COMODO
Creating Trust Online®

COMODO DOME ANTISPAM

Comodo Dome Antispam

Software Version 6.0

Admin Guide

Guide Version 6.6.051117

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1 Introduction to Dome Anti-spam 5
1.1 Logging-in to the Dome Antispam Module 6
1.2 Getting Started 8
1.3 The Main Interface 8
2 The Dashboard 10
2.1 System Usage Graphics 10
2.2 About Software 11
3 System Configurations 15
3.1 Services 16
3.2 License 18
3.3 Configuring System Settings 22
3.3.1 System General Settings 23
3.3.2 Cache Settings 23
3.3.3 Session Settings 24
3.3.4 GUI Customization 24
3.3.5 System Backup 25
3.3.6 System Restore 27
3.3.7 Log Upload Settings 28
3.3.8 Postmaster Settings 29
3.3.9 SMTP TLS Settings 30
3.3.10 Update Database 30
3.3.11 Syslog Server 31
3.4 Logs 32
3.4.1 Log Files 32
3.4.2 Purge Files 34
3.5 Tools 34
3.5.1 Check Connectivity 35
3.5.2 Clear SMTP Queue 40
3.6 System Usage Statistics 40
4 SMTP Configuration 46
4.1 SMTP (Send E-Mail Protocol) Settings 47
4.1.1 General Settings 48
4.1.2 Advanced Settings 49
4.1.3 Outbound Delivery Queue 53
4.2 Manage Domains 55
4.2.1 Managing Domain Names 56
4.2.2 Managing Domain Routes 63
4.2.3 Managing Smart Hosts 68
4.2.4 Default Domain Routing 71
4.3 Dome Antispam SMTP AUTH Connector 73
4.3.1 SMTP Authentication Settings 73

4.3.2 Block Users 76
4.3.3 Anomaly Detection 81
4.4 LDAP/Local DB/My SQL User Database 83
4.4.1 LDAP Profile 83
4.4.2 Local DB Users 87
4.4.3 My SQL User Database 93
4.5 Greylist 96
4.5.1 Greylist Ignored IP Addresses/Domains 97
4.6 Managing RBL Servers 99
4.7 Disclaimer 102
4.8 SMPT Relay 103
4.9 DomainKeys Identified Mail (DKIM) 104
4.10 Outgoing SMTP Limits 107
4.11 Incoming SMTP Limits 114
5 Modules 118
5.1 Anti-spam 119
5.1.1 Anti-spam General Settings 120
5.1.2 Authorized Trainers 121
5.1.3 Advanced Anti-spam Settings 122
5.1.4 Bayesian Training 123
5.1.5 Content Filter 124
5.1.6 Signature Whitelist 126
5.2 Anti-Virus 129
5.2.1 Anti-Virus General Settings 129
5.2.2 Advanced Anti-Virus Settings 131
5.3 Reputation Network (KRN) 132
5.4 Anti-Spoofing 134
5.5 SMTP IPS/FW 138
5.5.1 SMTP IPS General Settings 139
5.5.2 Whitelist IP Addresses 141
5.5.3 Blocked IP Addresses 143
5.5.4 Rate Control 146
5.6 Auto Whitelist 147
5.7 Data Leak Prevention (DLP) 148
5.8 Promotional 149
5.9 Attachment Verdict System 150
6 Profile Management 150
6.1 Adding and Configuring a New Profile 152
6.2 Editing a Profile 178
6.3 Deleting a Profile 179
7 Reports 180
7.1 Mail Logs Report 181
7.2 SMTP Queue Report 190

7.3 Delivery Logs Report 191
7.4 SMTP-AUTH Logs Report 192
7.5 Summary Reports 194
7.6 Domain Reports 201
7.7 Attachment Verdict Reports 205
8 Quarantine & Archive 207
8.1 Quarantine & Archive Settings 207
8.1.1 Quarantine & Archive General Settings 208
8.1.2 Email Reports Settings 208
8.2 Quarantine Logs 211
8.3 Archived Mails 219
About Comodo 228

1 Introduction to Dome Anti-spam

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 Dome Anti-spam is an antispam and threat prevention appliance that uses advanced filtering technologies, antivirus scanners and content analysis engines to quietly and effectively prevent unsolicited mail from entering your network.

Key Features

- LDAP control
- RBL (Realtime Blocking Lists)
- MX
- Reverse DNS
- White / grey / black lists, add titles which are industrially proven filtering techniques
- SRN Reputation Network
- Active Directory Integration
- Quarantine Reporting, Quarantine Webmail
- Reporting

Guide Structure

This guide is intended to take you through the installation, configuration and use of Comodo Dome Antispam.

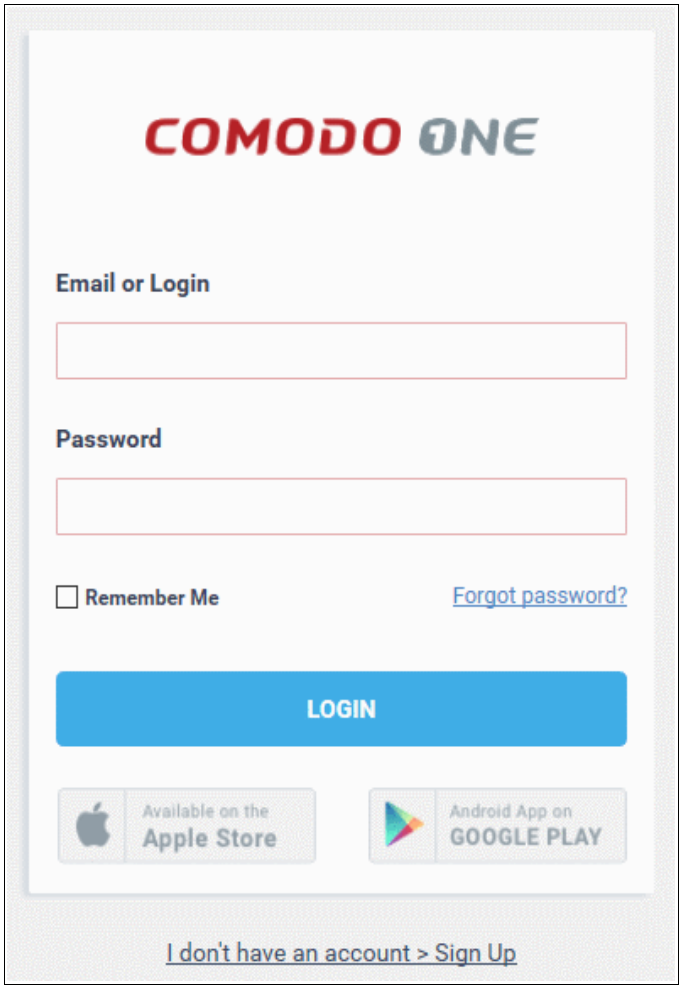
- Introduction to Dome Antispam
  - Logging-in to the Dome Anti-spam
  - Getting Started
  - The Main Interface
- The Dashboard
  - System Usage Graphics
  - About Software
- System Configurations
  - Services
  - License
  - Configuring System Settings
  - Logs
  - Tools
  - System Usage Statistics
- SMTP Configuration
  - SMTP (Send E-Mail Protocol) Settings
  - Manage Domains
  - Dome Antispam SMTP AUTH Connector
  - LDAP/Local DB/My SQL User Database
  - Greylist

- Managing RBL Servers
- Disclaimer
- SMPT Relay
- DomainKeys Identified Mail (DKIM)
- Outgoing SMTP Limits
- Incoming SMTP Limits

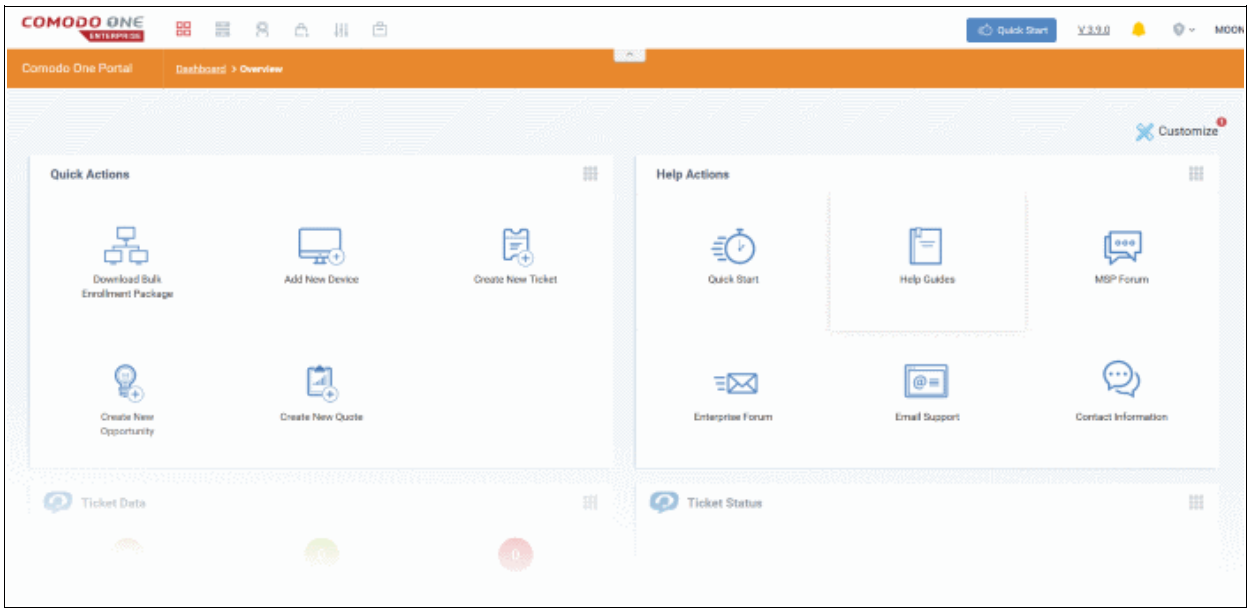
- Modules
  - Anti-spam
  - Anti-Virus
  - Reputation Network (KRN)
  - Anti-Spoofing
  - SMTP IPS/FW
  - Auto Whitelist
  - Data Leak Prevention (DLP)
  - Anti-Phishing
  - Promotional
  - Attachment Verdict System
- Profile Management
  - Adding and Configuring a New Profile
  - Editing a Profile
  - Deleting a Profile
- Reports
  - Mail Logs Report
  - SMTP Queue Report
  - Delivery Logs Report
  - SMTP-AUTH Logs Report
  - Summary Reports
  - Domain Reports
  - Attachment Verdict Reports
- Quarantine & Archive
  - Quarantine & Archive General Settings
  - Quarantine Logs
  - Archived Mails

1.1 Logging-in to the Dome Antispam Module

To access the Dome Antispam module, login to C1 with your user name and password at https://one.comodo.com/app/login.



