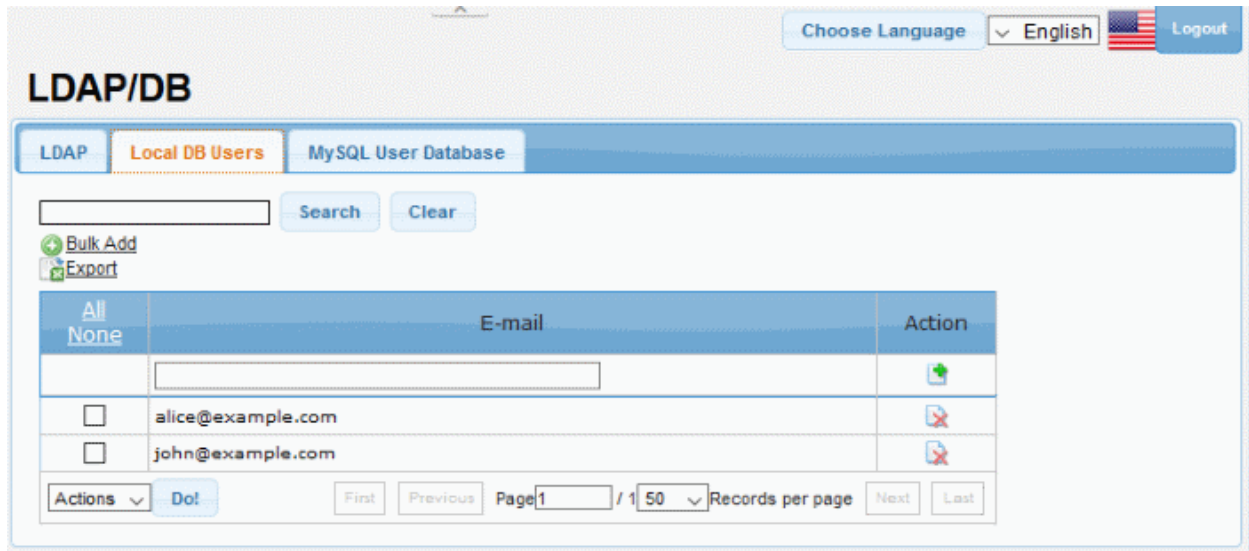
- Click the delete button beside a LDAP profile that you want to remove.



- Click 'OK' to confirm the deletion.

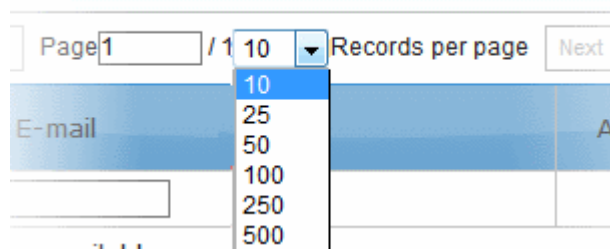
4.4.2 Local DB Users

- Secure Email Gateway allows you to add users to its local database for managed domains.
- This helps to ensure mails to invalid recipients are rejected before filtering begins.
- The users added here are available for selection in interfaces such as 'Managed Domains > Routes'.
- Click 'SMTP' > 'LDAP/DB' > 'Local DB Users' to open this interface.



Local DB Users - Table of Column Descriptions	
Column Header	Description
Email	The address of the user added to Secure Email Gateway
Actions	Add a user. Enter the user's email address in the field provided then click this button.
	Delete a user from the list. Use the check-boxes on the left to select users.

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



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

The interface allows administrators to:

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

To add a user

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

The screenshot shows the 'Local DB Users' tab selected. At the top, there are tabs for 'LDAP', 'Local DB Users', and 'MySQL User Database'. Below the tabs is a search bar with 'Search' and 'Clear' buttons. There are two links: 'Bulk Add' (with a green plus icon) and 'Export' (with a document icon). Below these is a table with three columns: 'All None', 'E-mail', and 'Action'. The first row of the table has 'user6@example.com' in the 'E-mail' column, circled in red. The 'Action' column for this row contains a green plus icon. Below the table are pagination controls: 'Actions' dropdown, 'Do!', 'First', 'Previous', 'Page 1 / 1', '50' dropdown, 'Records per page', 'Next', and 'Last'.

- Click the  button under the 'Action' column.

Note: You can add users for managed domains only.

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

To add multiple users

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

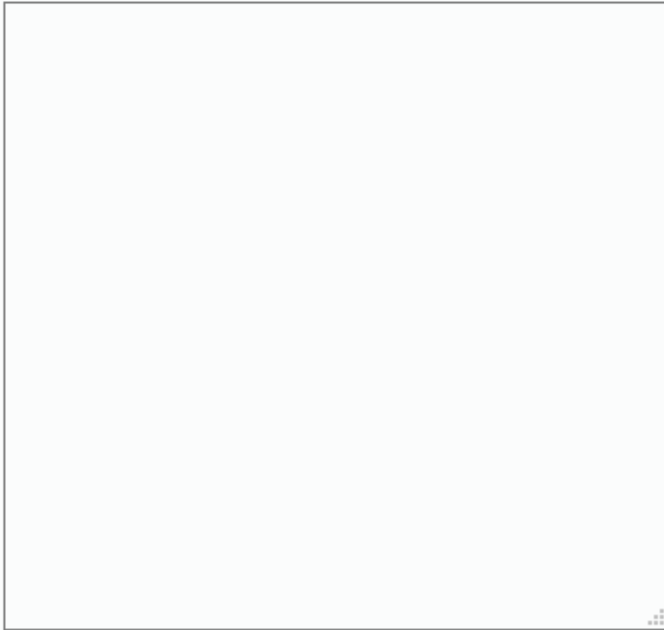
This screenshot is similar to the previous one, but the 'Bulk Add' link is circled in red. The table below it shows the 'E-mail' column with 'user6@example.com' entered.

The 'Bulk Add' screen will be displayed.

Add Local DB Users

Bulk Add

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



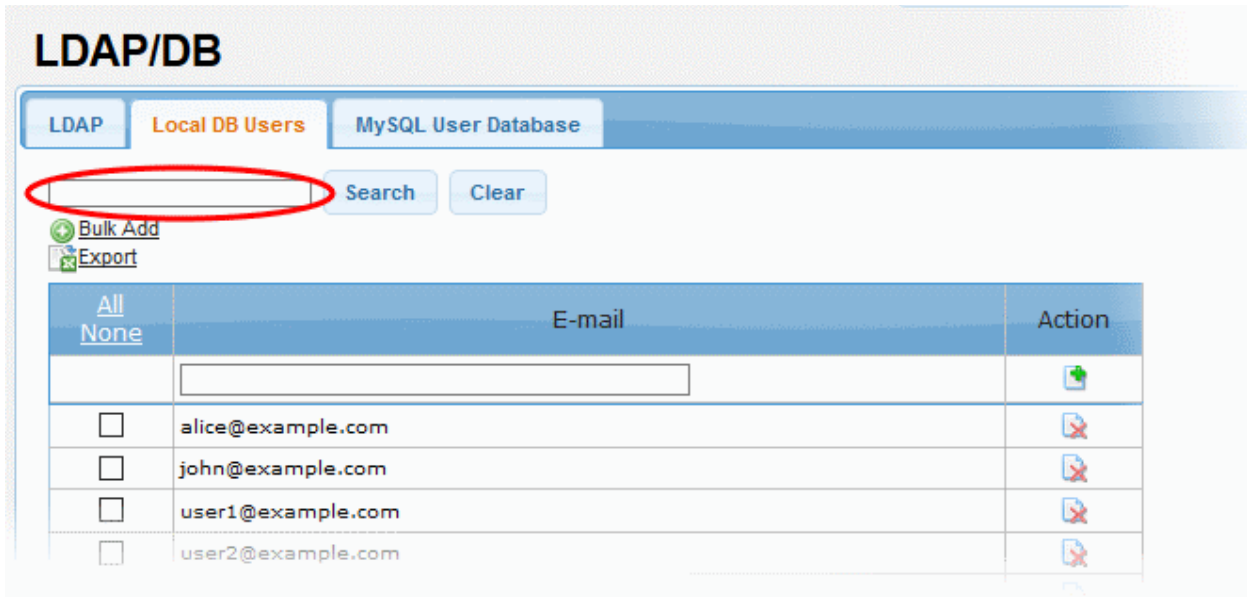
- Enter the users' email addresses each per line. The maximum allowed at a time is 500 users.
- Click 'Add'.

Note: You can add users for managed domains only.

The users will be added and displayed in the list.

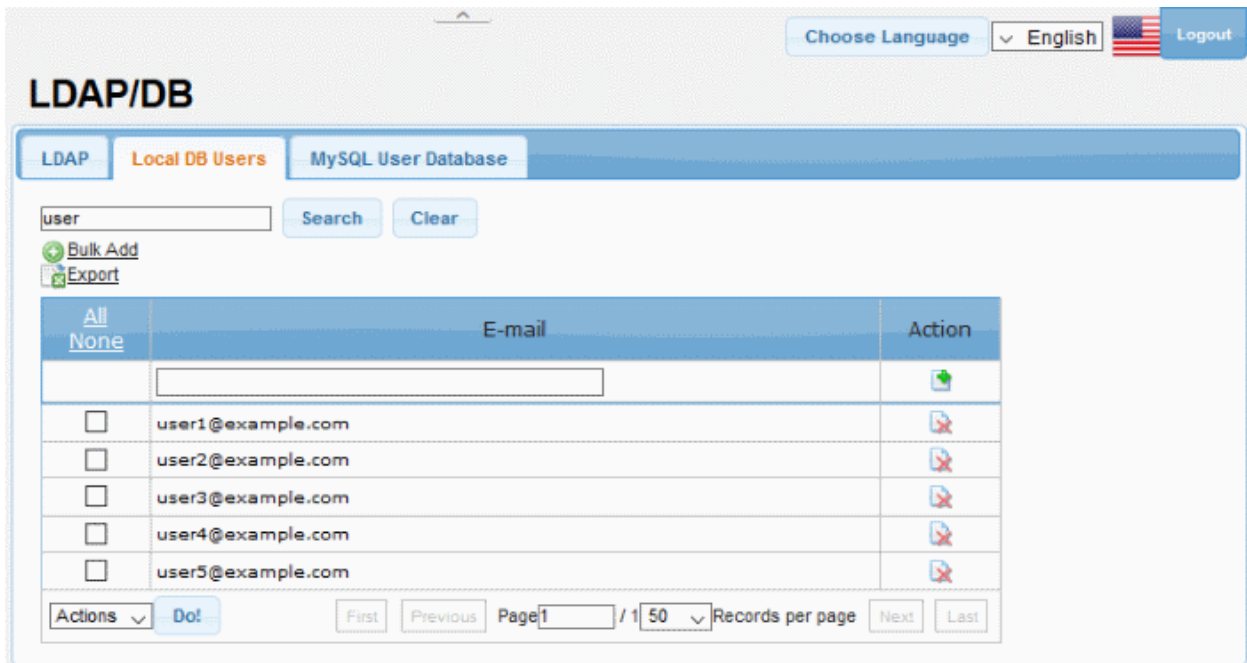
To search for users

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



- Click 'Search'.

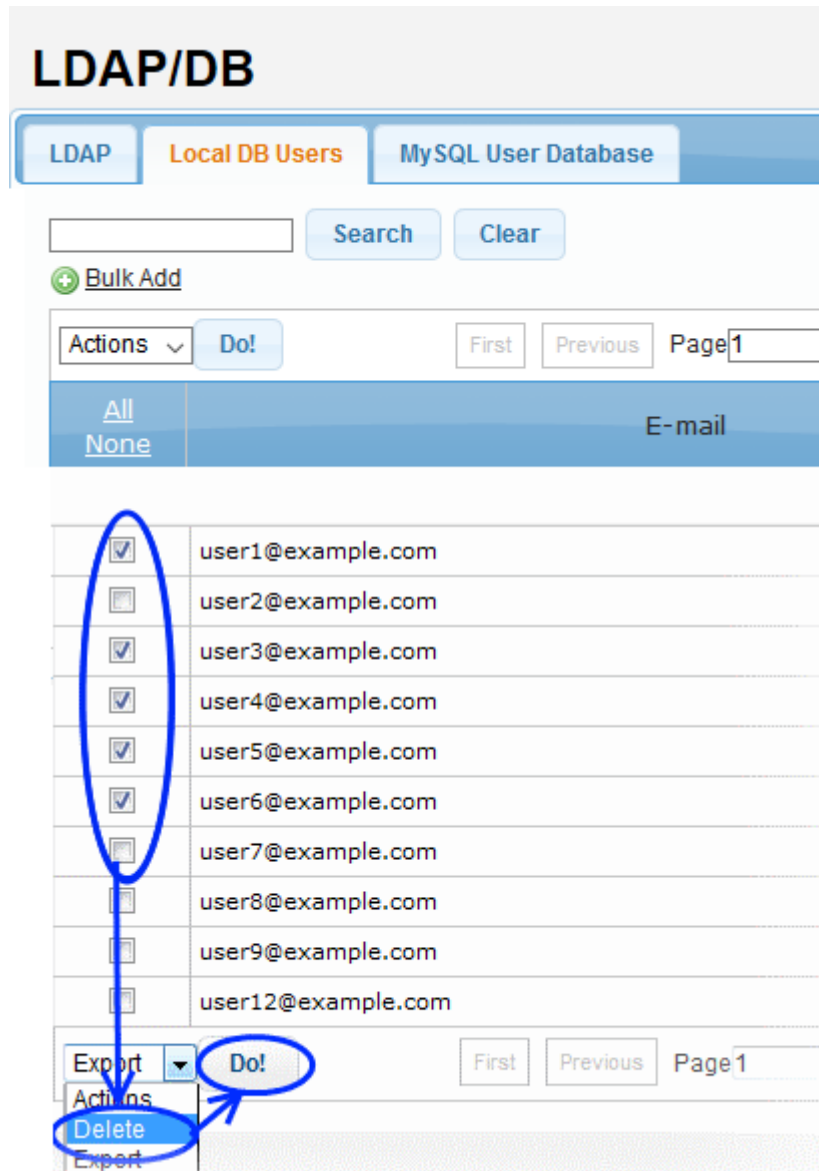
The items that contain the entered search text will be displayed.



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

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

- Use the check-boxes on the left to select specific users OR click the 'All' link
- Click the 'Export' link at the upper-left
- The exported file is in .txt format. Save the file as required

LDAP/DB

LDAP Local DB Users **MySQL User Database**

Search Clear

[Bulk Add](#)
[Export](#)

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

Actions First Previous Page 1 / 1 50 Records per page Next Last

4.4.3 My SQL User Database

- Secure Email Gateway is capable of verifying the validity of users by referring to a 'MySQL User Database' located on a remote server.
- If the recipient is not a valid user then email is rejected at the SMTP level. Since the filtering process is not engaged for invalid recipients, Secure Email Gateway'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 'SMTP' > 'LDAP/DB' > 'MySQL User Database':

Choose Language



LDAP/DB

LDAP Local DB Users **MySQL User Database**

[Add MySQL User Database](#)

Profile Name	Host Name or IP Address	Port	Database	SQL Clause	Action
Dome Antispam	192.168.199.31	25	DAS_DB	mail='%m'	
DAS	10.51.108.202	25	DAS_DB	mail='%m'	

Copyright© 2006-2018 Comodo Security Solutions, Inc. All rights reserved.
Dome Antispam name and logo are trademarks of Comodo Security Solutions, Inc.
Release: 6.7.1.8972932

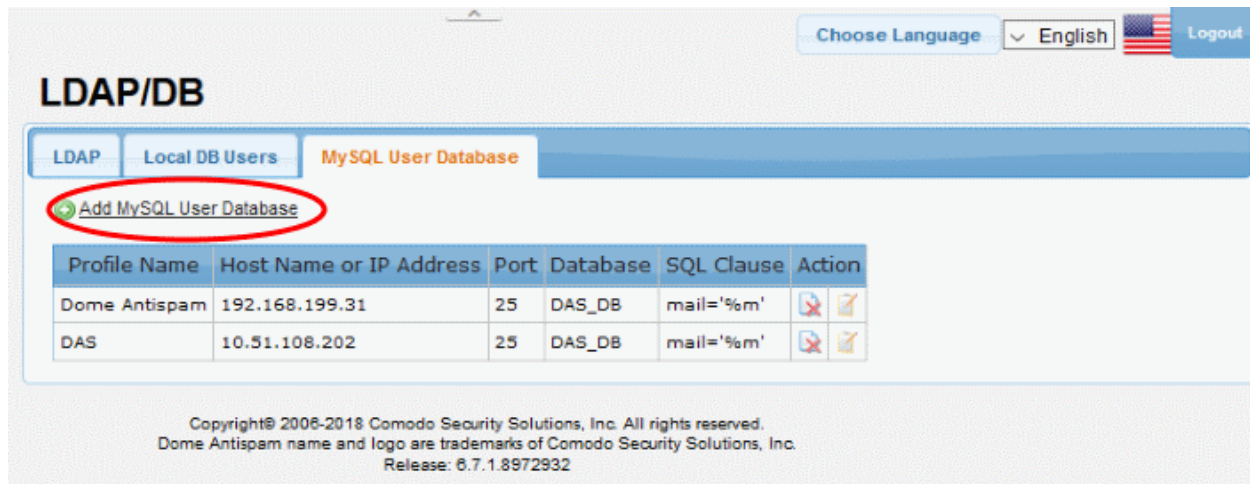
MySQL User Database Profile - Table of Column Descriptions	
Column Header	Description
Profile Name	The name of the MySQL User Database profile added to Secure Email Gateway
Host Name or IP Address	Displays the address of the system where the 'MySQL User Database' is located.
Port	Displays the port number to which Secure Email Gateway connects to.
Database	The name of the 'MySQL User Database'.
SQL Clause	The 'SQL clause' used to fetch the users' details.
Action	 Allows you to edit the details of the 'MySQL' profile
	 Allows you 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.



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

[Choose Language](#) | English [Logout](#)


New MySQL User Database

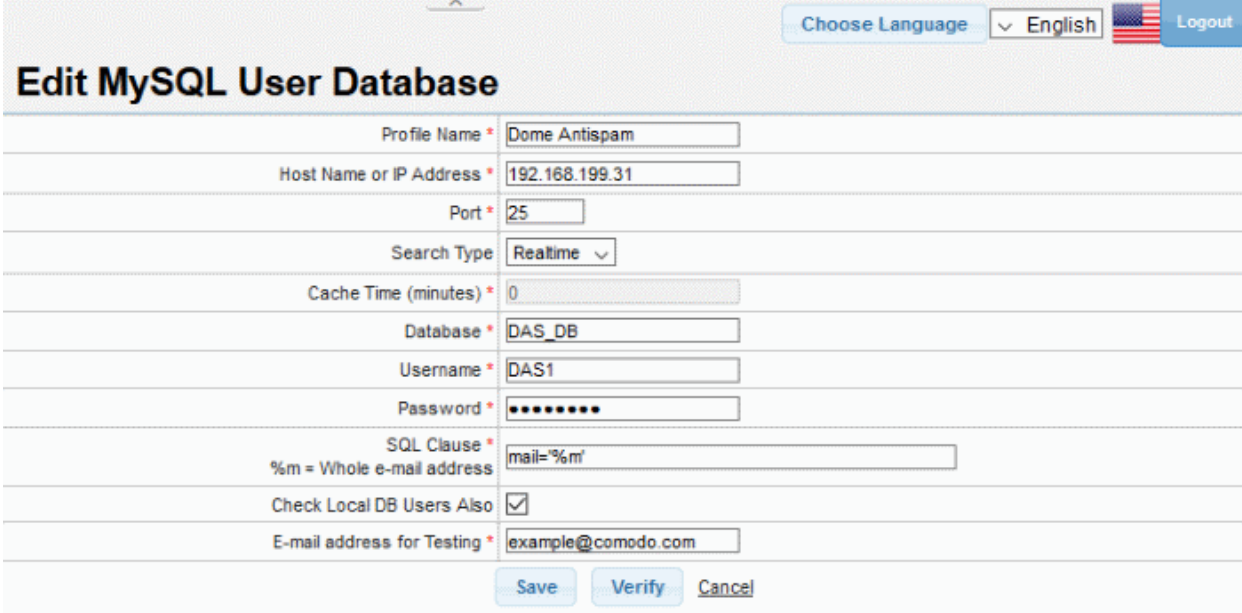
Profile Name *	<input type="text" value="Dome Antispam"/>
Host Name or IP Address *	<input type="text" value="192.168.199.31"/>
Port *	<input type="text" value="25"/>
Search Type	<input type="text" value="Realtime"/>
Cache Time (minutes) *	<input type="text" value="0"/>
Database *	<input type="text" value="DAS_DB"/>
Username *	<input type="text" value="DAS1"/>
Password *	<input type="password" value="*****"/>
SQL Clause *	<input type="text" value="mail='%m'"/>
<small>%m = Whole e-mail address</small>	
Check Local DB Users Also	<input checked="" type="checkbox"/>
E-mail address for Testing *	<input type="text" value="example@comodo.com"/>

MySQL User Database Profile -Table of Parameters	
Parameter	Description
Profile Name	Enter the name of the MySQL profile
Host Name or IP Address	Enter the hostname or IP address of the system where MySQL database is located.
Port	Enter the port number to which Secure Email Gateway should connect to.
Search Type	Select the type of search from the drop-down. The options available are: <ul style="list-style-type: none"> 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 'Verify' to check the entered parameters and connectivity are correct. If verification fails, the error message will be displayed.
- Click the 'Save' button to apply your changes.


To edit a MySQL profile

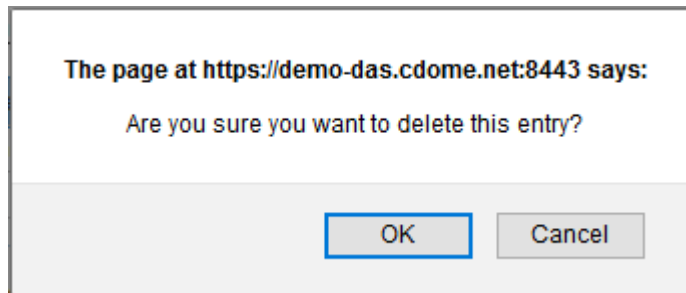
- Click the  button beside a 'MySQL' profile that you want to edit.



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

To delete a MySQL profile

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



- Click 'OK' to confirm the deletion.

4.5 Greylist

- Click 'SMTP' > 'Greylist' in the left menu.
- Greylisting is another form of spam control whereby Secure Email Gateway will temporarily reject mail from senders it does not recognize. Instead, it will send a 'try again later' message to the sending mail server.
- Upon receiving this message, legitimate mail servers will try to resend the mail after a delay. Secure Email Gateway will accept the resent mail providing it does not fall foul of its other filters.
- However, because of the prohibitive cost of re-sending millions of mails, spam servers are unlikely to perform this simple resend. This means greylisting can be very effective at blocking large amounts of spam at source.



- You have the option to disable greylisting entirely, or you can specify IP addresses/domains as exceptions (so CSEG will accept mail from them on first contact).

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

4.5.1 Greylist Ignored IP Addresses/Domains

- Click 'SMTP' > 'Greylist' to open the greylist screen.
- You can add IP addresses and domains as exceptions to the greylist policy.
- Mail from these addresses will be accepted immediately, without requiring the source mail server to resend. See '**Greylist**', if you'd like to read a description of greylisting.

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.

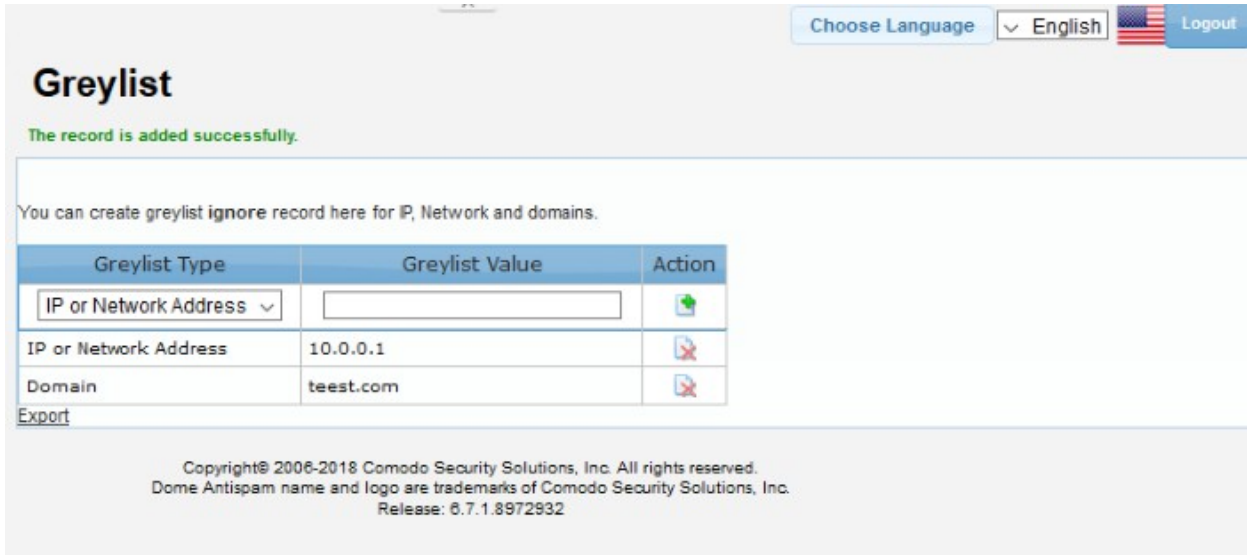
Action		To add an email source to Greylist ignore record, click this button after selecting and entering the details in the fields under 'Greylist Type' and 'Greylist Value' columns respectively.
		Allows you to delete a record from the list.

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


- For 'Greylist Type' select whether you want to create an exception for a domain or an IP address:




The screenshot shows the 'Greylist' management interface. At the top right, there are links for 'Choose Language', 'English', and 'Logout'. The main heading is 'Greylist'. A green message indicates 'The record is added successfully.' Below this, a text box states 'You can create greylist ignore record here for IP, Network and domains.' A table is displayed with the following data:

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

Below the table is an 'Export' link. At the bottom of the page, there is copyright information: 'Copyright© 2006-2018 Comodo Security Solutions, Inc. All rights reserved. Dome Antispam name and logo are trademarks of Comodo Security Solutions, Inc. Release: 6.7.1.8972932'.

- Type the specific domain name or IP address in the 'Greylist Value' field.
- Click the  button under the 'Action' column.





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

Choose Language English  [Logout](#)

Greylist


The record is added successfully.

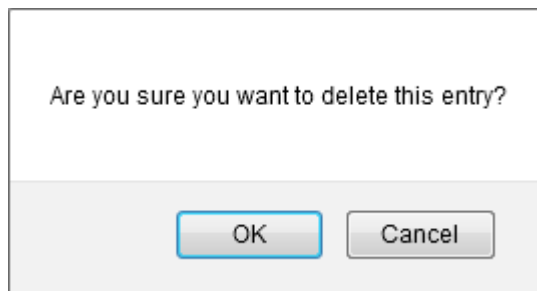
You can create greylist **ignore** record here for IP, Network and domains.

Greylist Type	Greylist Value	Action
<input type="text" value="IP or Network Address"/>	<input type="text"/>	
IP or Network Address	10.0.0.1	
IP or Network Address	10.108.51.202	
Domain	teest.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

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

[Export](#)

- Save the exported file to your system.

4.6 Manage RBL Servers

- Click 'SMTP' > 'RBL' to open this screen.
- A realtime blackhole list (RBL) is a list of mail servers that send spam, act as spam relays, or have sent mail containing viruses.
- Secure Email Gateway can block connections from addresses found in the realtime blackhole lists.
- You can add as many RBL servers as you wish. You can also enable or disable individual lists as required.

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

[Export](#)

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 you to delete an 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.score.senderscore.com	Return Path Reputation Network Blacklist	RBL	Yes	
zen.spamhaus.org	spamhaus	RBL	Yes	
psbl.surriel.com	Passive Spam Block List	RBL	Yes	
bl.spamcop.net	spamcop	RBL	Yes	

Export

The 'Add RBL server' screen will be displayed:

Add RBL server

Choose Language: English | 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 Secure Email Gateway. See '**Profile Management**' for more details about profiles.
- Click 'Save' to add the new RBL server.

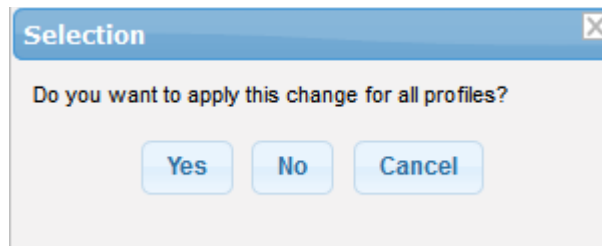
To enable/disable a RBL server

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



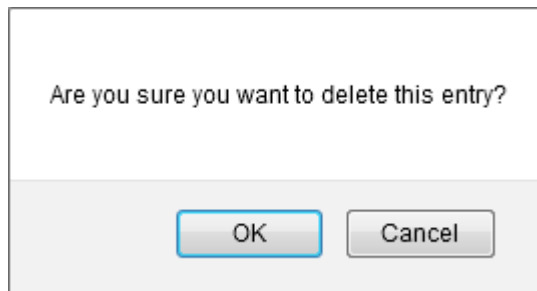
- Click 'Yes' to enable the server for all the profiles.
- Click 'No' to enable the server for the current profile.

The RBL servers can be enabled/disabled independently also for the profiles available in Secure Email Gateway. 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

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

[Export](#)

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

4.7 Disclaimer

- Secure Email Gateway allows you to insert disclaimers in outgoing mails for managed domains.
- The screen has two sections - 'Text Footer' and 'HTML Footer'.
 - The 'Text Footer' is for the disclaimer content, and the 'HTML Footer' can be used for corporate messages.
- Click 'SMTP' > 'Disclaimer' to open this screen.

Disclaimer

Logout

Managed Domain Name *	<input type="text" value="-Choose-"/>
Enabled	<input type="checkbox"/>
Text Footer	<div style="border: 1px solid #ccc; min-height: 100px;"></div>
HTML Footer	<div style="border: 1px solid #ccc; min-height: 100px;"></div>

Save
Cancel

- **Managed Domain Name:** Select the managed domain from the drop-down for which you want to add a disclaimer.
- **Enabled:** If selected, the messages will be inserted in the outgoing mails of the domain.

- **Text Footer:** Enter the disclaimer content in this field.
- **HTML Footer:** Enter content such as corporate message and so on in this field.
- Click 'Save'

To edit the disclaimer, open the screen, select the domain from the drop-down, edit the messages and click 'Save'.

4.8 SMTP Relay

- Click 'SMTP' > 'Relay' in the left-menu to open this interface.
- Adding endpoint details to relay list lets recipients not added to managed domains also send mails.

IP Range	Sender Domain Check	Action
<input type="text"/>	<input type="checkbox"/>	
192.168.2.1		
192.168.		
192.168.1.1		

Range Examples

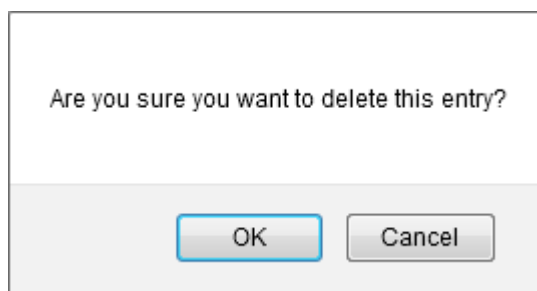
- 192.168.2.1 (only one IP address)
- 192.168.2.2-5 (IP addresses in the range 192.168.2.2 to 192.168.2.5)
- 192.168.2. (whole 192.168.2.0/24 C class)
- 192.168. (whole 192.168.0.0/16 B class)

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.

Office 365 Check

Secure Email Gateway supports Microsoft Office 365. [Click here](#) to know how to integrate and deploy Secure Email Gateway protection.

4.9 DomainKeys Identified Mail (DKIM)

- Click 'SMTP' > 'DKIM' to open this interface.
- DomainKeys Identified Mail (DKIM) is a method of authenticating outgoing mail. It allows senders to associate a domain with an outgoing mail.
- An electronic signature is inserted into the header of an outgoing mail to identify the mail source.
- Secure Email Gateway lets you create a new domain key for managed domains to authenticate outgoing mails.
- 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.

DKIM

Managed Domain Name *

Enable DKIM

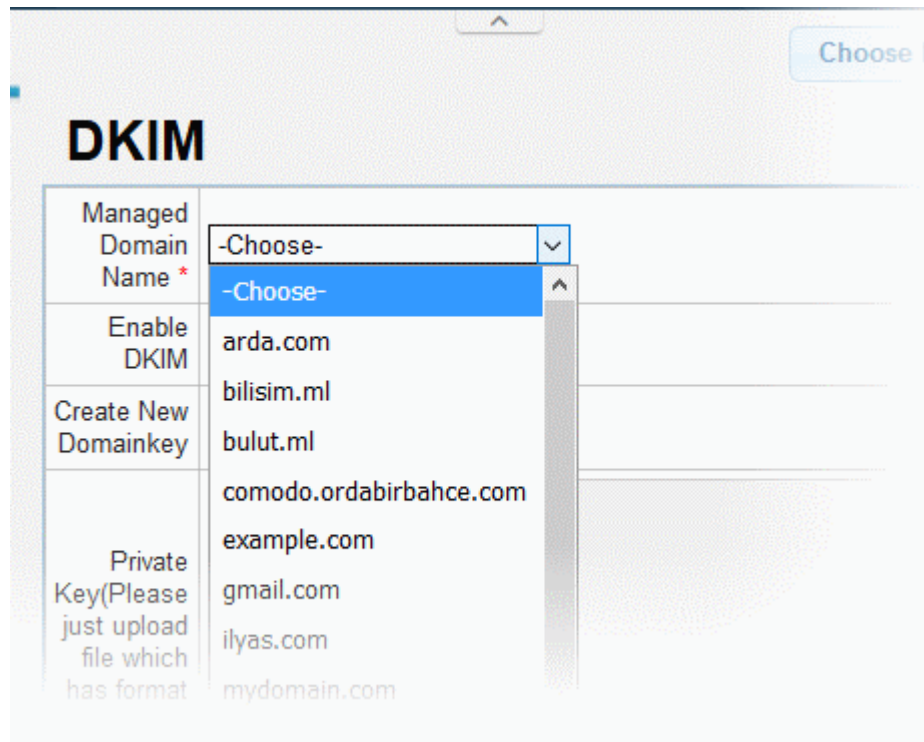
Create New Domainkey [Create](#)

Private Key(Please just upload file which has format .pem || key || .publickey)
[Download private key](#) [Import](#)

Public Key(Please just upload file which has format .pem || key || .publickey)
[Download public key](#) [Import](#)

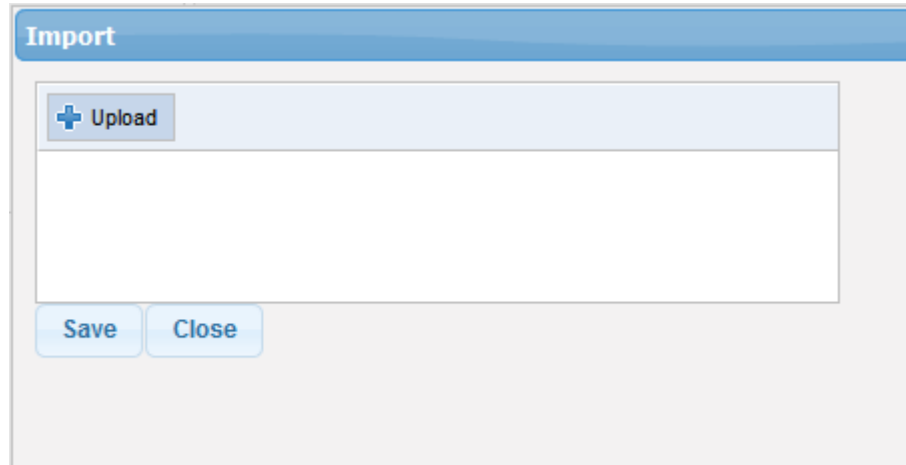
[Save](#) [View DNS register text](#) [Cancel](#)

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

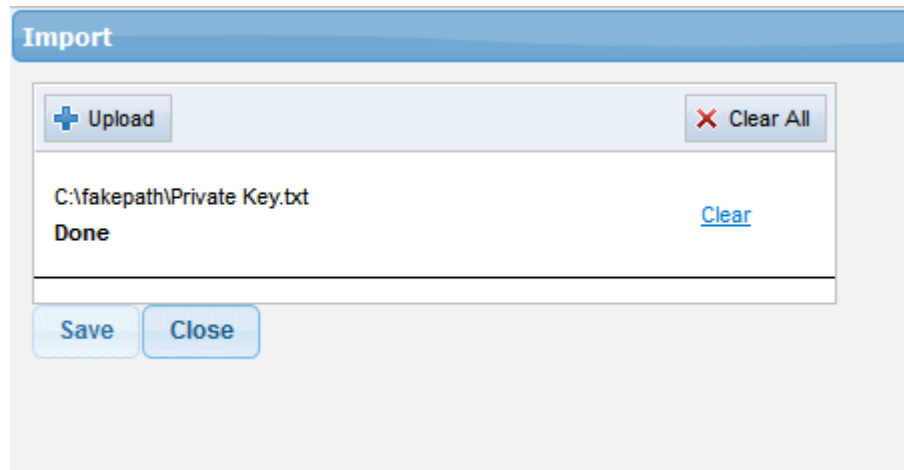


If you have the domain key that needs to be associated with your mails, then follow the steps below:

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



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



- 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 'Create' to generate a new domain key for the selected domain.

[Choose Language](#) ▾ English [Logout](#)

DKIM

Managed Domain Name *	<input type="text" value="comodo.ordabirbahce.com"/> ▾
Enable DKIM	<input checked="" type="checkbox"/>
Create New Domainkey	<input type="checkbox"/> Create
Private Key(Please just upload file which has format .pem key .publickey)	<pre>-----BEGIN RSA PRIVATE KEY----- MIICXgIBAAKBgQCwN6d4uE/od2wCfxdhqfulWSuNFLWBHg/RMS+Jfiok10/Qpi/f nm35Rmc9ZrkYb5KFVK8NkhXuTervT8QV2kHFbFfJJeJFFA2sAJu91KjYJTkDiOceF VAOTjwu7mF5pDzE42glwSTihqBHGR5XS3+GqygunC+q3NY3bFuPXRixuPwIDAQAB AoGBAKOfecSxN5I+Ue9bfSV1RZbMXZEJWqOCe2NeDWrYmF9PAdCWjztPi4P76F7u JA5Zgy6EfGrYa76z4OLHKsa1W31f0QpJPWdRUvUKg9Hc6EkN48XOr8de78r4ZuGO NqKAEMDjWidufCQBAIGEnv1meOeqvoHWXlIs+7pr3tDeNeJAKEA2jZzyJnNx8QH 0WHQRRNPXsa5EYCL2ksE4DJPPaguN6TChaBtp39H+QiHIYleus0m+TCA5PFjaMHF r7QRM/X9dQJBAM67hAMamnlRGWKwDokqSif0jEklo4L4m2/4UqRBXmQmNeN8PJ2J cP+TDi6bgxMa2GWISJnQm0Lbio2W4T0+gmMCQGSskqaOLx5nFqRHwGtGCWxUirXE dMF1sv4st9peaVRKs2QrK+wHERGYGaAjXl0acUyuUAIQROjj3WY+yuEKMLECQCX</pre> <p>Download private key Import</p>
Public Key(Please just upload file which has format .pem key .publickey)	<pre>-----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCwN6d4uE/od2wCfxdhqfulWSuN FLWBHg/RMS+Jfiok10/Qpi/fnm35Rmc9ZrkYb5KFVK8NkhXuTervT8QV2kHFbFfJ eJFFA2sAJu91KjYJTkDiOceFVAOTjwu7mF5pDzE42glwSTihqBHGR5XS3+Gqygun C+q3NY3bFuPXRixuPwIDAQAB -----END PUBLIC KEY-----</pre> <p>Download public key Import</p>
Save View DNS register text Cancel	

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

WARNING
✕

You must entry following DNS register:

```
TXT record for BIND: dkim._domainkey.comodo.ordabirbahce.com. IN TXT "v=DKIM1; k=rsa; t=y;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQD9ADvZFOYHglPg3hzCqERzWn41AKUSeymDEut7B9EBliYmmeJmnbv3cd3XR3Xyjk+Isx5UUVmeWj22xEfdHV
//IX9lqaRlr9CX3CxSgWznldJINjMQIDAQAB"
```

[Close](#)

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.