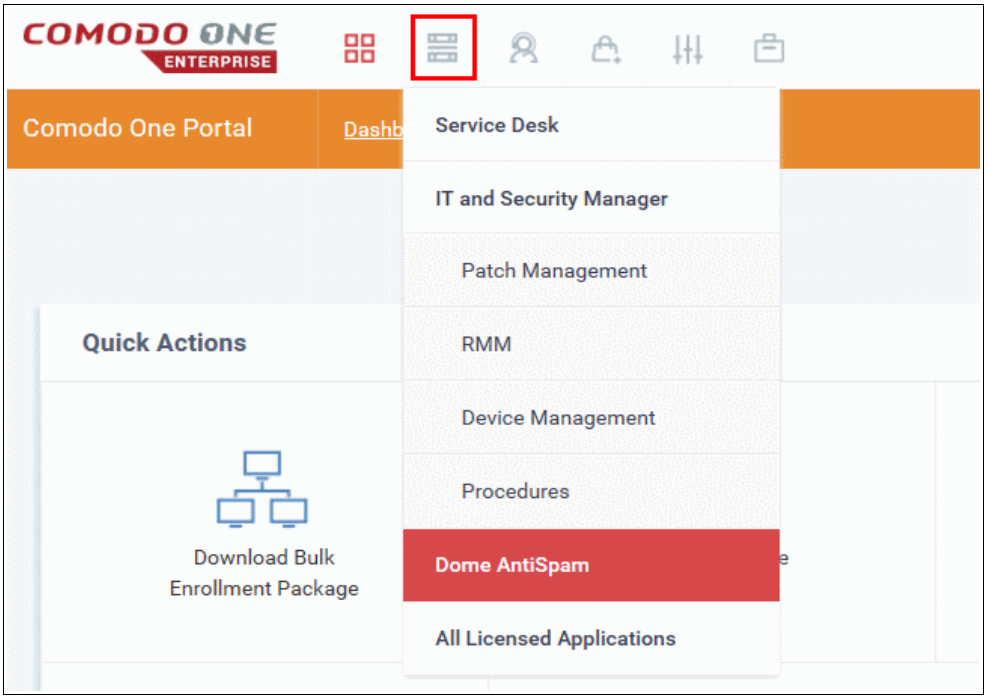
The C1 dashboard will be displayed.



To open the Dome Antispam module

- Once logged in, click 'Licensed Applications' at the top then click 'Dome Antispam'
- Alternatively, click 'All Licensed Applications' under 'Licensed Applications', then click the 'Dome Antispam' tile to open the DA module

After logging in to C1, you can open the Dome Antispam module by clicking 'Licensed Applications' > 'Dome Antispam':



By default, the Dome Antispam 'Dashboard' screen will be displayed.

1.2 Getting Started

After creating your Dome Antispam account, the next step is to configure your mail server to work with the Dome Antispam service.

Incoming Filtering Configuration

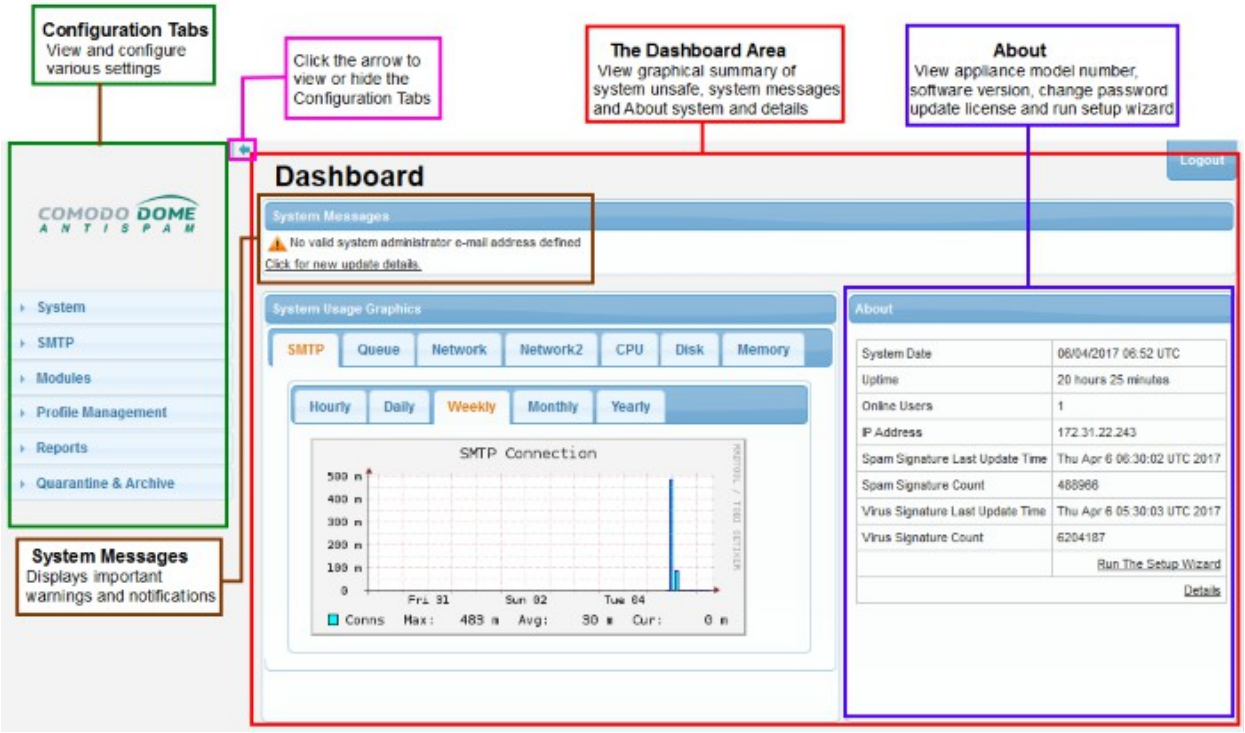
To configure incoming mail server, change your domain mx records to point to Dome Antispam. You will receive a mail that contains your account and service URL details, once your Dome Antispam instance is ready to use. To find out more information, contact Comodo support team.

Outgoing Filtering Configuration

Domain Antispam allows you to configure an outgoing filter that is independent of incoming email filtering. Contact Comodo Support, to obtain the outgoing route information. You need to provide these inputs in the Routes tab in SMTP > Domains. Refer to section 4.2.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 will apply for added domains. This setting is configured in the smart host section in Manage Domains.

1.3 The Main Interface

The admin console provides easy access to all modules, statistics and configuration screens in Comodo Dome Antispam.



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. Refer to '**System Configuration**' for more details.
- **SMTP:** Configure SMTP settings, add domains, add new LDAP profiles, create IP/domain greylists, set outgoing limits and more. Refer to '**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. Refer to the section **Modules** for more details.
- **Profile Management:** Configure various settings such as anti-virus, anti-spam, blacklist and more for default incoming and outgoing profile. Refer to the section '**Profile Management**' for more details.
- **Reports:** View and generate log reports for incoming and outgoing mails and a summary of mails categorized as spam, RBL, phishing and more. Refer to the section '**Reports**' for more details.
- **Quarantine & Archive:** Enables to configure Quarantine and Archive settings, view quarantined mail logs and archived mails. Refer to the section '**Quarantine & Archive**' for more details.