4.10 Outgoing SMTP Limits

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

To open the 'Outgoing Limits' screen,

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

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

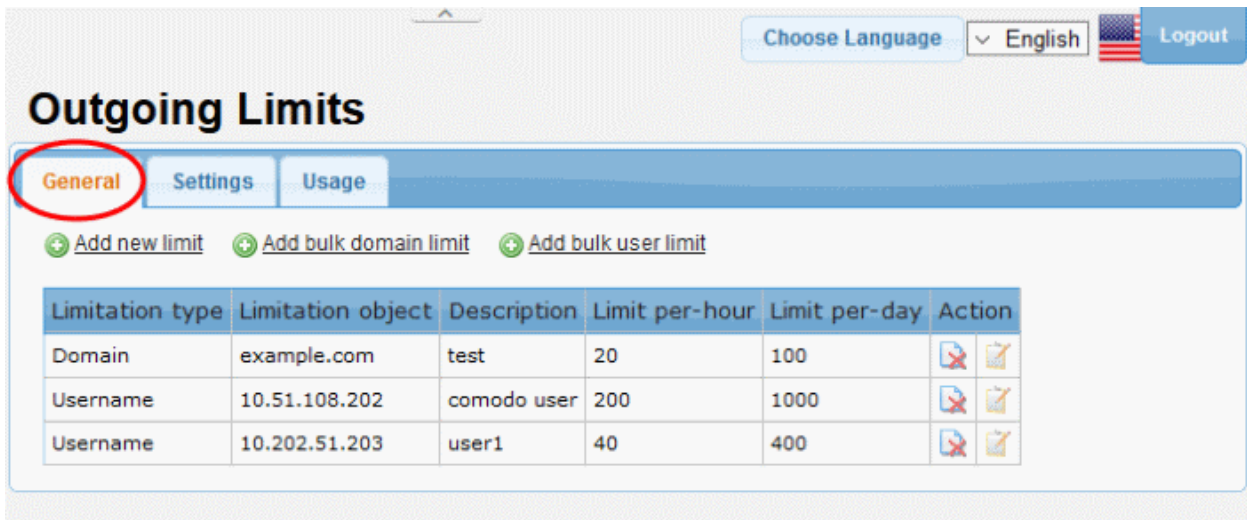
To configure outgoing limits for domains and users:


- Click the 'General' tab

Limitation type	Limitation object	Description	Limit per-hour	Limit per-day	Action
Domain	example.com	test	20	100	
Username	10.51.108.202	comodo user	200	1000	
Username	10.202.51.203	user1	40	400	

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 you to delete a limitation set for a domain or user
	 Allows you to edit a limitation set for a domain or user

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









Choose Language English  Logout

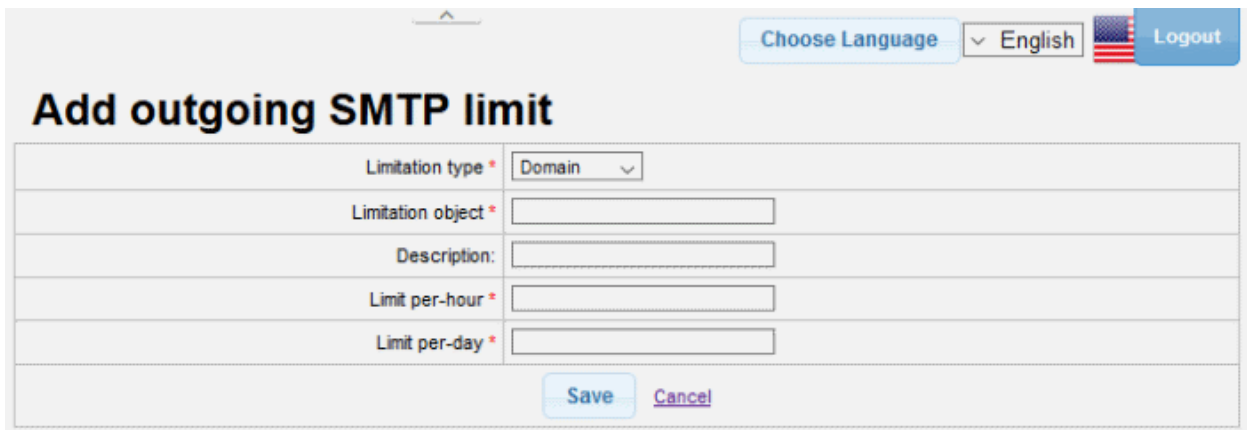
Outgoing Limits


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	example.com	test	20	100	 
Username	10.51.108.202	comodo user	200	1000	 
Username	10.202.51.203	user1	40	400	 

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



Choose Language English  Logout

Add outgoing SMTP limit

Limitation type * Domain

Limitation object *

Description:

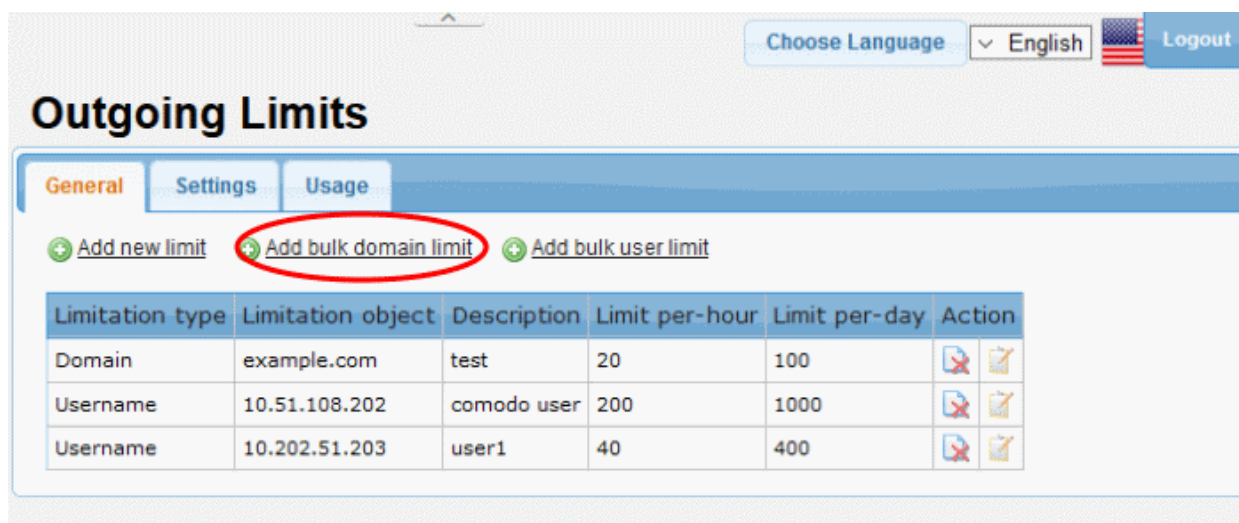
Limit per-hour *

Limit per-day *

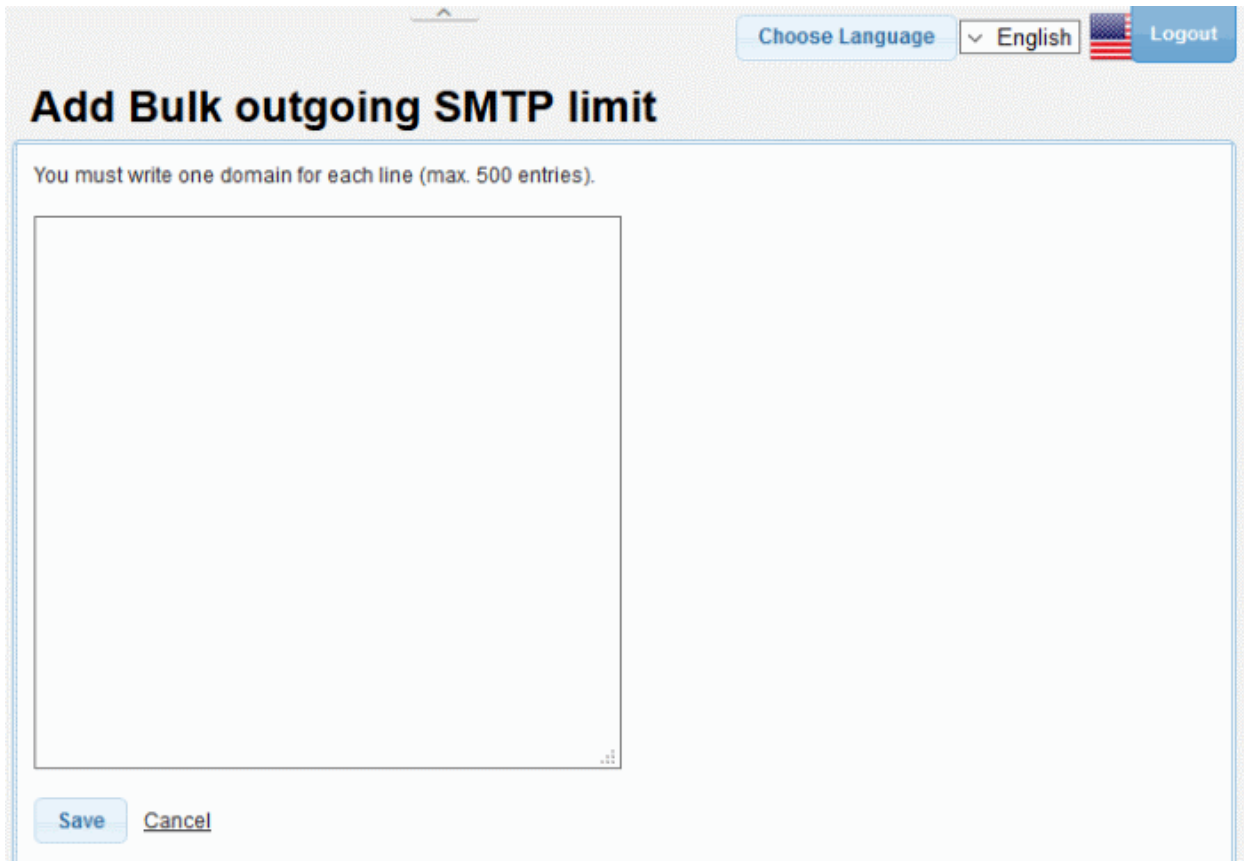
- **Limitation type:** Select whether you want to configure the limit for a domain or user from the drop-down
- **Limitation object:** Enter the name of the domain or username depending on your 'Limitation type' selection
- **Description:** Enter an appropriate description for the limitation
- **Limit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

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

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



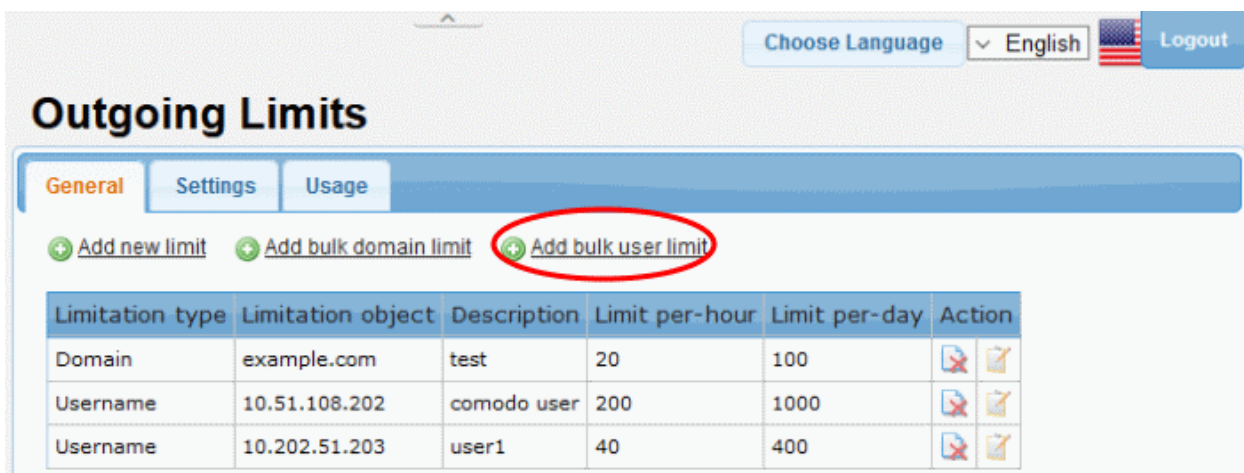
The 'Add Bulk outgoing SMTP limit' screen will be displayed.



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

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

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



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.

Choose Language English 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	example.com	test	20	100	
Username	10.51.108.202	comodo user	200	1000	
Username	10.202.51.203	user1	40	400	

- 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.

Choose Language English  Logout

Edit outgoing SMTP limit

Limitation type	Domain
Limitation object *	example.com
Description:	test
Limit per-hour *	20
Limit per-day *	100

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

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 you to customize the limitations added in the '[General](#)' tab.

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

Choose Language English Logout

Outgoing Limits

General Settings Usage

SMTP AUTH is enabled by user name limit for outgoing e-mail *	<input checked="" type="checkbox"/>
Enable the Limit for From Addresses *	<input checked="" type="checkbox"/>
Default hourly limit *	<input type="text" value="100"/>
Default daily limit	<input type="text" value="500"/>
Envelope sender must match SMTP-AUTH username	<input checked="" type="checkbox"/>
Default domain	<input type="text" value="10.108.51.202"/>
SMTP-AUTH username format *	<input checked="" type="checkbox"/> Username <input checked="" type="checkbox"/> Domain: <input checked="" type="radio"/> user@domain.com <input type="radio"/> user%domain.com
Enable System Admin e-mail notification for exceeded limits	<input checked="" type="checkbox"/>
Mail Subject	<input type="text" value="Outgoing Limits Notifi"/>
Mail From	<input type="text" value="korumail@comodo.co"/>
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>Giden e-posta limitini gecen hesap listesi</p> </pre>

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 'Save' to apply your changes.

Viewing outgoing mail usage details for domains and users

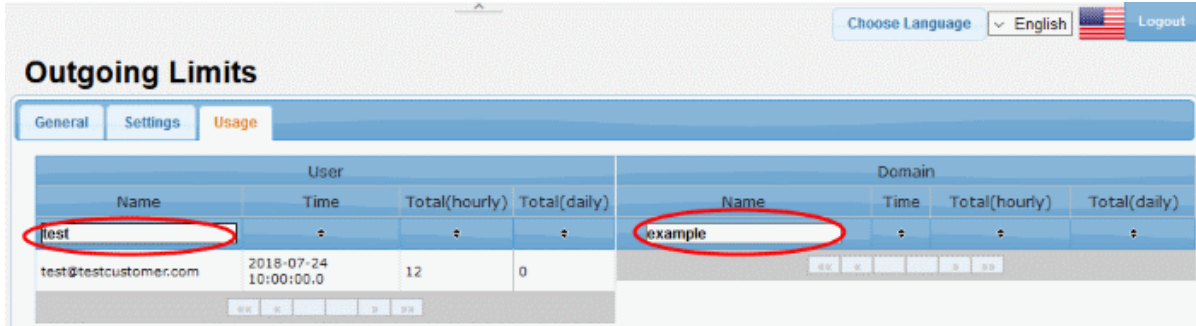
The 'Usage' tab allows you to view outgoing mails from users and domains covered by outgoing limits.


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.

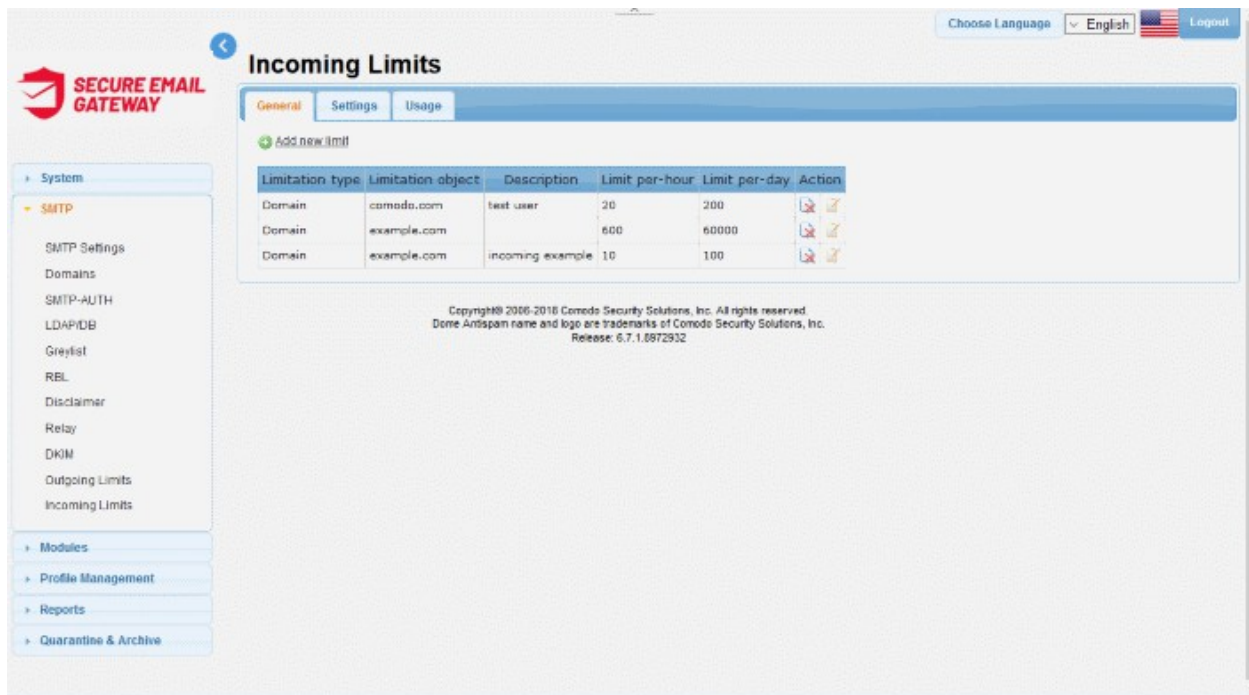
To search for a particular recipient, enter the first few letters of the recipient's name in either the 'User' or 'Domain' search field:



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

4.11 Incoming SMTP Limits

Secure Email Gateway lets you set limits for incoming mails for users as well as for domain names. Secure Email Gateway can be configured to allow only a certain number of incoming mails per hour and per day. You can add domains/usernames individually or in bulk.



- Click 'SMTP' > 'Incoming Limits' to open this screen
- The interface allows you 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

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

The screenshot shows the 'Incoming Limits' page with the 'General' tab selected. At the top right, there are options for 'Choose Language' (set to English) and a 'Logout' button. Below the title, there are tabs for 'General', 'Settings', and 'Usage'. A green '+ Add new limit' button is visible. The main content is a table with the following data:

Limitation type	Limitation object	Description	Limit per-hour	Limit per-day	Action
Domain	comodo.com	test user	20	200	
Domain	example.com		600	60000	
Domain	example.com	incoming example	10	100	

Incoming Limits: General - Table of Column Descriptions

Column Header	Description
Limitation Type	Indicates whether the limit is for a domain or user
Limitation Object	The domain or user to which the limit applies
Description	Text summary of the limitation
Limit per-hour	The number of incoming mails allowed per hour
Limit per-day	The number of incoming mails allowed per day
Action	Delete a limitation
	Edit a limitation

- The 'Add Incoming Limit' screen will open:



This screenshot is identical to the one above, but the '+ Add new limit' button is circled in red to highlight it.

The 'Add Incoming Limit' screen will be displayed.

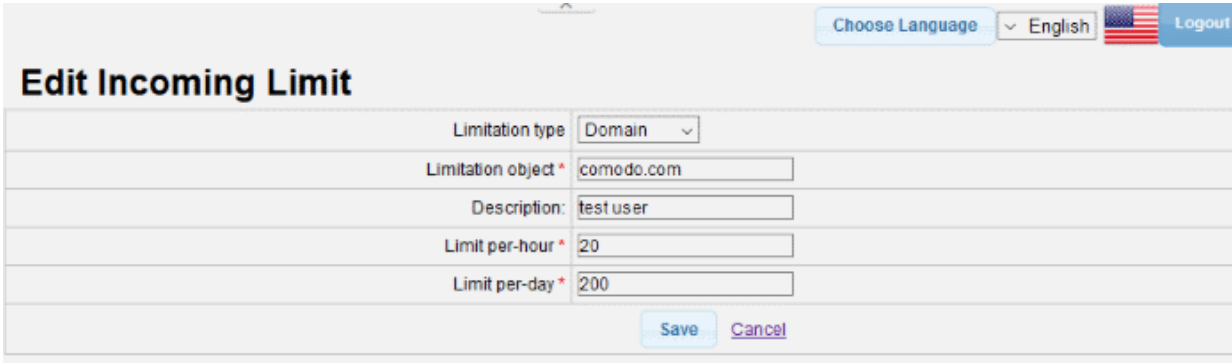
- **Limitation type:** Select whether you want to configure the limit for a domain or a user
- **Limitation object:** Enter the name of the domain or username depending on your 'Limitation type' selection
- **Description:** Enter an appropriate description for the limitation
- **Limit per-hour:** Enter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

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

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

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

The 'Edit Incoming Limit' screen will be displayed.



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 you to configure the settings such that the Secure Email Gateway 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 Secure Email Gateway console by default.

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

Choose Language English Logout

Incoming Limits

General Settings Usage

Default Template Loaded

Enable System Admin e-mail notification for exceeded limits	<input type="checkbox"/>
Mail Subject	Sender Limits Notifica
Mail From	korumail@ip-172-31-
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>

Save Defaults

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

- Click 'Save' to apply your changes.

Viewing incoming mail usage details for domains and users

The 'Usage' tab in the 'Incoming Limits' screen allows you 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.

User				Domain			
Name	Time	Total(hourly)	Total(daily)	Name	Time	Total(hourly)	Total(daily)
test@testcustomer.com	2018-07-24 10:00:00.0	12	0	test@korumail.tk	2018-07-24 10:00:00.0	9	0
test@example.com	2018-07-24 10:00:00.0	7	0	test@example.com	2018-07-24 10:00:00.0	7	0
test@korumail.tk	2018-07-24 10:00:00.0	9	0	test@testcustomer.com	2018-07-24 10:00:00.0	12	0

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'.

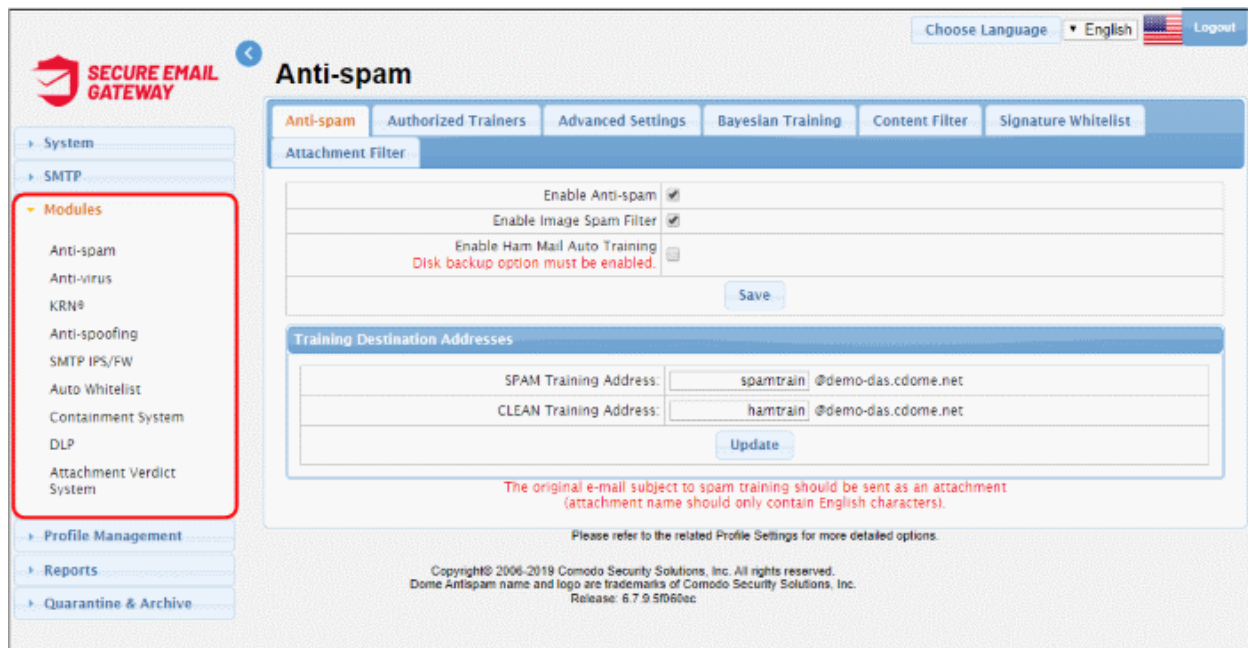
User				Domain			
Name	Time	Total(hourly)	Total(daily)	Name	Time	Total(hourly)	Total(daily)
exa	=	=	=	ko	=	=	=
test@example.com	2018-07-24 10:00:00.0	7	0	test@korumail.tk	2018-07-24 10:00:00.0	9	0

The intended recipient name will be displayed.

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

5 Modules

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



Click the following links for more details:

- [Anti-spam](#)
- [Anti-Virus](#)
- [Reputation Network \(KRN\)](#)
- [Anti-Spoofing](#)
- [SMTP IPS/FW](#)
- [Auto Whitelist](#)
- [Containment System](#)
- [Data Leak Prevention \(DLP\)](#)
- [Attachment Verdict System](#)

5.1 Anti-spam

- The anti-spam module lets you configure general and advanced settings, define authorized persons who can submit mail for spam training, upload material for Bayesian spam and HAM training, and add content filters.
- Secure Email Gateway uses our huge anti-spam database to accurately assign a spam-probability score to each message.
 - Depending on this score, the email is categorized as 'OK' (default = 40 points or below), 'Probable Spam' (default = 40-50 points), 'Spam' (default = 50-100 points) or 'Certainly Spam' (default = 100)

points and above).

- The anti-spam module must be enabled in order to activate the parameters in the profile settings. See **'Profile Management'** for more details about profile settings.
- Click 'Modules' > 'Anti-spam' to open the interface.

Choose Language English Logout

Anti-spam

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

Attachment Filter

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

Save

Training Destination Addresses

SPAM Training Address:	spamtrain @ip-172-31-25-154
CLEAN Training Address:	hamtrain @ip-172-31-25-154

Update

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

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

See the following sections for more details:

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

5.1.1 Anti-spam General Settings

- Click 'Modules' > 'Anti-spam' then the 'Anti-spam' tab
- From here, you can enable/disable the anti-spam engine, the image spam filter and the Ham trainer.
- The anti-spam module must be enabled in order to activate the anti-spam parameters specified in profile settings. See **'Profile Management'** for more details about profile settings.

Choose Language English Logout

Anti-spam

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

Attachment Filter

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

Training Destination Addresses

SPAM Training Address:	<input type="text" value="spamtrain @ip-172-31-25-154"/>
CLEAN Training Address:	<input type="text" value="hamtrain @ip-172-31-25-154"/>
Update	

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

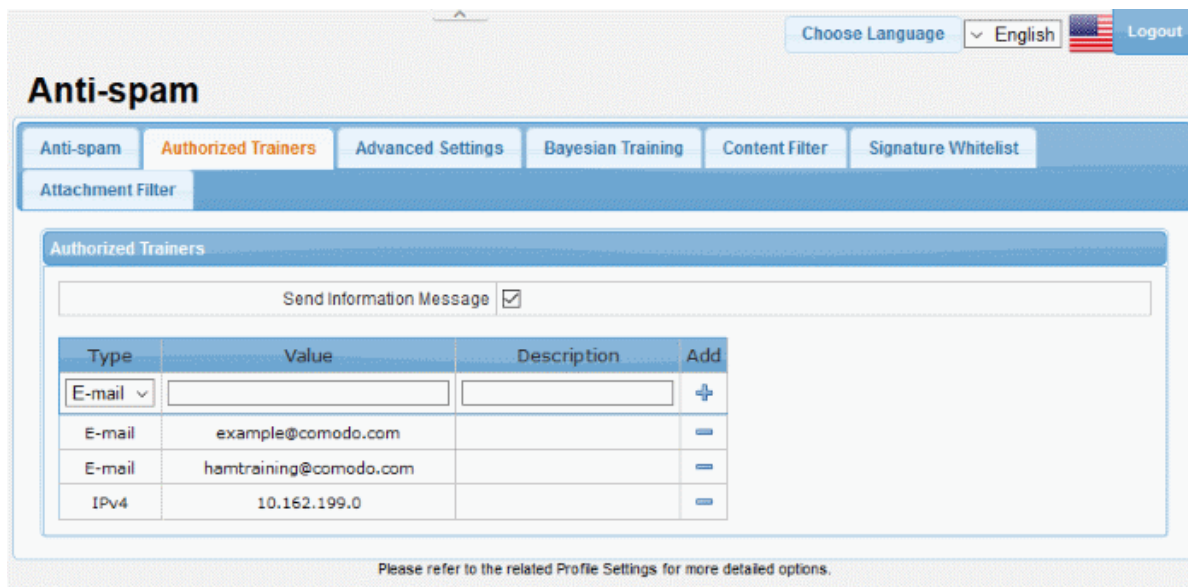
Please refer to the related Profile Settings for more detailed options.



Anti-spam General Settings - Table of Parameters	
Parameter	Description
Enable Anti-spam	<ul style="list-style-type: none"> 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. <p>See 'Profile Management' for more details about profile settings.</p>
Enable Image Spam Filter	<ul style="list-style-type: none"> Image based spam mails is when spam messages are embedded into images. This is designed to bypass text-based filters. Secure Email Gateway is capable of filtering image based emails also. Select this check box to activate the image spam filter.
Enable Ham Mail Auto Training	<ul style="list-style-type: none"> Ham is the opposite of spam. They are legitimate mails that you wish to allow. Secure Email Gateway can be trained to identify safe emails to accuracy/reduce false positives. Select this check box to activate the clean email training feature.
Training Destination Addresses	
SPAM Training Address	<ul style="list-style-type: none"> The address to which junk mail should be sent to train the engine. Enter the username part of the address. Mail you forward to this address will be analyzed by CSEG as an example of spam.
CLEAN Training Address	<ul style="list-style-type: none"> The address to which safe emails should be sent to train the engine. Enter the username part of the address. Mail you forward to this address will be analyzed by CSEG as an example of legitimate mail.

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

5.1.2 Authorized Trainers


- Click the 'Authorized Trainers' tab in the Anti-spam interface, to open the 'Authorized Trainers' screen
- Allows you to define the sources from which spam training emails can be sent.
- Submitting sample junk mail to Secure Email Gateway allows the system to learn, adapt and protect against new spam types.
- Training content will only be accepted from the sources you specify here.



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 you to add a source ID after filling the fields in the row
	 Allows you 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)**

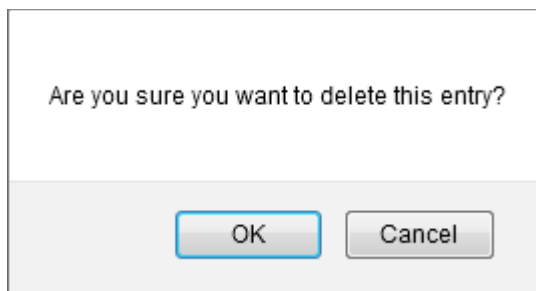
To add an authorized trainer

- 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

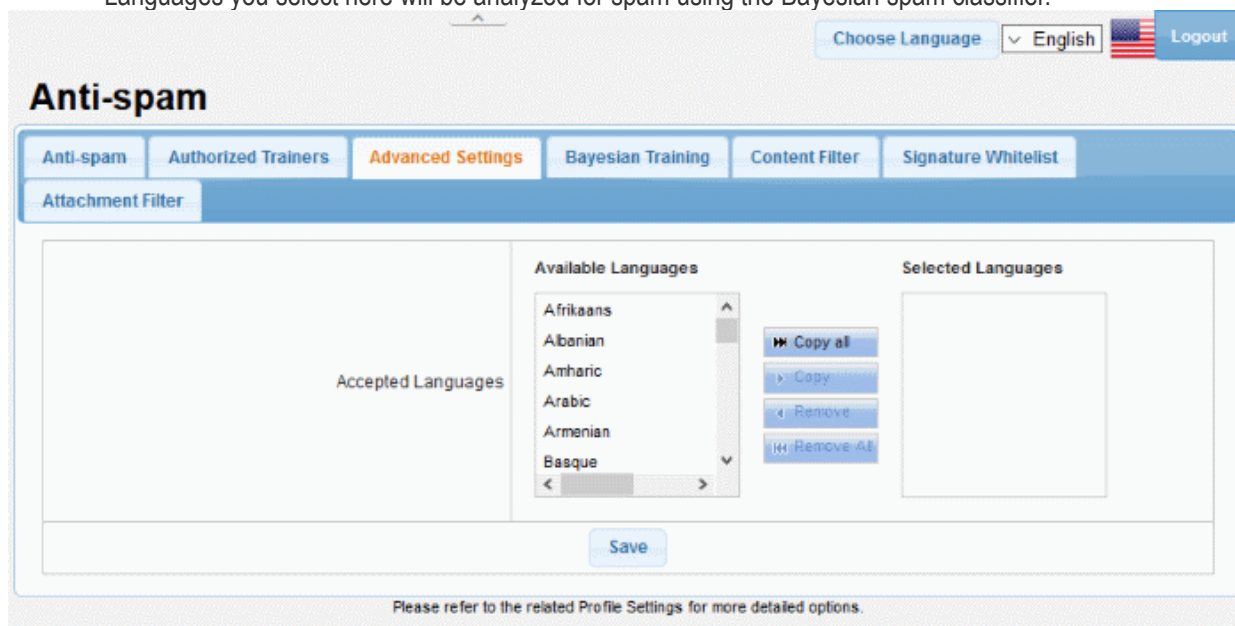
- Click the  button beside an entry that you want to remove.



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

5.1.3 Advanced Anti-spam Settings

- Click 'Modules' > 'Anti-spam' then the 'Advanced Settings' tab
- The 'Advanced Settings' screen lets you to configure language settings.
- Languages you select here will be analyzed for spam using the Bayesian spam classifier.



Accepted Languages:

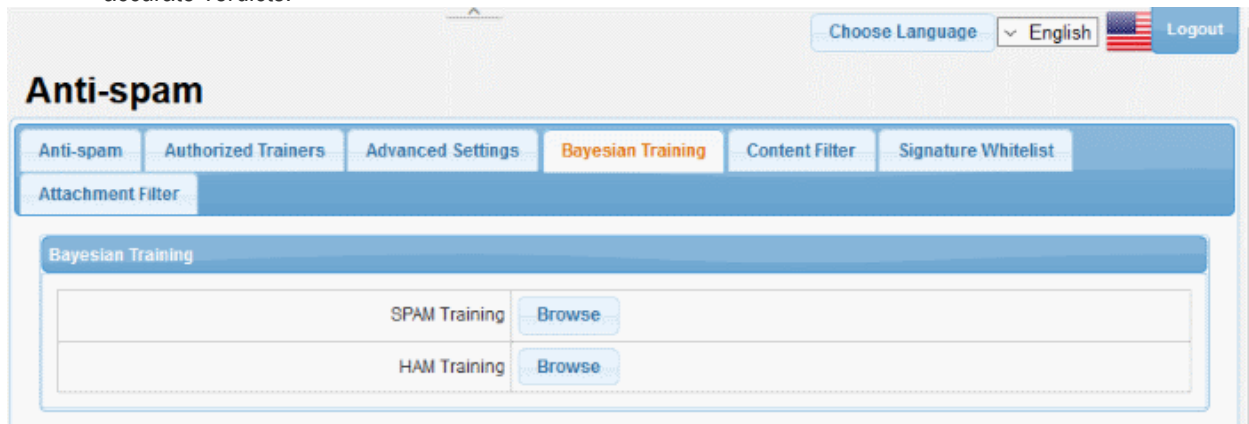
- The languages for which the Bayes spam engine should analyze the emails for spam.
- By default, a set of predefined languages is selected.
- To remove a language from the list, select it and click 'Remove All'.
- To move a language to the right side, select it and click 'Copy All'.

Click 'Save' to apply your changes.

5.1.4 Bayesian Training

- Click 'Modules' > 'Anti-spam' then the 'Bayesian Training' tab
- The Bayesian engine analyzes emails for patterns which may indicate that the mail is spam.

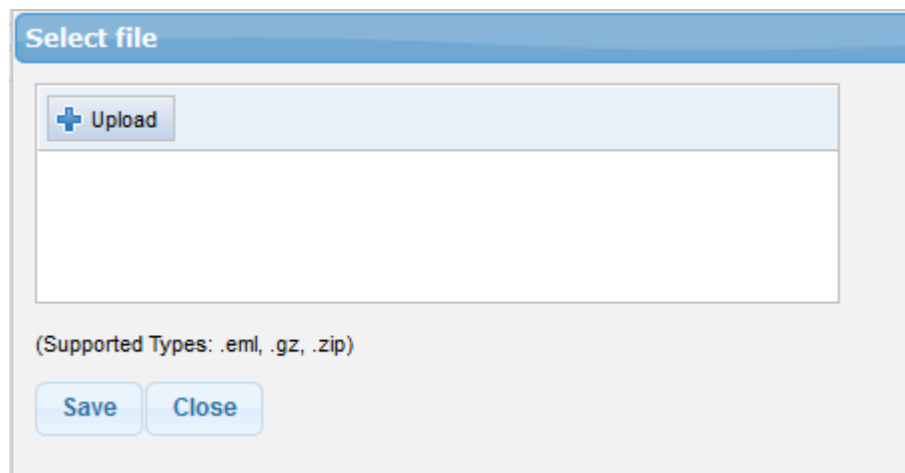
- You can upload sample spam and HAM (legitimate) emails in order to 'train' the engine to provide more accurate verdicts.



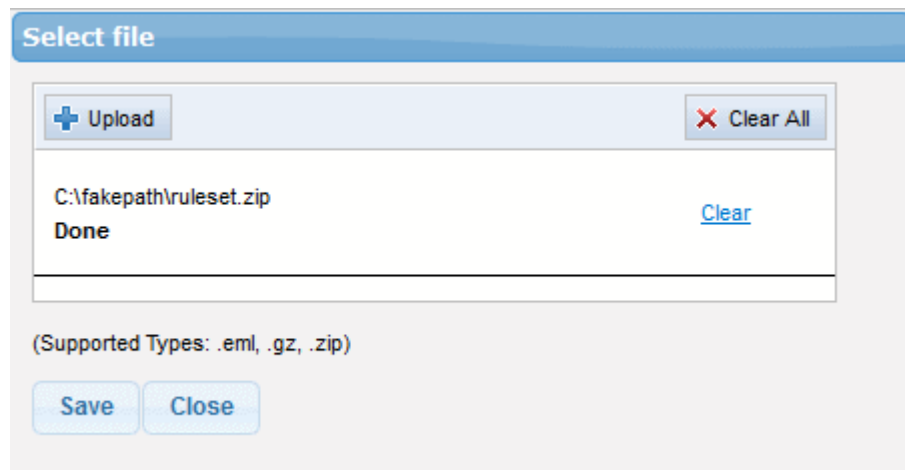
- **SPAM Training:** Allows to upload spam content to train the Bayesian spam engine
- **HAM Training:** Allows to upload safe content to train the Bayesian spam engine

To upload content

- Click 'Browse'



- Click 'Upload', 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

5.1.5 Content Filter

The content filter can detect words and patterns of words in an email then mark those messages as spam.

- Click 'Modules' > 'Anti-spam' then the 'Content Filter' tab:



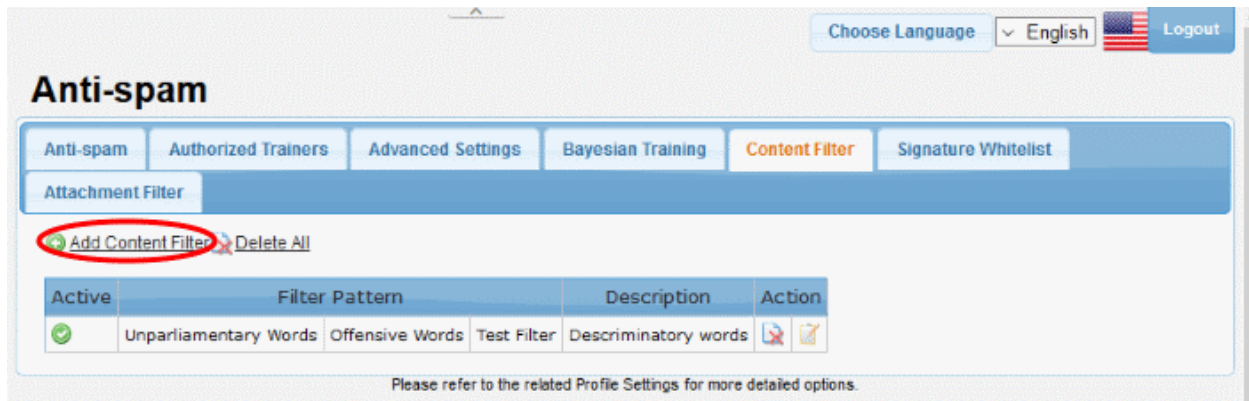
Content Filter - Table of Column Descriptions	
Column Header	Description
Active	Shows whether the content filter is enabled or disabled
Filter Pattern	The content type which will be detected.
Action	Delete the filter
	Edit the filter

The interface allows administrators to:

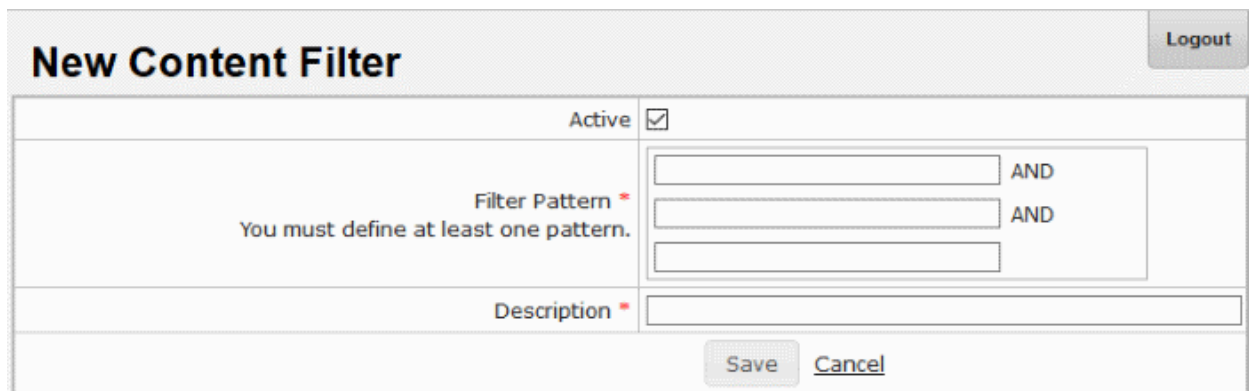
- **Add a new content filter**
- **Edit a content filter**
- **Delete a content filter**

To add a new content filter

- Click the 'Add Content Filter' link at the top.



The 'New Content Filter' screen will be displayed.

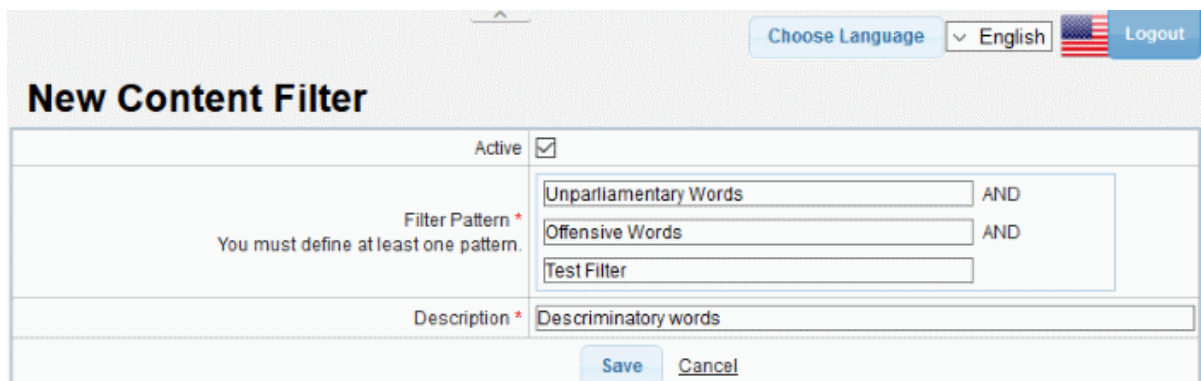


- **Active:** Select the check box to enable the content filter
- **Filter Pattern:** Enter the words or combination of words that should be checked and mark the email as spam.
- **Description:** Enter an appropriate name for the content filter

Click 'Save'. 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.

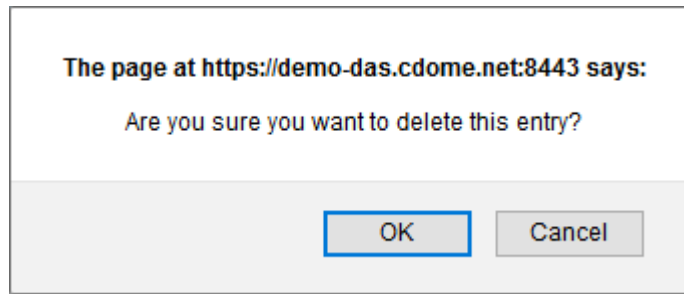


The 'Edit Content Filter' screen will be displayed.

- Edit the content filter as required and click 'Save'

To delete a content filter

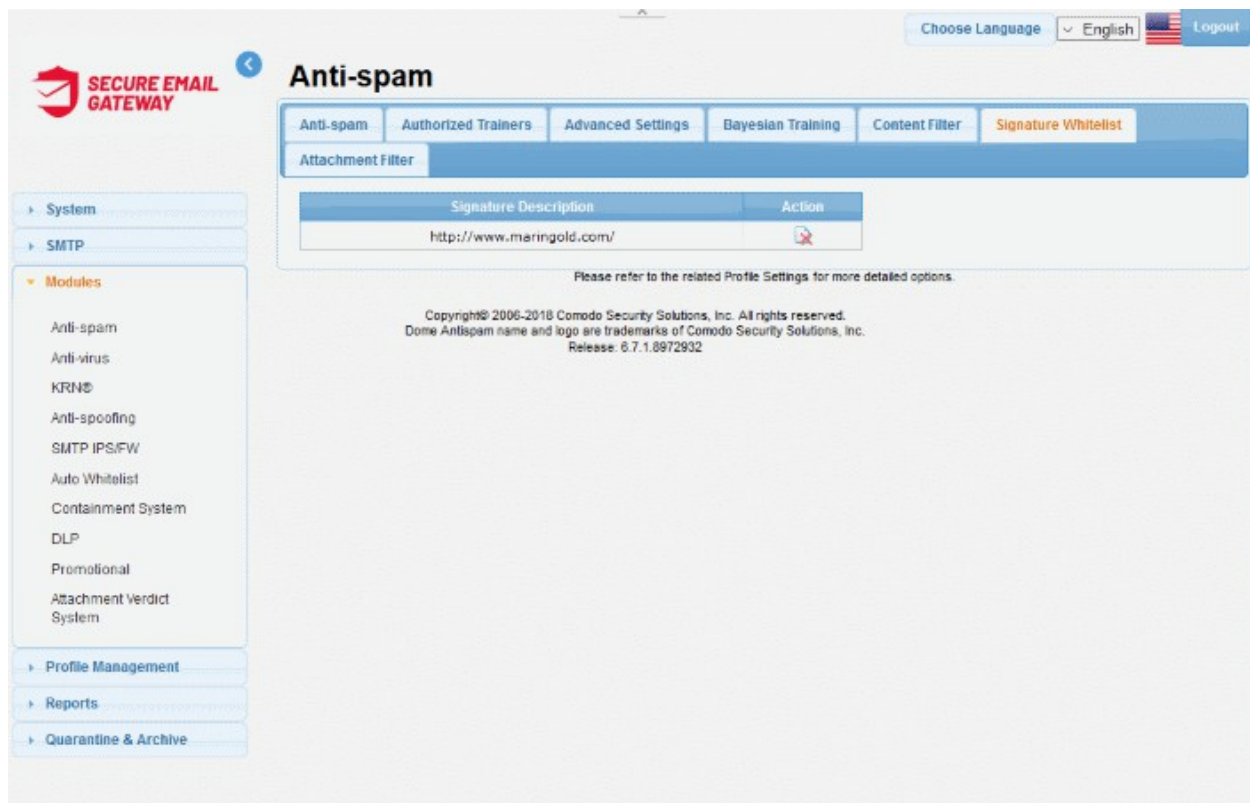
- Click the  button beside a filter that you want to remove



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

5.1.6 Signature Whitelist

- Click 'Modules' > 'Anti-spam' then click the 'Signature Whitelist' tab.
- SEG uses a blacklist of spam signatures to detect junk mail and spam.
- SEG will block messages that have a signature which matches a signature on the blacklist.
- If don't want this system to apply to a specific email address or domain, then you can add the signature to the whitelist.
- Mails with whitelisted signatures will be allowed through.
- You need to go into the mail logs interface to add signatures to the whitelist.



To whitelist emails in 'Mail Logs':

- Click 'Mail Logs' from reports menu.

Subject	Result	Received	Sender	Recipient(s)	IP	Details
	RELAY ERR	25/07/2018 03:03:51	spamer@tiscali.it	spamer@tiscali.it	204.188.203.187	Relay error: Recipient domain is not in the managed domains or Missing SMTP AUTH configuration
	RELAY ERR	25/07/2018 02:50:18	spamer@tiscali.it	spamer@tiscali.it	89.197.1.54	Relay error: Recipient domain is not in the managed domains or Missing SMTP AUTH configuration
	RELAY ERR	24/07/2018 22:27:14	spamer@tiscali.it	spamer@tiscali.it	192.110.157.9	Relay error: Recipient domain is not in the managed domains or Missing SMTP AUTH configuration
[!] PROBABLE SPAM]Incoming Li	PSPAM	24/07/2018 10:57:12	test@korumail.tk	test@bestcustomer.com	213.14.70.194	Classified as probable spam Score: 45.0
[!] PROBABLE SPAM]Incoming Li	PSPAM	24/07/2018 10:57:10	test@korumail.tk	test@bestcustomer.com	213.14.70.194	Classified as probable spam Score: 45.0
[!] PROBABLE SPAM]Incoming Li	PSPAM	24/07/2018 10:57:09	test@korumail.tk	test@bestcustomer.com	213.14.70.194	Classified as probable spam Score: 45.0
[!] PROBABLE SPAM]Incoming Li	PSPAM	24/07/2018 10:57:07	test@korumail.tk	test@bestcustomer.com	213.14.70.194	Classified as probable spam Score: 45.0
[!] PROBABLE SPAM]Incoming Li	PSPAM	24/07/2018 10:57:05	test@korumail.tk	test@bestcustomer.com	213.14.70.194	Classified as probable spam Score: 45.0
[!] PROBABLE SPAM]Incoming Li	PSPAM	24/07/2018 10:57:03	test@korumail.tk	test@bestcustomer.com	213.14.70.194	Classified as probable spam Score: 45.0
[!] PROBABLE SPAM]Incoming Li	PSPAM	24/07/2018 10:57:02	test@korumail.tk	test@bestcustomer.com	213.14.70.194	Classified as probable spam Score: 45.0
[!] PROBABLE SPAM]Incoming Li	PSPAM	24/07/2018 10:57:02	test@korumail.tk	test@bestcustomer.com	213.14.70.194	Classified as probable spam Score: 45.0
[!] PROBABLE SPAM]Incoming Li	PSPAM	24/07/2018 10:57:00	test@korumail.tk	test@bestcustomer.com	213.14.70.194	Classified as probable spam Score: 45.0
[!] PROBABLE SPAM]Incoming Li	PSPAM	24/07/2018 10:56:57	test@korumail.tk	test@bestcustomer.com	213.14.70.194	Classified as probable spam Score: 45.0
[!] PROBABLE SPAM]Incoming Li	PSPAM	24/07/2018 10:56:27	test@bestcustomer.com	test@korumail.tk	213.14.70.194	Classified as probable spam Score: 45.0
Incoming Limit	OK	24/07/2018 10:56:24	test@bestcustomer.com	test@korumail.tk	213.14.70.194	
Incoming Limit	OK	24/07/2018 10:56:23	test@bestcustomer.com	test@korumail.tk	213.14.70.194	
Incoming Limit	OK	24/07/2018 10:56:21	test@bestcustomer.com	test@korumail.tk	213.14.70.194	
Incoming Limit	OK	24/07/2018 10:56:18	test@bestcustomer.com	test@korumail.tk	213.14.70.194	
Incoming Limit	OK	24/07/2018 10:56:15	test@bestcustomer.com	test@korumail.tk	213.14.70.194	
Incoming Limit	OK	24/07/2018 10:54:55	test@bestcustomer.com	test@example.com	213.14.70.194	
Incoming Limit	OK	24/07/2018 10:54:49	test@bestcustomer.com	test@example.com	213.14.70.194	
Incoming Limit	OK	24/07/2018 10:54:48	test@bestcustomer.com	test@example.com	213.14.70.194	
Incoming Limit	OK	24/07/2018 10:54:46	test@bestcustomer.com	test@example.com	213.14.70.194	
Incoming Limit	OK	24/07/2018 10:54:44	test@bestcustomer.com	test@example.com	213.14.70.194	
Incoming Limit	OK	24/07/2018 10:54:42	test@bestcustomer.com	test@example.com	213.14.70.194	
[!] PROBABLE SPAM]Incoming Li	PSPAM	24/07/2018 10:53:22	test@example.com	test@bestcustomer.com	213.14.70.194	Classified as probable spam Score: 45.0

- Click the 'Advanced search' link.
- Select 'Result' from the first drop down.
- Select 'EQUALS' from the second drop down and then choose 'CERTAINLY SPAM'.

Received	25/07/2018 02:50:18
Queue ID	19759-1532487018-533437
Message ID	
Action	
Result	RELAY ERROR
Score	0.0
Sender	spamer@tiscali.it Add Email in Black List
Recipient(s)	spamer@tiscali.it
RFC2822 Sender	
RFC2822 Recipient(s)	
Subject	
IP	89.197.1.54 Add Black List
Location	London, England, United Kingdom
Size	0
Matched Profile	Default Incoming Profile (defined by user: admin)
Details	Relay error: Recipient domain is not in the managed domains or Missing SMTP AUTH configuration
Relayed	No

[Close](#)

- Select 'Add email to Whitelist' in sender field and 'Add Whitelist' in IP field. Next, choose the email that you need to whitelist and click the 'Add White Signature Lists' link.

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

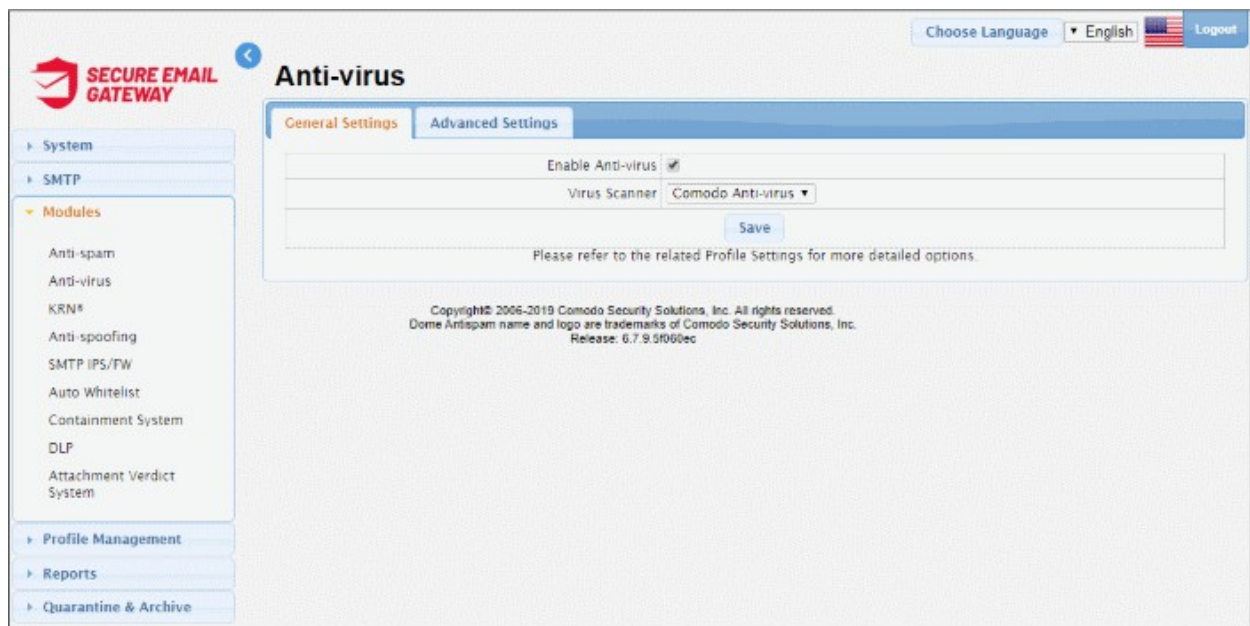
5.1.7 Attachment Filter

- Click 'Modules' > 'Anti-spam' > 'Attachment Filter' tab.
- This area lets you define how many archive levels should be checked by Secure Email Gateway.
 - For example, a zip file may contain another zip file inside it. A depth of '2' means Secure Email Gateway will check inside both files. However, if the 2nd zip contains another zip inside it, then Secure Email Gateway will block the entire attachment.

- **Maximum depth for archive files for attachment analysis:** Max. archive levels that will be analyzed. Enter the maximum number of nested archives which should be opened and examined for data-leak infringements. If an archive contains more sub-archives than this threshold then the entire attachment will be blocked.
- Click 'Save' to apply your choice.

5.2 Anti-Virus

- Click 'Modules' > 'Anti-virus' to open this interface
- Secure Email Gateway is capable of virus scanning all emails that pass through its engine. Comodo Antivirus is built into the system.
- The antivirus module must be enabled to activate the antivirus settings in a profile. See '**Profile Management**' for more details about profile settings.

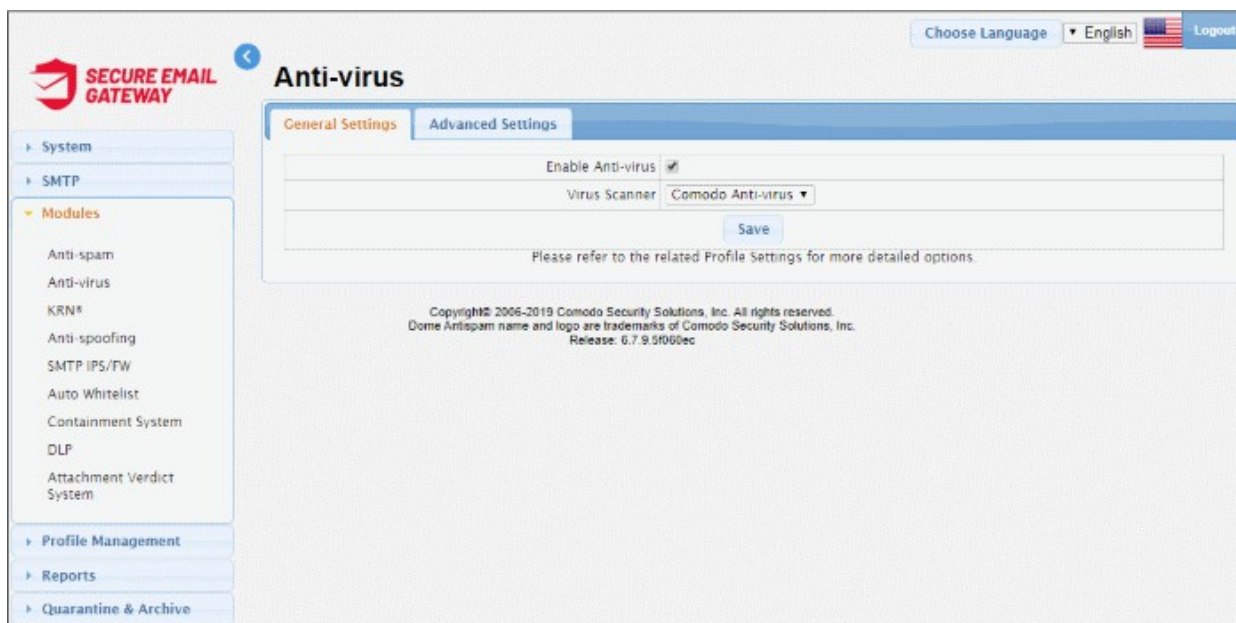


See the following sections for more details:

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

5.2.1 Anti-Virus General Settings

- Click 'Modules' > 'Anti-virus' > 'General Settings' to open this interface
- General settings let you enable/disable the AV module and select which AV engine you wish to use.
- The antivirus module must be enabled to activate the AV parameters in profile settings. See '[Profile Management](#)' for more details about profile settings.
- Click 'Antivirus' > 'General Settings' to open this interface.



Anti-virus General Settings - Table of Parameters

Parameter	Description
Enable Anti-virus	<ul style="list-style-type: none"> Select this to activate the anti-virus scanning engine. The anti-virus parameters specified in the profile settings will be activated only if this setting is enabled here. See 'Profile Management' for more details about profile settings.
Virus Scanner	<ul style="list-style-type: none"> Select the AV program from the drop-down that should be used for scanning the emails. The AV program available for selection is Comodo AV.

- Click 'Save' to apply your changes.

5.2.2 Advanced Anti-Virus Settings

- Click 'Modules' > 'Anti-virus' > 'Advanced Settings' to open this interface
- The 'Advanced Settings' screen lets you configure granular settings like the the max size of email+attachments that should be scanned.
- Please note that if the maximum size is surpassed then the antivirus filter for the particular email will not be applied.

Choose Language English Logout

Anti-virus

General Settings
Advanced Settings

Max Mail Size *	<input type="text" value="25"/> MB
Max Threads Number *	<input type="text" value="10"/>
Time Out *	<input type="text" value="120"/>
Max Directory Recursion *	<input type="text" value="15"/>
Max Files *	<input type="text" value="10000"/>
Max Scan Size *	<input type="text" value="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"/>
Phishing Action	Discard ▾
Quarantine phishing Mails	<input type="checkbox"/>
Scan Archive Files	<input checked="" type="checkbox"/>

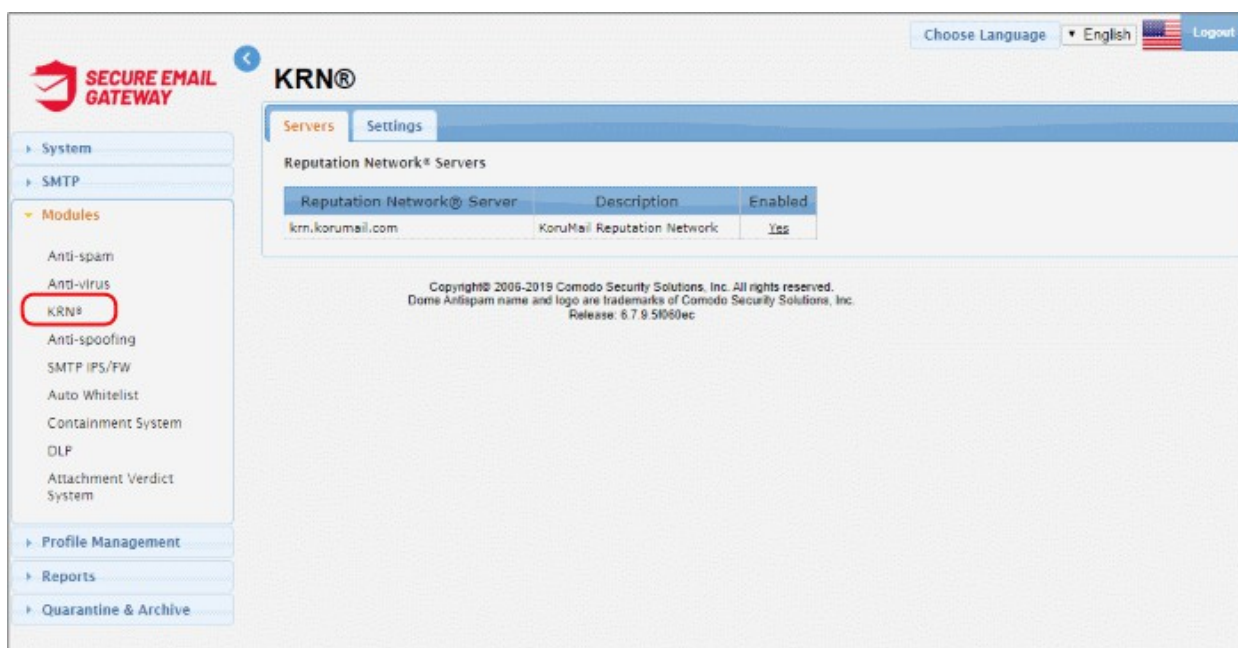
Save Default Cancel

Anti-virus Advanced Settings - Table of Parameters	
Parameter	Description
Max Mail Size	The maximum email size (message + attachments) 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 email signature
Enable Phishing URL checks	If enabled, AV scanner checks for emails that originated from phishing URLs
Phishing Action	You can reject or accept invalid recipients.
Quarantine Phishing Mails	If enabled, the AV scanner will place phishing emails in quarantine. Quarantined mails can be accessed by users through the webmail interface.
Scan Archive Files	If enabled, archived mails will also be scanned. The types of mail that should be archived and their related settings are configured in profile settings. See ' Profile Management ' for more details about profile settings.

- Click 'Save' to apply your changes.
- To restore the default 'Anti-virus Advanced Settings' value, click the 'Default' button.

5.3 Korumail Reputation Network (KRN)

- Click 'Modules' > 'KRN®' to open this interface
- Korumail reputation network is an IP scoring system developed by Comodo. The system helps Secure Email Gateway accurately classify mail sent from IP addresses in the network.
- It not only includes traditional features such as real-time IP blacklists (**RBL**), but also has 'whitelist' and 'greylisting' features.



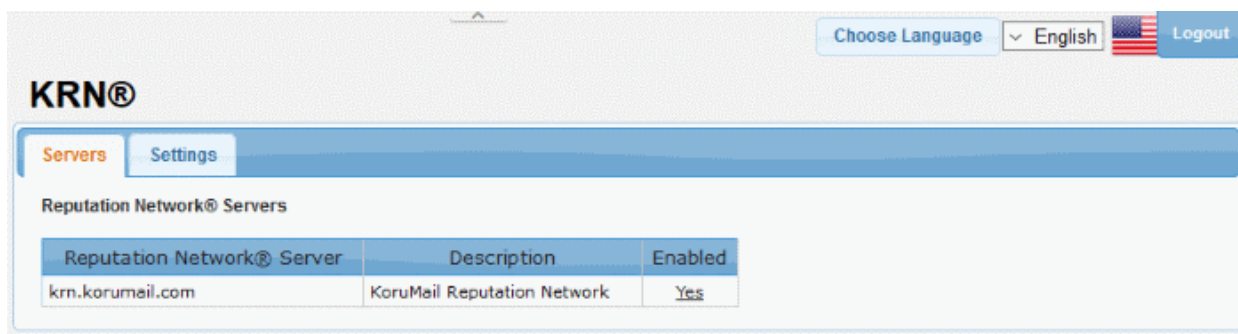
The interface allows admins to:

- **Enable / disable a KRN server**
- **Configure KRN settings**

To enable / disable a KRN server

A newly added KRN server will be enabled by default.

- To switch a KRN server between enabled and disabled statuses, click the 'Yes' or 'No' link under the 'Enabled' column.



KRN Settings

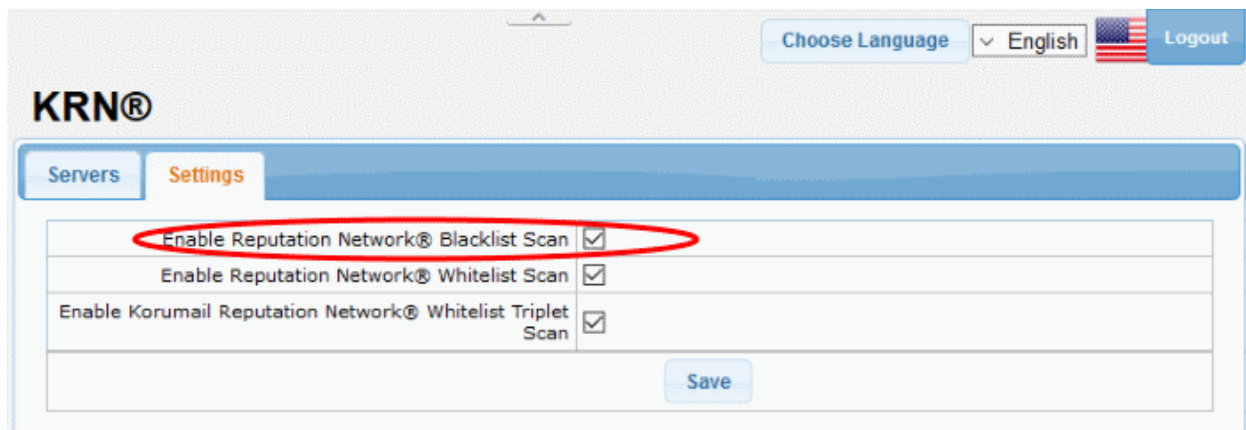
- The settings interface lets you enable/disable KRN blacklist and whitelist scans.
- These scans must be enabled if you wish to take advantage of the KRN features in profile settings.
- See '**Profile Management**' for more details about profile settings.

The 'Settings' tab in KRN module allows you to:

- **Enable / disable KRN blacklist scan**
- **Enable / disable KRN whitelist scan**

To enable / disable DARN blacklist scan

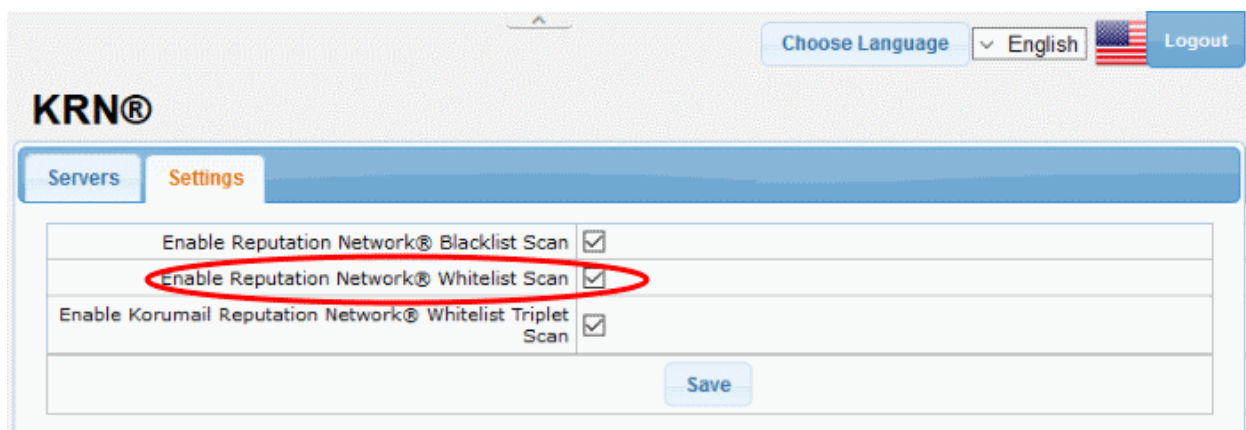
- Click the 'Settings' tab in the KRN® interface



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

To enable / disable KRN whitelist scan

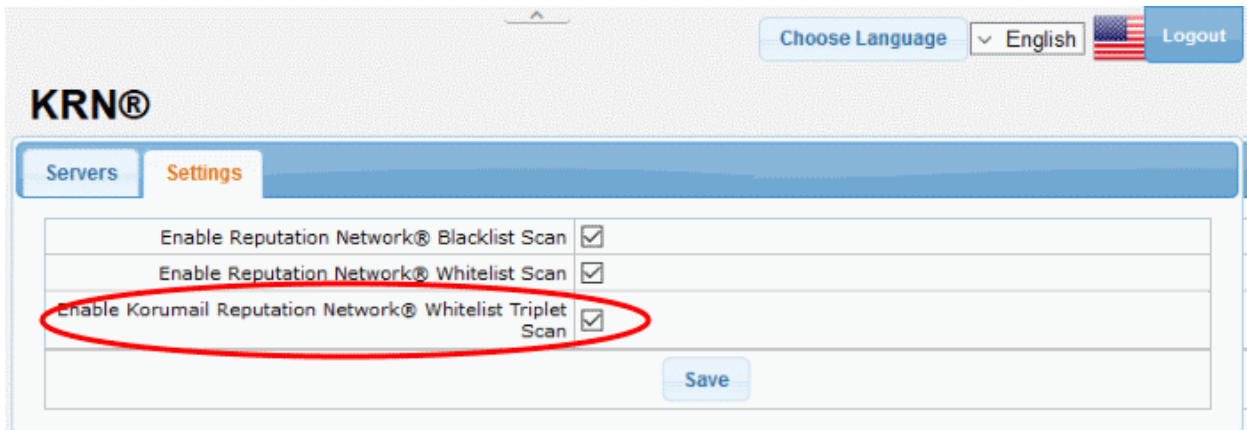
- Click the 'Settings' tab in the KRN® interface



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

To enable / disable KRN whitelist Triplet scan

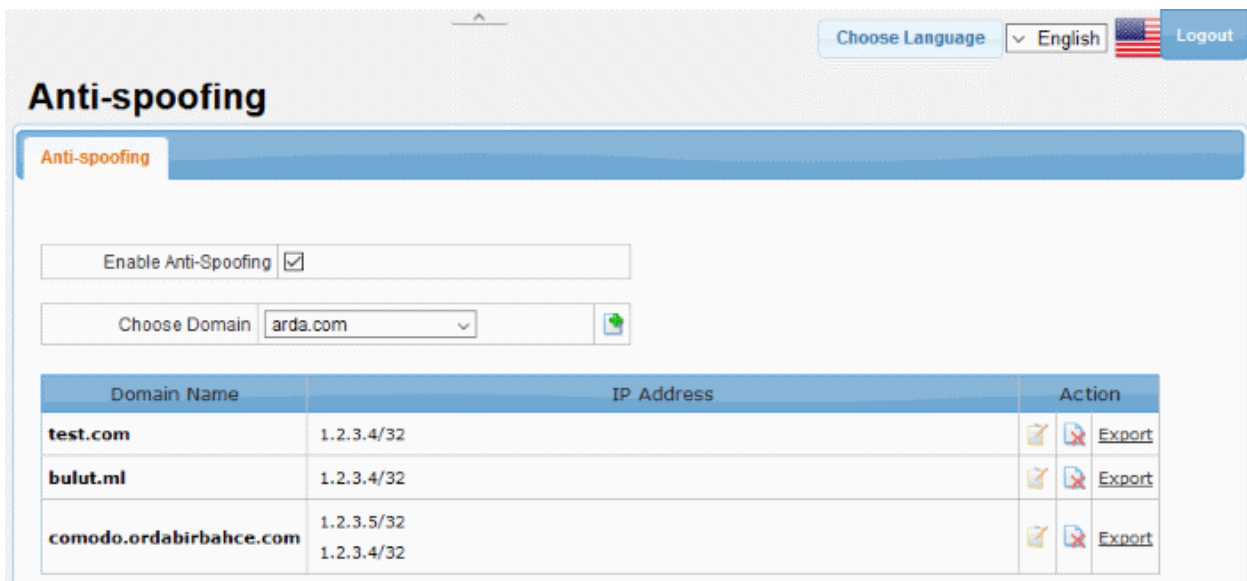
- Click the 'Settings' tab in the KRN® interface
- Secure Email Gateway can scan the sender address, domain and IP tuple address list by enabling this option





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

5.4 Anti-Spoofing

- Click the 'Modules' tab on the left, then click 'Anti-spoofing', to open the 'Anti-spoofing' interface
- 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 Secure Email Gateway 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.
- Secure Email Gateway 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.



- Select the 'Enable Anti-Spoofing' check box to add IP addresses for your domains.

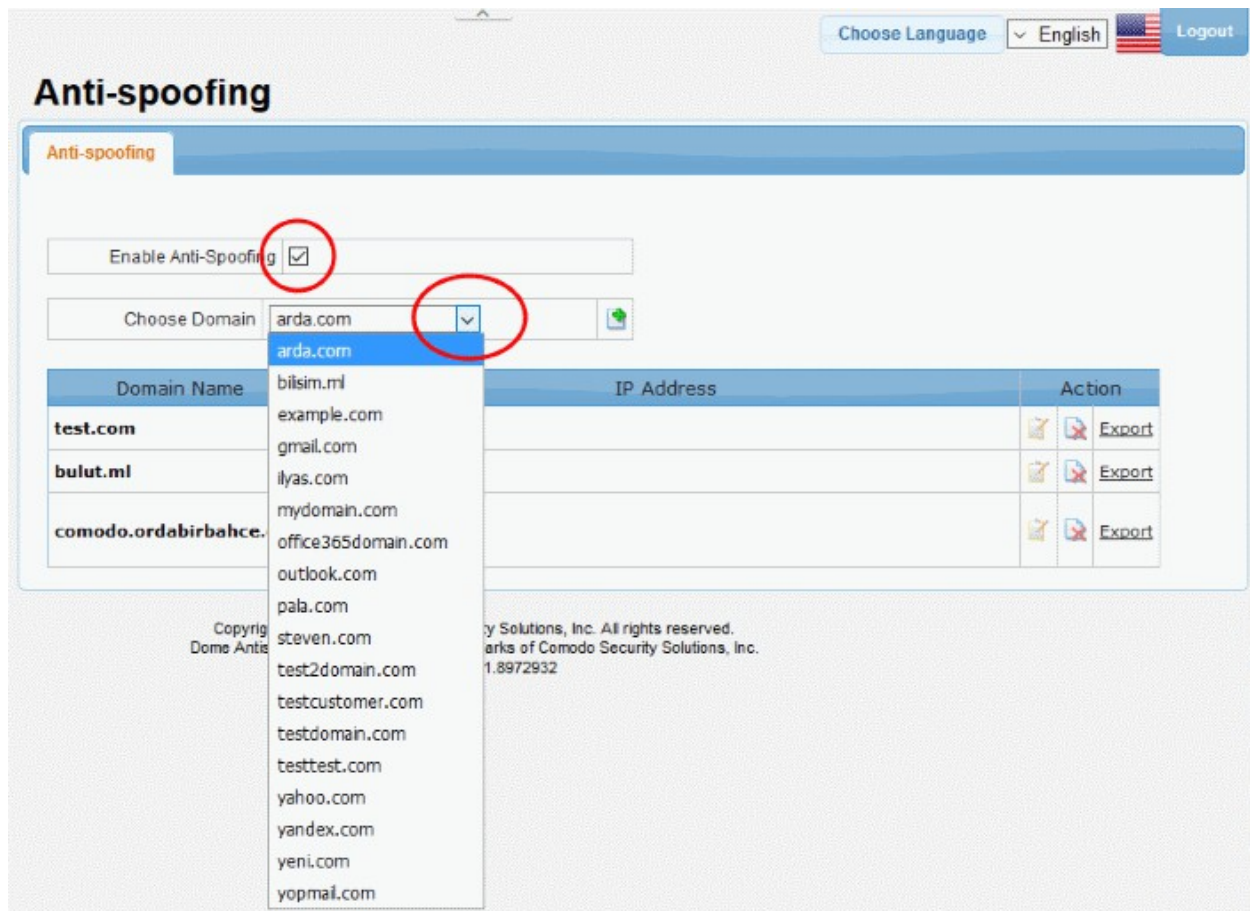
Anti-Spoofing - Table of Column Descriptions	
Column Header	Description
Domain Name	Displays the name of the protected domain
IP Address	Displays IP range added for the domain
Action	 Delete the selected domain
	 Edit the domain IP address
	Export Allows to export the IP address for a domain


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**

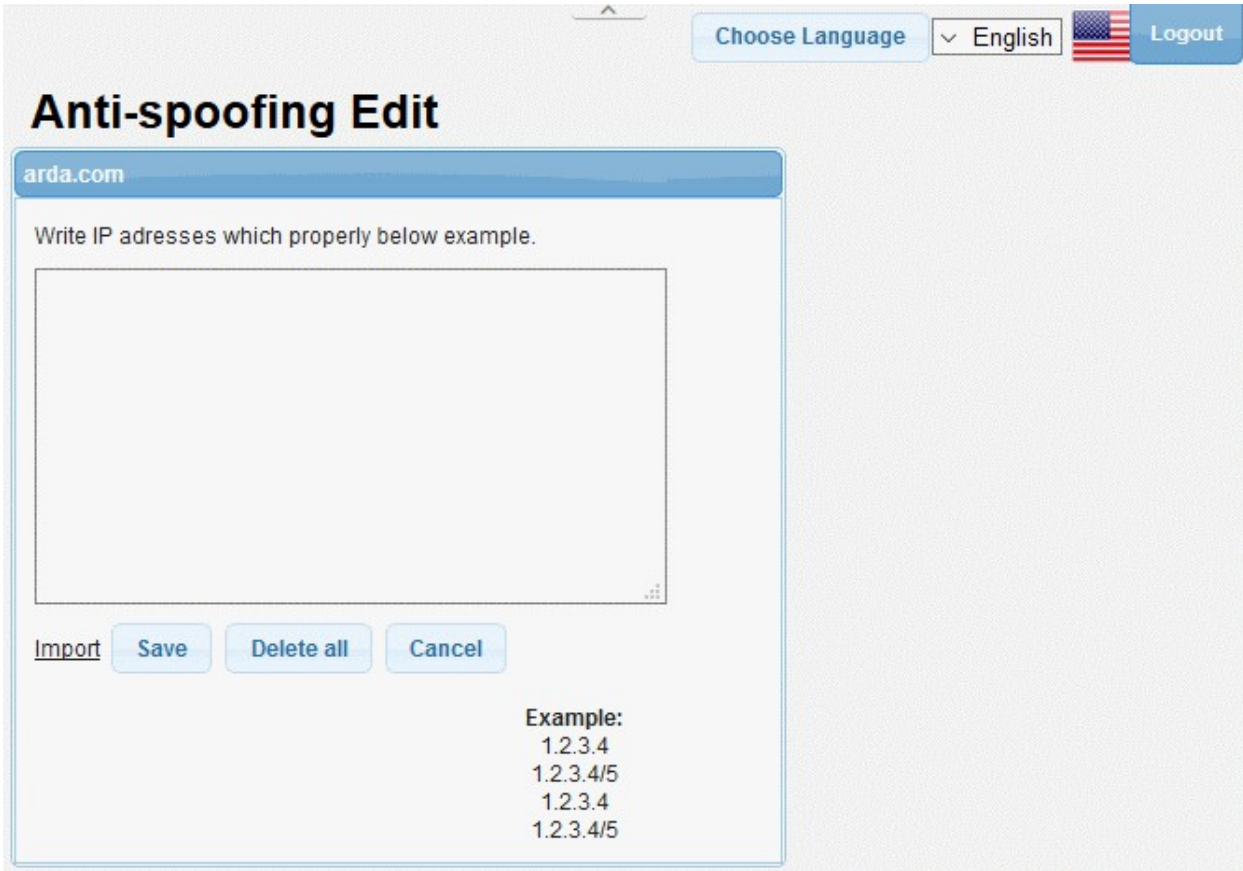
To add an IP range for a domain

- Select the 'Enable Anti-Spoofing' option
- Select the domain for which you want to add the IP range



- Click the  button

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



Choose Language English Logout

Anti-spoofing Edit

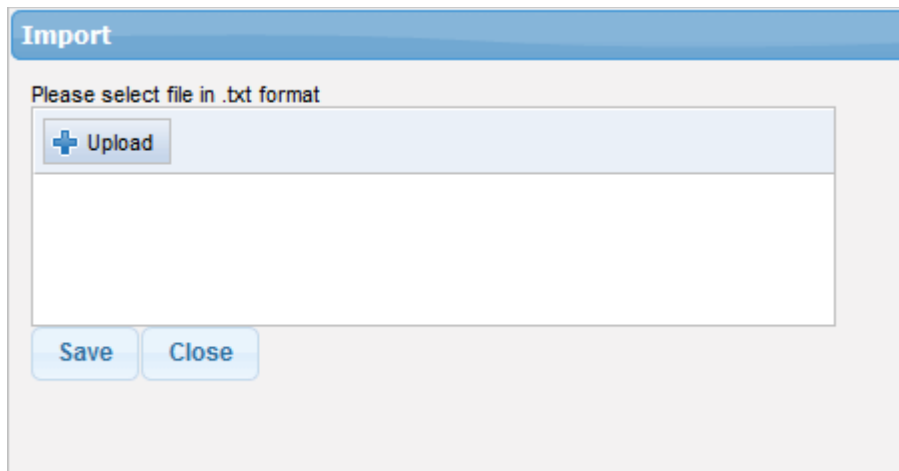
arda.com

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



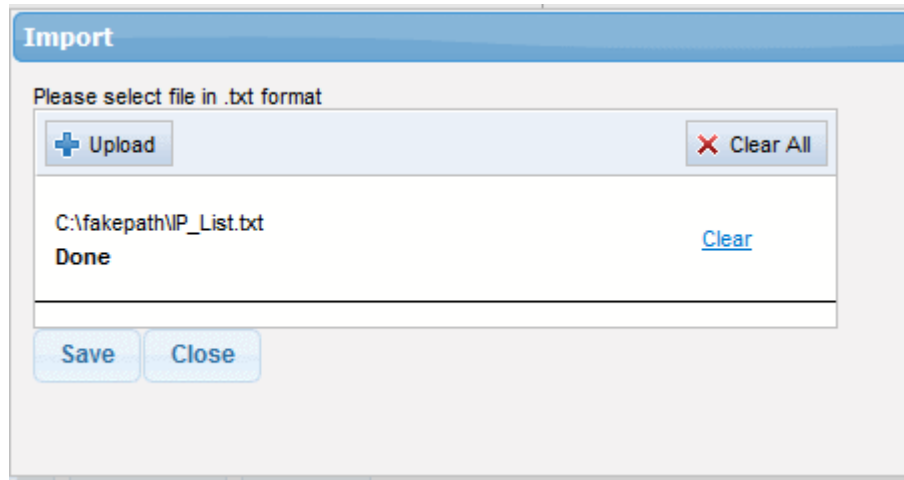
Import

Please select file in .txt format

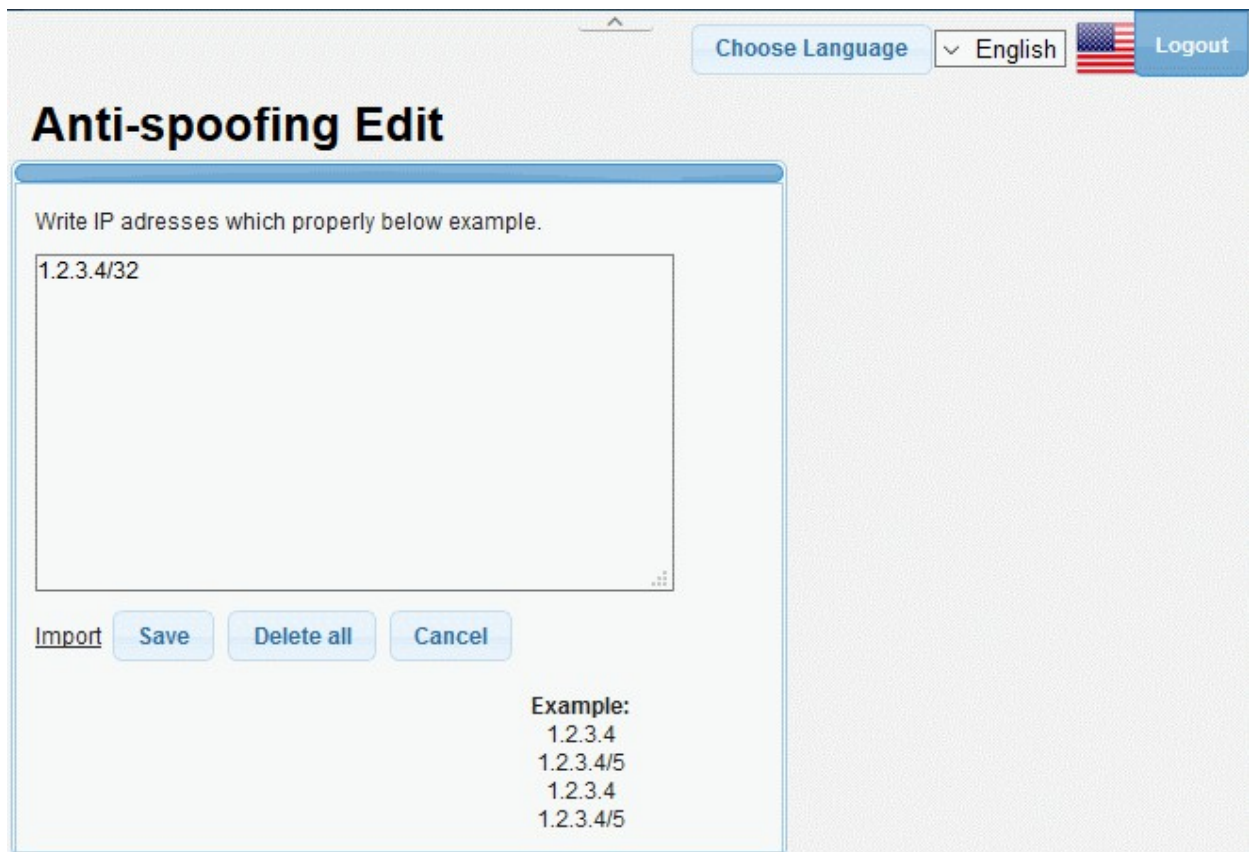
[+ Upload](#)

Save Close

- Click 'Upload', 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 'Clear All' at the top.
- Click 'Save'



- 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.