Dashboard

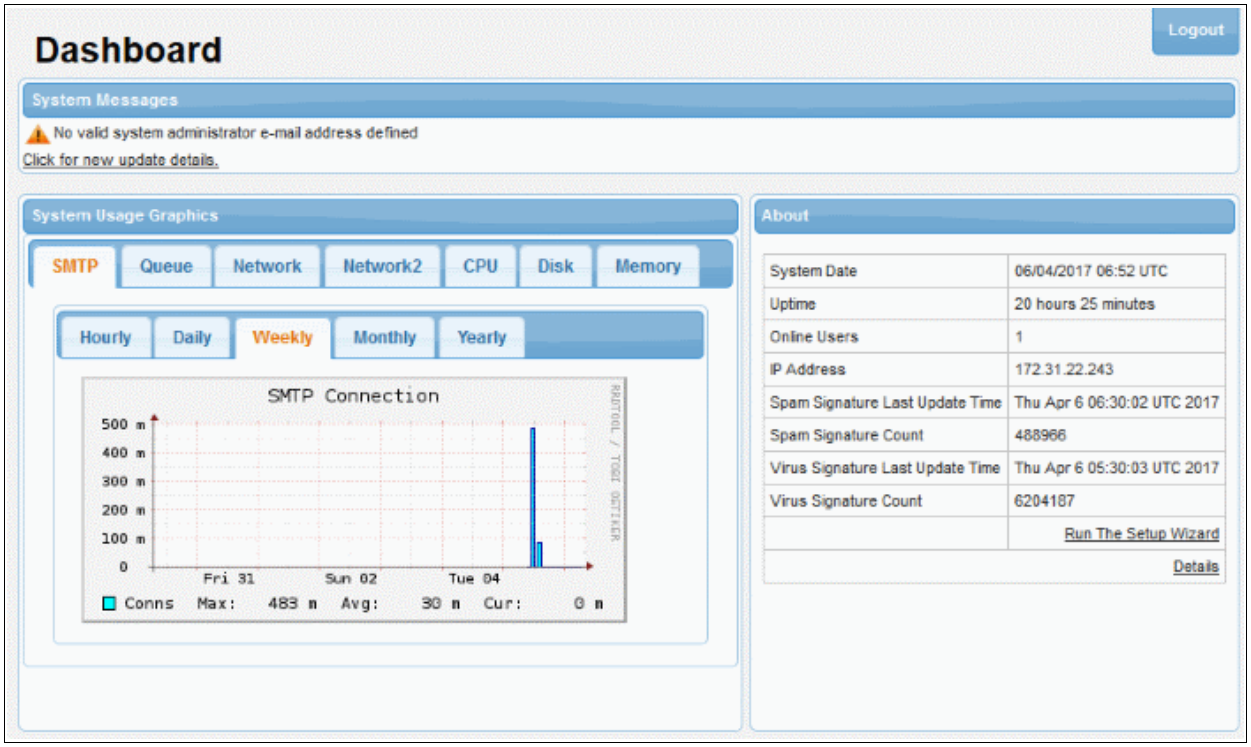
After logging-in to the console, the first screen displayed is the '**Dashboard**'. It provides at-a-glance view of system usage such as SMTP, Queue mails, network utilization rate, CPU and memory utilization.

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

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 'Comodo Dome Antispam' logo at the top left.



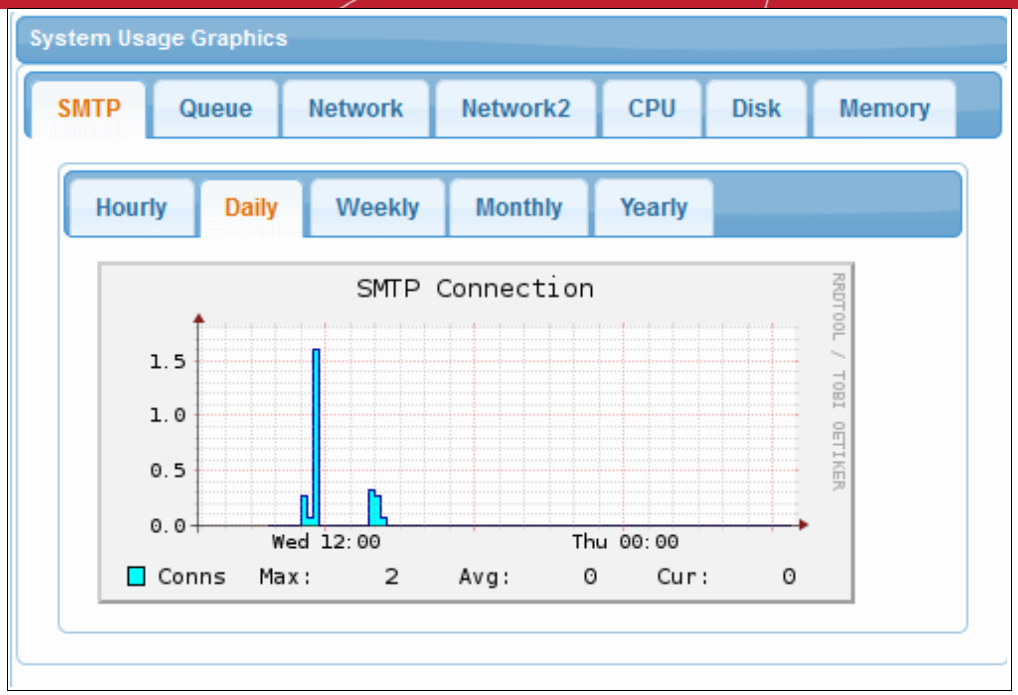
The 'System Messages' displays error messages or important notifications that might affect the performance of the messaging gateway.

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

- System Usage Graphics
- About Software

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.

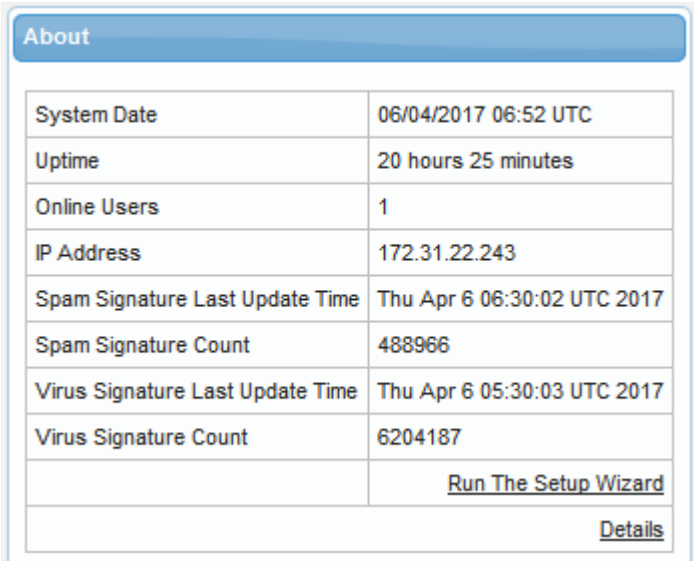


- **SMTP:** Displays the maximum, average and current SMTP connections to Dome Antispam for the selected period.
- **Queue:** Displays the maximum, average and current emails in queue for the selected period.
- **Network:** Displays the network utilization rate of the system for the selected period.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

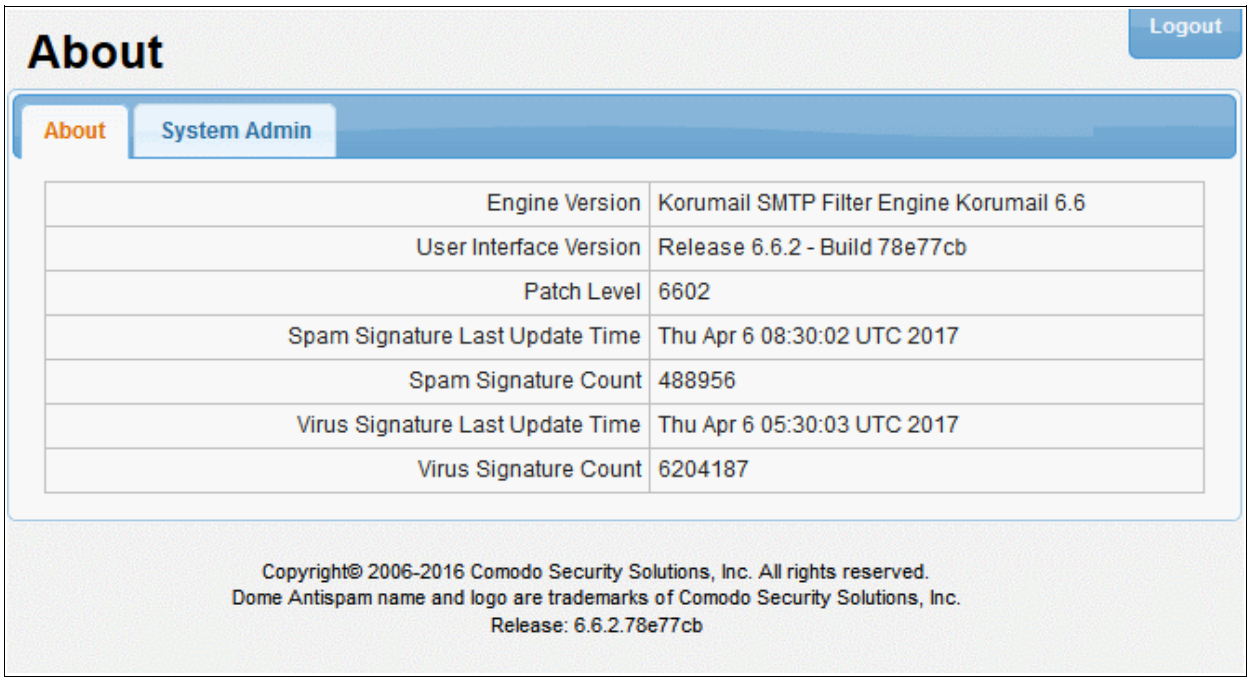
Refer to the System Usage Statistics section for more details about each of the item.