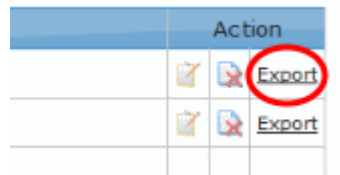
- Edit the address as required and click the 'Save' button.

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



- The SPF IP list will be downloaded as a text file to your system.

5.5 SMTP IPS/FW

- Click the 'Modules' tab > 'SMTP IPS/FW'.
- Secure Email Gateway's SMTP Intrusion Prevention System (IPS) and Firewall (FW) module provide protection against Denial of Service (DoS) and SYN attacks.
- SYN attacks are dealt with using SYN Cookies and SYN Cache features.
- DoS attacks are blocked by deploying various usage limitations.
- For example, Secure Email Gateway can limit the number of connections it accepts in a certain time-period. The IPS/FW module will block IPs that want make more connections more than the limit. You can specify the limit in a security profile.
- The module also lets you create whitelist and block rules to better control spam. The rate control feature, a subset of the DoS protection system, allows you to control how many connections are allowed within the specified time from the same IP address.

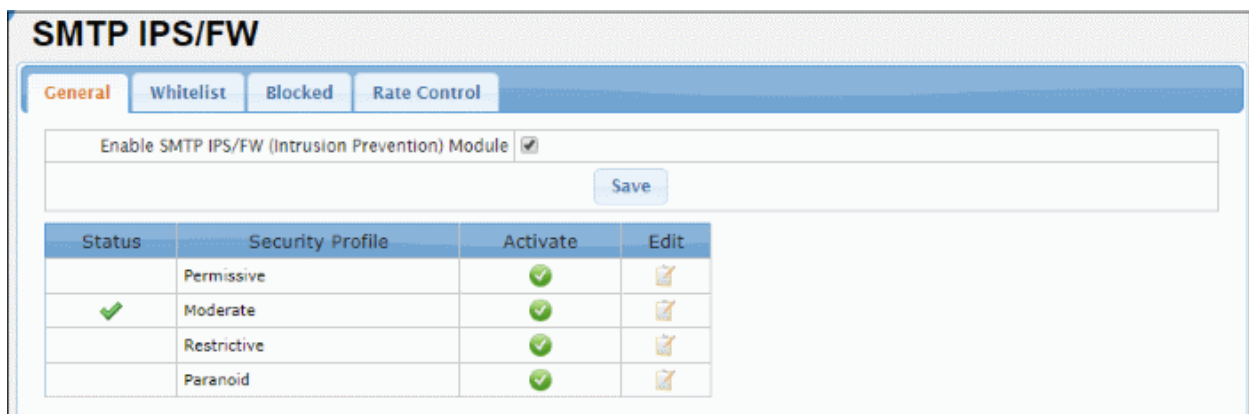


See the following sections for more details.

- **SMTP IPS General Settings**
- **Whitelist IP Addresses**
- **Blocked IP Addresses**
- **Rate Control**

5.5.1 SMTP IPS General Settings


- Click Modules > 'SMTP IPS/FW' > 'General' tab in the 'SMTP IPS/FW' screen.
- Enable/disable the intrusion prevention system (IPS) and configure a security profile for Secure Email Gateway.
- The IPS allows Secure Email Gateway to control the number of SMTP connections from any single IP address.
- This helps to detect and block spam/denial-of-service attacks and aids traffic management.



- SMTP IPS/FW (Intrusion Prevention) Module: Activate the module. The relevant settings specified in the security profile will now be applied.

The module has a set of predefined security profiles with different 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 active.
Security Profile	<ul style="list-style-type: none"> The profile determines how strict Secure Email Gateway should be regarding simultaneous connections from the same IP address. Click the 'Edit' button to see the specific details of each profile. You are free to edit a profile as you wish.
Activate	Enable the profile. Please note that only one security profile can be active at a time.
Edit	 Modify the settings of the profile.

The interface allows you 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.

Edit IPS profile

Logout

Security profile	Permissive
Number of connections threshold to return SMTP 451 message	<input style="width: 50px;" type="text" value="10"/>
Number of connections threshold to block remote IP	<input style="width: 50px;" type="text" value="100"/>
Limit simultaneous connections	<input type="checkbox"/>
Maximum number of simultaneous sessions from a single IP address	<input style="width: 50px;" type="text" value="0"/>
Limit the rate of new SMTP connections	<input type="checkbox"/>
New SMTP connection interval (seconds)	<input style="width: 50px;" type="text" value="0"/>
New SMTP connection rate per interval	<input style="width: 50px;" type="text" value="0"/>

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"> Max. connections before Secure Email Gateway will refuse further connections and send 451 errors messages to the sender. If you wish to unblock this sender, please contact domesupport@comodo.com to whitelist or unblock the IP.
Number of connections threshold to block remote IP	Max. connections before Secure Email Gateway firewall blocks the source IP address.
Limit simultaneous connections	Enable controls on the number of simultaneous connections. See settings below.
Maximum number of simultaneous sessions from a single IP address	Maximum number of sessions that can be opened by a single IP address after limiting instant SMTP connections.
Limit the rate of new SMTP connections	If enabled, the parameters 'New SMTP connection interval' and 'New SMTP connection rate' can be specified to set limitations on new SMTP connections.
New SMTP connection interval (seconds)	The time between a new connection and the previous connection.
New SMTP connection rate per interval	Maximum number of new SMTP connections in specified interval.

- Click 'Save' to apply your changes.
- Click the 'Restore Defaults' button to restore the parameters to factory setting.

5.5.2 Whitelist IP Addresses

- Click Modules > 'Whitelist' tab in the SMTP IPS/FW module.
- Whitelisted IP addresses will not be filtered by the SMTP IPS module.

[Choose Language](#) | English [Logout](#)



SMTP IPS/FW

General | Whitelist | Blocked | Rate Control

Successfully Saved.

IP or Network Address	Description	Action
<input type="text"/>	<input type="text"/>	
100.12.125.15	test	
10.51.108.202/32	Example whitelist IP	


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

Whitelist Settings - Table of Column Descriptions	
Column Header	Description
IP or Network Address	The details of endpoint IP/networked addresses that are whitelisted.
Description	The description provided for the IP/Network address.
Action	 Allows you to add a Network or IP address after entering the details in the row.
	 Allows you 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.

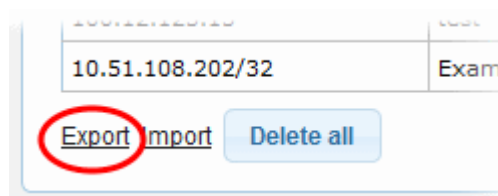
The address will be added and listed as whitelisted.

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 'Delete all' 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

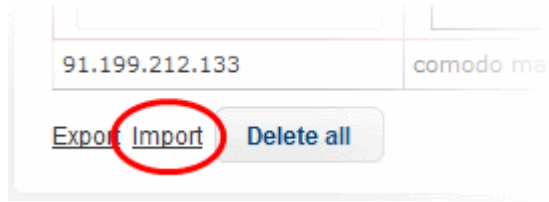
- Click the 'Export' link at the bottom of the screen



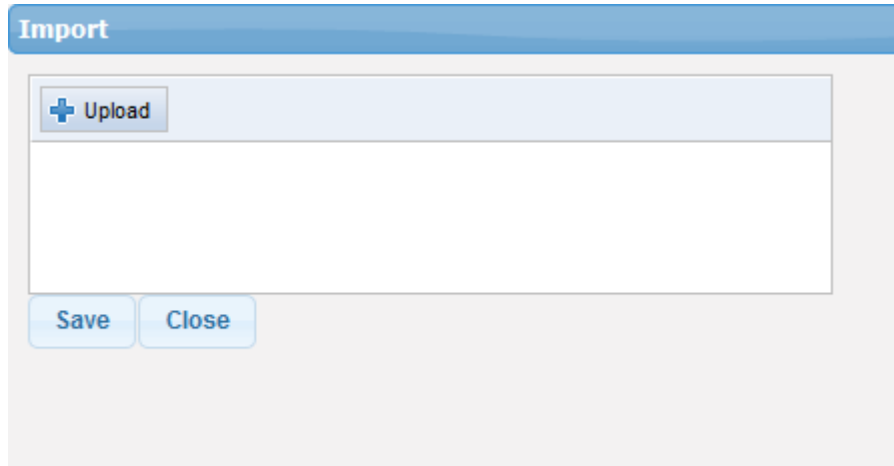
- The list will be exported in .txt format.

To import lists of whitelisted network or IP addresses from files

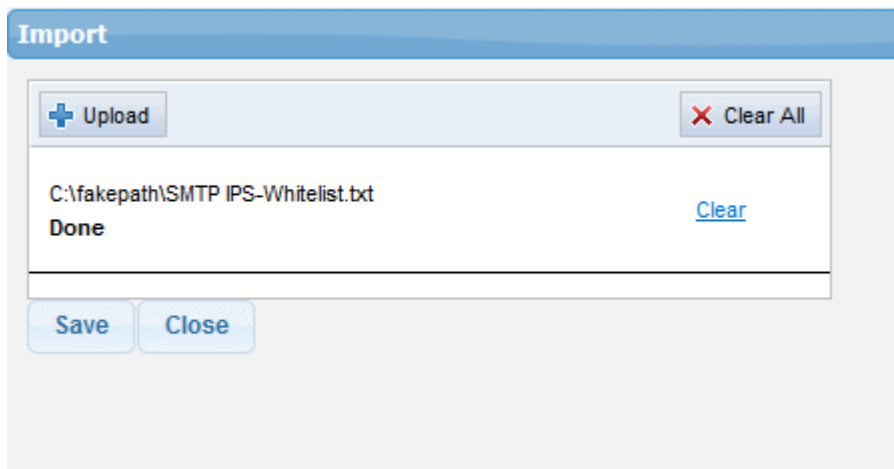
- Click the 'Import' link at the bottom of the screen



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



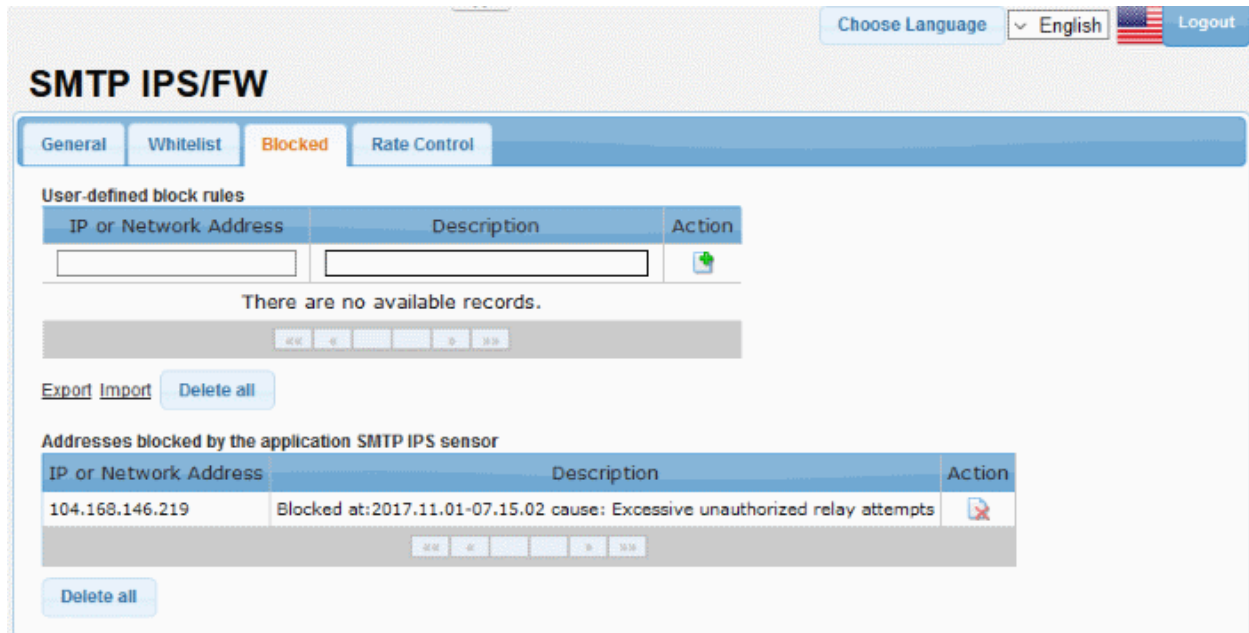
- Repeat the process to add more files to the list.



- To remove a file from the list, click the 'Clear' link beside it.
- To remove all the files, click 'Clear All' at the top.
- Click 'Save'.

5.5.3 Blocked IP Addresses

- Click Modules > 'Blocked' tab in the SMTP IPS/FW module.
- Add IP addresses to the blacklist so that mails from these sources never reach the SMTP level for processing.
- This page lists blocked by policy rules and IPs blocked by the intrusion prevention module.
- Admins can unblock IP addresses by simply deleting the row from the table.




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 you to:


- **Add a network or IP address to be blocked**
- **Delete a blocked network or IP address from the list**
- **Export the blocked network or IP address details**
- **Import lists of network or IP addresses from files to be blocked**
- **Delete an automatically blocked network or IP address by SMTP IPS sensor from the list**

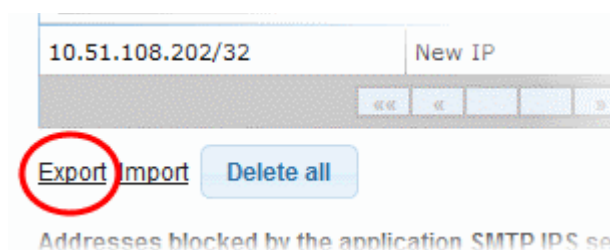
To add a network or IP address to be blocked

- Enter the IP or Network address details in the first field
- Enter an appropriate description for the address in the field under 'Description'.
- Click the  button.

The address will be added and listed.

To delete a blocked network or IP address from the list

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

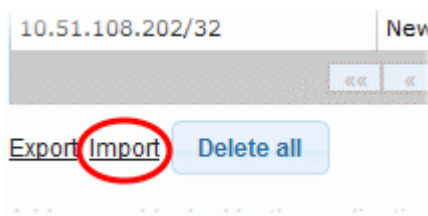


To export the blocked network or IP address details

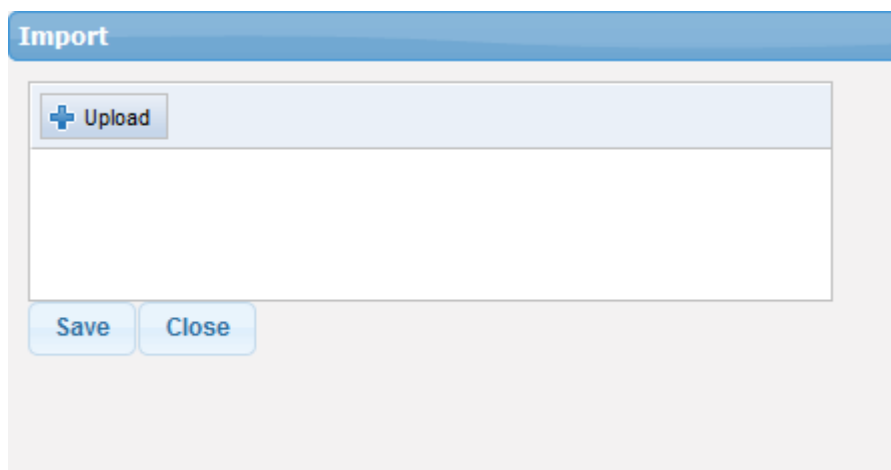
- Click the 'Export' link at the bottom of the screen
- The list will be exported as a text file.

To import lists of network or IP addresses from files to be blocked

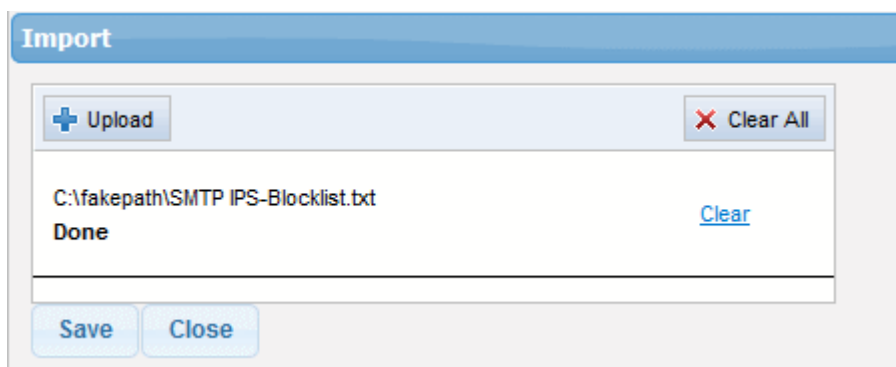
- Click the 'Import' link at the bottom of the screen



- Click 'Upload', 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 'Clear All' at the top.
- Click 'Save'.

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

If you know the IP addresses blocked by the SMTP IPS sensor is a trusted source, then you can delete it from the list.

- In the 'Addresses blocked by Secure Email Gateway SMTP IPS sensor' table, click the  button beside

an address that you want to delete.

Addresses blocked by the application SMTP IPS sensor

IP or Network Address	Description	Action
104.168.146.219	Blocked at:2017.11.01-07.15.02 cause: Excessive unauthorized relay attempts	

Delete all

- Click 'OK' in the confirmation screen

The page at https://demo-das.cdome.net:8443 says:

Are you sure you want to delete this entry?

Prevent this page from creating additional dialogs

5.5.4 Rate Control

- Click the 'Rate Control' tab in the SMTP IPS/FW module.
- The 'Rate Control' feature protects an organization from spammers that send huge amounts of mail to your mail server.
- It counts the number of suspicious mails sent by a source in a set period of time. If the value exceeds the specified threshold then the sender IP is added to the blacklist.

Choose Language English Logout

SMTP IPS/FW

General Whitelist Blocked **Rate Control**

	Enable	Total Received E-Mail Number	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

Rate Control Settings - Table of Column Descriptions	
Column Header	Description
Category	<ul style="list-style-type: none"> • SPAM - Mails that are categorized as spam • LDAP - Verification of LDAP users. When incoming mails are for users that are not in LDAP, the originating IP address will be blacklisted. For example, if the number of mails is set as 50, and the threshold percentage as 50%, then if from a source if the number of mails for non LDAP users exceeds 25 within the check interval, then the source will be blacklisted • RELAY - IPs from which mails can be sent by users who are not available on the mail server. • CERTAINLY SPAM - Mails that are categorized as definite spam. • VIRUS - Mails that are categorized as with virus
Enable	Activate or disable the Rate Control for a mail category
Total Received Mails	<p>The number of mails that need to be received in the specified interval before Secure Email Gateway will activate threshold checks.</p> <p>If Secure Email Gateway receives this number of mails from a source within the 'check interval' time, it will check what % of those mails are spam/relay/etc. If this exceeds the figure specified as the threshold then it will blacklist the sender.</p>
Check interval (in hours)	Enter the time in hours for the specified number of mails to be checked for a category.
Threshold (percentage)	<ul style="list-style-type: none"> • 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 'Save' to apply your changes.

5.6 Auto Whitelist

- Secure Email Gateway allows administrators to automatically whitelist incoming and outgoing mails to and from specific email addresses.
- The 'Auto Whitelist' module must be enabled to activate the whitelisting of addresses specified in profile settings. See '**Profile Management**' 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'.

- **Enable Autowhitelisting:** Activate automatic whitelist checks on incoming and outgoing emails
- **Auto Whitelist Threshold:** How many emails must be exchanged before the remote sender is added to the whitelist. Note - The threshold should be reached within the number of days specified in the 'Auto Whitelist Maximum Day Count' field.
- **Auto Whitelist Maximum Day Count:** To activate auto-whitelisting, Secure Email Gateway must receive the amount of mails in the threshold field within the number of days specified here.
- Click 'Save' to apply your changes.

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

Auto Whitelist details

The Auto Whitelist tab displays emails which have been whitelisted by currently active profiles.

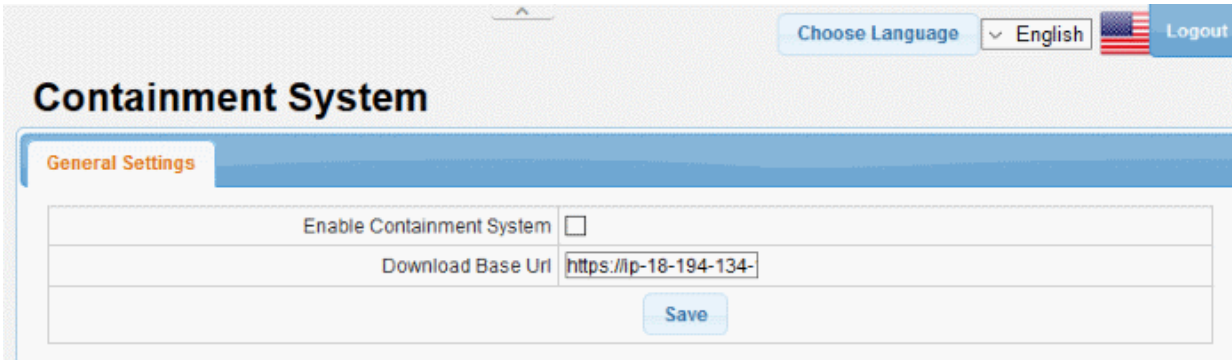
Auto Whitelist - Table of Column Headers	
Column Header	Description
Local Address	The recipient's email address
Remote Address	The sender's email address
Last Messaging Time	The time of the most recent sent or received mail
Local Messaging Count	The number of mails received
Remote Messaging Count	The number of messages sent
Action	 Deletes auto-whitelisted items

5.7 Containment System

- Containment protects users from zero-day malware by opening any untrusted attachments in a secure, virtual environment. This environment is known as the container.
- Items in the container are not allowed to access other processes or user data and will write to a virtual hard-drive and registry. This isolation means the attachment cannot damage the host machine nor steal confidential information.
- Process in brief:
 - Secure Email Gateway checks the trust rating of all attachments. PDF and .exe attachments with a trust rating of 'Unknown' are removed and replaced with a link.
 - The link allows recipients to download a special version of the file wrapped in Comodo's containment technology.
 - The file will be open in a virtual container on the endpoint

To configure containment system,

- Click the 'Modules' tab on the left, then click 'Containment System'.



The screenshot shows the 'Containment System' configuration page in the admin console. At the top right, there are options for 'Choose Language' (set to English) and a 'Logout' button. The main heading is 'Containment System'. Below it, the 'General Settings' tab is active. The configuration area contains two fields: 'Enable Containment System' with an unchecked checkbox, and 'Download Base Url' with the value 'https://ip-18-194-134-'. A 'Save' button is positioned below the 'Download Base Url' field.

- **Enable Containment System:** When enabled, files that have an 'Unknown' trust rating are contained.
- **Download Base Url:** The URL from which users will download the wrapped version of the file.
- Click 'Save' to apply your changes.

See **Attachment Verdict System** if you need more information on file ratings.

5.8 Data Leak Prevention (DLP)

- Click the 'Modules' > 'DLP'.
- Secure Email Gateway is integrated with a DLP (Data Leak Prevention) engine that prevents data theft via emails.
- The engine searches for configured words in incoming and outgoing mails and applies actions as per the settings in the profile. Actions include quarantining the mail and / or notifying the administrator.
- The DLP module must be enabled in order to activate the DLP parameters specified in the profile settings. See **Profile Management** for more details about profile settings.

- **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. This option is deselected by default.

See '**Profile Management**' for more details about profile settings.

- Click 'Save' to apply your changes.

5.9 Attachment Verdict System

- Click Modules > Attachment Verdict System.
- The 'Attachment Verdict System' settings area enables administrators to configure settings related to the analysis of email attachments.
- If enabled, the 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.

Attachment Verdict System - Table of Column Headers

Column Header	Description
Enable Attachment Verdict System	If enabled, Secure Email Gateway 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. This option is disabled



	by default.
CAM Key	Comodo Accounts Manager License key. The customers must sign up with Comodo Accounts Manager and order the Secure Email Gateway product to avail a license key.
Hostname	Hostname of the file attachment verdict system. This is set to the Comodo Valkyrie server by default. Only change this if you have established a different server with Comodo support.

Please note that, if the 'Enable Attachment Verdict System is enabled' and the 'Send files that not found in File Verdict System' in the **profile** is disabled, then the unknown files are not uploaded to Valkyrie for analysis. To view reports of attachment verdict system, see **Attachment Verdict Reports**.

6 Profile Management

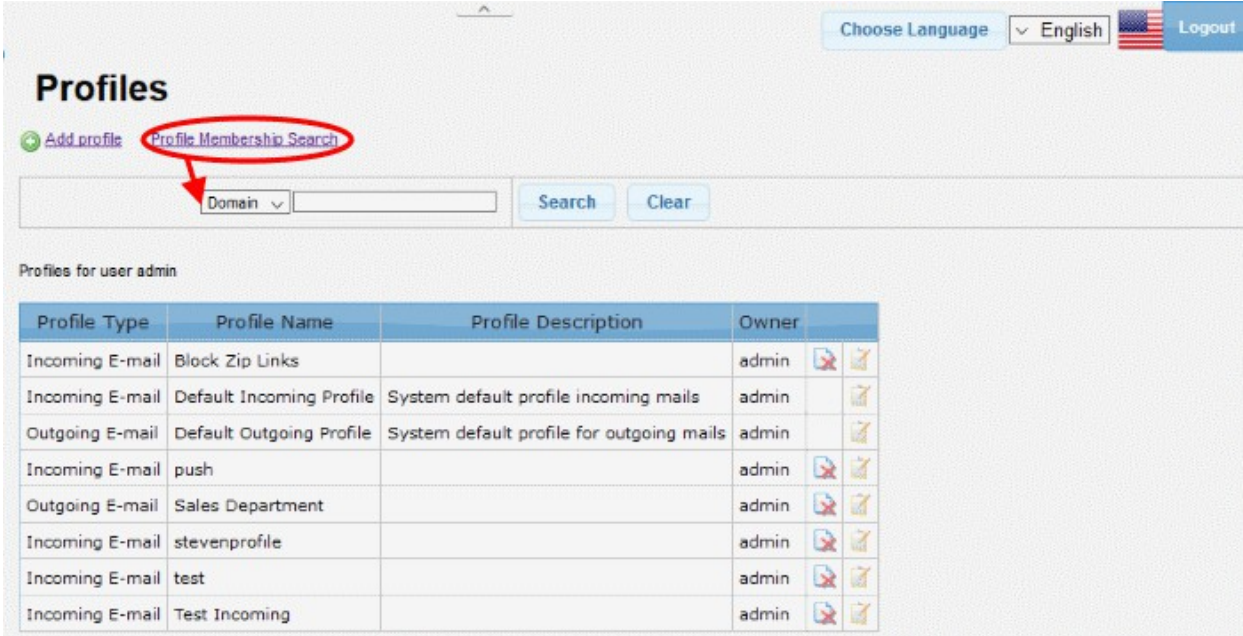
- Click the 'Profile Management' tab on the left, then click 'Profiles'
- Profiles are a collection of settings for Secure Email Gateway features such as 'Anti-virus', 'Anti-spam', 'Black List' and White List'. Profile can be applied to domains and/or users.
- There are two kinds of profiles that can be created in Secure Email Gateway - 'Incoming E-mail' and 'Outgoing E-mail'. Admins can apply different profiles for incoming mails and outgoing mails.
- Secure Email Gateway ships with a set of default incoming and outgoing profiles that can be edited but not deleted.

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	ilyaspala.ml_incoming		admin		

Profiles - Table of Column Headers	
Column Header	Description
Profile Type	Indicates whether the type of rules defined is for incoming or outgoing mails.
Profile Name	The name of the policy. The name of default policy will be auto filled.
Profile Description	A short description provided for a mail security policy
Owner	The name of the group to which the profile creator belongs
Action	 Allows you 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 you 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	Block Zip Links		admin
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	push		admin
Outgoing E-mail	Sales Department		admin
Incoming E-mail	stevenprofile		admin
Incoming E-mail	test		admin
Incoming E-mail	Test Incoming		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	Owner
Incoming E-mail	Block Zip Links		admin

- 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	Block Zip Links		admin	
Incoming E-mail	Default Incoming Profile	System default profile incoming mails	admin	

- To remove the details in the search field, click 'Clear'.
- 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**

6.1 Add and Configure a New Profile

- Click the 'Add profile' link in the 'Profiles' screen:
- Profiles let you configure how Secure Email Gateway's scanners and filters should handle mail on your protected domains.
- The items that can be set in a profile include Anti-virus, Anti-spam, SMTP, Attachment Filter, Black List, White List, Header Filter, Archive and Quarantine, Data Leak Prevention (DLP) and Realtime Blackhole List (RBL).

Profiles

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

Domain

Profiles for user admin

Profile Type	Profile Name	Profile Description	Owner	
Incoming E-mail	Block Zip Links		admin	
Incoming E-mail	Default Incoming Profile	System default profile incoming mails	admin	

The 'Add New Profile' screen will be displayed:

Choose Language English Logout

Add New Profile

- Parameters

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

Archive And Quarantine
Rules
E-Mail Classification
Geolocation Restrictions
RBL
DLP
Attachment Verdict System

Profile Type *	<input type="text" value="Incoming E-mail"/>	
Profile Name *	<input type="text"/>	
Description	<input type="text"/>	
Username *	<input type="text" value="admin"/>	
Domain Members <small>You can only select domains that are not member of any profile.</small>	<div style="border: 1px solid #ccc; padding: 5px;"> <ul style="list-style-type: none"> arda.com bilism.ml gmail.com ilyas.com mydomain.com office365domain.com outlook.com </div>	<div style="border: 1px solid #ccc; padding: 5px;"> <ul style="list-style-type: none"> <input type="button" value="Copy all"/> <input type="button" value="Copy"/> <input type="button" value="Remove"/> <input type="button" value="Remove All"/> </div>
E-mail Members <small>You can enter any e-mail address here.</small>	<input type="text" value="Import"/>	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

Profiles - Table of Parameters	
Parameter	Description
Profile Type	Select whether you want to apply rules to incoming mails or outgoing mails
Profile Name	Enter a name for the customized policy you rule set create
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 to add domains to the profile. <ul style="list-style-type: none"> The left-hand box displays domains that were added in the Manage Domains section. Any domain that is already added to another profile will not be listed here.

	<ul style="list-style-type: none"> Select domains in the right-hand box then click 'Copy' to add them to the profile. All users which are members of imported domains will receive this profile.
Email Members	<p>Allows administrators to add users to the profile.</p> <ul style="list-style-type: none"> Incoming profiles - only users which belong to domains in the 'Manage Domains' section can be added. Outgoing profiles - you can add users which belong to domains that are not in the 'Manage Domains' section.
Import	<p>Allows you to add users to the profile by importing them from a saved file. The same limitations mentioned above apply to imported users.</p>

- Click 'Save'

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

Profiles

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

Domain

Profiles for user admin

Profile Type	Profile Name	Profile Description	Owner	
Incoming E-mail	Block Zip Links		admin	
Incoming E-mail	Default Incoming Profile	System default profile incoming mails	admin	

The interface allows administrators to configure profile parameters for:

- Anti-virus**
- Anti-spam**
- Black List**
- White List**
- SMTP Settings**
- Attachment Filter**
- Header Filter**
- Archive and Quarantine**
- Rules**
- E-Mail Classification**
- Geolocation Restrictions**
- Realtime Blackhole List (RBL)**
- Data Leak Prevention (DLP)**
- Containment System**

- **Attachment Verdict System**

Note: All tabs are disabled until you complete and save the details of the domain members.

Anti-virus

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Anti-virus' tab

The screenshot shows the 'Add New Profile' page for 'example incoming - Parameters'. The 'Anti-virus' tab is active. A green message states 'Settings saved successfully'. Below this, a table contains the following settings:

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

At the bottom of the form, there are 'Save' and 'Cancel' buttons.

- **Enable Anti Virus:** Select the check box to enable the anti-virus engine for this profile. Please note the '**Anti-virus**' module should be enabled for this parameter to become active.
- **Quarantine mails containing virus:** Mails detected with viruses will be quarantined. Users can log into the 'Quarantine Webmail' interface to view his/her mails that are quarantined.
- Click 'Save' to apply your changes.

Anti-spam

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Anti-spam' tab

Add New Profile

example incoming - Parameters

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

Archive And Quarantine
Rules
E-Mail Classification
Geolocation Restrictions
RBL
DLP
Containment System

Attachment Verdict System

Settings saved successfully

Enable Anti SPAM	<input checked="" type="checkbox"/>
Use a dedicated bayesian database for this profile	<input type="checkbox"/>
Maximum MB that an e-mail enters spam filtering	<input type="text" value="1"/>
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"/>

Profiles: Anti-spam Settings - Table of Parameters	
Parameter	Description
Enable Anti SPAM	Select the check box to enable the anti-spam engine for this profile. Please note the 'Anti-spam' module should be enabled for this parameter to become active.
Use a dedicated bayesian database for this profile	Select the check box to enable the anti-spam engine to use Bayesian database also for detecting spam mails. Please note the 'Bayes Spam engine' in the 'Advanced Settings' section of 'Anti-spam' module should be enabled for this parameter to become active.
Maximum MB that an e-mail enters spam filtering	Enter the maximum size of emails for which spam filtering will be enabled. If the size of an email exceeds the entered value, then the email will not be scanned and placed in queue for delivery to the recipient.
Certainly spam points	Enter a value between 1 and 100 that will classify an email as definitely spam. Suggested values are between 90 - 100 points.
Spam points	Enter a value between 1 and 100 that will classify an email as spam. Suggested values are between 51 - 89 points.
Probable spam points	Enter a value between 1 and 100 that will classify an email as probable spam. Suggested values are between 40 - 50 points.
Certainly spam action	Select the action that has to be taken for emails that are categorized as definitely spam. The options available are:

	<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 'Save' to apply your changes.

Black List

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Black List' tab


The screenshot shows the 'Add New Profile' page for 'example incoming - Parameters'. The 'Black List' tab is active. A table displays the following data:

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

Below the table, it says "There are no available records." and provides buttons for "Export", "Import", "Delete all", and "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 you to add a blacklist type after filling the fields in the row

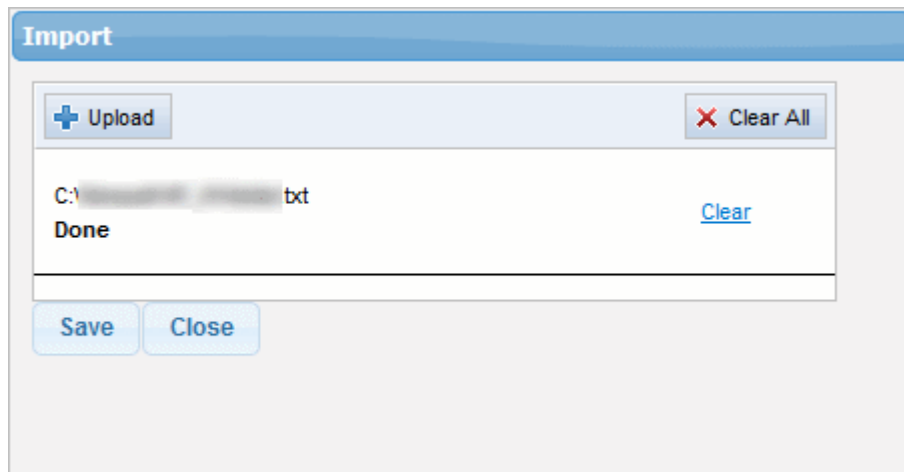
		Allows you to delete a blacklist type from the list
--	---	---


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



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

The file will be added.





- Repeat the process to add more files.
- To remove a file, click the 'Clear' link beside it.
- To remove all the added files, click 'Clear All' at the top right.
- To import the list from the files, click 'Save'.
- To delete a 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 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Whitelist' tab

Profiles: White List Settings - Table of Column Descriptions

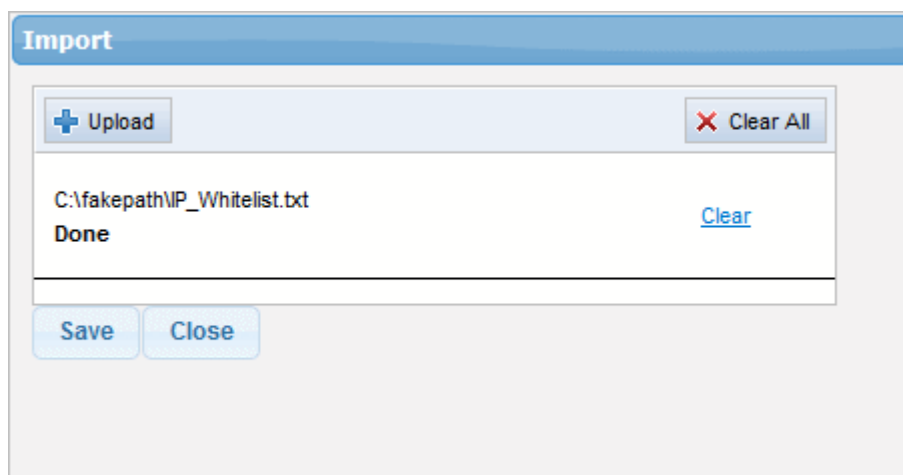
Column Header	Description	
Whitelist Type	Select the type of source that has to be whitelisted. The options available are: <ul style="list-style-type: none"> • IPv4 Address • IPv6 Address • E-mail • Domain • IPv4 Network • IPv6 Network 	
Whitelist Value	Enter the details for the type of whitelist selected in the first column.	
Comment	Provide an appropriate description for the blacklisted source	
Action		Allows you to add a whitelist type after filling the fields in the row
		Allows you to delete a whitelist type from the list


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



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

The file will be added.



- Repeat the process to add more files.
- To remove a file, click the 'Clear' link beside it.
- To remove all the added files, click 'Clear All' at the top right.
- To import the list from the files, click 'Save'.
- To delete a whitelist type from the list, click  under the 'Action' column header and click 'OK' in the confirmation screen.
- To remove all the whitelisted sources, click the 'Delete all' link and click 'OK' in the confirmation screen.

SMTP

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'SMTP Settings' tab

Choose Language English Logout

Add New Profile

example incoming - Parameters

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

Archive And Quarantine Rules E-Mail Classification Geolocation Restrictions RBL DLP Containment System

Attachment Verdict System

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-KRN Mails	<input type="checkbox"/>
Anti-spoofing Action	Reject v
KRN Action	Reject v
RBL Action	Reject v

Save Cancel

Profiles: SMTP Settings - Table of Parameters	
Parameter	Description
Refuse mails sent by fake local users	If enabled, Secure Email Gateway 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, Secure Email Gateway 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 Secure Email Gateway 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, Secure Email Gateway accepts the mail and initiates the filtering process.
Activate Layer-7 DoS	If enabled, Secure Email Gateway will activate the Layer 7 Denial of Service protection

protection	feature.
Quarantine Antispoofing Mails	If enabled, the spoofing mails will be Quarantined.
Quarantine RBL-KRN Mails	If enables, the RBL and KRN mails will be Quarantined.
Anti-spoofing Action	Select the action to be performed when the condition is met for a mail. The options available are: Reject - The mail will be rejected and a reject response will be sent to the sender's mail server Discard – The mail will be rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface.
KRN Action	Select the action to be performed when the condition is met for a mail. The options available are: Reject - The mail will be rejected and a reject response will be sent to the sender's mail server Discard – The mail will be rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface.
RBL Action	Select the action to be performed when the condition is met for a mail. The options available are: Reject - The mail will be rejected and a reject response will be sent to the sender's mail server Discard – The mail will be rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface.

- Click 'Save' to apply your changes.