2.2 About Software

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

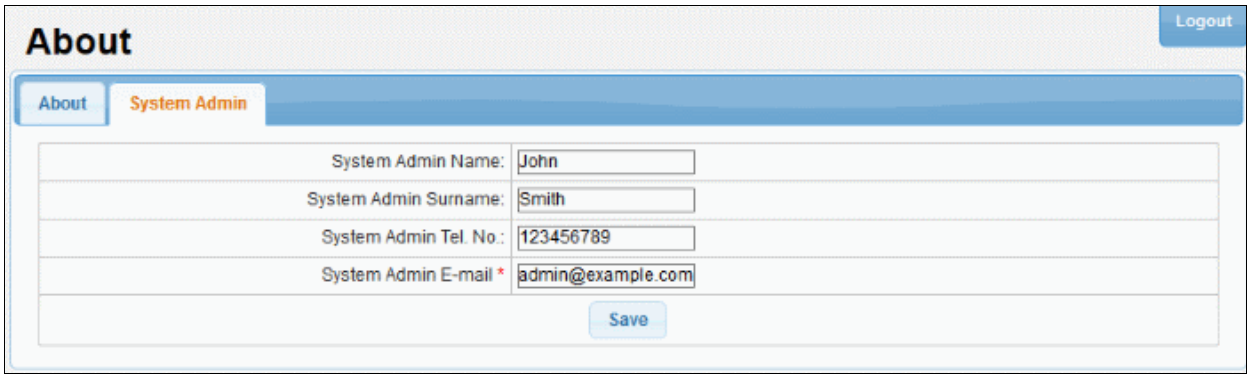


Clicking the 'Details' link at the bottom opens another 'About' screen that provides more details:



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

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



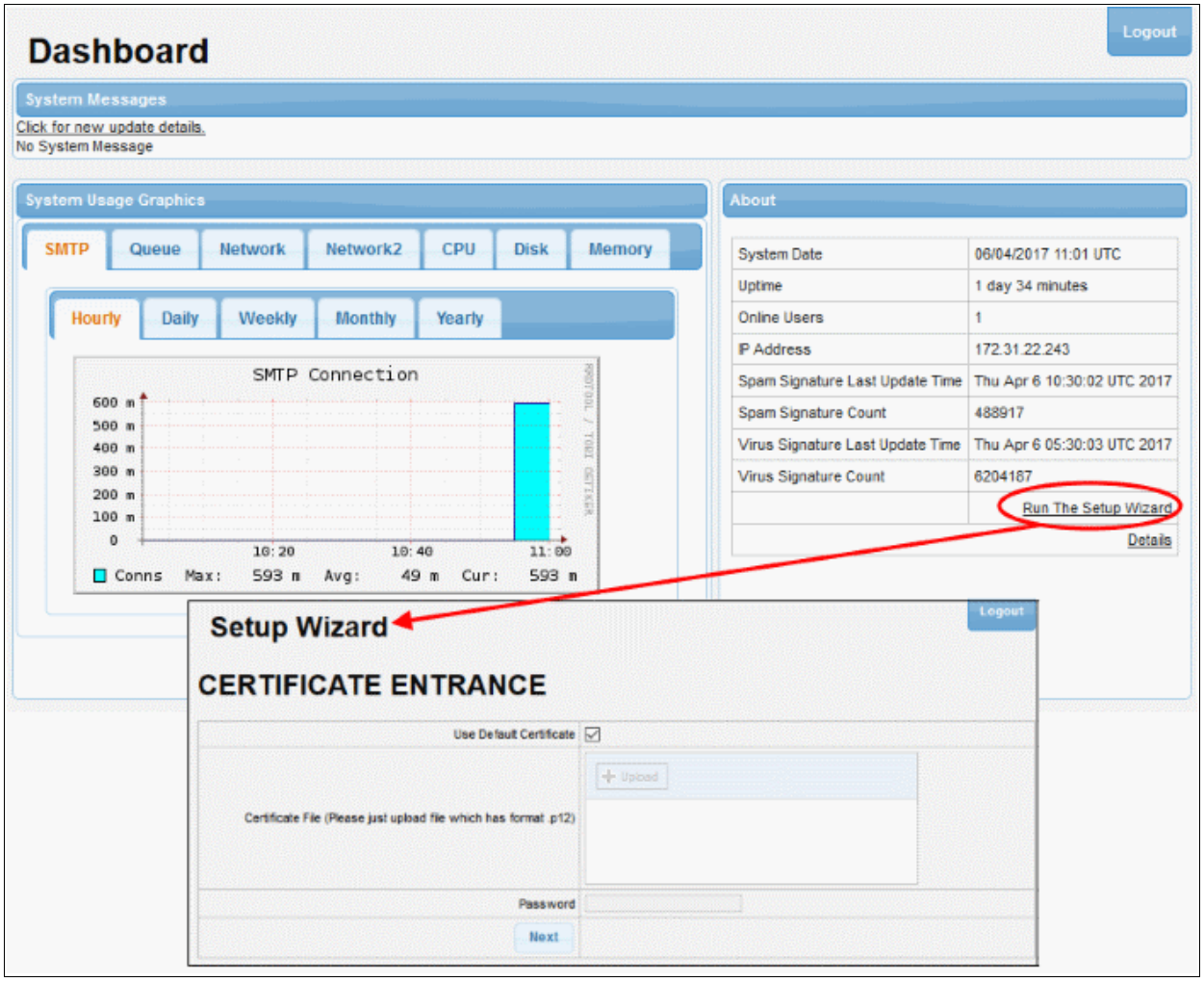
- When the SMTP IPS module blocks IP addresses, a list of the blocked IP's will be sent to the e-mail address shown in this interface.
- If the field 'System Admin E-mail' is left blank then an error message will be displayed in 'System Messages' in the dashboard.
- Click 'Save' after completing all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

Run Setup Wizard

Allows you to quickly configure protection on a mail server.

To run the setup wizard:

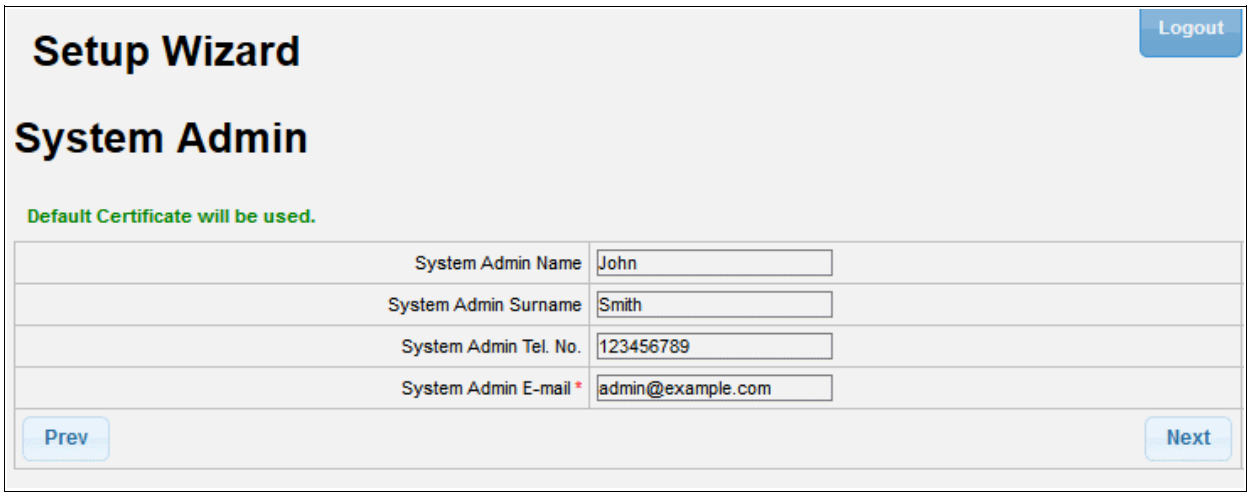
- Click the 'Run the setup wizard' link.
- The setup wizard screen will be displayed. This allows you to choose the SSL certificate you wish to use on your console, as well as system admin details, LDAP profiles, 'Managed Domains', 'Routes' and 'Relay' details.



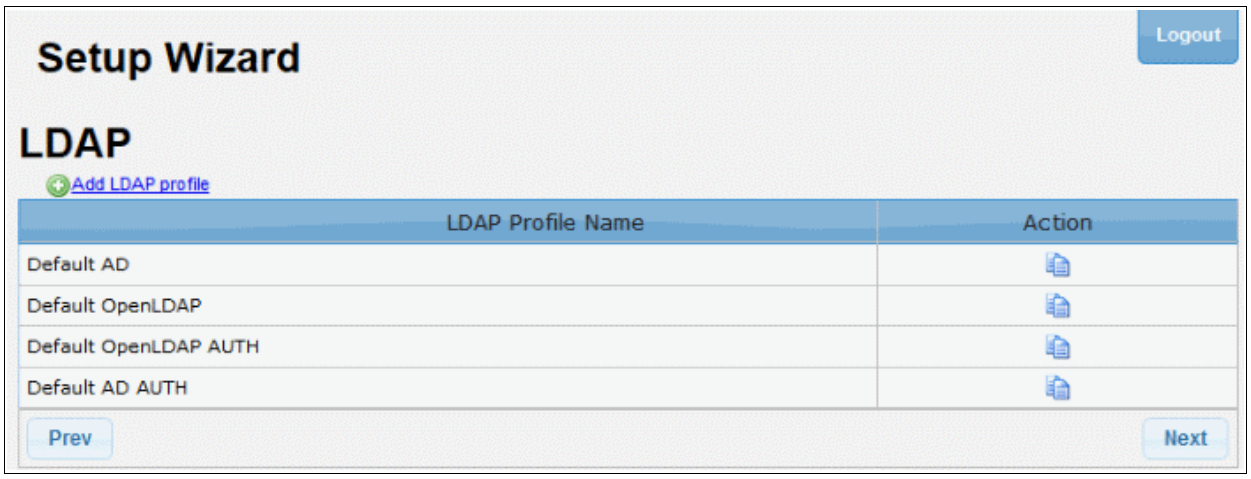
An SSL certificate is required to provide secure, HTTPS access to your Dome Antispam admin console. The 'Certificate Entrance' screen lets you choose which type of SSL certificate you wish to use. You have two options:

- 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 Dome Antispam console on the AWS instance. Details of your Dome Antispam domain will have been sent to your registered email after you signed up for the account.
- Use the default, self-signed certificate. Dome Antispam 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.

- Click next to enter admin details such as 'System Admin Name', 'System Admin Surname', 'System Admin Tel. No' and 'System Admin E-mail'.

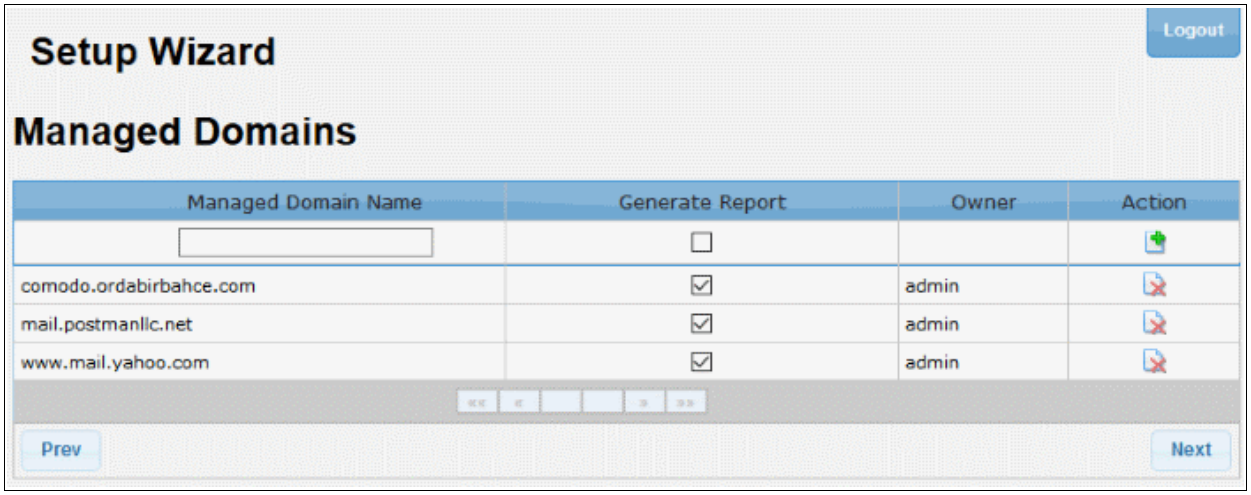


- Click 'Next', to enter 'LDAP' information:



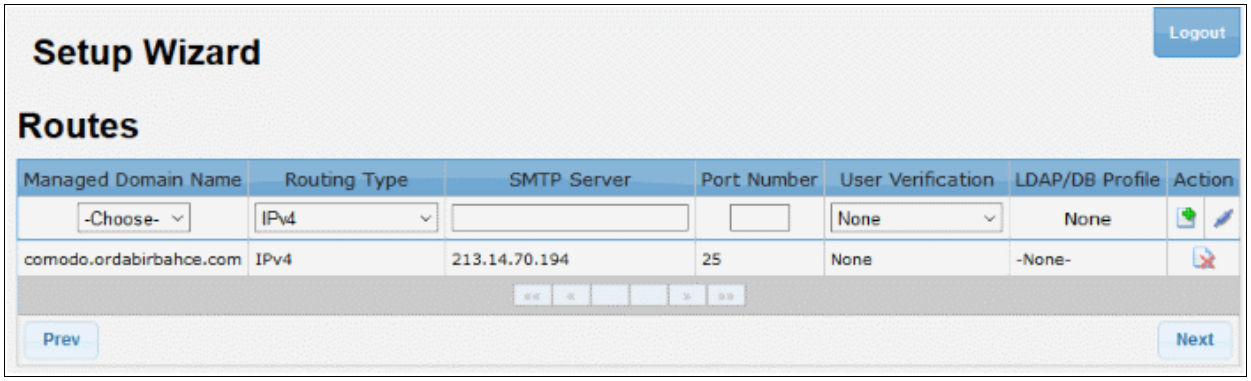
Refer to the LDAP section for more details.

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



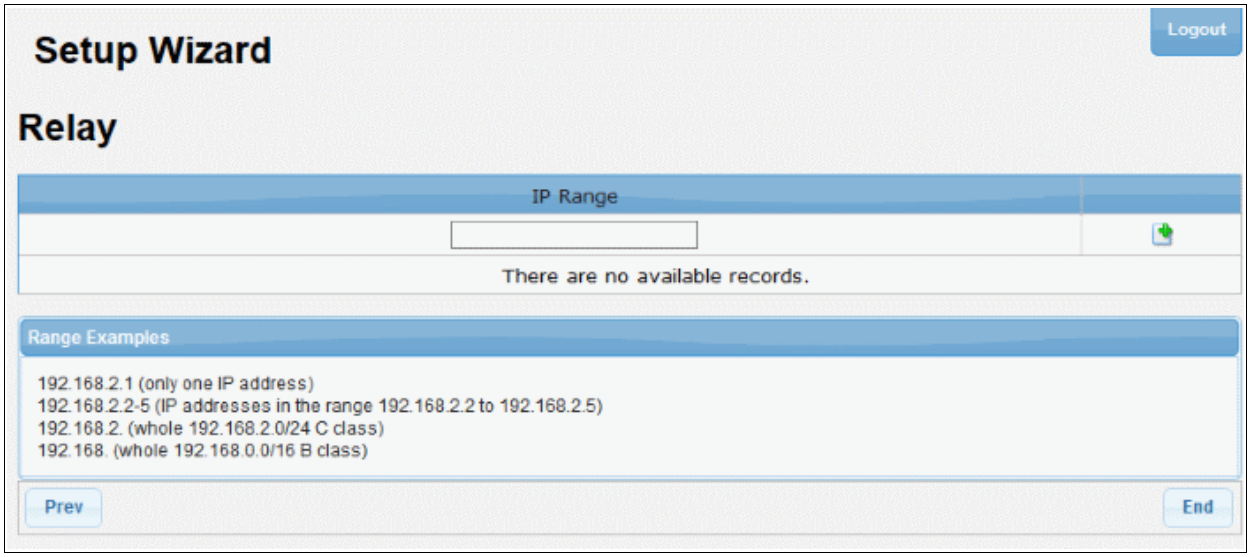
Refer to the Manage Domains section for more details.

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



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

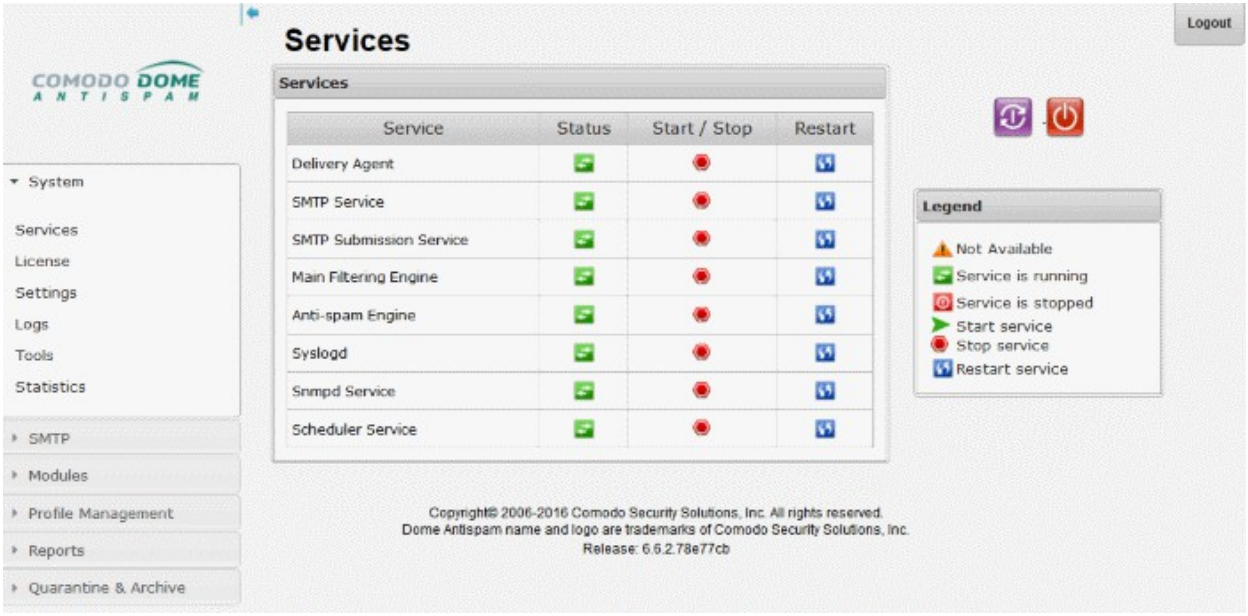
- Click 'Next', to enter details of 'Relay'.