Attachment Filter

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Attachment Filter' tab

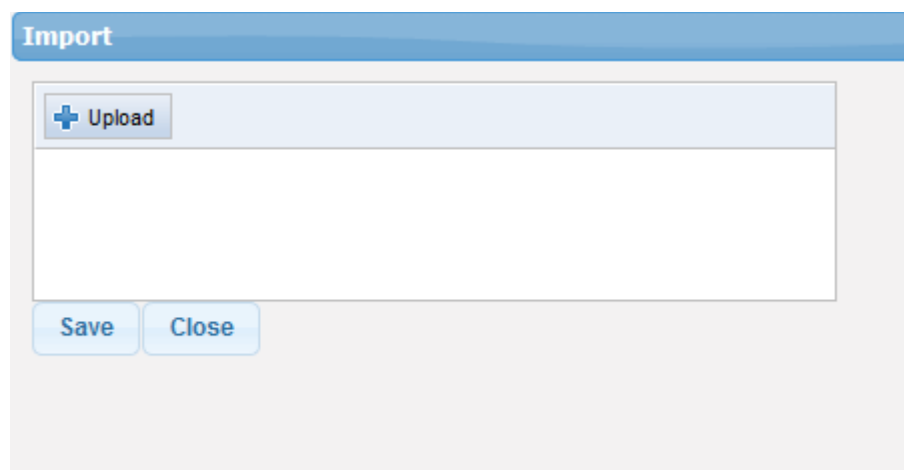
The screenshot shows the 'Add New Profile' page in the Comodo Secure Email Gateway Enterprise Admin interface. The 'Attachment Filter' tab is selected. A success message 'Settings saved successfully' is displayed. Below it, a table shows the configuration for the attachment filter:

Addition		Action
Malware	Equals To	Remove Attachment

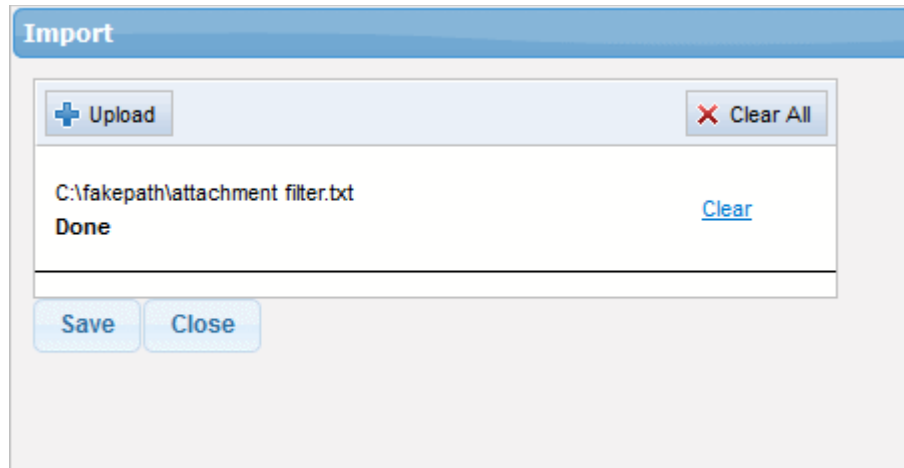
Below the table, it states 'There are no available records.' and provides links for 'Export', 'Import', 'Delete all', and 'Cancel'.

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 Quarantined Email web interface. • Remove attachment - The mail will be delivered to the recipient without the attachment.
	<div style="display: flex; align-items: center;">  Allows you to add an attachment filter rule after filling the fields in the row </div>
	<div style="display: flex; align-items: center;">  Allows you to delete attachment filter rule from the list </div>


- To save the list of 'Attachment Filter' rules, click the 'Export' link and save it to your system
- To import a list of 'Attachment Filter' rules from a saved file, click the 'Import' link



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

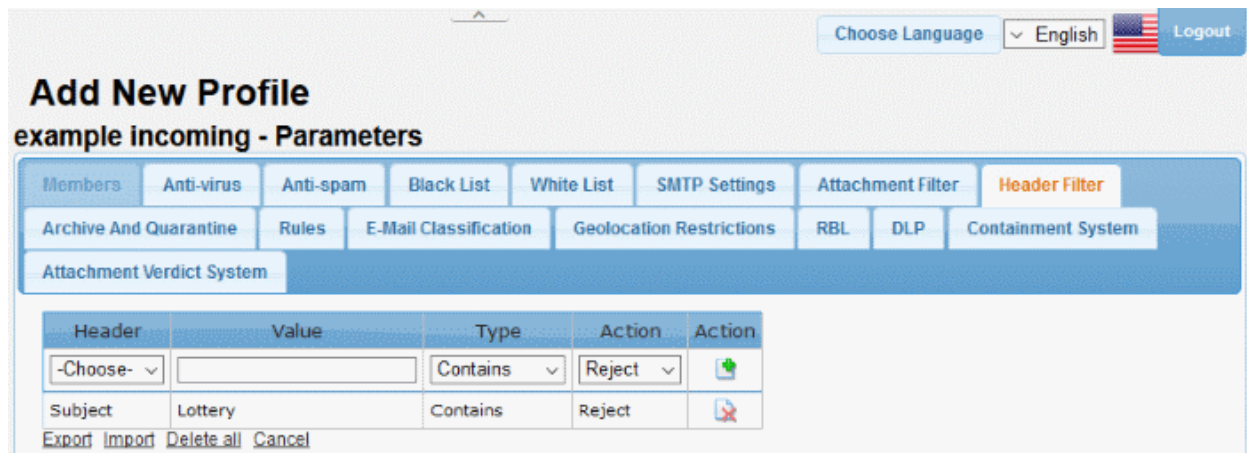


The file will be added.



- Repeat the process to add more files.
- To remove a file, click the 'Clear' link beside it.
- To remove all the added files, click 'Clear All' at the top right.
- To import the list from the files, click 'Save'.
- To delete an 'Attachment Filter' rule from the list, click the  button under the last column and click 'OK' in the confirmation screen.
- To remove all the 'Attachment Filter' rules, click the 'Delete all' link and click 'OK' in the confirmation screen.

Header Filter

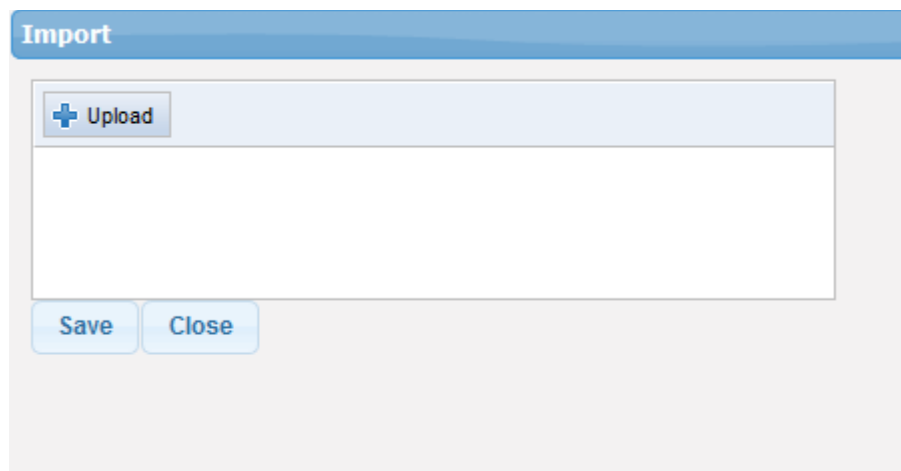
- Click the 'Header Filter' tab



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

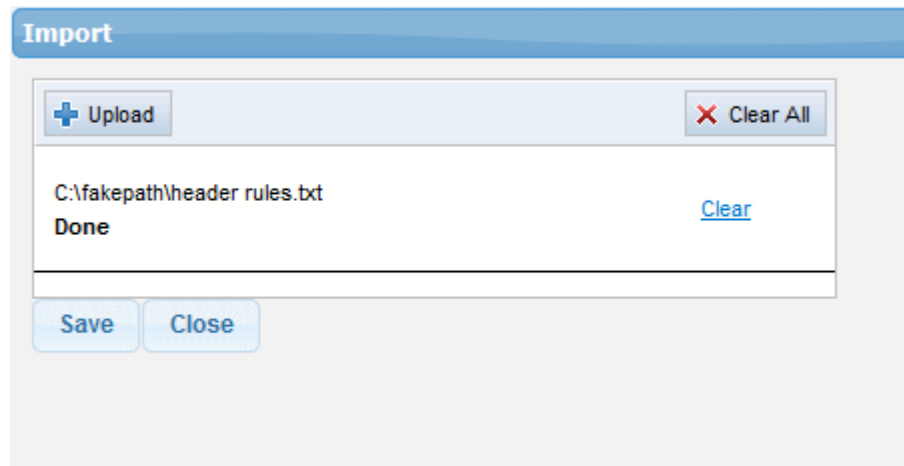
	<ul style="list-style-type: none"> From
Value	Enter the keyword that should be scanned for the selected header type.
Type	Select the condition from the drop-down. The options available are: <ul style="list-style-type: none"> Contains Equals to Starts with Ends with
Action	Select the action to be performed 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 you to add a 'Header Filter' rule after filling the fields in the row
	 Allows you to delete a 'Header Filter' rule from the list


- To save the list of 'Header Filter' rules, click the 'Export' link and save it to your system
- To import a list of 'Header Filter' rules from a saved file, click the 'Import' link



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

The file will be added.



- Repeat the process to add more files.
- To remove a file, click the 'Clear' link beside it.
- To remove all the added files, click 'Clear All' at the top right.
- To import the list from the files, click 'Save'.
- To delete a 'Header Filter' rule from the list, click the  button under the last column and click 'OK' in the confirmation screen.
- To remove all the 'Header Filter' rules, click the 'Delete all' link and click 'OK' in the confirmation screen.

Archive and Quarantine

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Archive and Quarantine' tab

Choose Language English Logout

Add New Profile

example incoming - Parameters

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

Archive And Quarantine
Rules
E-Mail Classification
Geolocation Restrictions
RBL
DLP
Containment System

Attachment Verdict System

Archive method	Forward
Archive mailbox	backup@korumail.com
Send daily quarantine report to recipients	<input type="checkbox"/>
Quarantine release operation	<input checked="" type="checkbox"/>

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	This field becomes active only when an archive method is selected in the first row. Enter the mail address to which the archived and quarantined mails will be sent.
Send daily quarantine report to recipients	If enabled, the users will receive daily reports of their quarantined mails. Users can view their quarantined mails in the 'Secure Email Gateway Quarantine Webmail' interface by clicking the 'Quarantine Webmail' link in the 'Login' screen.
Quarantine Release Operation	Allows users to release their mails from quarantine
Archive Flags	
Mails with CLEAN content	If enabled, mails that are categorized as safe will be archived as per the 'Archive

	method' setting done in the first row.
Mails with CERTAINLY SPAM content	If enabled, mails that are categorized as 'Certainly Spam' will be archived as per the 'Archive method' setting done in the first row.
Mails with SPAM content	If enabled, mails that are categorized as 'Spam' will be archived as per the 'Archive method' setting done in the first row.
Mails with PROBABLE SPAM content	If enabled, mails that are categorized as 'Probable Spam' will be archived as per the 'Archive method' setting done in the first row.
Mails matched by CONTENT FILTER rules	If enabled, mails that are filtered for content per the settings done in ' Content Filter ' in the ' Anti-spam ' module will be archived as per the 'Archive method' setting done in the first row.
Mails containing VIRUS	If enabled, mails that are categorized are with virus will be archived as per the 'Archive method' setting done in the first row.

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

Rules

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Rules' tab

Edit profile: ilyaspala.ml_incoming

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

Archive And Quarantine
Rules
E-Mail Classification
Geolocation Restrictions
RBL
DLP
Containment System

Attachment Verdict System

PROMO

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

SOCIAL

Social Action	<input type="text" value="OK+TAG"/>
Social Tag	<input type="text" value="[SOCIAL]"/>
Quarantine social mails	<input checked="" type="checkbox"/>

FORUM

Forum Action	<input type="text" value="OK+TAG"/>
Forum Tag	<input type="text" value="[FORUM]"/>
Quarantine forum mails	<input checked="" type="checkbox"/>

NEWSLETTER

Newsletter Action	<input type="text" value="OK+TAG"/>
Newsletter Tag	<input type="text" value="[NEWSLETTER]"/>
Quarantine newsletter mails	<input checked="" type="checkbox"/>

UPDATE

Update Action	<input type="text" value="OK+TAG"/>
Update Tag	<input type="text" value="[UPDATE]"/>
Quarantine update mails	<input checked="" type="checkbox"/>

PHISHING

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
PROMO	
Promotion Tag	Promotional emails are sent to the recipient with the tag as entered in this field.
Promotional Action	<p>Select the action when the condition is met for a 'Rules' setting in a promotional mail. The options available are:</p> <ul style="list-style-type: none"> OK + TAG - The tagged mail is sent to the recipient. OK – The mail is sent to the recipient without tag Reject - The mail is rejected and a reject response us sent to the sender mail server. Discard - The mail is rejected without notifying the sender. The user can view

	the email using the 'Quarantined Email' web interface.
Quarantine Promotional Mails	If enabled, promotional mails are quarantined.
SOCIAL	
Social Action	Select the action when the condition is met for a 'Rules' setting in a social mail. The options available are: <ul style="list-style-type: none"> • OK + TAG - The tagged mail is sent to the recipient. • OK – The mail is sent to the recipient without tag • Reject - The mail is rejected and a reject response is sent to the sender mail server. • Discard - The mail is rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface.
Social Tag	Social emails are sent to the recipient with the a tag as entered in this field.
Quarantine social mails	If enabled, social mails are quarantined
FORUM	
Forum Action	Select the action when the condition is met for a 'Rules' setting in a forum mail. The options available are: <ul style="list-style-type: none"> • OK + TAG - The tagged mail is sent to the recipient. • OK – The mail is sent to the recipient without tag • Reject - The mail is rejected and a reject response is sent to the sender mail server. • Discard - The mail is rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface.
Forum Tag	Forum based emails are sent to the recipient with the tag as entered in this field.
Quarantine forum mails	If enabled, forum mails are quarantined
NEWSLETTER	
Newsletter Action	Select the action when the condition is met for a 'Rules' setting in a newsletter mail. The options available are: <ul style="list-style-type: none"> • OK + TAG - The tagged mail is sent to the recipient. • OK – The mail is sent to the recipient without tag • Reject - The mail is rejected and a reject response is sent to the sender mail server. • Discard - The mail is rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface.
Newsletter Tag	Newsletter emails are sent to the recipient with the tag as entered in this field.
Quarantine newsletter mails	If enabled, newsletter mails are quarantined
UPDATE	
Update Action	Select the action when the condition is met for a 'Rules' setting in a update mail. The

	<p>options available are:</p> <ul style="list-style-type: none"> • OK + TAG - The tagged mail is sent to the recipient. • OK – The mail is sent to the recipient without tag • Reject - The mail is rejected and a reject response is sent to the sender mail server. • Discard - The mail is rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface.
Update Tag	Update emails are sent to the recipient with the tag as entered in this field.
Quarantine update mails	If enabled, update mails are quarantined
PHISHING	
Enable Phishing Check	If enabled, checks for phishing emails.
Phishing Action	<p>Select the action 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 is sent to the recipient. • OK – The mail is sent to the recipient without tag • Reject - The mail is rejected and a reject response is sent to the sender mail server. • Discard - The mail is rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface.
Phishing Tag	Phishing emails are sent to the recipient with the a tag as entered in this field.
Quarantine Phishing Mails	If enabled, phishing mails are quarantined.

- Click 'Save' to apply your changes.

Email Classification

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Email Classification' tab

Choose Language English Logout

Add New Profile

example incoming - Parameters

Members Anti-virus Anti-spam Black List White List SMTP Settings Attachment Filter Header Filter
 Archive And Quarantine Rules **E-Mail Classification** Geolocation Restrictions RBL DLP Containment System
 Attachment Verdict System

Settings saved successfully

Category	Status	Tag	Action	Quarantine
PROMO	<input checked="" type="checkbox"/>	PROMO	Discard	<input checked="" type="checkbox"/>
SOCIAL	<input checked="" type="checkbox"/>	SOCIAL	Tag Only	<input type="checkbox"/>
FORUM	<input checked="" type="checkbox"/>	FORUM	Tag Only	<input type="checkbox"/>
NEWSLETTER	<input checked="" type="checkbox"/>	NEWSLETTER	Tag Only	<input checked="" type="checkbox"/>
UPDATE	<input checked="" type="checkbox"/>	UPDATE	Tag Only	<input type="checkbox"/>

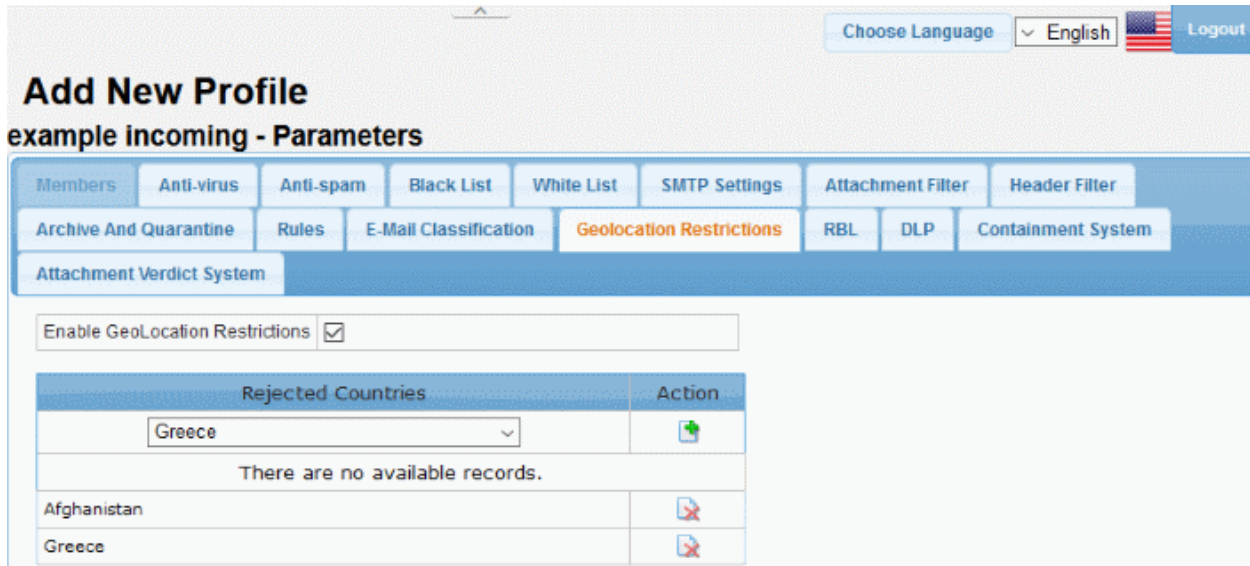
Save Cancel

Category	The type of mail received
Status	Whether the rule is enabled or not
Tag	The name prefixed to the email to show the email classification. For example, promotional email subjects are prefixed with [PROMO].
Action	Select the action to be performed when the condition is met for a 'Rules' setting in a forum mail. The options available are: <ul style="list-style-type: none"> Discard - The mail will be rejected without notifying the sender. The user can view the email using the 'Quarantined Email' web interface. TAG Only – The tagged mail will be sent to the recipient. Reject - The mail will be rejected and a reject response will be sent to the sender mail server. OK – The mail will be sent to the recipient without tag
Quarantine	If enabled, the corresponding category of mails will be quarantined



- Click 'Save' to apply your changes.

Geolocation Restrictions

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Geolocation Restrictions' tab



Profiles: Geolocation Restrictions Settings - Table of Column Descriptions

Column Header	Description	
Rejected Countries	Select the country you want Secure Email Gateway to reject. Please note that you have to enable SMTP > General settings >	
Action		Allows administrators to add a country after selecting it in the row
		Allows administrators to delete the country from the list

Realtime Blackhole List (RBL)

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'RBL' tab

Choose Language English Logout

Add New Profile

example incoming - Parameters

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

Archive And Quarantine | Rules | E-Mail Classification | Geolocation Restrictions | **RBL** | DLP | Containment System

Attachment Verdict System

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

First
Up
Down
Last

The screen displays the RBL servers that are available by default and added manually. See **'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 you to activate or deactivate a RBL server in the list. If a server is disabled, Secure Email Gateway skips it and refers to the next server in line.

The control buttons next to the table allows to reorder the RBL server list for checking the blacklisted IP addresses available in the servers. The enabled RBL server listed first will be checked first and move down the order. Use the control buttons to move a server up or down the order.

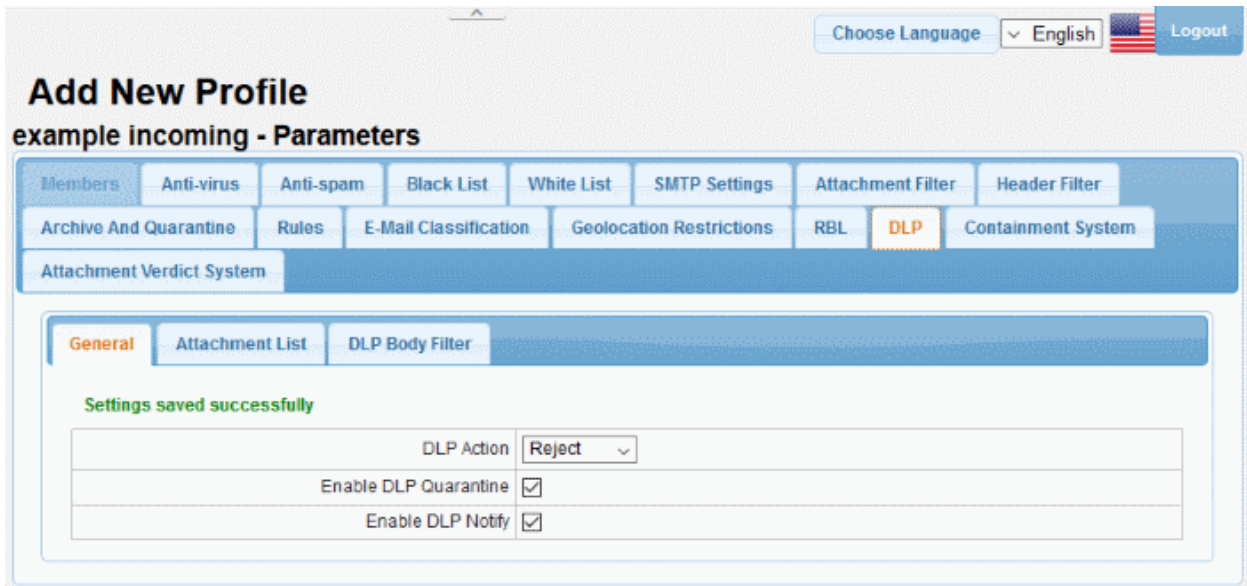
Server Host Address	Description	Type	Enable
bl.spamcop.net	spamcop	RBL	Yes
zen.spamhaus.org	spamhaus	RBL	Yes
bl.score.senderscore.com	Return Path Reputation Network Blacklist	RBL	No
10.108.51.202		RBL	Yes
psbl.surriel.com	Passive Spam Block List	RBL	Yes

First
Up
Down
Last

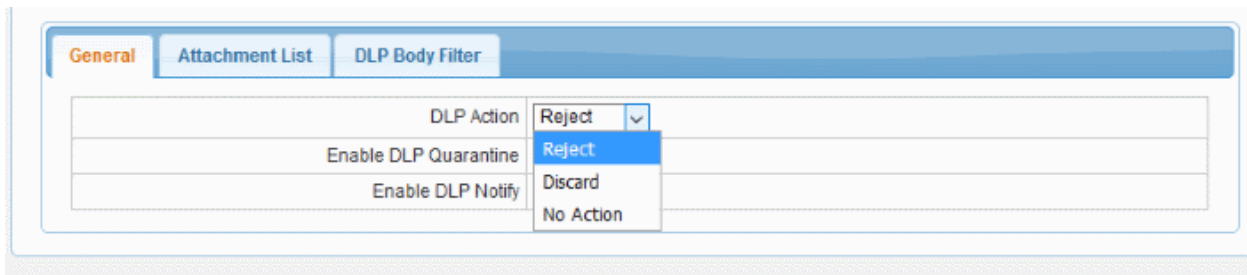
Data Leak Prevention (DLP)

The DLP feature is capable of scanning mails for important key words such as credit card, social security numbers, attachments and takes action as per the settings. Please note that the DLP module should be enabled for the settings configured here to take effect. See **'Data Leak Prevention'** for more details.

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'DLP' tab



DLP General Settings



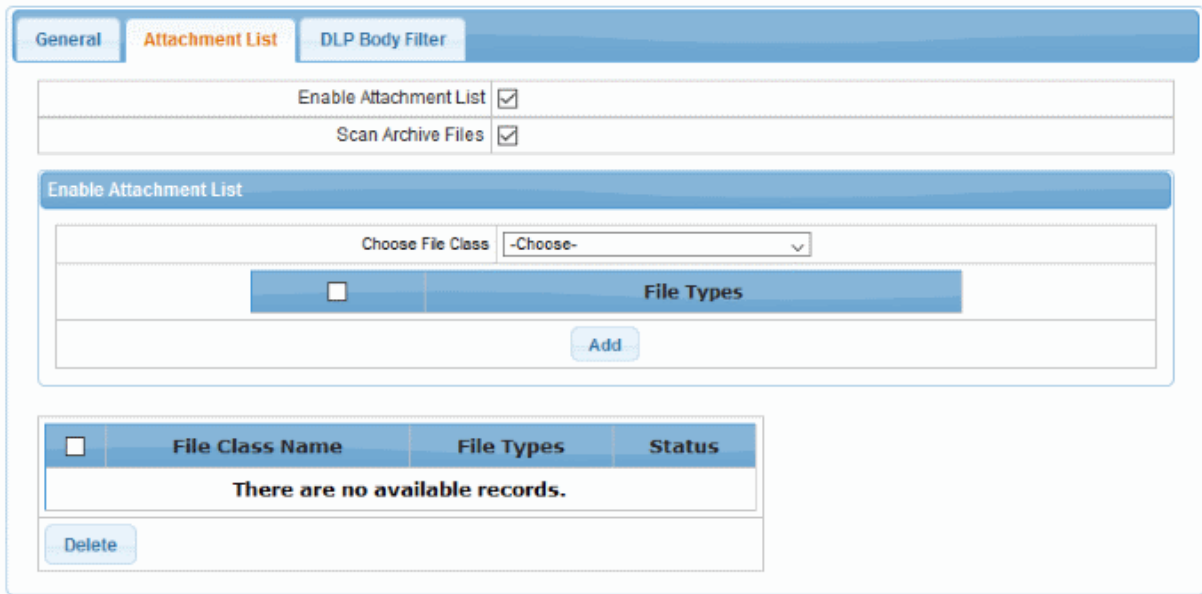
- **DLP Action** - These settings determine what action should be taken if Secure Email Gateway detects a message that could present a data leak.

The options available are:

- **No Action** - The mail will be allowed and the system admin will be notified if 'DLP Notify' is enabled.
- **Reject** - The mail will be rejected and a reject warning will be sent to the sender's email address.
- **Discard** - The mail will be deleted and if 'DLP Quarantine' is enabled, it will be quarantined and the system admin will be notified.
- **Enable DLP Quarantine** – If selected, SEG quarantines mails with data leak. Please note the setting in 'DLP Action' should be 'Discard' for mails to be quarantined.
- **Enable DLP Notify** – If selected, SEG alerts the system admin about DLP breaches.

Attachment List

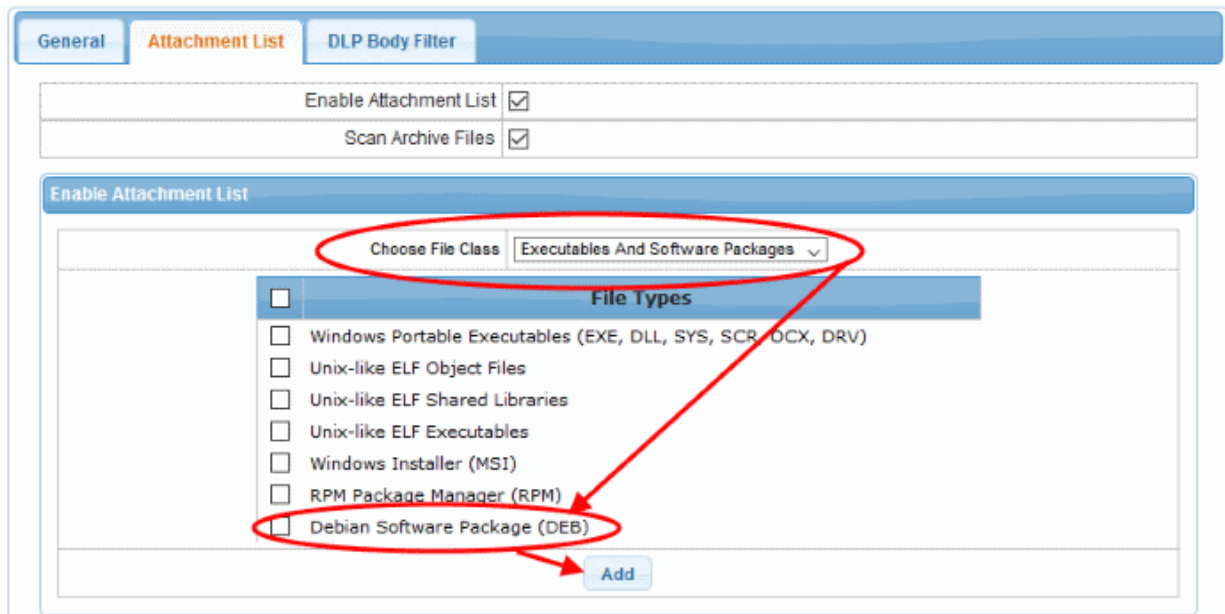
- Click the 'Attachment List' tab



- **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"/>	Microsoft Office Files	Microsoft Word 2007+ Files	Active
<input type="checkbox"/>	Executables And Software Packages	RPM Package Manager (RPM)	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'. Secure Email Gateway comes with three predefined DLP Body Filters and allows the administrators to add more filters as required.

General
Attachment List
DLP Body Filter

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	

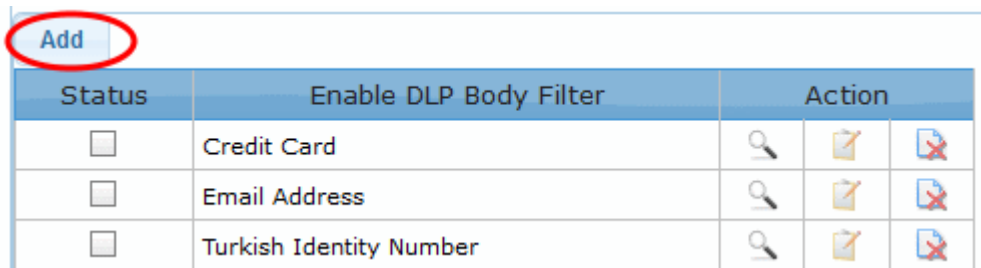
- **Enable DLP Body Filter:** Select the check box to apply the configured body filters










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

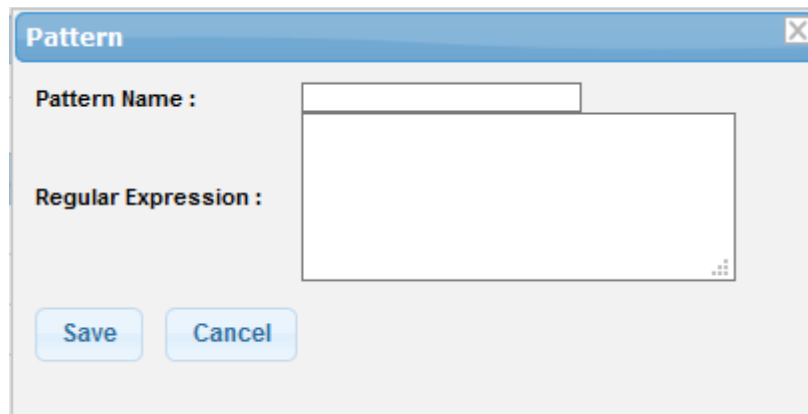
To add a new DLP body filter

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



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.



Pattern [X]

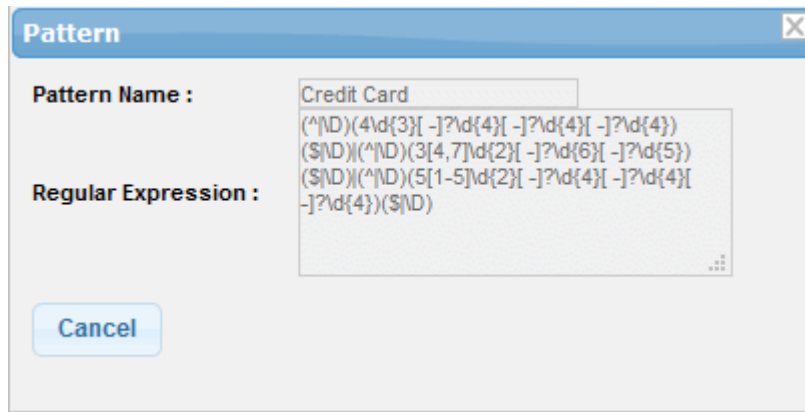
Pattern Name :

Regular Expression :

- 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

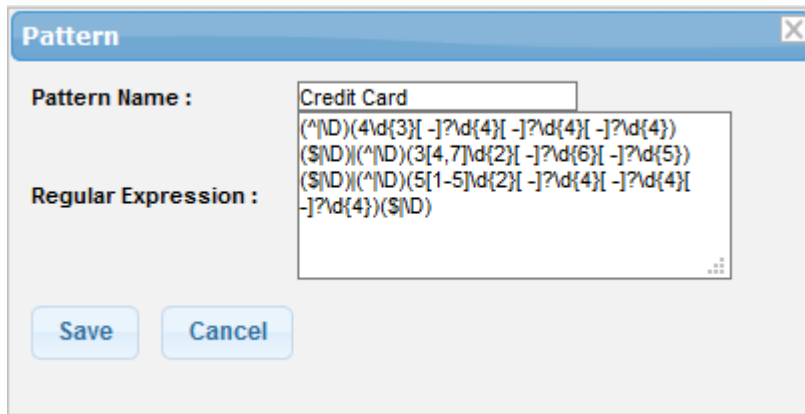
- Click the  icon beside a body filter that you want to view the details



- Click the 'Cancel' button or close the dialog to return to main screen.


To edit a body filter

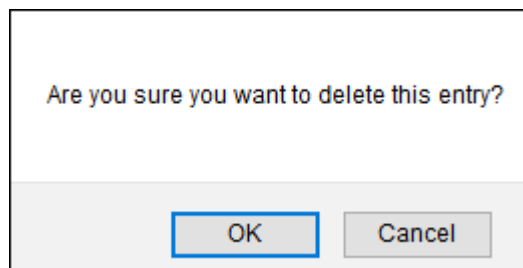
- Click the  icon beside a body filter that you want to edit the details



- 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.

Containment System

The 'Containment System' enables administrators to configure profile settings related to the containment analysis. If enabled, containment system will run email attachments in the containment environment (windows executable files and pdf files).

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right

- Click the 'Containment System' tab

Edit profile: TechWriting

Members
Anti-virus
Anti-spam
Black List
White List
SMTP Settings
Attachment Filter
Header Filter
Archive And Quarantine
Rules
E-Mail Classification
Geolocation Restrictions
RBL
DLP
Containment System

Attachment Verdict System

Enable Containment System	<input type="checkbox"/>
Files which are accepted. *	<input type="checkbox"/> windows executable <input type="checkbox"/> pdf
Apply for whitelists	<input type="checkbox"/>
Only Administrator can unwrap	<input type="checkbox"/>
Unwrap the sandbox after specified time (mins)	<div style="display: flex; align-items: center;"> <div style="text-align: center; width: 50px;">1</div> <div style="text-align: center; width: 50px;">60</div> <div style="flex-grow: 1; border-bottom: 1px solid #ccc; position: relative;"> <div style="position: absolute; left: -5px; top: -5px;">▼</div> </div> <div style="text-align: center; width: 50px;">5</div> </div>
Unwrap the sandbox after specified running count	<div style="display: flex; align-items: center;"> <div style="text-align: center; width: 50px;">2</div> <div style="text-align: center; width: 50px;">10</div> <div style="flex-grow: 1; border-bottom: 1px solid #ccc; position: relative;"> <div style="position: absolute; left: -5px; top: -5px;">▼</div> </div> <div style="text-align: center; width: 50px;">2</div> </div>

Containment System - Table of Column Headers

Column Header	Description
Enable Containment System	If enabled, email attachments (pdfs and windows executables) will be 'wrapped' with containment code before delivery. This means they will open in an isolated, virtual environment known as the container, instead of directly on the endpoint. The attachment will open as normal from the end-user's point-of-view, but it will not be allowed to access important system files, user data or to cause damage to the host system.
Files which are accepted	If enabled, will deliver files in the chosen format
Apply for whitelists	If enabled, Secure Email Gateway will also analyze white-listed sources.
Only Administrator can unwrap	<p>Safe files in the containment when run are unwrapped immediately for both users and admins. Malicious files are blocked.</p> <p>Contained files for which results are unsure (not safe nor malicious) are unwrapped if specified time or count (mentioned in rows below) is reached.</p> <p>If this setting is:</p> <ul style="list-style-type: none"> Enabled - Only admins can unwrap contained files for which results are unsure (not safe nor malicious) Disabled – Both admins and users can unwrap contained files for which results are unsure (not safe nor malicious)
Unwrap the sandbox after specified time (mins)	Unsure files (not safe nor malicious) when run are moved out of containment after the specified time. Move the slider to set the time.
Unwrap the sandbox after specified running count	Unsure files (not safe nor malicious) when opened 'X' times as specified here are moved out of containment. Move the slider to set the count.

Attachment Verdict System

The 'Attachment Verdict System' settings area enables administrators to configure settings related to the analysis of email attachments. If enabled, the 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.

- Click 'Profile Management' > 'Profiles'
- Locate the profile you want to work on and click the 'Edit' button on the right
- Click the 'Attachment Verdict System' tab


Attachment Verdict System - Table of Column Headers

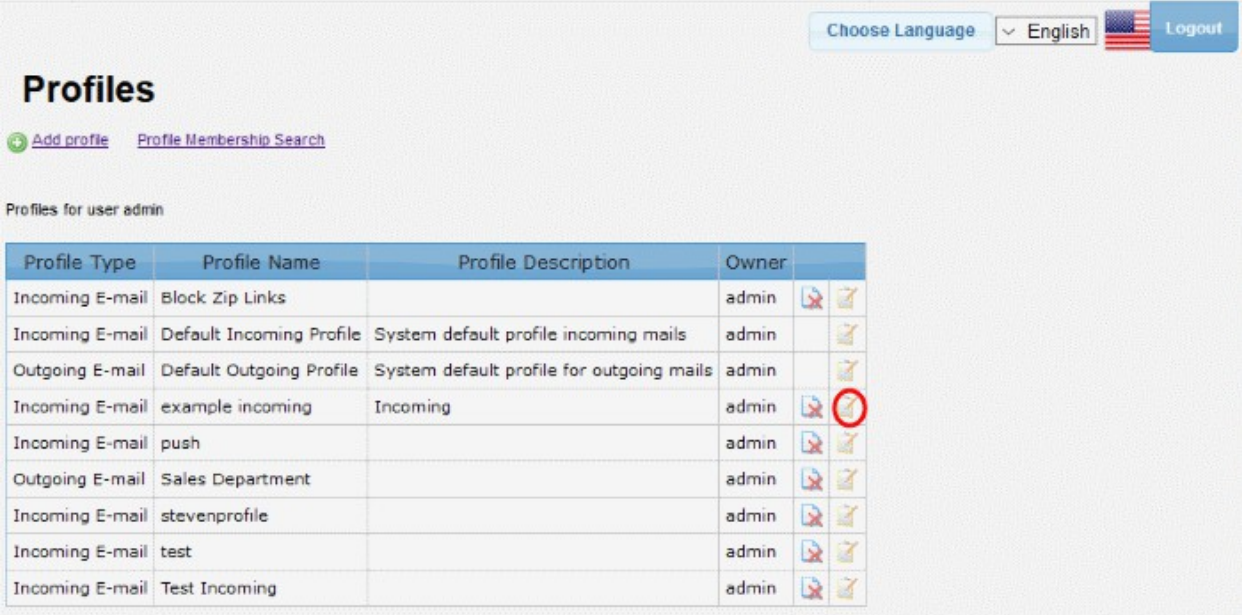
Column Header	Description
Enable Attachment Verdict System	<ul style="list-style-type: none"> • If enabled, Secure Email Gateway will automatically check the trust rating of Windows executables and pdf files in Comodo's file look up server (FLS). The verdict from the FLS can be 'Clean', 'Malware' or 'Unknown'. • Clean attachments will be allowed to proceed while malware attachments will be automatically quarantined (providing 'Quarantine mails containing viruses' is enabled in the antivirus section of the profile). • 'Unknown' files will be submitted to Comodo's real-time file analysis system, Valkyrie, for behavior testing. • Valkyrie's tests will determine whether the unknown file is clean or malware and apply the appropriate action as mentioned above.
Malware Probability Value	<ul style="list-style-type: none"> • The threshold at which Secure Email Gateway will designate an unknown file as 'malware' based on Valkyrie results. Comodo recommend that administrators leave this setting at the default and only move it after consultation with Comodo support. • Valkyrie examines the behavior of unknown files and assigns a score indicating how likely it is that the file is malware. Under the default settings, a score of 46+ is classed as malware. • Raising the value in this slider means Secure Email Gateway is more tolerant/less likely to class attachments as malware.
Apply for whitelists	If enabled, Secure Email Gateway will also analyze white-listed sources.
Send files that not found in	If enabled, Secure Email Gateway will upload files rated 'Unknown', to the attachment


File Verdict System	verdict system for detailed behavior analysis
Auto-submission in queue waiting time	Define in seconds how long Secure Email Gateway 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. See **Attachment Verdict Reports**, to view reports of attachment verdict system.

6.1.1 Edit a Profile

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












Choose Language English  Logout

Profiles

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

Profiles for user admin

Profile Type	Profile Name	Profile Description	Owner	
Incoming E-mail	Block Zip Links		admin	
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	example incoming	Incoming	admin	
Incoming E-mail	push		admin	
Outgoing E-mail	Sales Department		admin	
Incoming E-mail	stevenprofile		admin	
Incoming E-mail	test		admin	
Incoming E-mail	Test Incoming		admin	

The 'Edit Profile' screen will be displayed.

Choose Language English Logout

Edit profile: example incoming

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

Archive And Quarantine
Rules
E-Mail Classification
Geolocation Restrictions
RBL
DLP
Containment System

Attachment Verdict System

Profile Type *	<input type="text" value="Incoming E-mail"/>			
Profile Name *	<input type="text" value="example incoming"/>			
Description	<input type="text" value="Incoming"/>			
Username *	<input type="text" value="admin"/>			
Domain Members You can only select domains that are not member of any profile.	<table style="width: 100%; border: none;"> <tr> <td style="border: 1px solid #ccc; padding: 5px;"> bilisim.ml gmail.com ilyas.com mydomain.com pala.com test2domain.com testcustomer.com </td> <td style="border: none; padding: 5px; text-align: center;"> <input type="button" value="Copy all"/> <input type="button" value="Copy"/> <input type="button" value="Remove"/> <input type="button" value="Remove All"/> </td> <td style="border: 1px solid #ccc; padding: 5px;"> arda.com office365domain.com outlook.com </td> </tr> </table>	bilisim.ml gmail.com ilyas.com mydomain.com pala.com test2domain.com testcustomer.com	<input type="button" value="Copy all"/> <input type="button" value="Copy"/> <input type="button" value="Remove"/> <input type="button" value="Remove All"/>	arda.com office365domain.com outlook.com
bilisim.ml gmail.com ilyas.com mydomain.com pala.com test2domain.com testcustomer.com	<input type="button" value="Copy all"/> <input type="button" value="Copy"/> <input type="button" value="Remove"/> <input type="button" value="Remove All"/>	arda.com office365domain.com outlook.com		
E-mail Members You can enter any e-mail address here.	<div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> example@arda.com example@office365domain.com test@outlook.com </div> <div style="text-align: right; margin-top: 5px;"><input type="button" value="Import"/></div>			

- Edit the parameters as required. The procedure is similar to adding a new profile. See '[Adding and Configuring a New Profile](#)' for more details.