Refer to 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

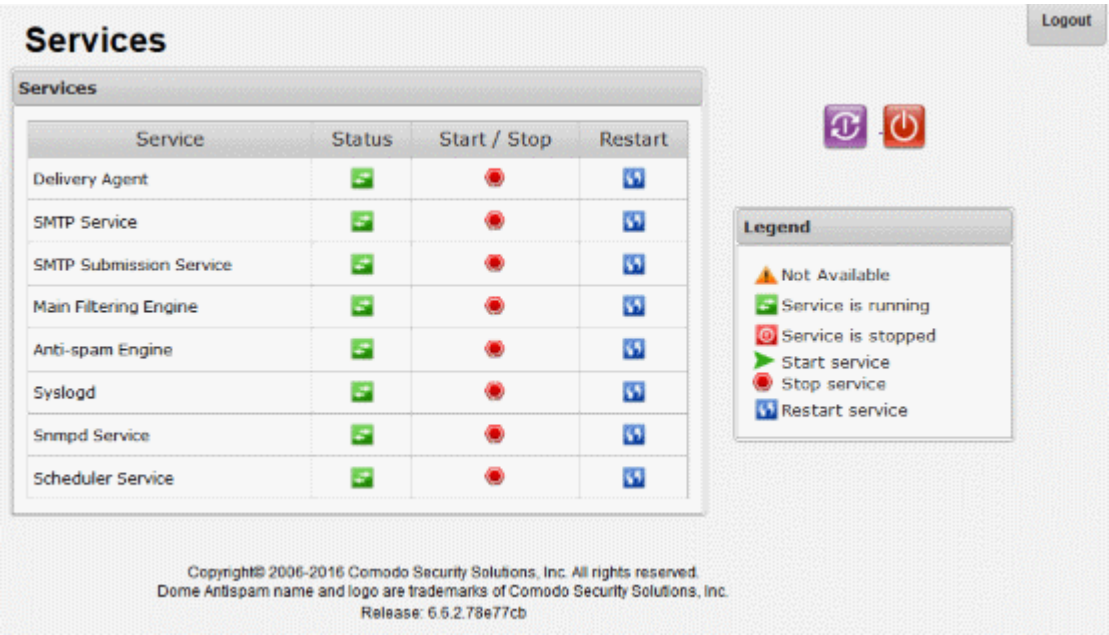


- **Services**: Allows you to start or stop various services such as delivery agent, SMTP, Snmpd, scheduler and more. Refer to the section '**Services**' for more details.
- **License:** View and update Dome Antispam licenses from this interface. Refer to the section '**License**' for more details.
- **Settings:** Configure various system settings such as Cache, Session, Backup and more. Refer to the section '**Configuring System Settings**' for more details.
- **Logs:** View and download mail log files and configure how long the system should retain mail log records, archived mails and quarantined mails. Refer to the section '**Logs**' for more details.
- **Tools:** Allows admin users to check connectivity such as SMTP, Ping, Nslookup, Telnet as well as clear SMTP queue. Refer to the section '**Tools**' for more details.
- **Statistics:** View the graphical summary of system usage. Refer to the section '**System Usage Statistics**' for more details.

3.1 Services

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

- To view and configure Dome Antispam services, click the 'System' tab on the left then 'Services':



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

Description of the Services	
Column Header	**Description**
Dome Antispam Delivery Agent	The service forwards the emails processed by Dome Antispam to target email server.
Dome Antispam SMTP Service	The service that filters emails on hosted domain names on Dome Antispam. 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 - Dome Antispam 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.
Dome Antispam 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 Dome Antispam Delivery Agent.
Anti-spam Engines	Dome Antispam engines scans emails and specifies spam scores controlling thousands of spam signatures such as header and bayesian-based content filtering. This scores are used to define an e-mail as spam.
Dome Antispam DB Connector	The Postgre SQL services running on Dome Antispam's internal database of quarantined emails and archives.
Syslogd	The daemon service that stores system logs in rsyslog format.
Snmpd Service	It is an Simple Network Management Protocol (SNMP) agent which binds to port and acts on SNMP management application's requests and sends the requested information to the requester.

Anti-virus Module	Dome Antispam includes Comodo's anti-viurs programs as a built in solution.
Scheduler Service	This service organizes the programs that runs periodically. This feature in Dome Antispam 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.

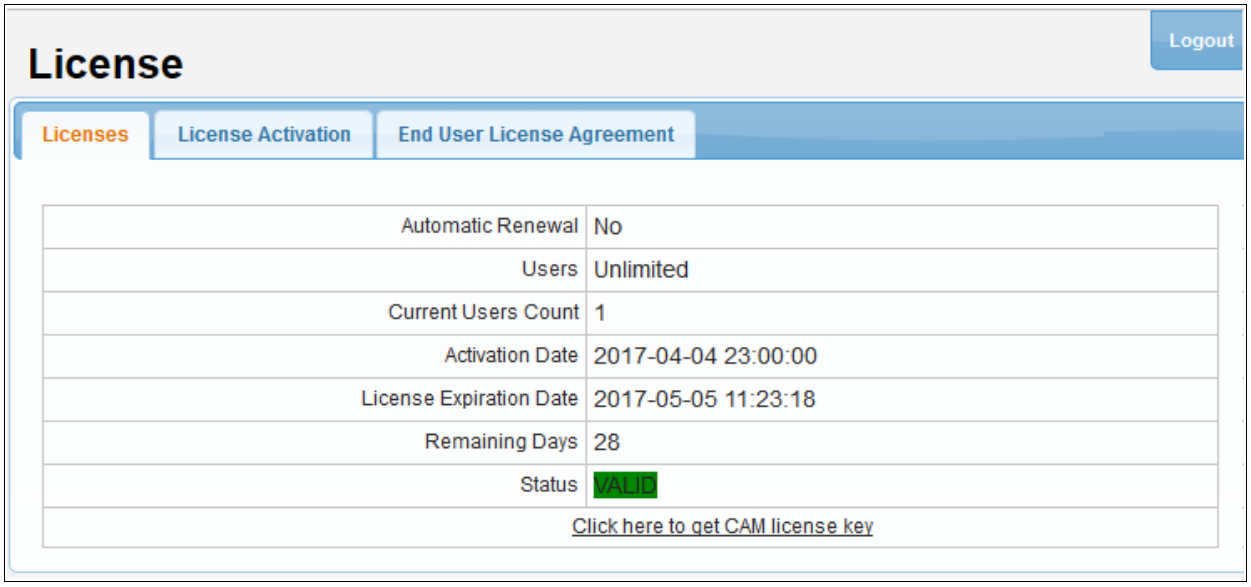
- To restart a service, click on the button under the 'Restart' column. If the service is running, it will stop and restart again. If the service is stopped, then it will restart.
- To shutdown the Dome Antispam, click on the button.
- To reboot the Dome Antispam, click on the button.

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. Dome Antispam 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 Dome Antispam license, click the 'System' tab on the left menu,then 'License'

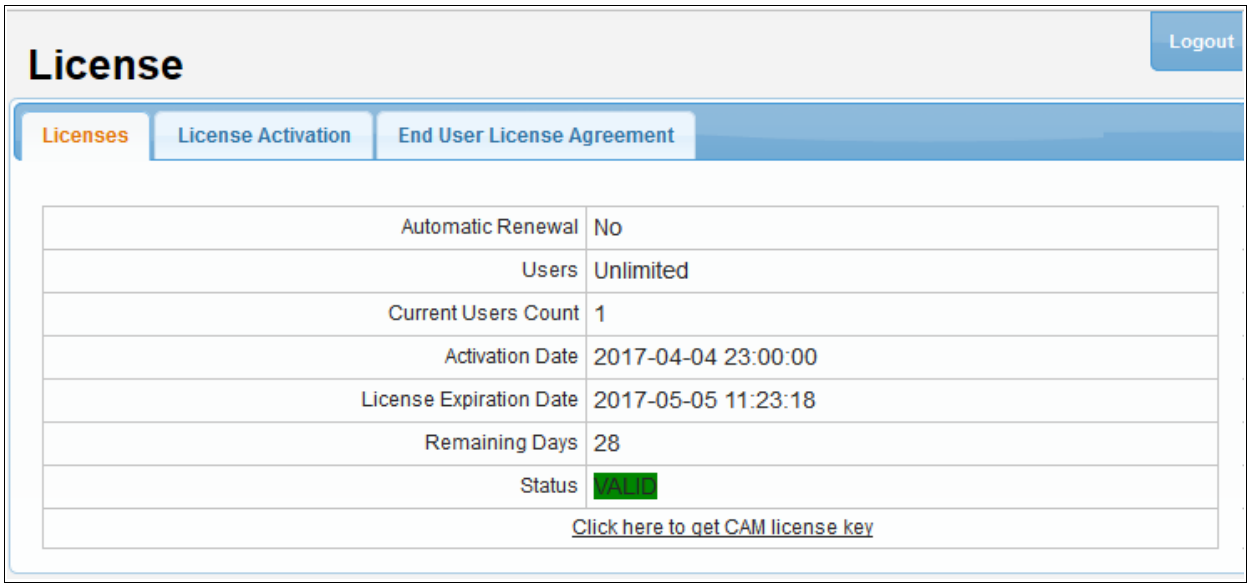


From here you can:

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

To view the details of current license

- Click the 'Licenses' tab

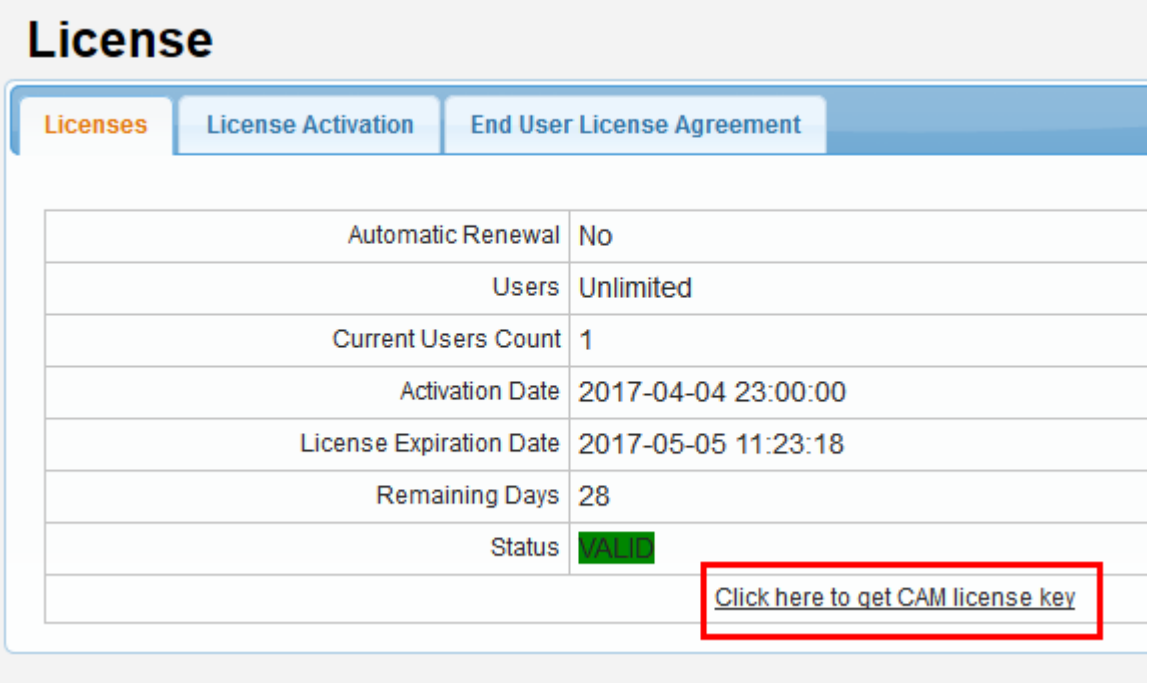


License - Table of Column Descriptions	
Column Header	**Description**
CAM Automatic Renewal	Indicates whether automatic license renewal is enabled.
CAM Max Users	Maximum quantity of users that can be enrolled
CAM Current User Count	Number of users currently using the product license

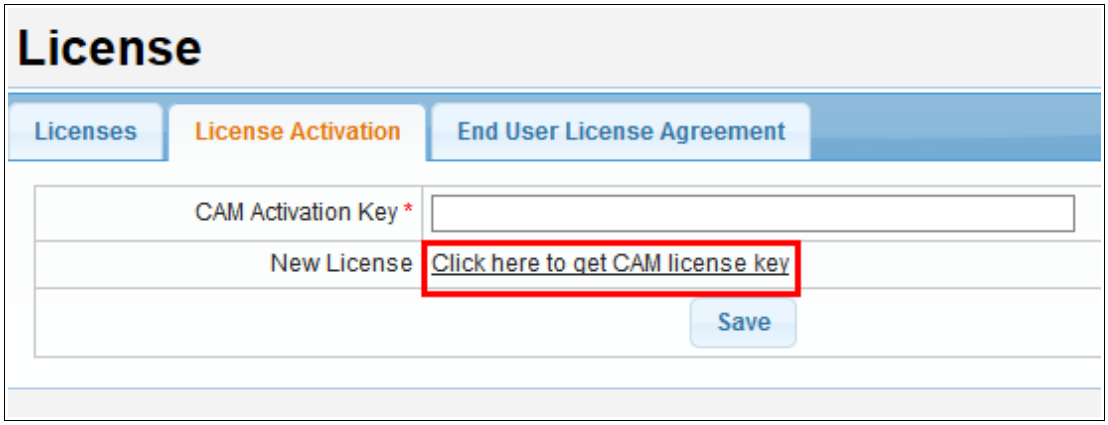
CAM Activation Date	Date when the license was activated.
CAM License Expiration Date	Date when the license expires.
Remaining Days	Number of days left before the license expires.
CAM License Status	Indicates whether the license is valid or expired.

To purchase a license

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



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



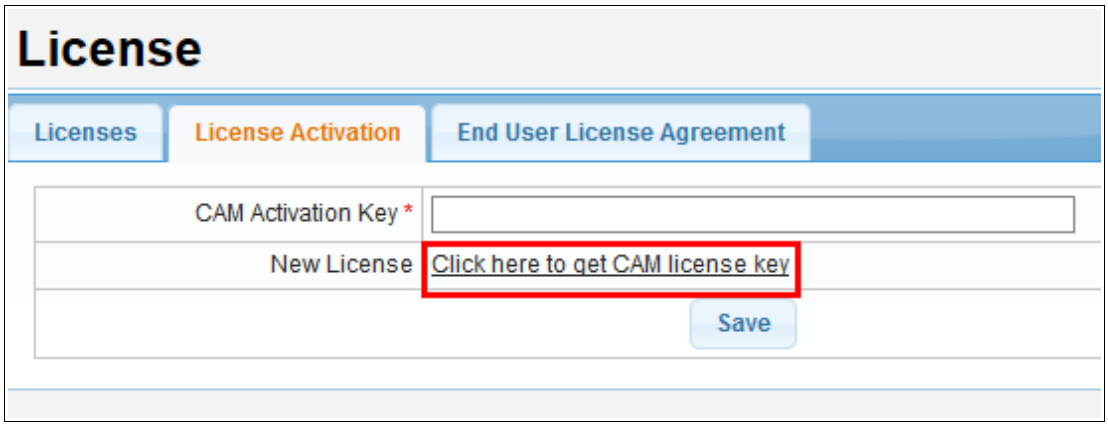
You will be taken to Comodo Accounts Manager (CAM) login page at https://accounts.comodo.com/account/login

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

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

To activate your license

- Click the 'License Activation' tab.

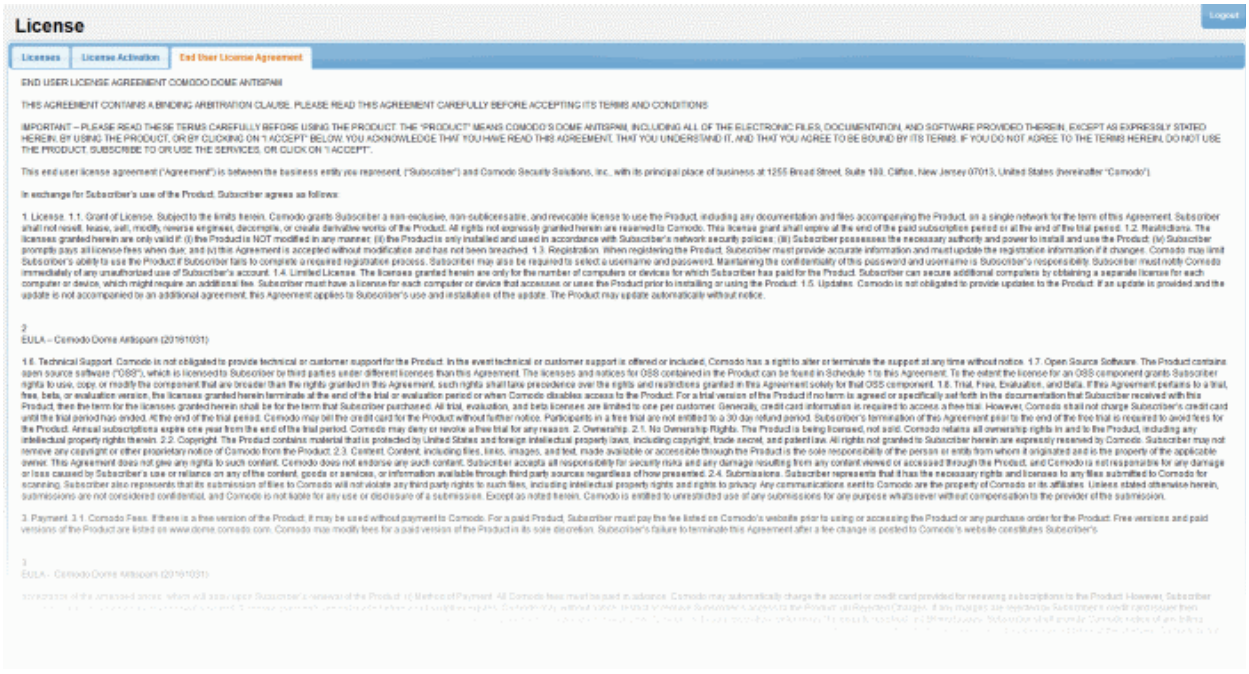


- Copy and paste the license key that was sent to your email address from Comodo in the 'CAM Activation Key' field.
- Click the 'Save' button.