6.1.2 Delete a Profile

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

Choose Language English Logout

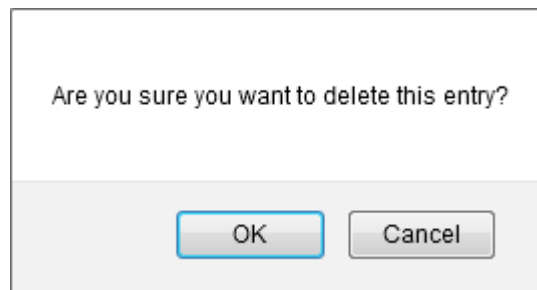
Profiles

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

Profiles for user admin

Profile Type	Profile Name	Profile Description	Owner	
Incoming E-mail	Block Zip Links		admin	
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	example incoming	Incoming	admin	
Incoming E-mail	push		admin	
Outgoing E-mail	Sales Department		admin	
Incoming E-mail	stevenprofile		admin	
Incoming E-mail	test		admin	
Incoming E-mail	Test Incoming		admin	

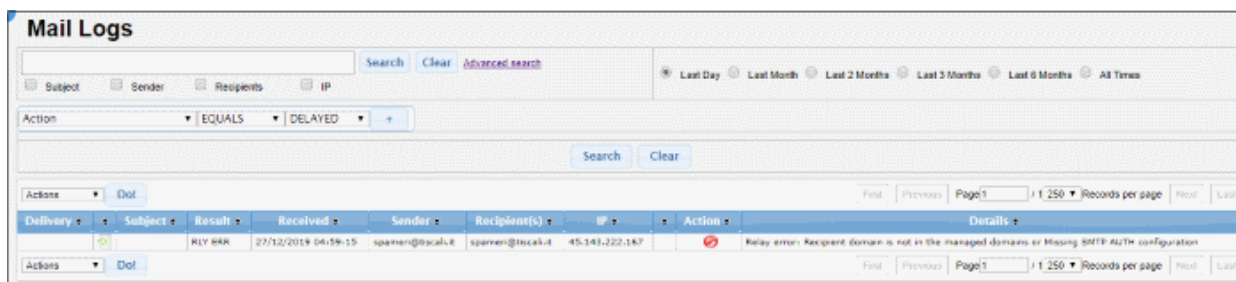
- Click 'OK' to confirm the deletion.



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

7 Reports

- The 'Reports' section in Secure Email Gateway provides comprehensive details of all mails for protected domains that were routed via Secure Email Gateway.
- 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.

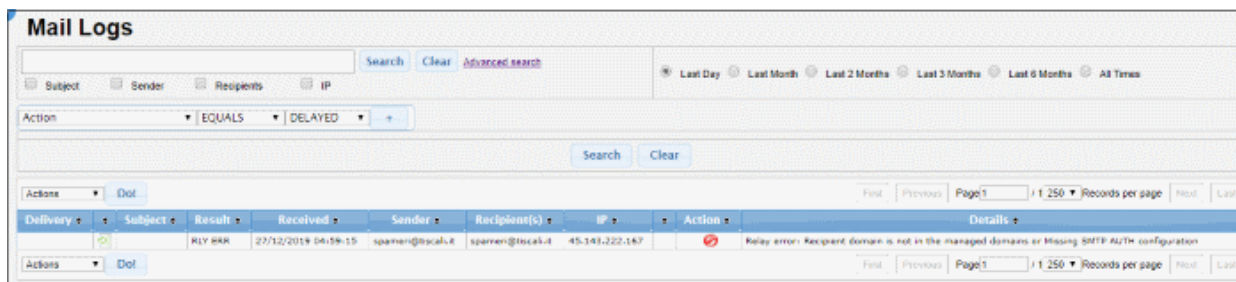






See the following sections for more details:

- [Mail Logs Report](#)
- [SMTP Queue Report](#)
- [Delivery Logs Report](#)
- [SMTP-AUTH Logs Report](#)
- [Summary Report](#)
- [Domain Report](#)
- [Attachment Verdict Reports](#)
- [Original Mail Request](#)

7.1 Mail Logs Report

- Click 'Reports' and then click 'Mail Logs'
- The 'Mail Logs' report provides complete details of incoming and outgoing mails for all domains that have been added to Secure Email Gateway.
- The logs show the subject of the mail, date and time received by Secure Email Gateway, the result of the filtering process and more.



Mail Logs Report - Table of Column Descriptions	
Column Header	Description
Delivery	Indicates the status of mail delivery. The statuses are: <ul style="list-style-type: none"> • Success • Temporary Error • Permanent Error
Icon	The arrow icon indicates whether the mail is incoming or outgoing
Subject	The content of the email subject line.
Result	The verdict on an email after filtering. For example, 'CSPAM' means Secure Email Gateway found the mail was 'Certainly Spam'.
Received	Date and time Secure Email Gateway received the email.
Sender	Email address information of the originator
Recipient(s)	Domain name of the receiver
IP	The network address of the system from where the mail was sent. The next column displays the flag of the originating country.
Action	Status of the mail after filtering. Place your mouse over an icon to view a description of the action. <ul style="list-style-type: none">  - Relayed: The mail successfully passed the filtering process and was passed onto the target mail server.  - Rejected: The mail was not accepted by Secure Email Gateway. A rejection message was sent to the sender.  - Discarded: Quarantined mail  - Delayed: Indicates the source is greylisted.
Details	Reason why a particular action was taken on a mail. For example, why it was rejected, delayed etc.

At the top and bottom of the screen, you have the option to set the number of records to be displayed per page and export the report in CSV format.

To configure the number of records to be displayed per page

- Click the 'Records per page' drop-down

First Previous Page 1 / 2 250 Records per page Next Last

Recipient(s)	IP			Details
ri@tiscali.it	204.188.205.187		Relay error: Recipient domain not found in the managed domains or Missi	
ri@tiscali.it	89.197.1.54		Relay error: Recipient domain not found in the managed domains or Missi	
ri@tiscali.it	192.110.157.9		Relay error: Recipient domain not found in the managed domains or Missi	
estcustomer.com	213.14.70.194		Classified as probable spam	
estcustomer.com	213.14.70.194		Classified as probable spam Score: 45.0	
estcustomer.com	213.14.70.194		Classified as probable spam Score: 45.0	
estcustomer.com	213.14.70.194		Classified as probable spam Score: 45.0	
estcustomer.com	213.14.70.194		Classified as probable spam Score: 45.0	
estcustomer.com	213.14.70.194		Classified as probable spam Score: 45.0	

- 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

Mail Logs

Search Clear

Subject Sender Recipients IP

Actions

Actions	Subject	Result	Received	
Save As CSV				
		RLY ERR	25/07/2018 03:05:51	spameri@t
		RLY ERR	25/07/2018 02:50:18	spameri@t
		RLY ERR	24/07/2018 22:27:14	spameri@t

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

The page at <https://demo-das.cdome.net:8443> says:

Are you sure want to save all e-mail records as CSV?

- Download and save the report to 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.

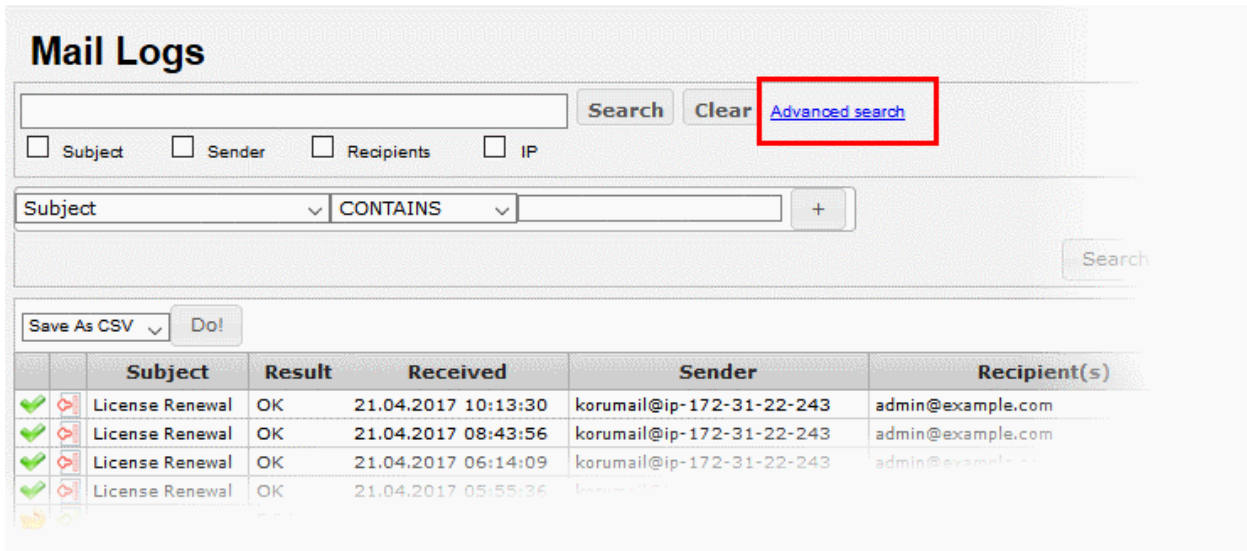
Subject	Result	Received	Sender	Re
	RLY ERR	25/07/2018 03:05:51	spameri@tiscali.it	spameri@
	RLY ERR	25/07/2018 02:50:18	spameri@tiscali.it	spameri@
	RLY ERR	24/07/2018 22:27:14	spameri@tiscali.it	spameri@
[!! PROBABLE SPAM]Incoming Li	PSPAM	24/07/2018 10:57:12	test@korumail.tk	test@te-

- To search for records based on the entries under 'Subject', 'Sender', 'Recipients' and / or 'IP' columns, enter the text or number fully or partially in the field and click the 'Search' button
- To search for records based on the entries under a particular column or columns, select the respective check boxes, enter the text or number fully or partially in the field and click the the 'Search' button. For example, if you want to search for a particular record for sender and recipients, select the 'Sender' and 'Recipients' check boxes, enter the text fully or partially in the field and click the 'Search' button.

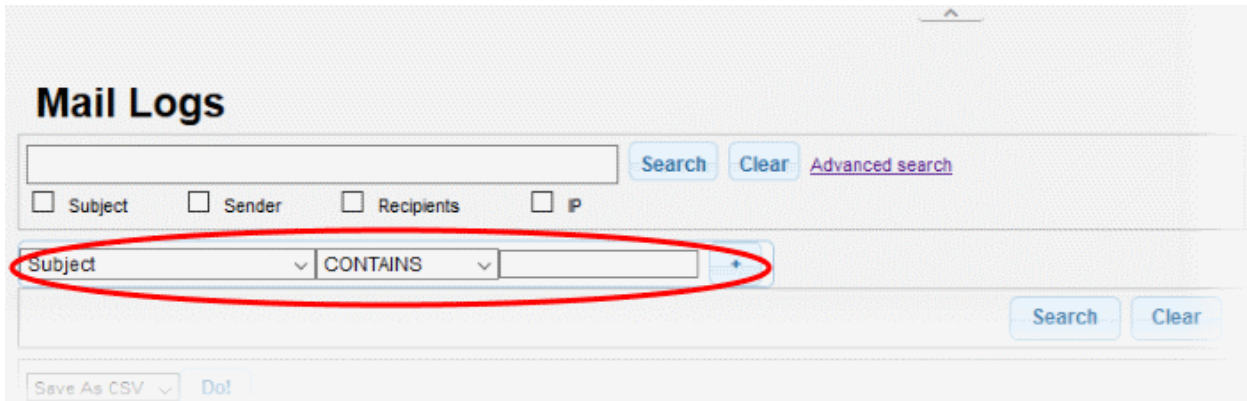
Advanced Search

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

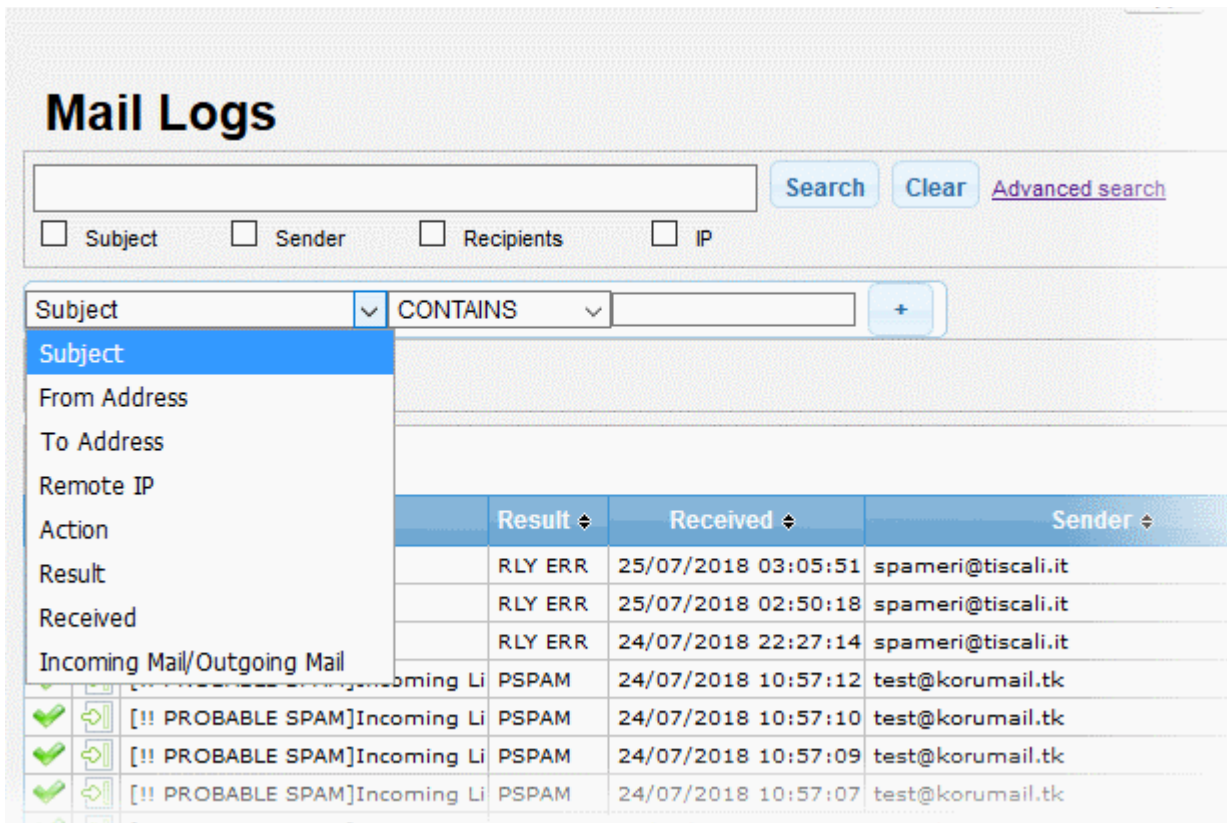
- Click the 'Advanced Search' link at the top of the screen.



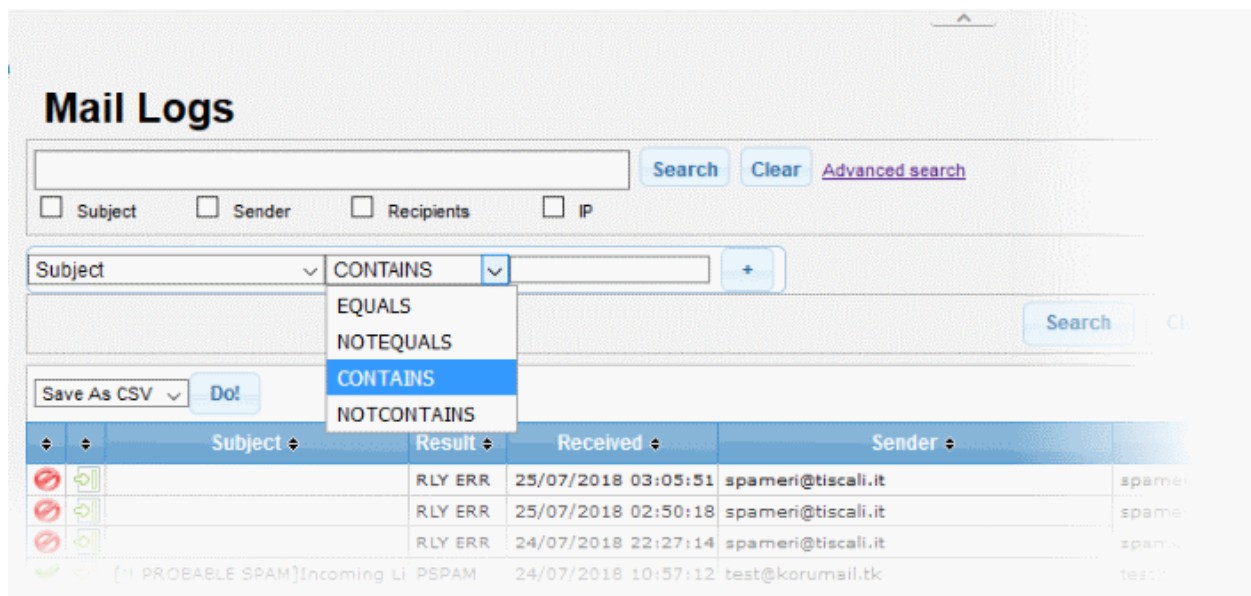
The 'Advanced Search' option will be displayed.



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



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



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

Mail Logs

[Search](#) [Clear](#) [Advanced search](#)

Subject Sender Recipients IP

Subject CONTAINS Important +

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

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

Mail Logs

[Search](#) [Clear](#) [Advanced search](#)

Subject Sender Recipients IP

Action EQUALS DELAYED +

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


Save As CSV Do!

↕	↕	Subject	Result	Received	Sender	Recipient
🚫	📧		RLY ERR	25/07/2018 03:05:51	spameri@tiscali.it	spameri@tisc
🚫	📧		RLY ERR	25/07/2018 02:50:18	spameri@tiscali.it	spameri@tisc
🚫	📧		RLY ERR	24/07/2018 22:27:14	spameri@tiscali.it	spameri@tisc

If you select 'Received' in the first column, then you can enter a date or select from the calendar.

Mail Logs

[Search](#) [Clear](#) [Advanced search](#)
 Subject Sender Recipients IP

Received EQUALS  +


Save As CSV [Do!](#)


		July, 2018									
		Sun	Mon	Tue	Wed	Thu	Fri	Sat			
		27	1	2	3	4	5	6	7		
		28	8	9	10	11	12	13	14		
		29	15	16	17	18	19	20	21	cali.it	
		30	22	23	24	25	26	27	28	cali.it	
		31	29	30	31	1	2	3	4	cali.it	
	[!! PROBABLE SPAM]Incoming Li	32	5	6	7	8	9	10	11	ail.tk	
	[!! PROBABLE SPAM]Incoming Li								Today		ail.tk
	[!! PROBABLE SPAM]Incoming Li	24/07/2018 10:57:05					test@korumail.tk				ail.tk
	[!! PROBABLE SPAM]Incoming Li	24/07/2018 10:57:07					test@korumail.tk				ail.tk
	[!! PROBABLE SPAM]Incoming Li	24/07/2018 10:57:05					test@korumail.tk				ail.tk
	[!! PROBABLE SPAM]Incoming Li	24/07/2018 10:57:03					test@korumail.tk				ail.tk
	[!! PROBABLE SPAM]Incoming Li	24/07/2018 10:57:02					test@korumail.tk				ail.tk


You can add more filters by clicking  for narrowing down your search.


Mail Logs


[Search](#) [Clear](#) [Advanced search](#)
 Subject Sender Recipients IP


Received EQUALS 



AND From Address NOTEQUALS 


OR To Address CONTAINS 


AND Remote IP EQUALS 

AND Action EQUALS DELAYED 

AND Result EQUALS ANTISPOOFING REJECT 

AND Received EQUALS  

AND 

OR 

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

You can remove a filter by clicking the  button beside it.

You can create a filter rule by selecting 'AND' or 'OR' option beside each of the added filter.

- Click 'Clear' to remove the advanced search rules.
- Click 'Search' to start the search per the filter rule.

The items will be searched for in the ascending order and results displayed.

- To remove the advanced search field, click the 'Advanced search' link again.

Administrators can filter results on monthly basis. The filters available are 'Last Month', 'Last 2 Months', 'Last 3 Months', 'Last 6 Months' and 'All Times'.

Last Month
 Last 2 Months
 Last 3 Months
 Last 6 Months
 All Times

Details of a Log Entry

- Clicking anywhere on the row of a log record will display the details of the mail log.

Mail Logs ✕

Received	25/07/2018 02:50:18
Queue ID	19759-1532487018-533437
Message ID	
Action	
Result	RELAY ERROR
Score	0.0
Sender	spameri@tiscali.it Add Email In Black List
Recipient(s)	spameri@tiscali.it
RFC2822 Sender	
RFC2822 Recipient(s)	
Subject	
IP	89.197.1.54 Add Black List
Location	London, England, United Kingdom
Size	0
Matched Profile	Default Incoming Profile (defined by user: admin)
Details	Relay error: Recipient domain is not in the managed domains or Missing SMTP AUTH configuration
Relayed	No

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 Secure Email Gateway.

- To add the sender or domain to blacklist/whitelist, click the drop-down in the 'Sender' row.

Sender	spameri@tiscali.it Add Email In Black List
Recipient(s)	spameri@tiscali.it
RFC2822 Sender	
RFC2822 Recipient(s)	
Subject	

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

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

The changes will be saved and mails from the sender will be applied the new settings by Secure Email Gateway.

- To add the originating IP to blacklist/whitelist, click the drop-down in the 'IP' row.

RFC2822 Recipient(s)	
Subject	
IP	192.110.157.9 Add Black List
Location	Graham, Washin Add Black List
Size	0 Add White List
Matched Profile	Default Incoming Profile (defined by user: admin)
Details	Relay error: Recipient domain is not in the managed domains or Missing SMTP AUTH configuration

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

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

The changes will be saved and mails from the IP will be applied the new settings by Secure Email Gateway.

You can view the previous or next record by click the buttons at the top of a details screen.

7.2 SMTP Queue Report

- Click 'Reports' > 'SMTP Queue'.
- The 'SMTP Queue' report shows details of mails that are queued for delivery.

SMTP Queue

Choose Language: English | English | Login

Total messages: 28
 Messages with local recipients: 0
 Messages with remote recipients: 28
 Messages with bounces: 0
 Messages with in process: 0

Re-process queue | Page 1 / 1 | 100 Records per page | Next | Last

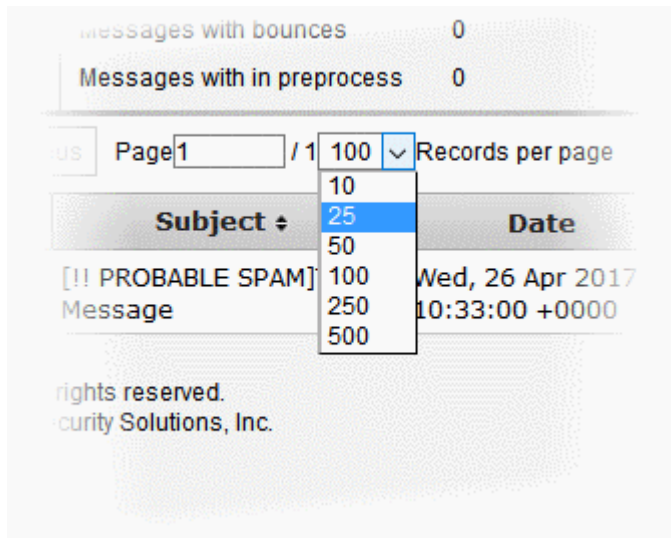
ID	From	To	Subject	Date	Size	Action
41997408	"test@testcustomer.com" <test@testcustomer.com>	"test@example.com" <test@example.com>	Incoming Limit	Tue, 24 Jul 2018 10:54:47 +0000	1.07 KB	
41997422	"test@korumail.tk" <test@korumail.tk>	"test@testcustomer.com" <test@testcustomer.com>	[!] PROBABLE SPAM]Incoming Limit	Tue, 24 Jul 2018 10:57:01 +0000	1.12 KB	
41997418	mailer-daemon@ip-172-31-25-154	test@testcustomer.com	failure notice	24 Jul 2018 11:23:04 -0000	1.71 KB	
41997483	"test@example.com" <test@example.com>	"test@testcustomer.com" <test@testcustomer.com>	Incoming Limit	Tue, 24 Jul 2018 10:53:15 +0000	1.08 KB	
41997451	"test@example.com" <test@example.com>	"test@testcustomer.com" <test@testcustomer.com>	Incoming Limit	Tue, 24 Jul 2018 10:52:43 +0000	1.08 KB	
41997482	"test@example.com" <test@example.com>	"test@testcustomer.com" <test@testcustomer.com>	Incoming Limit	Tue, 24 Jul 2018 10:53:13 +0000	1.08 KB	
41997437	"test@testcustomer.com" <test@testcustomer.com>	"test@example.com" <test@example.com>	Incoming Limit	Tue, 24 Jul 2018 10:54:44 +0000	1.07 KB	
41997412	mailer-daemon@ip-172-31-25-154	test@testcustomer.com	failure notice	24 Jul 2018 11:03:02 -0000	1.71 KB	
41997427	"test@korumail.tk" <test@korumail.tk>	"test@testcustomer.com" <test@testcustomer.com>	[!] PROBABLE SPAM]Incoming Limit	Tue, 24 Jul 2018 10:57:10 +0000	1.12 KB	
41997412	"test@korumail.tk" <test@korumail.tk>	"test@testcustomer.com" <test@testcustomer.com>	[!] PROBABLE SPAM]Incoming Limit	Tue, 24 Jul 2018 10:56:56 +0000	1.12 KB	
41997426	"test@korumail.tk" <test@korumail.tk>	"test@testcustomer.com" <test@testcustomer.com>	[!] PROBABLE SPAM]Incoming Limit	Tue, 24 Jul 2018 10:57:08 +0000	1.12 KB	
41997475	mailer-daemon@ip-172-31-25-154	test@testcustomer.com	failure notice	24 Jul 2018 11:23:08 -0000	1.71 KB	
41997421	"test@korumail.tk" <test@korumail.tk>	"test@testcustomer.com" <test@testcustomer.com>	[!] PROBABLE SPAM]Incoming Limit	Tue, 24 Jul 2018 10:56:59 +0000	1.12 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	The content of the email subject line.
Date	Date and time that the mail was sent
Size	Size of the file in kilobytes
Action	Delete the mail from the SMTP queue

At the top and bottom of the screen you have the option to set the number of records to be displayed per page.

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 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.

7.3 Delivery Logs Report

While **'Mails Logs'** record all incoming and outgoing mail traffic, 'Delivery Logs' record only those mails accepted by mail servers.

- Click 'Reports' > 'Delivery Logs' to open the interface

Delivery Logs						
<input type="text"/>			<input type="button" value="Search"/>	<input type="button" value="Clear"/>	Advanced search	
<input type="checkbox"/> Sender	<input type="checkbox"/> Recipients	<input type="checkbox"/> IP				
			<input type="button" value="First"/>	<input type="button" value="Previous"/>	Page 1 / 1	<input type="button" value="Next"/>
			250		Records per page	<input type="button" value="Last"/>
Result	Received	Sender	Recipient(s)	IP	Details	
	18/11/2019 09:21:46	korumail@deme-das.cdome.net	ilyas.pala@comodo.com	178.255.82.9	250 OK 1574068906 queupid 11619	
	18/11/2019 09:15:04	korumail@deme-das.cdome.net	ilyas.pala@comodo.com	178.255.82.9	451 Greylisting activated for 18.194.124.124, please try again soon	

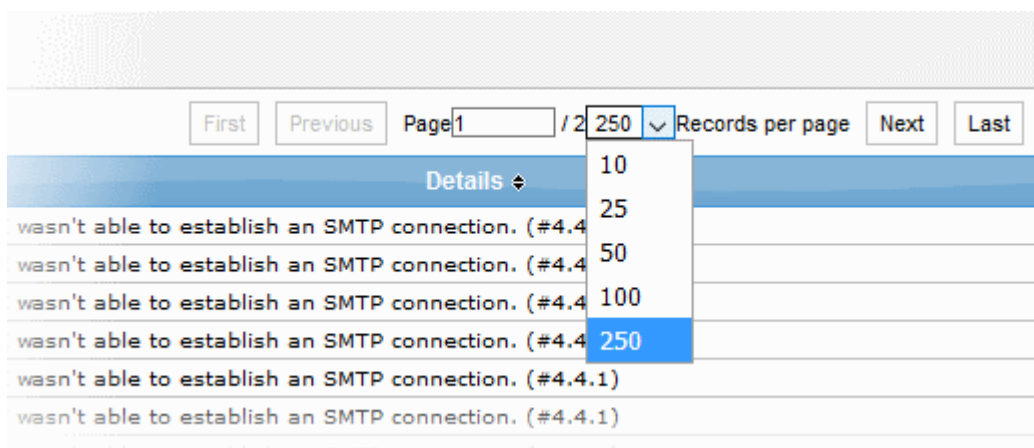
Delivery Logs Report - Table of Column Descriptions	
Column Header	Description
Result	Indicates the status of the mail processed by mail server. The tool tip on hovering the mouse cursor over an icon displays the action. - Success: Indicates the mail has been successfully delivered to the recipient. - Permanent Error: Indicates the mail server failed to deliver the mail to the recipient. - Temporary: Indicates it is temporary error and the server will try again to deliver.
Received	Date and time Secure Email Gateway received the email.
Sender	Email address information of the originator
Recipient(s)	Email address information of the receiver

IP	The network address of the system from where the mail was sent. The next column displays the flag of the originating country.
Details	Provides information such as the message ID and reasons for permanent and temporary error

At the top and bottom of the screen, you have the option to set the number of records to be displayed per page.

To configure the number of records to be displayed per page

- Click the 'Records per page' drop-down



- 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.

7.4 SMTP-AUTH Logs Report

The 'SMTP-AUTH Logs Report' contains logs of every SMTP client log-in that required authentication.

- Click reports then 'SMTP-AUTH Logs' to open the interface.

SMTP-AUTH Logs				
User <input type="text"/>				
IP <input type="text"/>				
Date From <input type="text"/>				
Date To <input type="text"/>				
Result <input type="text" value="-Choose-"/>				
<input type="button" value="Search"/> <input type="button" value="Clear"/>				
<input type="button" value="First"/> <input type="button" value="Previous"/> <input type="text" value="Page 1"/> / <input type="text" value="1"/> <input type="text" value="100"/> Records per page <input type="button" value="Next"/> <input type="button" value="Last"/>				
Date	IP		User	Result
25/12/2019 12:18:27	158.69.182.96		guest@ec2-18-194-134-124.eu-central-1.compute.amazonaws.com	FAILED
25/12/2019 12:18:12	158.69.182.96		guest@ec2-18-194-134-124.eu-central-1.compute.amazonaws.com	FAILED
25/12/2019 12:17:53	158.69.182.96		guest@ec2-18-194-134-124.eu-central-1.compute.amazonaws.com	FAILED
25/12/2019 12:17:37	158.69.182.96		guest@ec2-18-194-134-124.eu-central-1.compute.amazonaws.com	FAILED
25/12/2019 12:17:22	158.69.182.96		guest@ec2-18-194-134-124.eu-central-1.compute.amazonaws.com	FAILED
25/12/2019 12:17:07	158.69.182.96		guest@ec2-18-194-134-124.eu-central-1.compute.amazonaws.com	FAILED
25/12/2019 12:16:53	158.69.182.96		guest@ec2-18-194-134-124.eu-central-1.compute.amazonaws.com	FAILED
25/12/2019 12:16:39	158.69.182.96		guest@ec2-18-194-134-124.eu-central-1.compute.amazonaws.com	FAILED

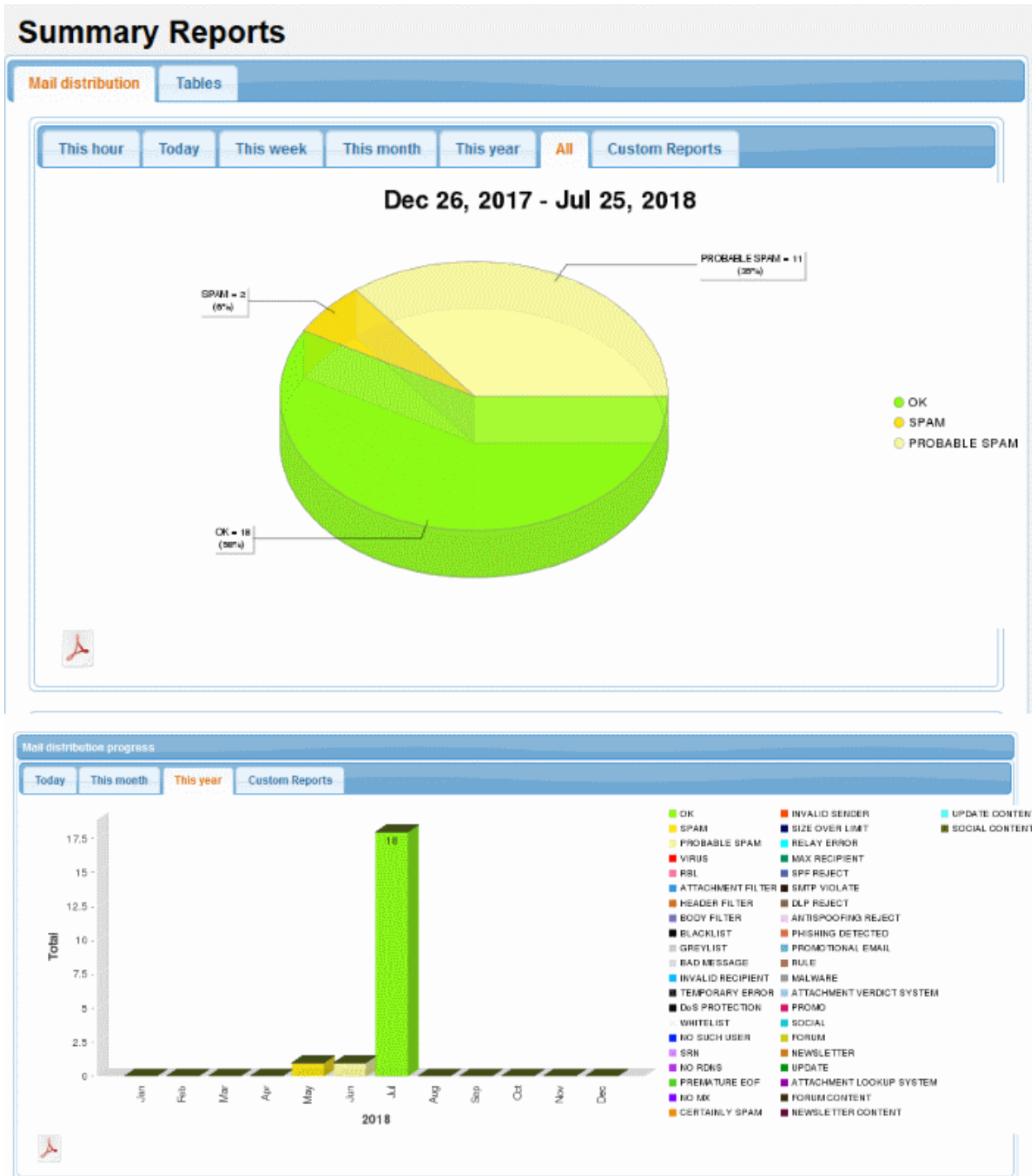
SMTP-AUTH Logs Report - Table of Column Descriptions	
Column Header	Description
Result	Indicates the status of the mail processed by SMTP mail server. Success : Indicates that the SMTP client has logged in successfully Failed: Indicates that the SMTP client login has failed
User	The name of the SMTP mail client
IP	The network address of the SMTP mail client
Date	Date and time information of the event log

The 'Search' options allows you to search for a particular record or records based on the 'User', 'IP', 'Date From', 'Date To' or 'Result' of the authentication of SMTP client log-in.

- 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'.

7.5 Summary Reports

- Click 'Reports' and then click 'Summary Reports'
- The 'Summary Reports' screen in Secure Email Gateway 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 daily, weekly, monthly, yearly, full from the time of installation and custom reports.
- The lower portion displays the results in bar chart format and is available on hourly, monthly and yearly basis.



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

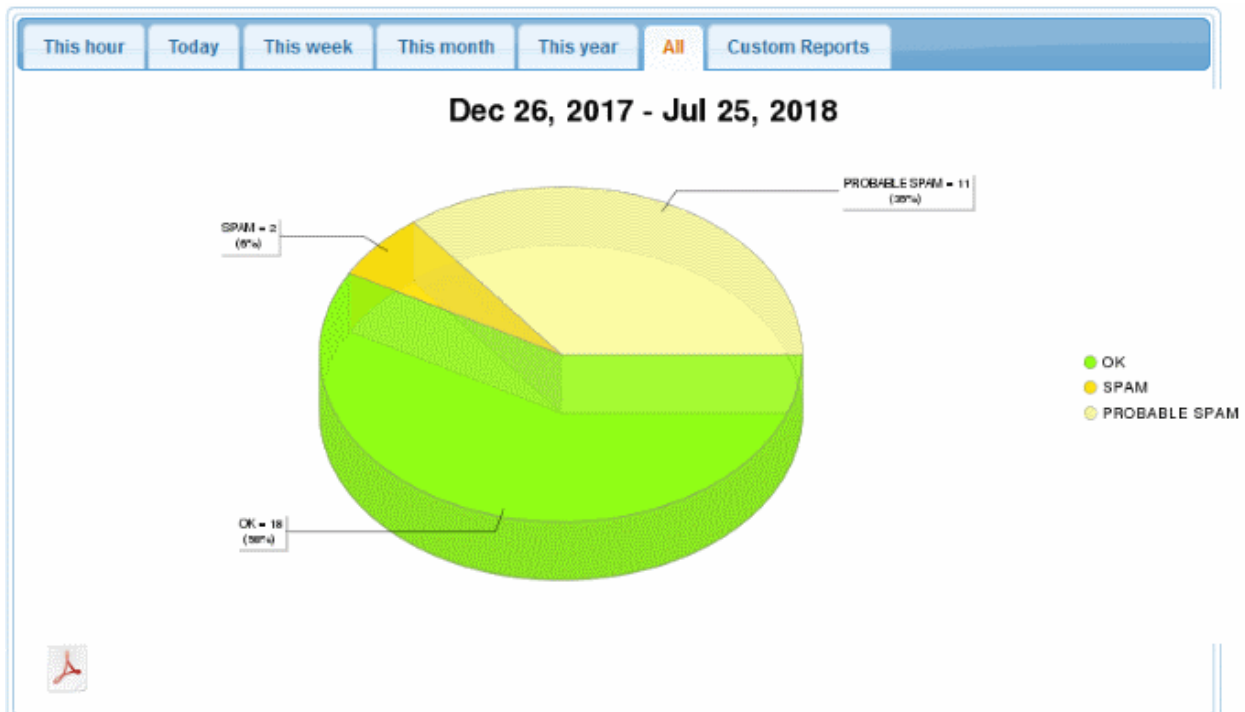
The results in **pie chart** format at the top and **bar chart** format at the bottom will be displayed.

- 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 daily, weekly, monthly, yearly and the time of Secure Email Gateway installation. You can also view reports for a customized duration by entering the required dates.

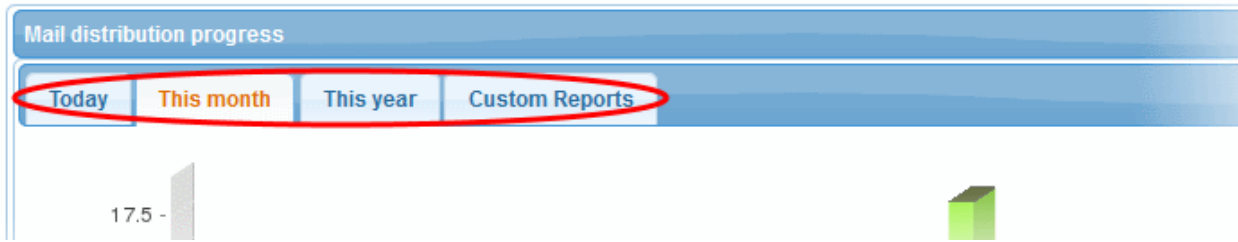


The different segments of the pie chart provides the details of the filtering results for the selected period such as mails categorized as spam, phishing, blacklisted and so on.

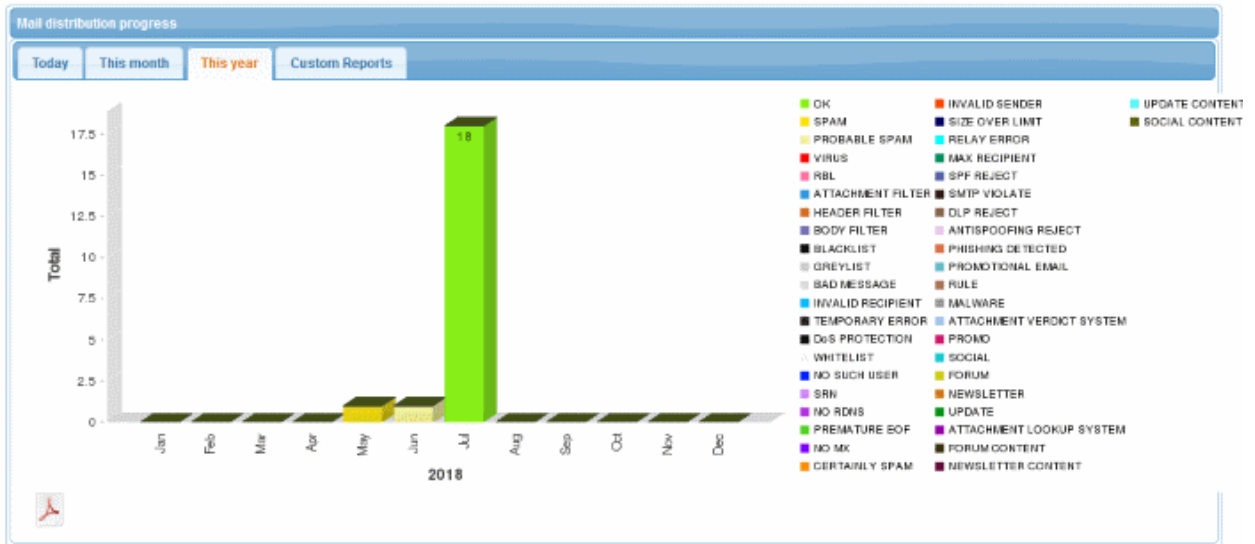
- To download the pie chart results, click the PDF icon  and save the PDF file to your system.

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 pie chart results, click the PDF icon  and save the PDF file to your system.

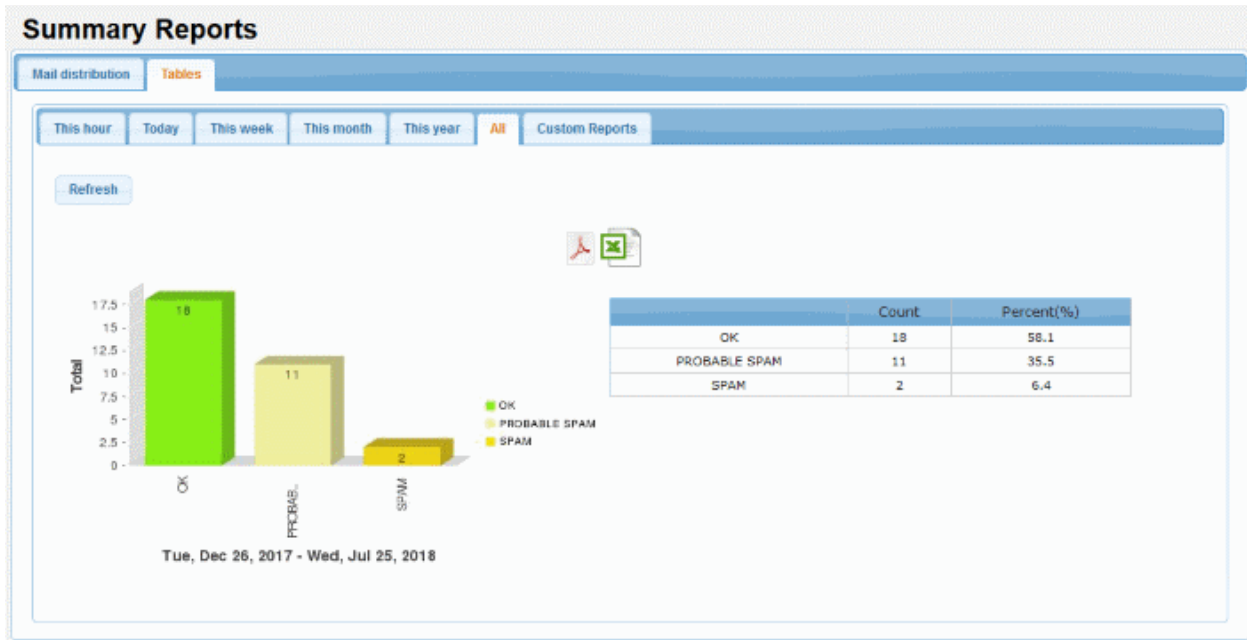
To view and download the report in table format

- 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 Secure Email Gateway 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.



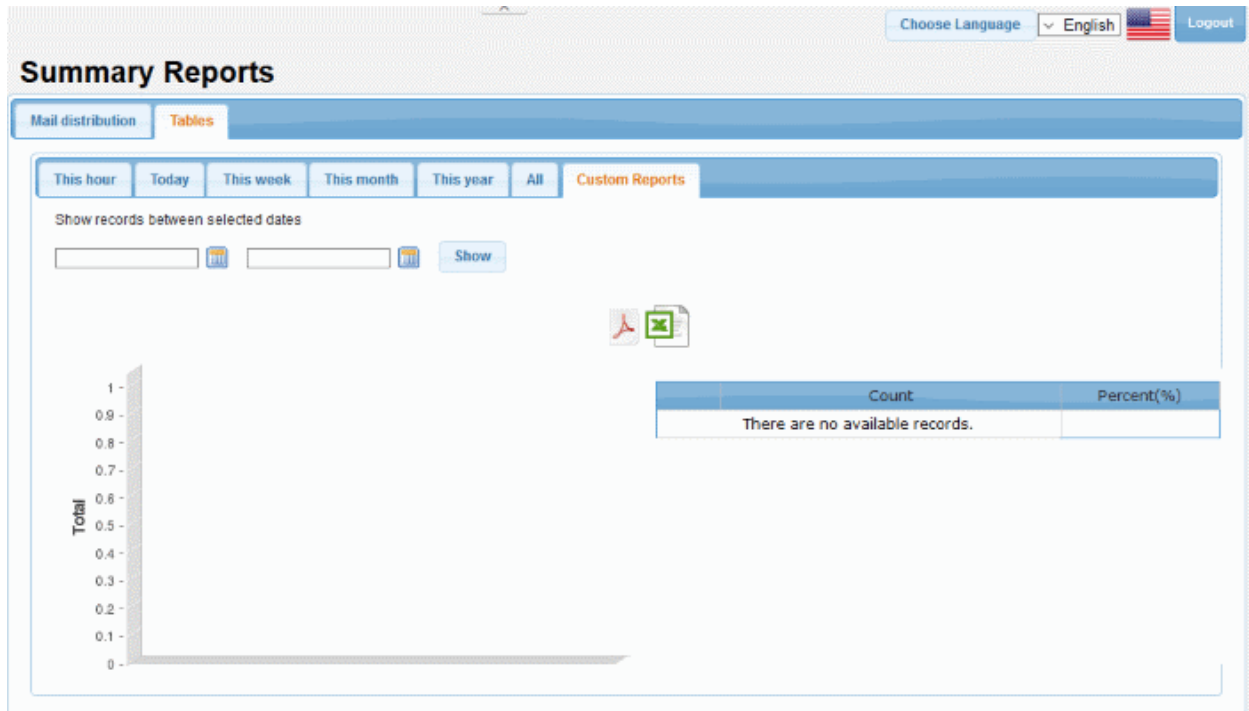
The report for the selected period will be displayed. The first column indicates the categorization of mails, the second column displays the number for each category and the third column provides the results in percentage for each category.

- To download the bar chart results, click the PDF icon 
- To download the report in XLS (spreadsheet) format, click the XLS icon 
- The pdf and xls files will be downloaded to the local folder.

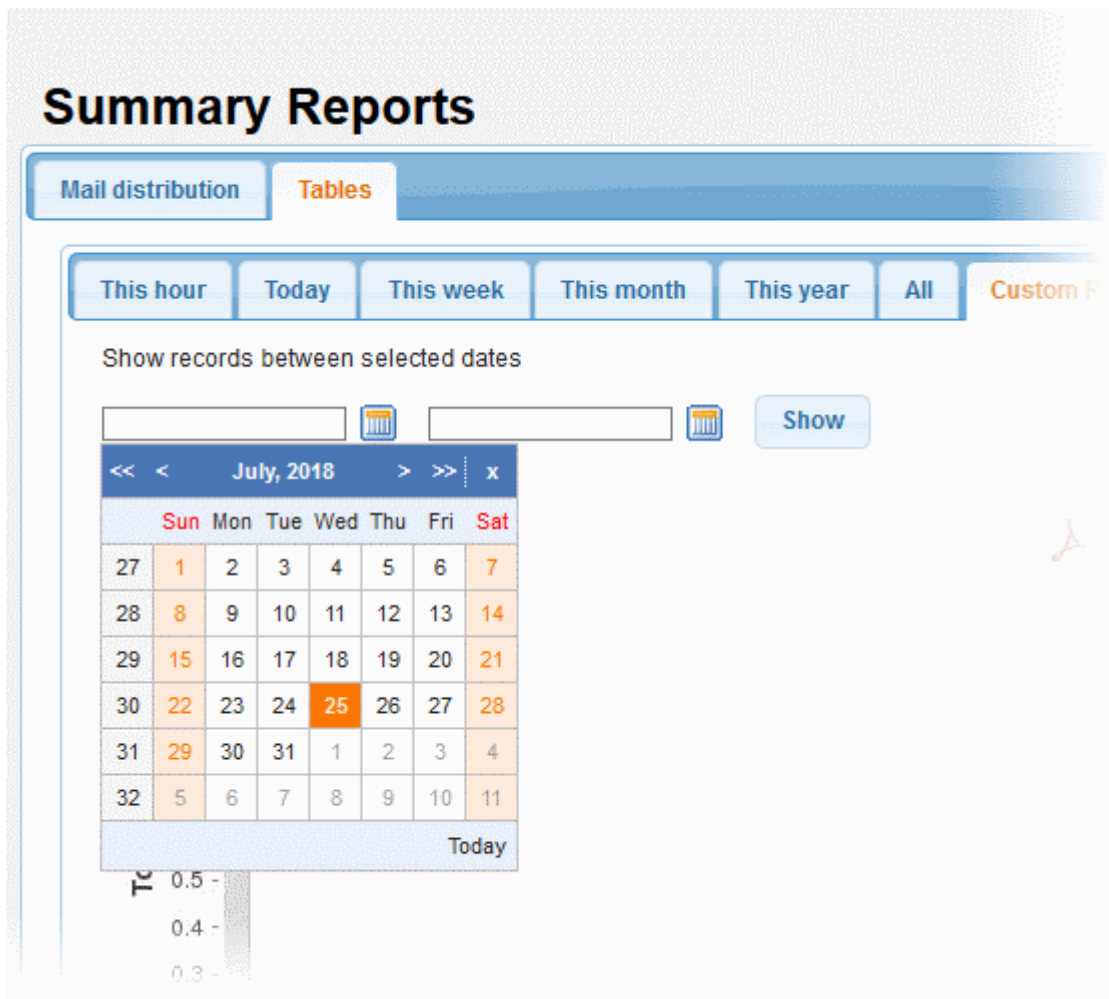
To generate a custom report in table format

- Click the 'Custom Reports' tab at the top

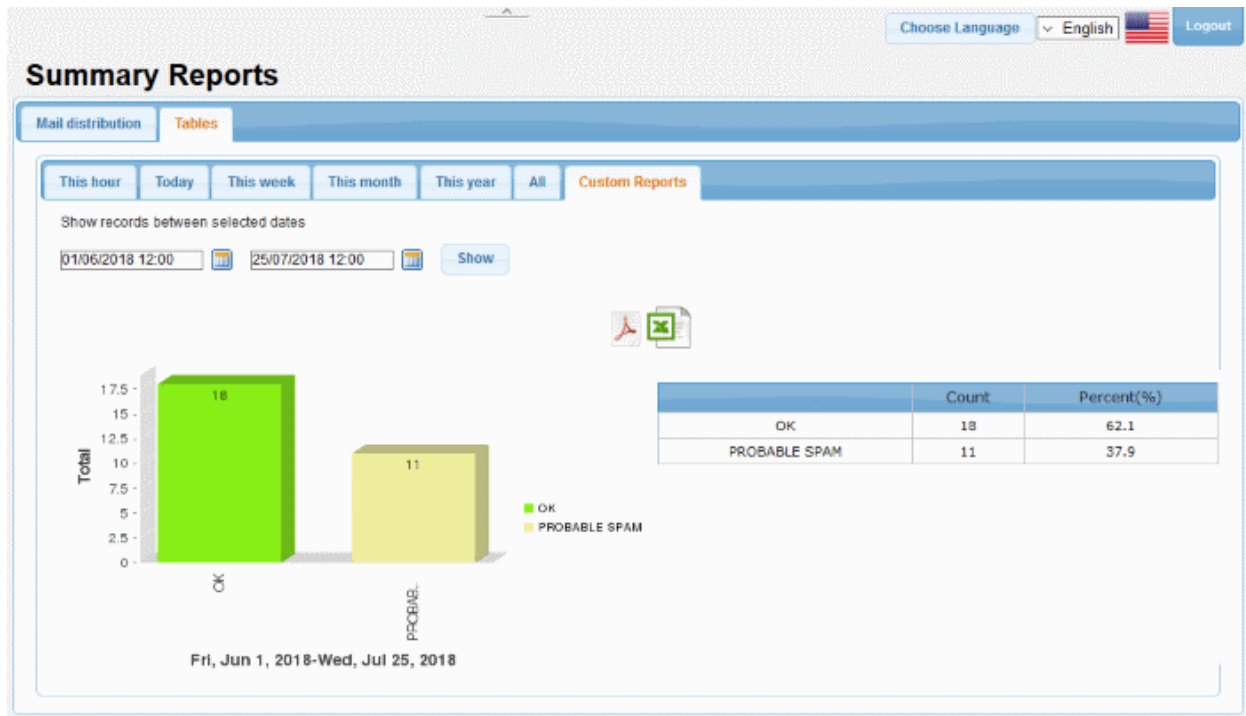
The fields to select the 'From' and 'To' period will be displayed.





- 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.

Summary Reports

Mail distribution **Tables**

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

Show records between selected dates

01/06/2018 12:00 25/07/2018 12:00 Show

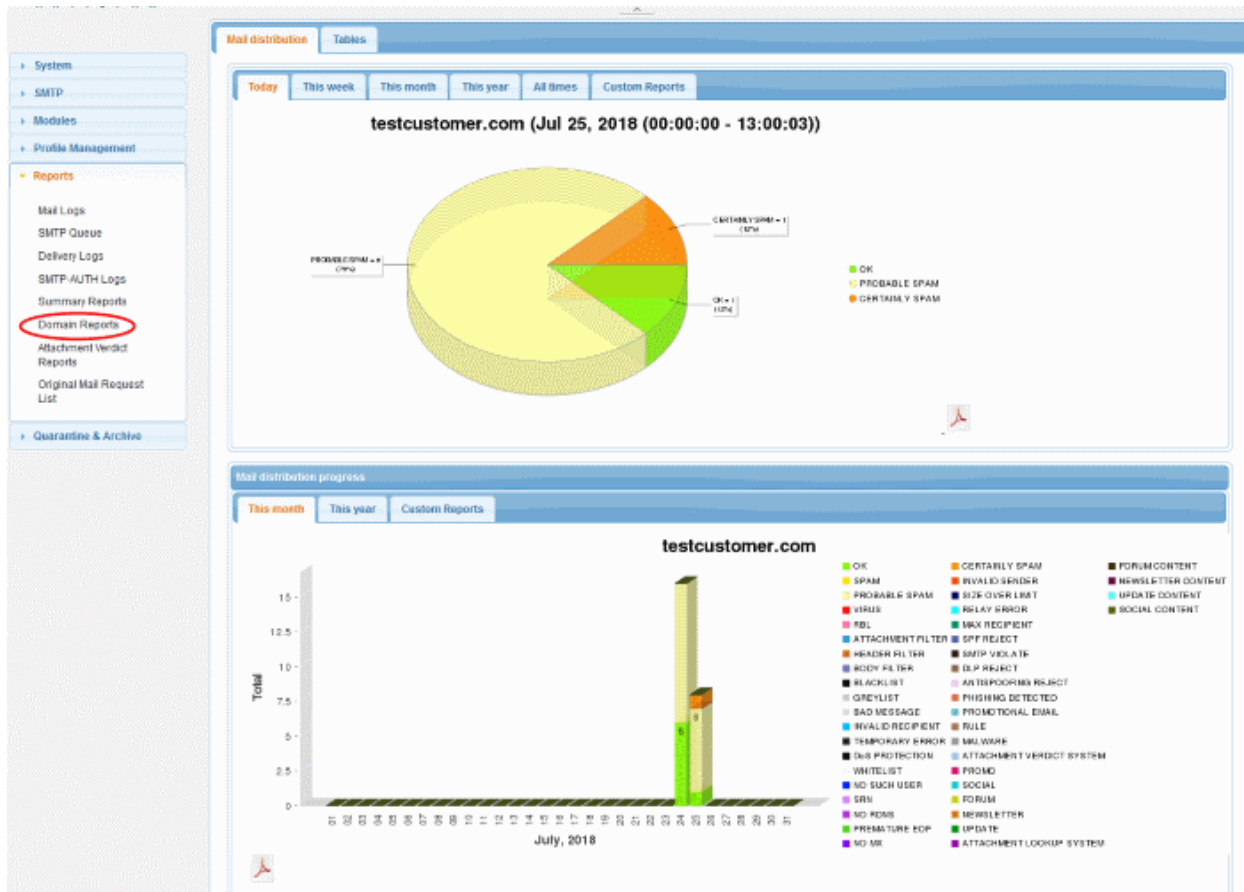
April, 2018						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
14	1	2	3	4	5	6
15	8	9	10	11	12	13
16	15	16	17	18	19	20
17	22	23	24	25	26	27
18	29	30	1	2	3	4
19	6	7	8	9	10	11
01/06/2018	Clean	12:00	Today			

Legend:
■ OK
■ PROBABLE SPAM

7.6 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.

- Click the PDF icon  and download the report to PDF, 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: testcustomer.com Get reports!

Mail distribution Tables

Today This week This month This year All times Custom Reports

Show records between selected dates

25/07/2018 12:59 25/07/2018 12:59 Show

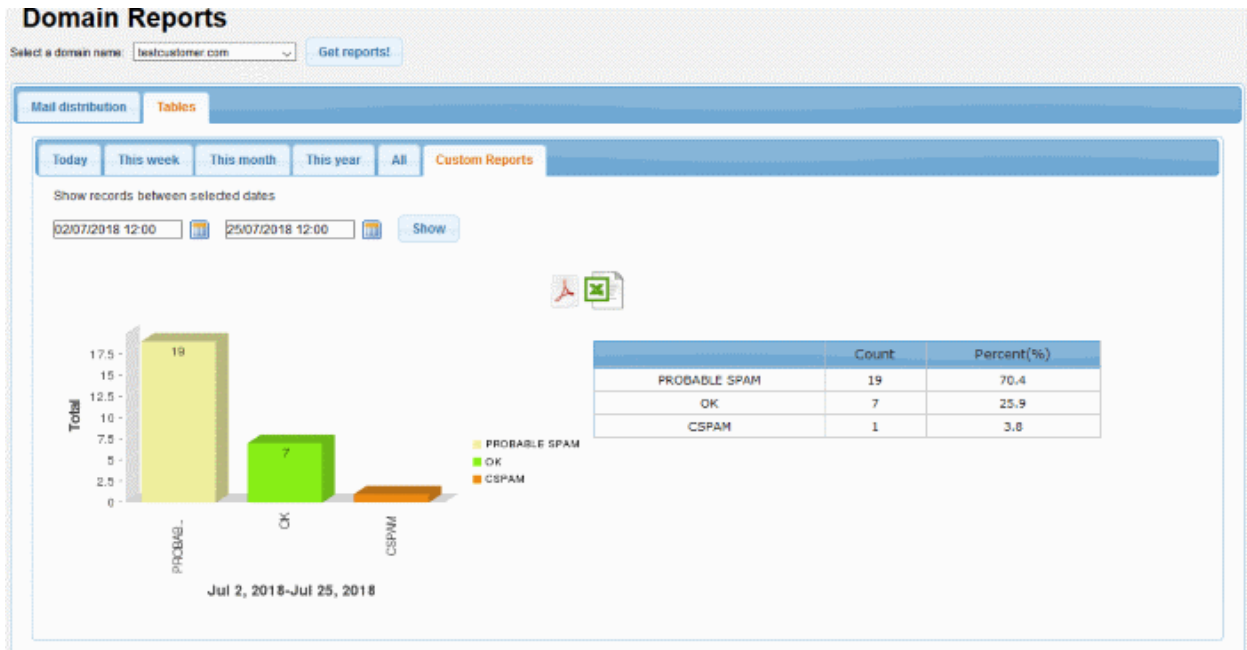
July, 2018

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	1	2	3	4	5	6
28	8	9	10	11	12	13
29	15	16	17	18	19	20
30	22	23	24	25	26	27
31	29	30	31	1	2	3
32	5	6	7	8	9	10



25/07/2018 Clean 12:59 Today

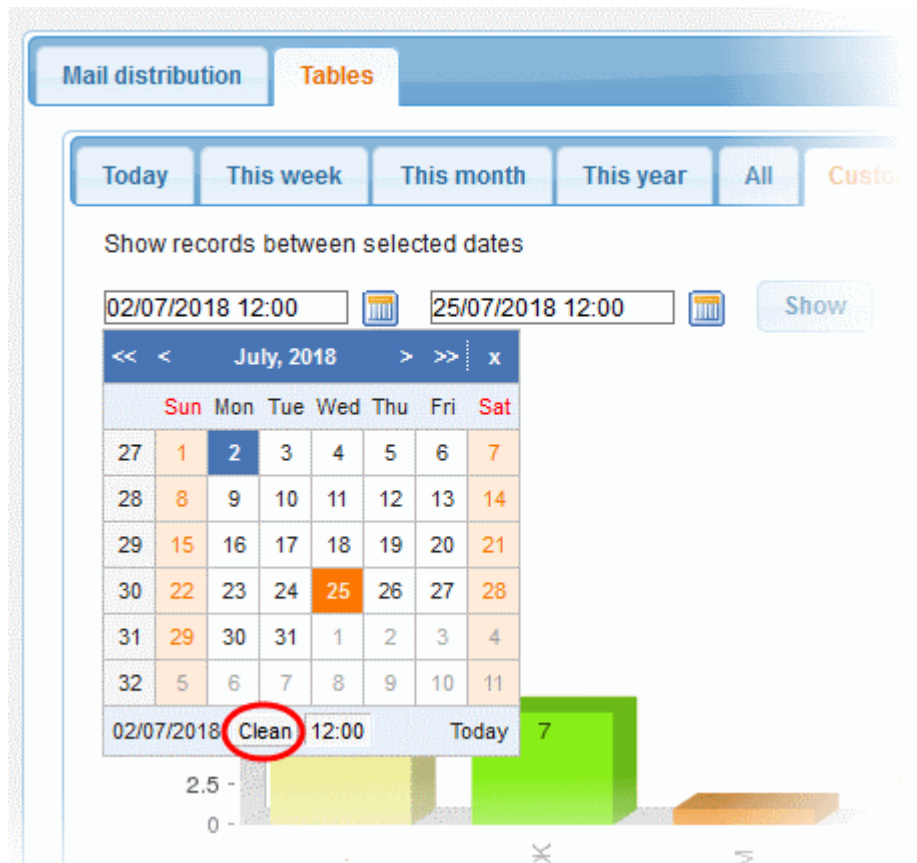
- Click on the fields or calendar icon and select the period from the calendar.

- Click 'Show' after selecting the custom period.



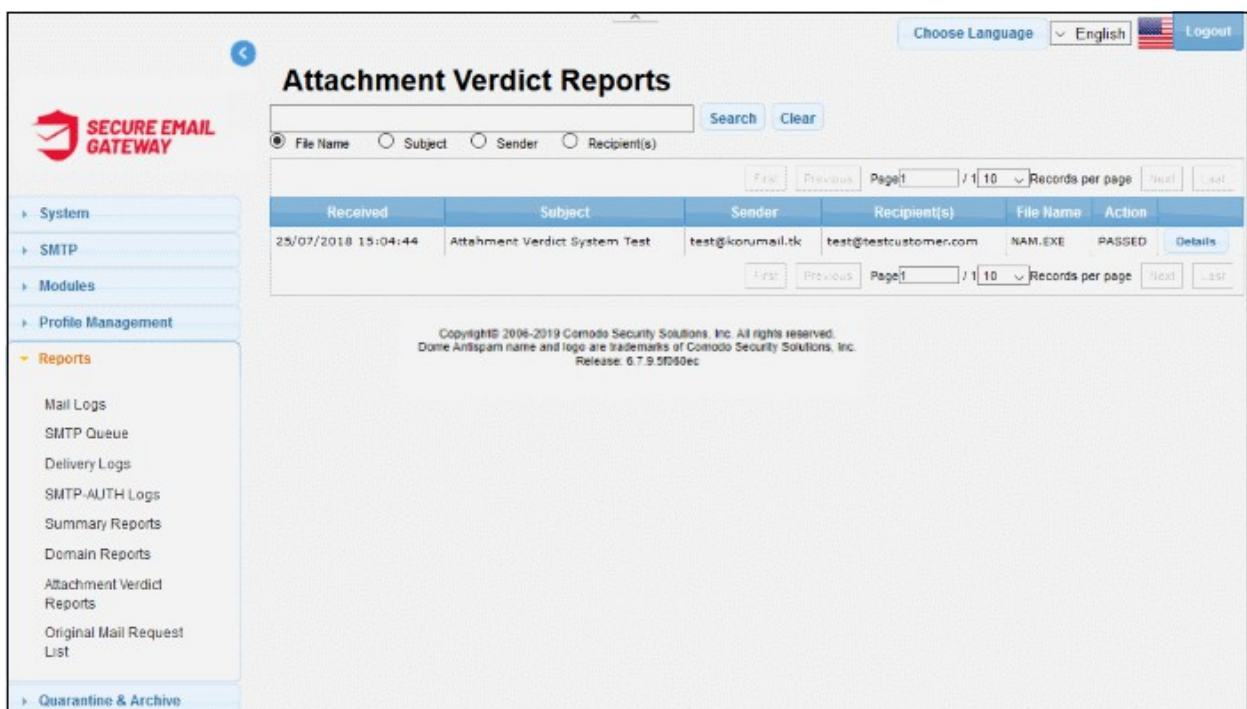
The report for the selected custom period will be displayed. The first column indicates the categorization of mails, the second column displays the number for each category and the third column provides the results in percentage for each category.

- 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.



7.7 Attachment Verdict Reports

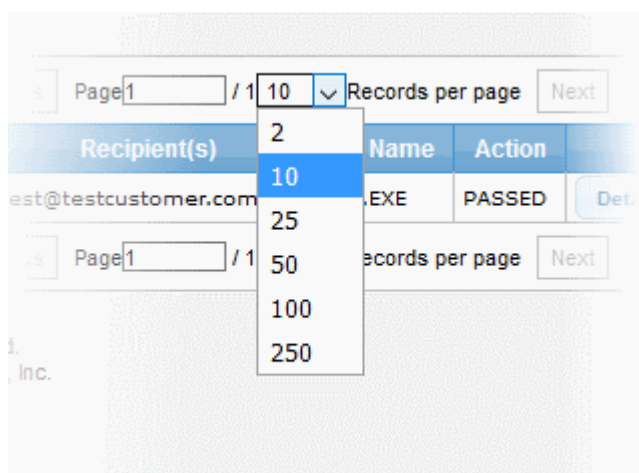
- Click 'Reports' on the left then click 'Attachment Verdict Reports'.
- The 'Attachment Verdict Reports' interface contains all the email attachment files for which Secure Email Gateway has returned a verdict and the corresponding actions taken.



Attachment Verdict Report - Table of Column Descriptions	
Column Header	Description
Received	Date and time of email received by Secure Email Gateway.
Subject	Content in the 'Subject' line of the mails containing attachment.
Sender	Domain details of the email sender.
Recipient(s)	Domain name of the receiver
File Name	File that is given a verdict.
Action	Result of the valkyrie analysis verdict. For example 'Passed' or 'Rejected'

To configure the number of records to be displayed per page

- Click the 'Records per page' drop-down



- 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.

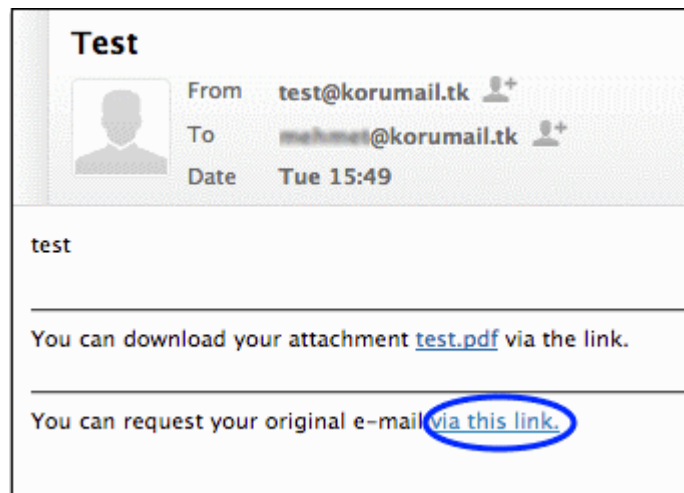
The 'Search' options allows you to search for a particular record or records based on the 'Filename', 'Subject', 'Sender' or 'Recipient(s)' of the file with verdict.

- 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 'Search'
- To refresh search, click 'Clear'.

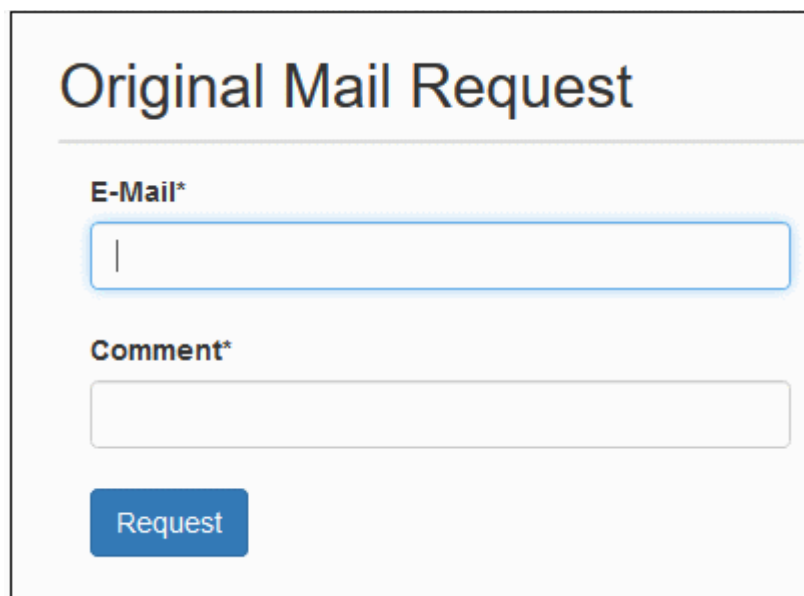
7.8 Original Mail Request

- Click 'Reports' > 'Original Mail Request List' to view this interface.
- Secure Email Gateways' containment feature replaces untrusted attachments with a link that allows the recipient to download a 'safe' version of the file. The safe version will open inside a secure container on the user's computer.
- The 'Original Mail Request' feature lets recipients download the original version of a mail IF its attachments get contained.

- Recipients can request the original by clicking a link in their email. The request must then be approved by an admin before the mail is released.



- Click the original email link and complete the short request form:



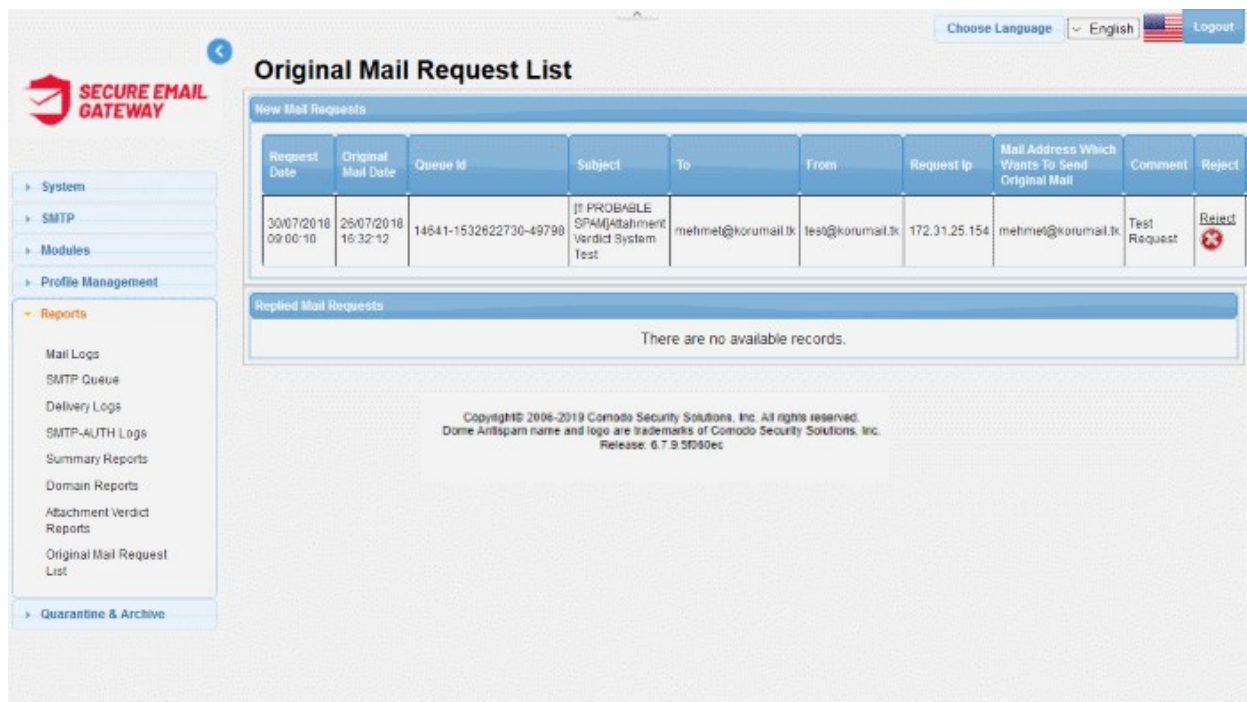
Original Mail Request

E-Mail*

Comment*

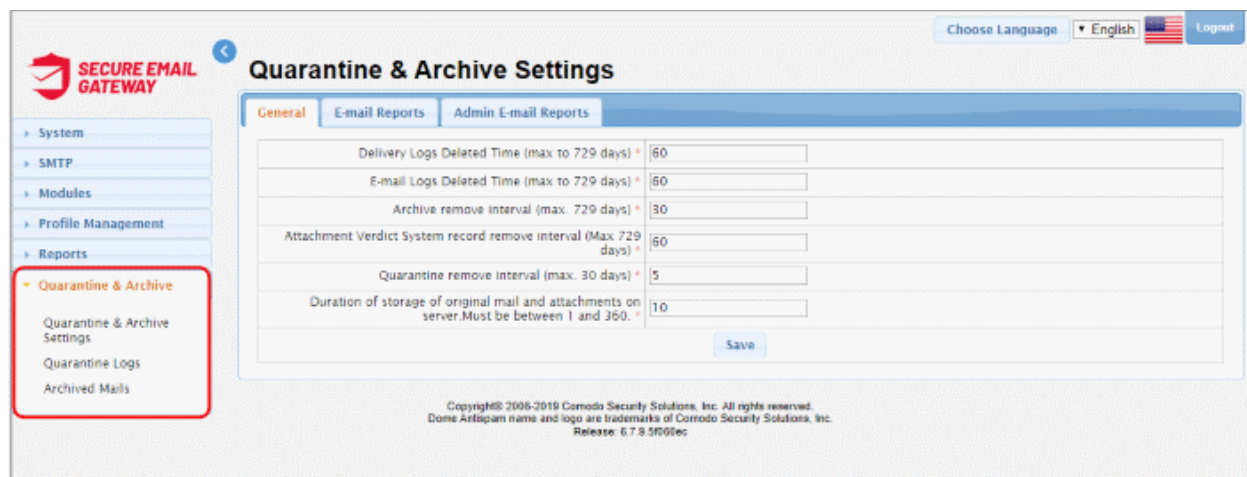
Request

- Administrators can approve or reject the request in 'Reports' > 'Original Mail Request List':



8 Quarantine & Archive

- The 'Quarantine & Archive' sections allows administrators to configure the number of days that logs and archived files should be retained in Secure Email Gateway.
- 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](#)

8.1 Quarantine & Archive Settings

- Click 'Quarantine & Archive' > 'E-mail Reports'
- End-users can view their quarantined emails in the web interface.
- The 'Email Report' section allows administrators to configure the URL of the 'Quarantine Webmail' page. You can also configure the email notification subject line, from address, body text, and the time the mail should be sent out.
- To enable quarantine reports:
 - Activate 'Send daily quarantine report to recipients' in the '**Archive And Quarantine**' tab of the profile applied to your users.

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

Click the following links for more details:

- [Quarantine & Archive General Settings](#)
- [Email Reports Settings](#)

8.1.1 Quarantine & Archive General Settings

- Click 'Quarantine & Archive' > 'Quarantine & Archive Settings'
- The 'Quarantine & Archive Settings' interface lets you set retention periods for mail logs, quarantine logs and archived mail.
- You can also set the method of user authentication. This is required for users to access their quarantined messages in the webmail interface.

Choose Language English Logout

Quarantine & Archive Settings

General
E-mail Reports
Admin E-mail Reports

Delivery Logs Deleted Time (max to 729 days) *	<input type="text" value="60"/>
E-mail Logs Deleted Time (max to 729 days) *	<input type="text" value="60"/>
Archive remove interval (max. 729 days) *	<input type="text" value="30"/>
Attachment Verdict System record remove interval (Max 729 days) *	<input type="text" value="60"/>
Quarantine remove interval (max. 30 days) *	<input type="text" value="5"/>
Duration of storage of original mail and attachments on server. Must be between 1 and 360. *	<input type="text" value="10"/>

Save

Quarantine & Archive General Settings - Table of Parameters	
Parameter	Description
Delivery Logs Deleted Time	Enter the number of days for which the email delivery logs will be retained. The maximum period is 729 days. See 'Delivery Logs Report' for more details.
E-mail Logs Deleted Time	Enter the number of days for which the email logs will be retained. The maximum period is 729 days. See 'Mail Logs Report' for more details.
Archive remove interval	Enter the number of days for which the archived mail records will be retained. The maximum period is 729 days. See 'Archived Mails' for more details.
Attachment Verdict System record remove Interval	Enter the number of days for which the Attachment verdict records will be retained. The maximum period is 729 days. See 'Attachment Verdict System' for more details.
Quarantine remove interval	Enter the number of days after which the 'Quarantined Logs' will be removed. The maximum period that can be set is 30 days. See 'Quarantine Logs' for more details.
Duration of storage of original mail and attachments on server	This setting pertains to Containment. Specify the number of days that emails including attachments should be retained on SEG server. The period should be between 1 and 360 days. Original emails and contained attachments are deleted after this period.

- Click 'Save' to apply your changes.

8.1.2 Email Reports Settings

- Click Quarantine & Archive' tab > 'E-mail Reports' tab in the 'Quarantine & Archive' screen.
- Secure Email Gateway 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.
- 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.

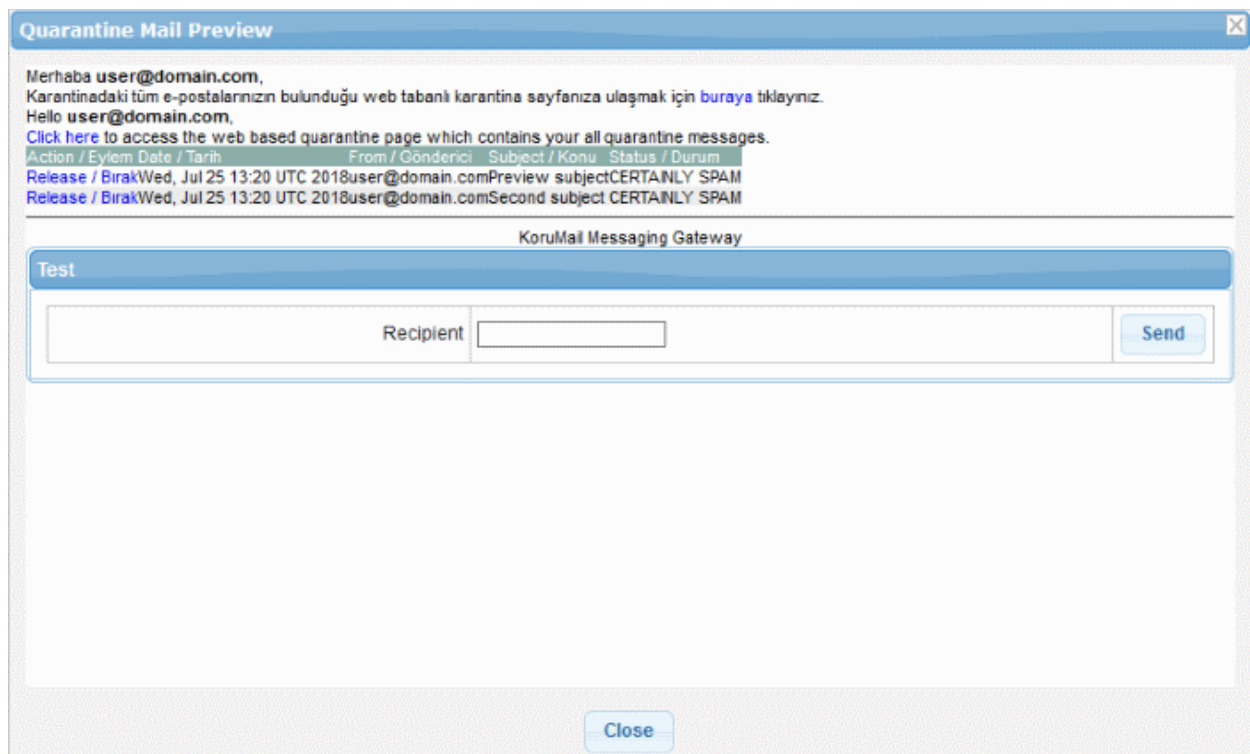
Quarantine & Archive Settings

General
E-mail Reports
Admin E-mail Reports

Mail Subject	<input type="text" value="E-mail Quarantine Re"/>
Mail From	<input type="text" value="korumail@ip-172-31-25-1"/>
Base URL	<input type="text" value="https://ip-172-31-25-1"/>
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: 2px;"> 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>

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



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

8.1.3 Admin E-mail Reports Settings

- Click 'Quarantine & Archive Settings' > 'Admin E-mail Reports' tab in the 'Quarantine & Archive' screen.
- Secure Email Gateway allows administrators to access all quarantined emails via a separate web based quarantine page that contains all their quarantined messages.

- The 'Admin Email Reports' section allows admins to configure the URL of the 'Quarantine Webmail' page, the email notification subject line, from address, to address mail message template and the days and time the email should be sent to users.

The screenshot shows the 'Quarantine & Archive Settings' interface. At the top right, there is a language selector set to 'English' and a 'Logout' button. Below the title, there are three tabs: 'General', 'E-mail Reports', and 'Admin E-mail Reports'. The 'Admin E-mail Reports' tab is active. The form contains the following fields:

- Mail Subject:** E-mail Quarantine Re
- Mail From:** korumail@ip-172-31-1
- Mail To:** (empty)
- Base URL:** https://ip-172-31-25-1
- Mail Template:** (empty text area)
- Days To Send:** All days (Monday through Sunday) are checked.
- Send Hour:** A dropdown menu is open, showing times from 00:00 to 23:00. 15:00 is selected.

A 'Save' button is located at the bottom center of the form.

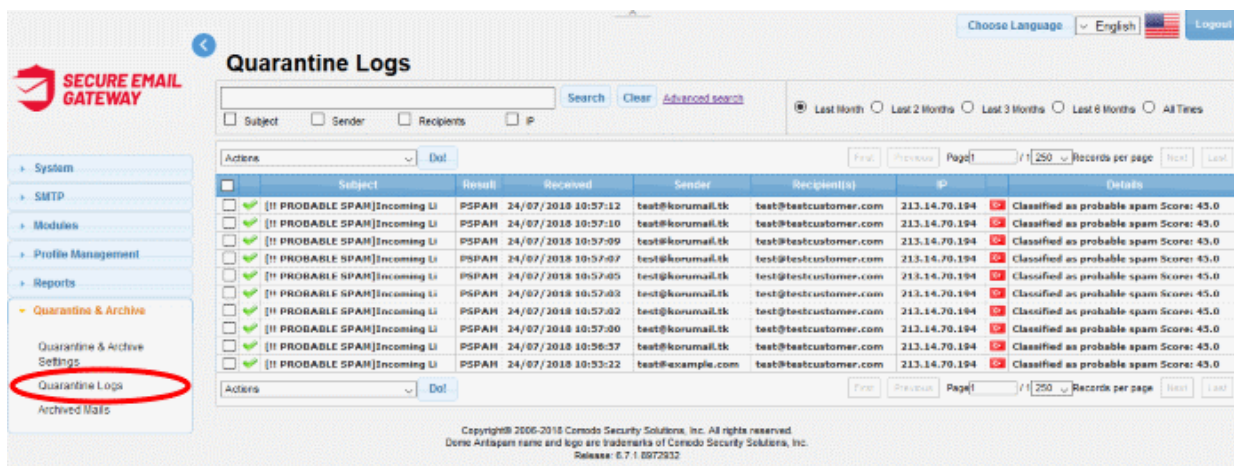
Quarantine & Archive – Admin E-mail Reports Settings - Table of Parameters

Parameter	Description
Mail Subject	Enter the content for subject line for the automated email report
Mail From	Enter the address from which the email reports will be sent
Mail To	Enter the administrator's email address at which the email reports will be received
Base URL	Enter URL of 'Quarantine Webmail' page that users should access to view their quarantined emails
Mail Template	The message body of the mail.
Days to Send	Select the day(s) when you want to send the email notifications
Send Hour	Select the hour of the day to send the email notifications for the selected days.

- Click 'Save' to apply your changes.

8.2 Quarantine Logs

- Click 'Quarantine & Archive' then 'Quarantine Logs'
- A log is created every time a mail is placed in quarantine. These logs can be viewed in the 'Quarantine Logs'.
- You can set how long logs are kept in the '**Quarantine & Archive General Settings**' area.
- The interface allows you to take actions such as delete, mark as 'not spam', resend the message to the intended recipient and more.



Quarantine Logs - Table of Column Descriptions

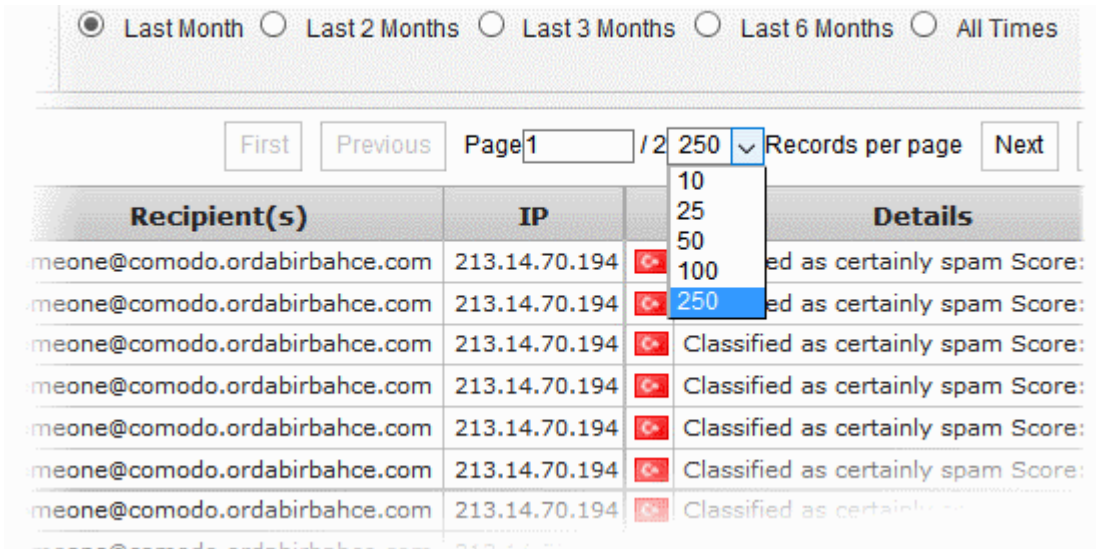
Column Header	Description
Icon	Status of action for the mail applied by SEG after the filtering process. Placing your mouse cursor over an icon will show a description of the action. - Relayed: Indicates the mail has successfully passed the filtering process and user verified. - Rejected: Indicates the mail is rejected by SEG after the filtering process and reject message sent to the sender mail server. - Discarded: Indicates the mail is quarantined
Subject	The content in the 'Subject' line of the mails
Result	The verdict on a email after filtering process. For example, 'CSPAM' means Secure Email Gateway found the mail was 'Certainly Spam'.
Received	Date and time of email was received by Secure Email Gateway
Sender	Email address information of the originator
Recipient(s)	Email address information of the receiver
IP	The network address of the system from where the mail was sent.

Details	Reason why a mail is quarantined and spam score if it is marked as spam.
---------	--

At the top and bottom of the screen, you have the option to set the number of records to be displayed per page and take desired actions such as delete, mark as not spam and so on.

To configure the number of records to be displayed per page

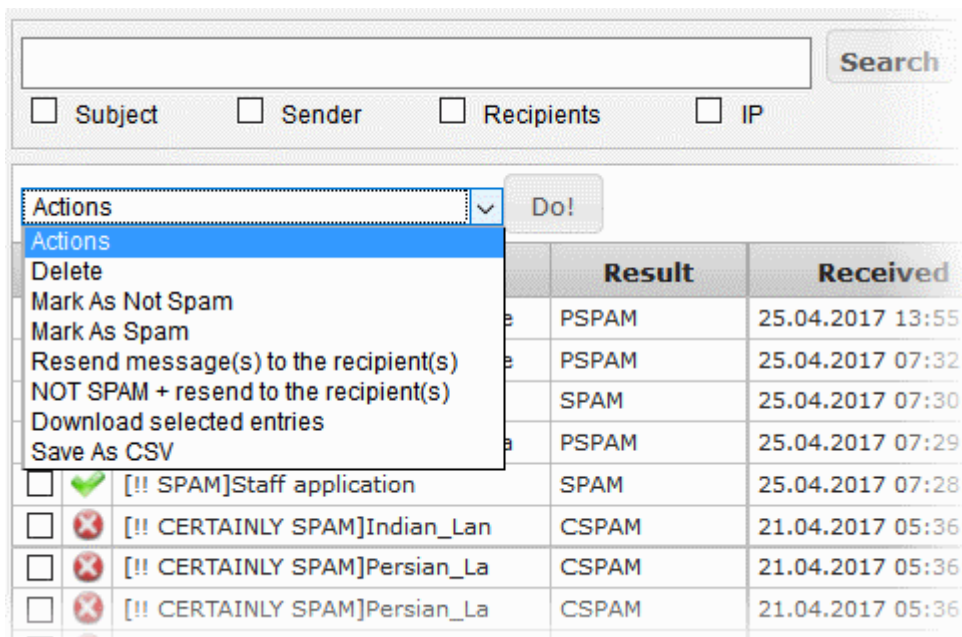
- Click the 'Records per page' drop-down



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

To take actions on log entries

- Click the 'Actions' drop-down



- Select the desired action from the drop-down and click 'Do'

Log Details

- Clicking anywhere on the row of a log record will display the details of the quarantined mail log.

The screenshot shows a 'Mail Logs' window with a table of log entries. The selected entry is expanded to show the following details:

Received	24/07/2018 10:57:12
Queue ID	23198-1532429832-155266
Message ID	26817.9269946529-sendEmail@mehmets-iac-2
Action	✓
Result	PROBABLE SPAM
Score	45.0
Sender	test@korumail.tk Add Email In Black List +
Recipient(s)	test@testcustomer.com
RFC2822 Sender	"test@korumail.tk" <test@korumail.tk>
RFC2822 Recipient(s)	"test@testcustomer.com"
Subject	[PROBABLE SPAM]Incoming Limit
IP	213.14.70.194 Add Black List +
Location	Turkey
Size	809 B
Matched Profile	Default Incoming Profile (defined by user: admin)
Details	Classified as probable spam
Relayed	No

At the bottom of the details view, there are several action buttons: [Download](#), [Forward](#), [Resend](#), [Resend as attachment](#), [Not spam](#), [Spam](#), [Close](#), and [Details](#).

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 Secure Email Gateway.

- To forward the mail, click 'Forward', enter the mail ID in the 'Email Forward' dialog and click 'Send'.

The 'E-mail Forward' dialog box contains a text input field labeled 'E-mail :', a 'Send' button, and a 'Close' button.

- Click 'Resend' to send the mail again.
- Click 'Resend as attachment' to send the mail as an attachment.
- To save the log record to your computer, click the 'Download' link and save the mail record.
- To add the sender or domain to blacklist/whitelist, click the drop-down in the 'Sender' row.

Score	104.0
Sender	buyuklukucuklu@pala.com Add Email In Black List
Recipient(s)	someone@comodo.ordabirb
RFC2822 Sender	buyuklukucuklu@pala.com
RFC2822 Recipient(s)	someone@comodo.ordabirbahce.com
Subject	[!! CERTAINLY SPAM]Persian_Lang_this_is_test : اونی یک تمهه است
IP	213.14.70.194 Add Black List

- 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 'Save' .

The changes will be saved and mails from the sender will be applied the new settings by Secure Email Gateway.

- 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

Not spam Close

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

IP Description

Save
Close

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

The changes will be saved and mails from the IP will be applied the new settings by Secure Email Gateway.

You can view the previous or next record by click the buttons at the top of a details screen.

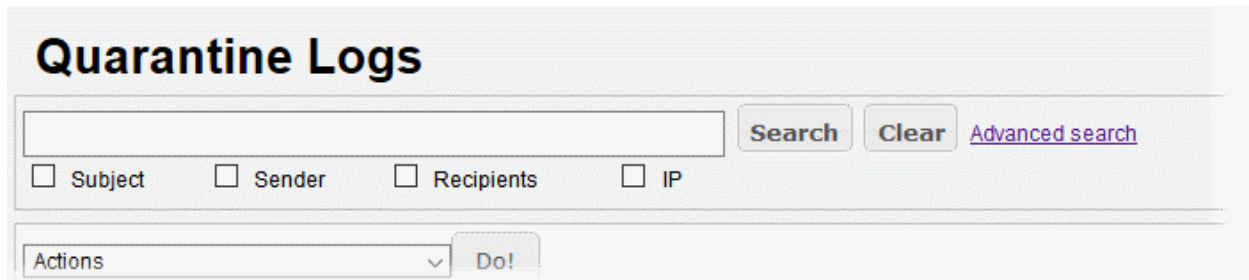
Search Options

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.



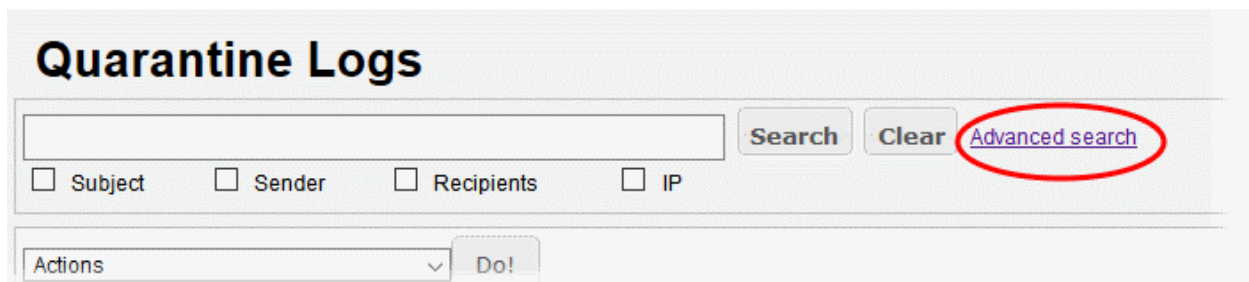
The screenshot shows the 'Quarantine Logs' interface. At the top, there is a search input field, a 'Search' button, a 'Clear' button, and a link for 'Advanced search'. Below the input field are four checkboxes labeled 'Subject', 'Sender', 'Recipients', and 'IP'. At the bottom, there is a dropdown menu for 'Actions' and a 'Do!' button.

- 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 'Search'
- 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 'Search'. 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 'Search'.

Advanced Search

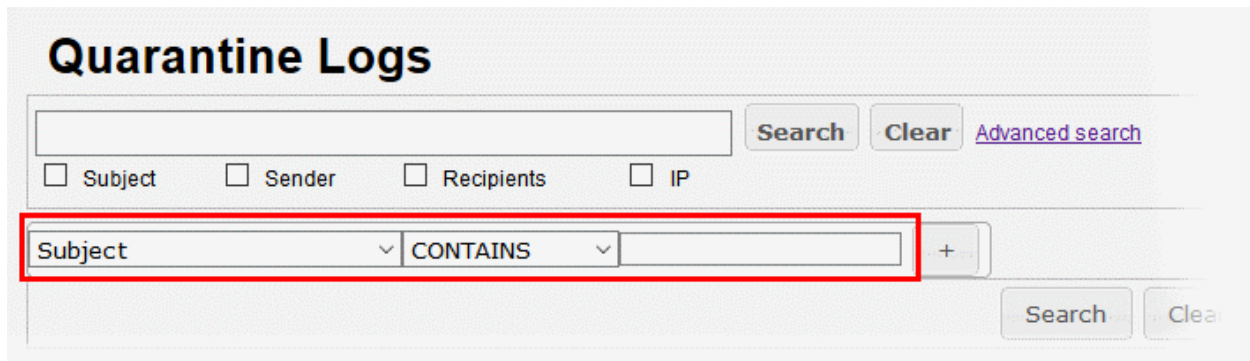
The 'Advanced Search' option allows you a more granular search by including rules and filters.

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

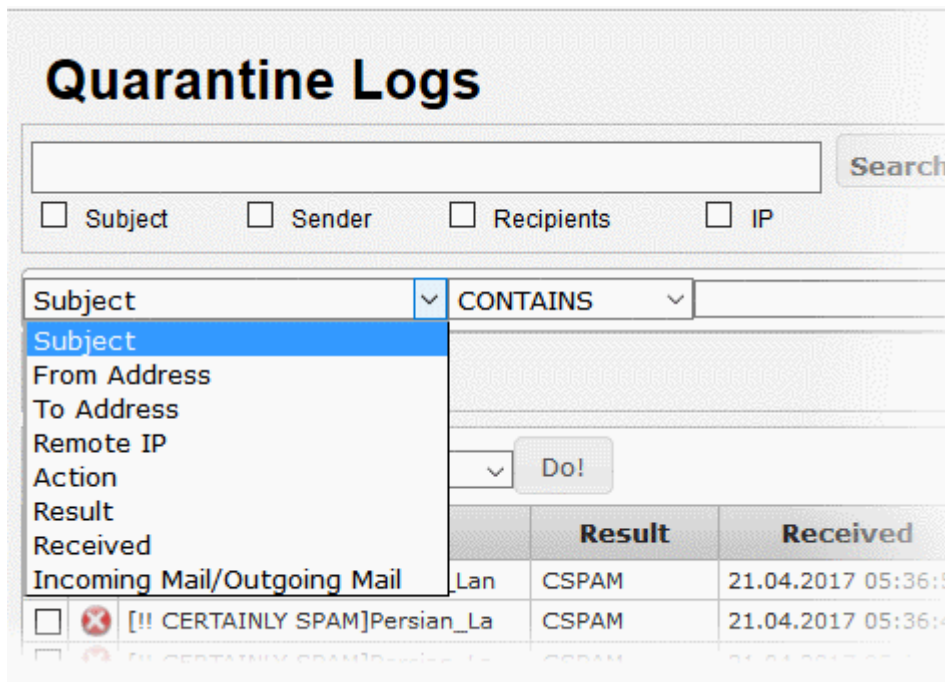


This screenshot is identical to the previous one, but the 'Advanced search' link is circled in red to highlight it.

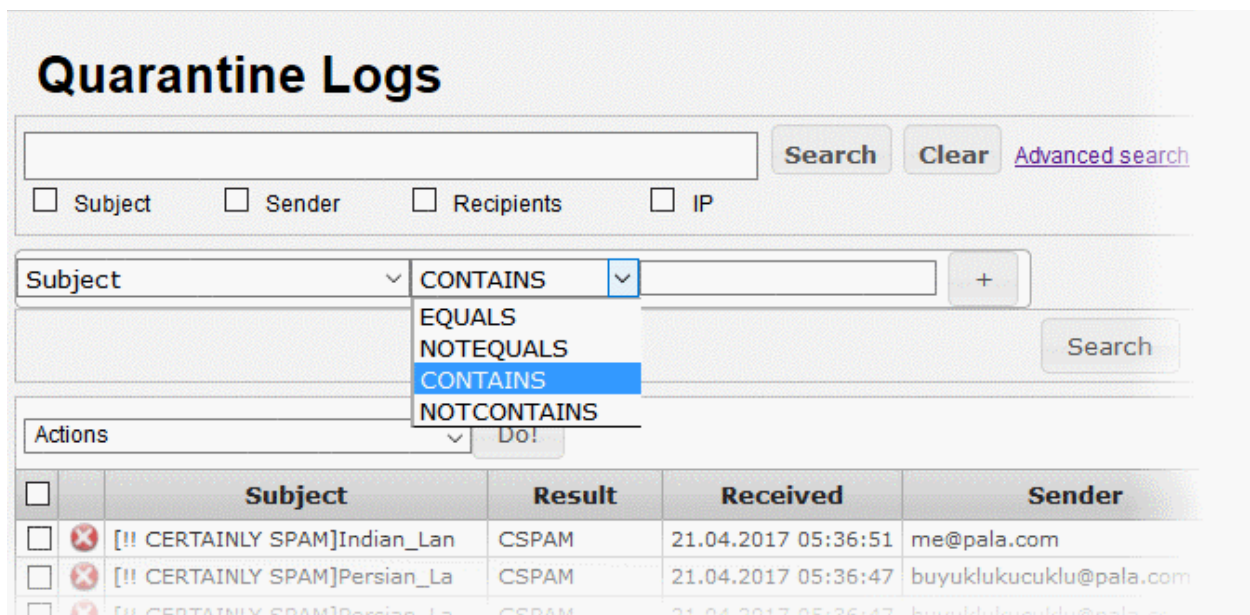
The 'Advanced Search' option will be displayed.



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



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



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

Quarantine Logs

Search [] Clear [Advanced search](#)

Subject Sender Recipients IP

Subject Important Search

Actions

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

Quarantine Logs

Search [] Clear [Advanced search](#)

Subject Sender Recipients IP

Action DELAYED Search

AND EQUALS

Actions

<input type="checkbox"/>	Subject	Result	Received	Sender
<input type="checkbox"/>	Subject	Result	Received	Sender

If you select 'Received' in the first column, then you can enter a date or select from the calendar.

Quarantine Logs

[Advanced search](#)
 Subject Sender Recipients IP

Received EQUALS

Actions Do!

		April, 2017								
		Sun	Mon	Tue	Wed	Thu	Fri	Sat		
		13	26	27	28	29	30	31	1	
		14	2	3	4	5	6	7	8	
		15	9	10	11	12	13	14	15	
		16	16	17	18	19	20	21	22	
		17	23	24	25	26	27	28	29	
		18	30	1	2	3	4	5	6	
		Today								

<input type="checkbox"/>	<input type="checkbox"/>	Subject	Result	Sender
<input type="checkbox"/>	<input checked="" type="checkbox"/>	[!! CERTAINLY SPAM]Indian_Lan	CSPAM	om
<input type="checkbox"/>	<input checked="" type="checkbox"/>	[!! CERTAINLY SPAM]Persian_La	CSPAM	uklu@pala.com
<input type="checkbox"/>	<input checked="" type="checkbox"/>	[!! CERTAINLY SPAM]Persian_La	CSPAM	uklu@pala.com
<input type="checkbox"/>	<input checked="" type="checkbox"/>	[!! CERTAINLY SPAM]Persian_La	CSPAM	uklu@pala.com
<input type="checkbox"/>	<input checked="" type="checkbox"/>	[!! CERTAINLY SPAM]Persian_La	CSPAM	uklu@pala.com
<input type="checkbox"/>	<input checked="" type="checkbox"/>	[!! CERTAINLY SPAM]Abyssinian	CSPAM	uklu@pala.com

You can add more filters by clicking  for narrowing down your search.

Quarantine Logs

[Advanced search](#)
 Subject Sender Recipients IP

Received EQUALS

AND From Address EQUALS

OR To Address EQUALS

AND Remote IP EQUALS

OR Action EQUALS DELAYED

OR Result EQUALS ANTISPOOFING REJECT

You can remove a filter by clicking the  button beside it.

You can create a filter rule by selecting 'AND' or 'OR' option beside each of the added filter.

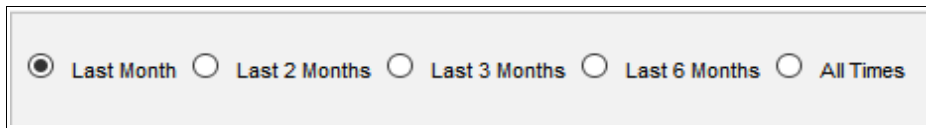
- Click 'Clear' to remove the advanced search rules.
- Click 'Search' to start the search per the filter rule.

The items will be searched for in the ascending order and results displayed.

- To remove the advanced search field, click the 'Advanced search' link again.

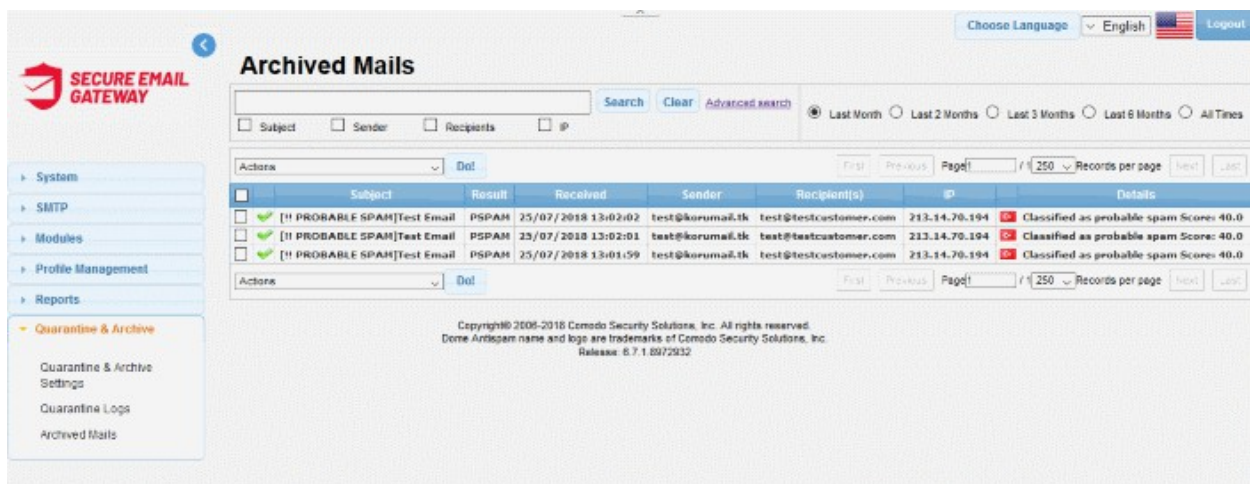
Administrators can filter results on monthly basis. The filters available are 'Last Month', 'Last 2 Months', 'Last 3 Months', 'Last 6 Months' and All Times.

- To view the results of the last month, click the 'Last Month' radio button.



8.3 Archived Mails

- Click 'Quarantine & Archive' > 'Archived Mails'
- The 'Archived Mails' interface displays a log 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 you to take actions such as to delete, mark as spam, mark as not spam and more.



Archived Mails - Table of Column Descriptions

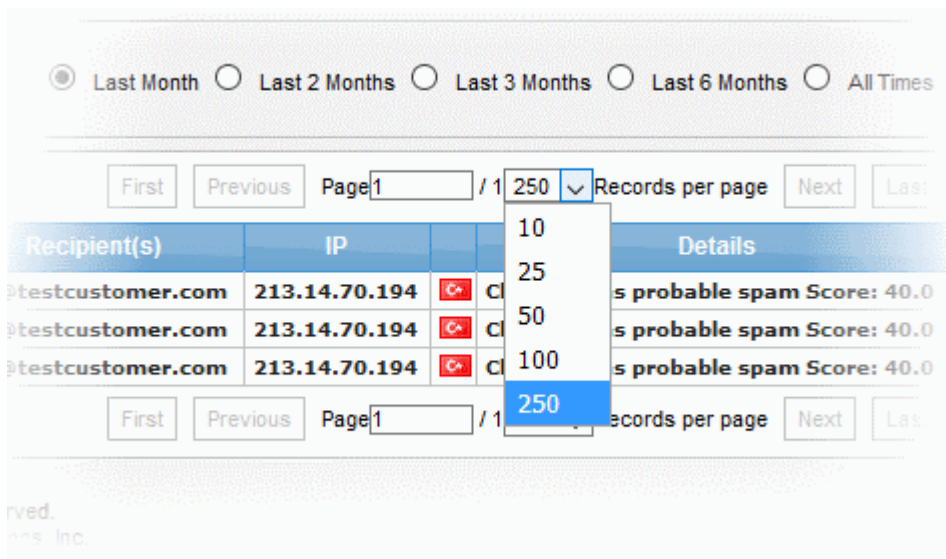
Column Header	Description
Icon	<p>Indicates the status of the mail after the filtering process. Placing your mouse cursor over an icon will show a description of the action.</p> <ul style="list-style-type: none"> Relayed: Indicates the mail successfully passed the filtering process - Rejected: Indicates the mail was rejected by Secure Email Gateway and a reject message was sent to the sender's mail server. - Discarded: Indicates the mail is quarantined
Subject	The content in the 'Subject' line of the mails
Result	The verdict on an mail after the filtering process.
Received	Date and time Secure Email Gateway received the email

Sender	Email address information of the originator
Recipient(s)	Email address information of the receiver
IP	The network address of the system from where the mail was sent.
Details	Reason why a mail is quarantined and spam score if it is marked as spam.

At the top and bottom of the screen, you have the option to set the number of records to be displayed per page and take desired actions such as delete, mark as not spam and so on.

To configure the number of records to be displayed per page

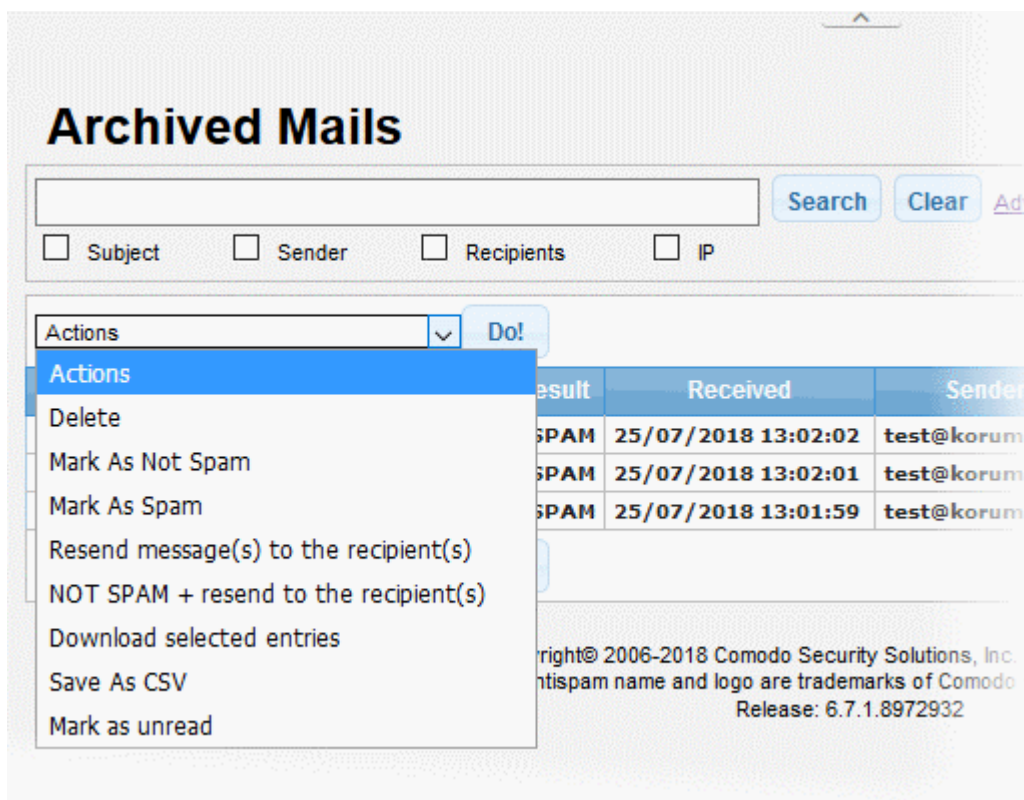
- Click the 'Records per page' drop-down



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

To act on log entries

- Click the 'Actions' drop-down



- Select the desired action from the drop-down and click 'Do'

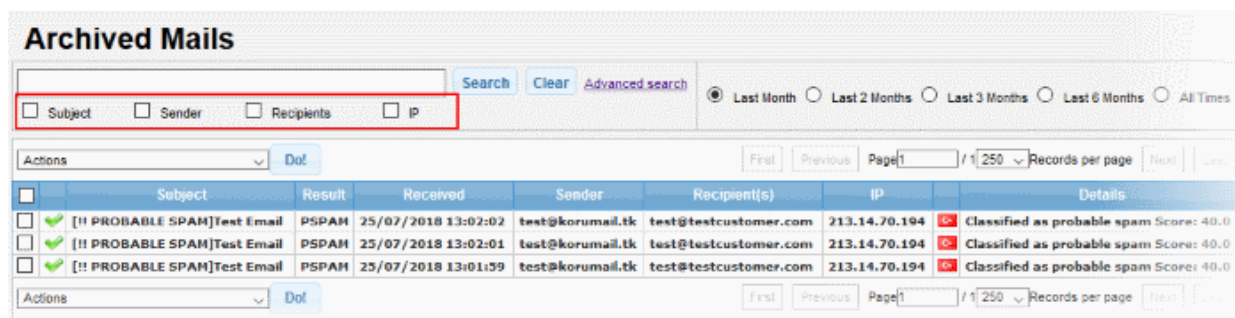
Search Options

You can search for a particular record or records in the quarantine log by using simple or advanced search feature.

- **Simple Search**
- **Advanced Search**

Simple Search

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

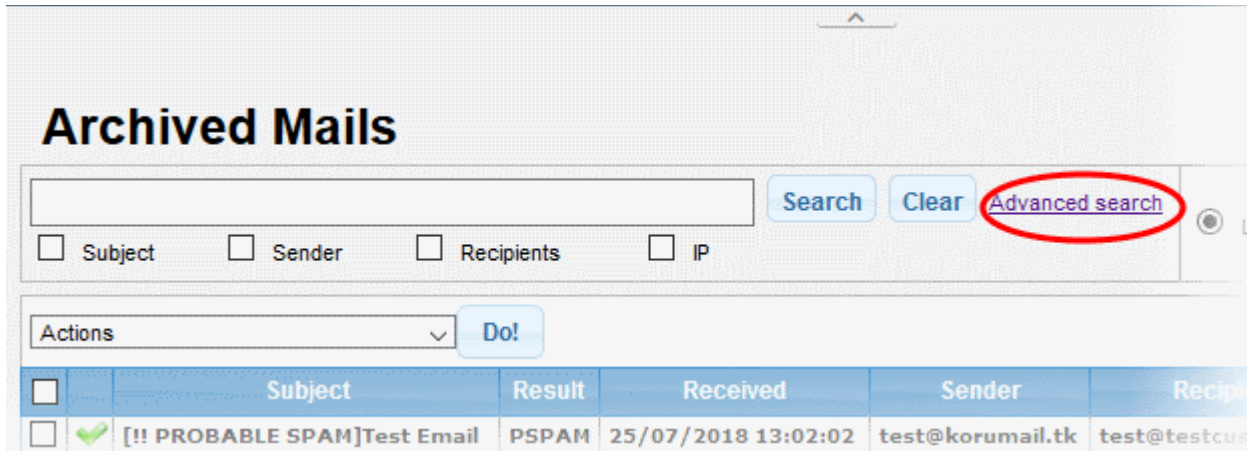


- To search for records based on the entries under 'Subject', 'Sender', 'Recipients' and / or 'IP' columns, enter the text or number fully or partially in the field and click 'Search'
- To search for records based on the entries under a particular column or columns, select the respective check boxes, enter the text or number fully or partially in the field and click the 'Search'. 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 'Search'.

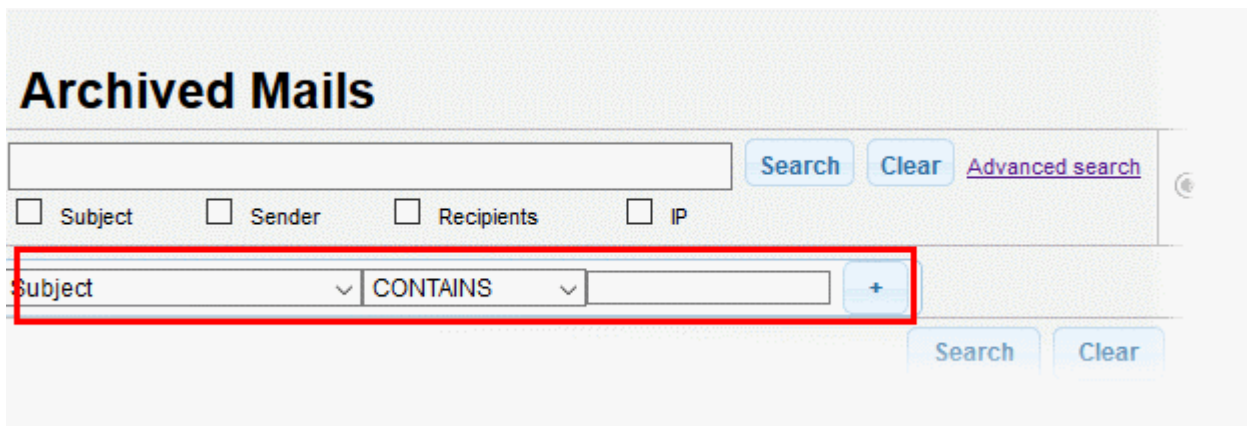
Advanced Search

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

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



The 'Advanced Search' option will be displayed.



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

Archived Mails

Subject Sender Recipients IP

Subject	CONTAINS	
Subject From Address To Address Remote IP Action Result Received Incoming Mail/Outgoing Mail	<input type="button" value="Do!"/>	

	Result	Received
message	PSPAM	25.04.2017 07:32:4

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

[Ac](#)

Subject Sender Recipients IP

Subject	CONTAINS	
	EQUALS NOTEQUALS CONTAINS NOTCONTAINS	

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

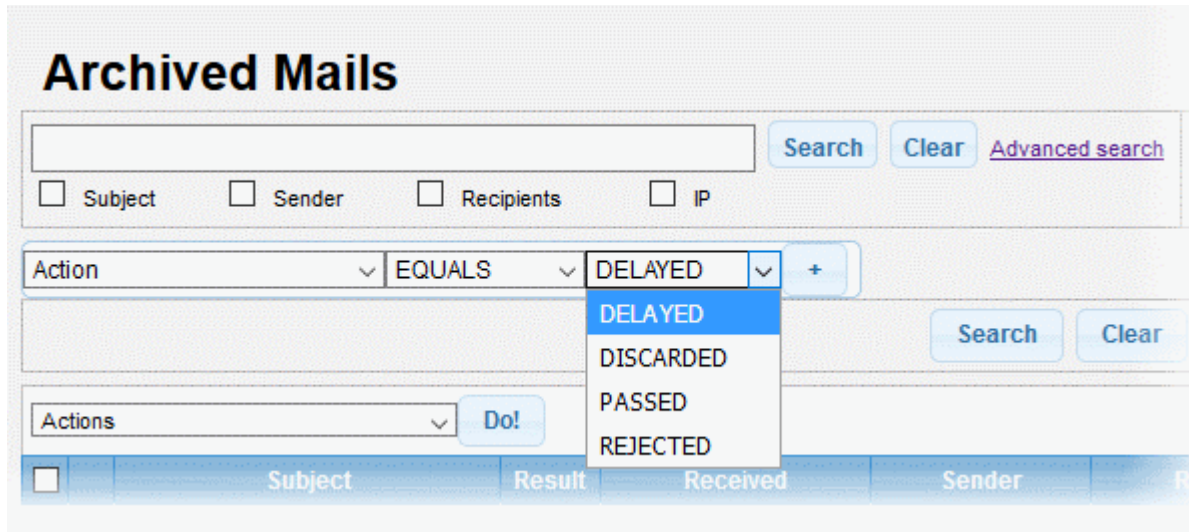
Archived Mails

[Advanced search](#)

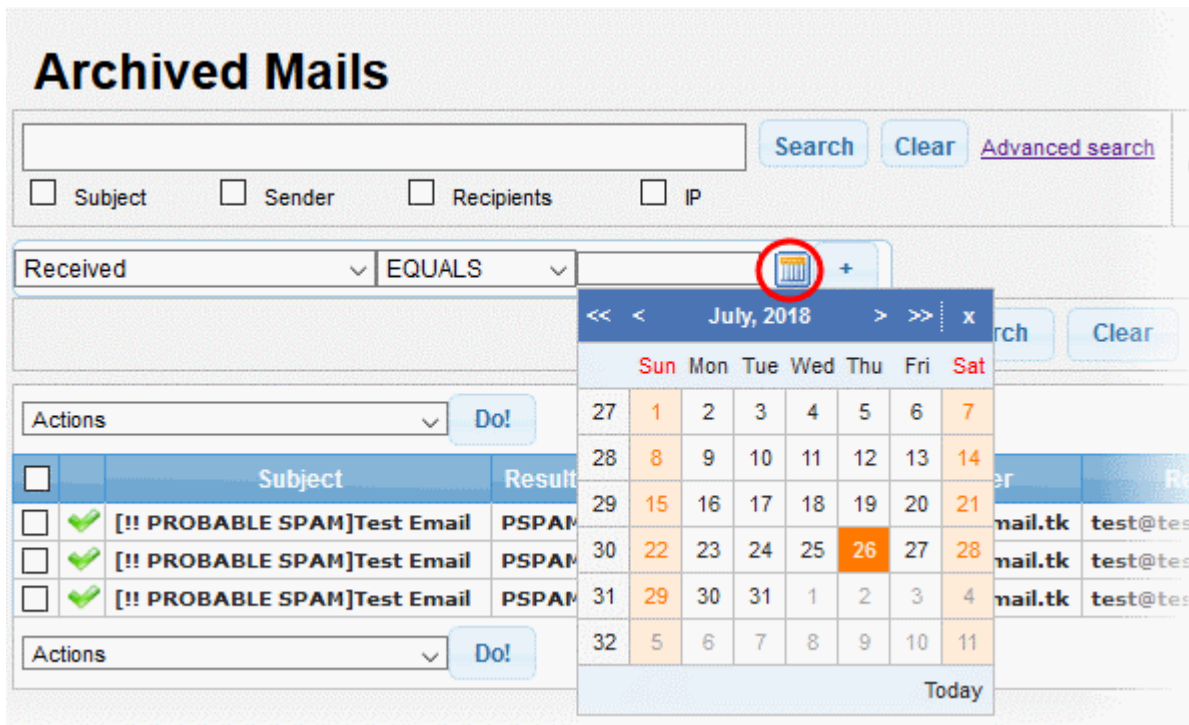
Subject Sender Recipients IP


Subject	CONTAINS	
---------	----------	--

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.

You can remove a filter by clicking the  button beside it.

You can create a filter rule by selecting 'AND' or 'OR' option beside each of the added filter.

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

- Click 'Search' to start the search per the filter rule.

The items will be searched for in the ascending order and results displayed.

- To remove the advanced search field, click the 'Advanced search' link again.

Administrators can filter results on monthly basis. The filters available are 'Last Month', 'Last 2 Months', 'Last 3 Months', 'Last 6 Months' and All Times.

- To view the results of the last month, click the 'Last Month' radio button.

Last Month
 Last 2 Months
 Last 3 Months
 Last 6 Months
 All Times

Details of a Log Entry

- Clicking anywhere on the row of a log record will display the details of the archived mail log.

Mail Logs
✕

Received	25/07/2018 13:02:02
Queue ID	24504-1532523722-182151
Message ID	908615.080497356-sendEmail@mehmets-imac-2
Action	✔
Result	PROBABLE SPAM
Score	40.0
Sender	test@korumail.tk Add Email In Black List +
Recipient(s)	test@testcustomer.com
RFC2822 Sender	"test@korumail.tk" <test@korumail.tk>
RFC2822 Recipient(s)	"test@testcustomer.com"
Subject	[! PROBABLE SPAM]Test Email
IP	213.14.70.194 Add Black List +
Location:	Turkey
Size	801 B
Matched Profile	Default Incoming Profile (defined by user: admin)
Details	Classified as probable spam
Relayed	No

Download
Forward
Resend
Resend as attachment
Not spam
Spam
Close
Details

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 Secure Email Gateway.

- To forward the mail, click 'Forward', enter the mail ID in the 'Email Forward' dialog and click 'Send'.

E-mail Forward

E-mail :

Send
Close

- Click 'Resend' to send the mail again.
- Click 'Resend as attachment' to send the mail as an attachment.
- To save the log record to your computer, click the 'Download' link and save the mail record.
- To add the sender or domain to blacklist/whitelist, click the drop-down in the 'Sender' row.

Sender	test@korumail.tk	Add Email In Black List	+
Recipient(s)	test@testcustomer	Add Email In Black List	
RFC2822 Sender	"test@korumail.tk"	Add Email In White List	
RFC2822 Recipient(s)	"test@testcustomer	Add Domain In Black List	
Subject	[! PROBABLE SPAM]	Add Domain In White List	
IP	213.14.70.194	Add Black List	+
Location:	Turkey		
Size	801 B		

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

Description

Save
Close

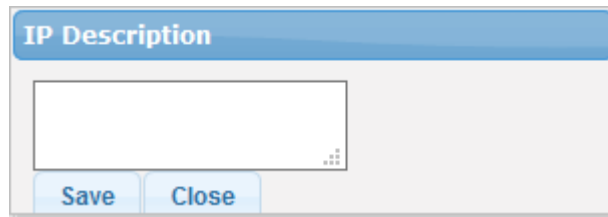
- Enter the reason for changing the category and click the 'Save' button.

The changes will be saved and mails from the sender will be applied the new settings by Secure Email Gateway.

- To add the originating IP to blacklist/whitelist, click the drop-down in the 'IP' row.

Subject	[! PROBABLE SPAM]Test Message		
IP	46.2.135.238	Add Black List	+
Location:	Atakoy, Diyarbakir	Add Black List	
Size	665 B	Add White List	
Matched Profile	Default Outgoing Profile (defined by user: admin)		

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



The image shows a dialog box titled "IP Description". It features a blue header bar with the title. Below the header is a large, empty white text input field. At the bottom of the dialog, there are two buttons: "Save" and "Close", both with a light blue background and dark blue text.

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

The changes will be saved and mails from the IP will be applied the new settings by Secure Email Gateway.

You can view the previous or next record by click the   buttons at the top of a details screen.

About Comodo Security Solutions

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

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

About Comodo Cybersecurity

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

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

<https://www.comodo.com>

Email: EnterpriseSolutions@Comodo.com