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

End User License Agreement (EULA)

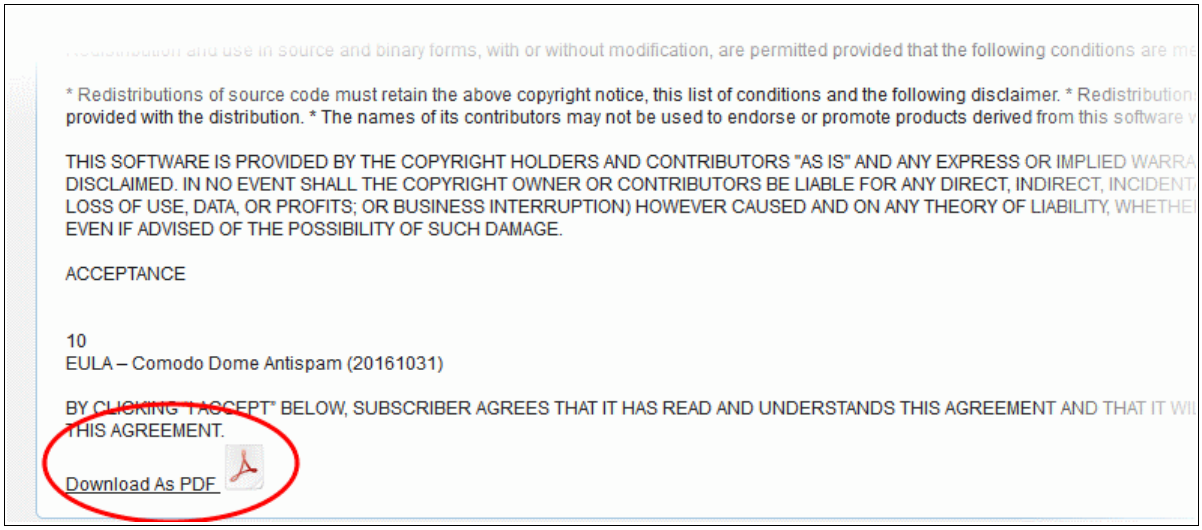
- Click the 'End User License Agreement' tab.



- 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.

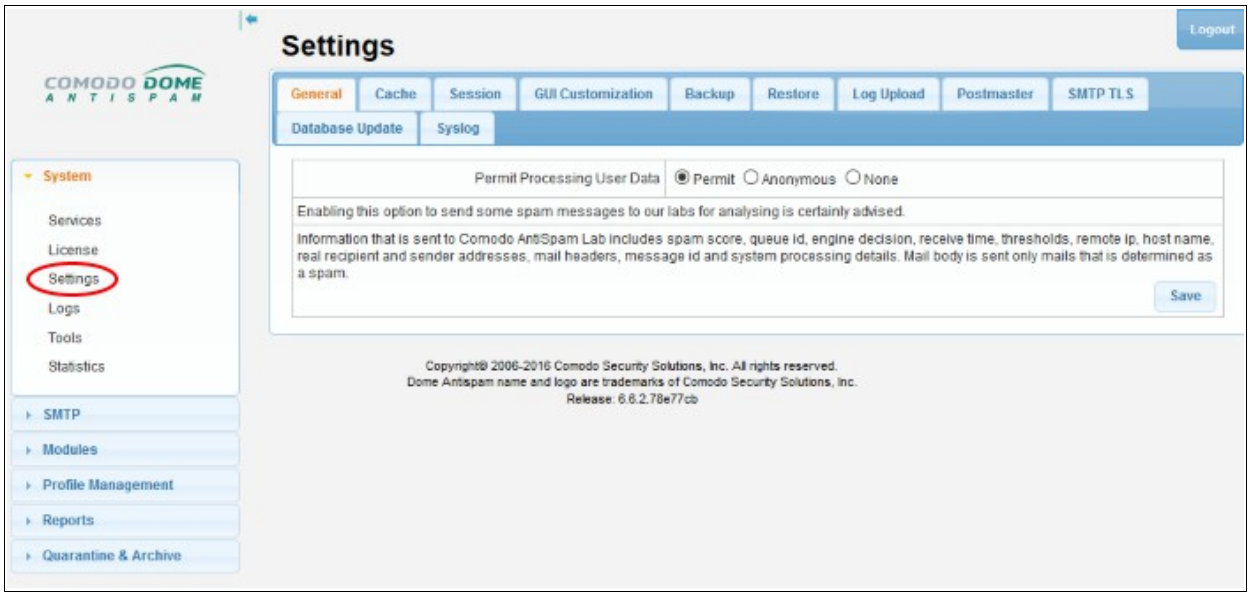


The pdf will be downloaded.

3.3 Configuring System Settings

The 'Settings' interface lets you configure all aspects of Dome Antispam.

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



Click the following links for more details:

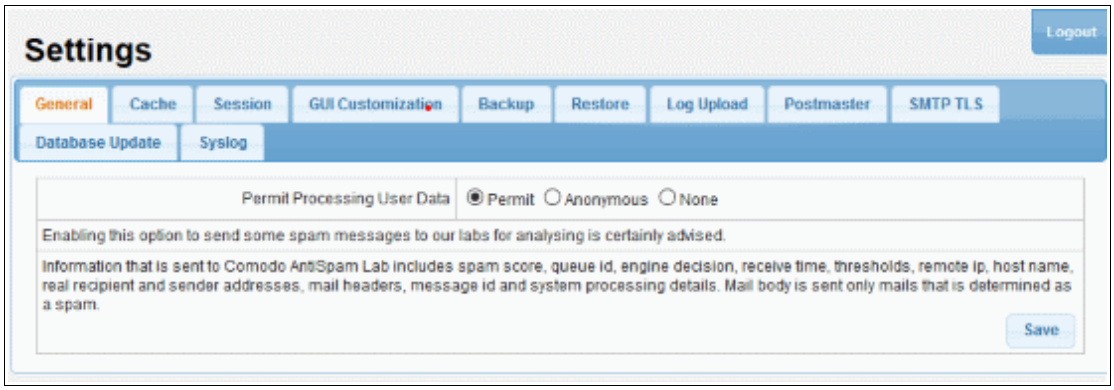
- General
- Cache
- Session
- GUI Customization
- Backup
- Restore
- Log Upload
- Postmaster

- SMTP TLS
- 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'.

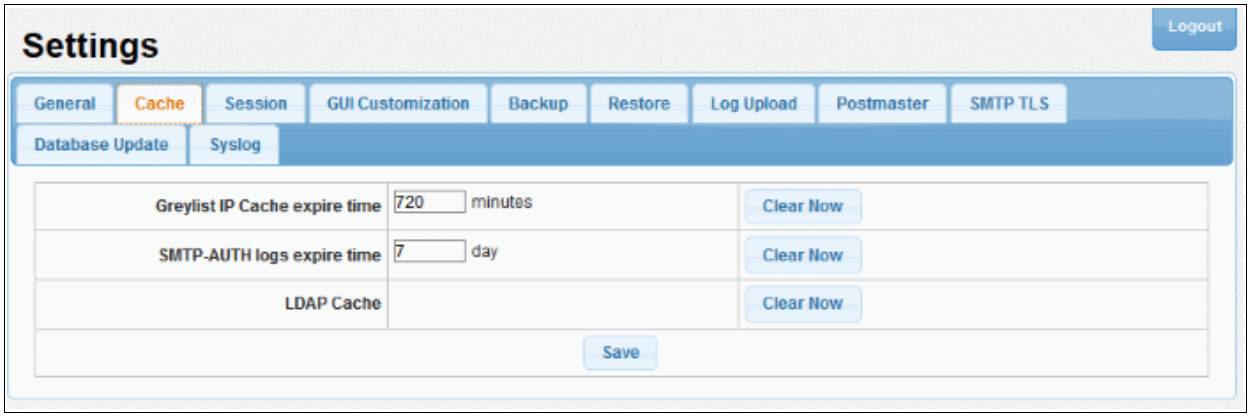


- **Permit Processing User Data:**
  - Permit - Selected spam messages will be uploaded to Comodo labs for analysis.
  - Anonymous - Selected spam messages will be uploaded anonymously, without data which links them to your company or users.
  - None - Spam messages will not be uploaded to Comodo.
-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



- **Greylist IP Cache expire time:** Dome Antispam 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.

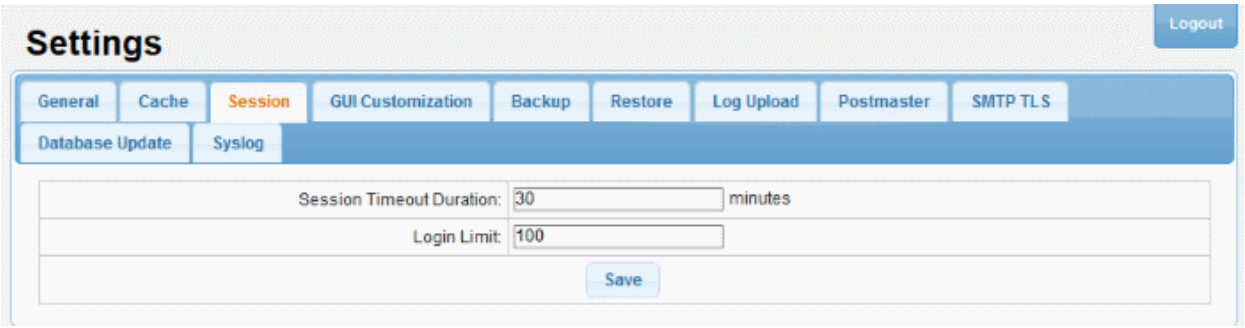
- **SMTP AUTH logs expire time:** The end user authentication log details of SMTP clients are cached for the entered days and after that they are deleted.
- **LDAP Cache:** LDAP authentication details are cached and Dome Antispam does not query the LDAP server.

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

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'.

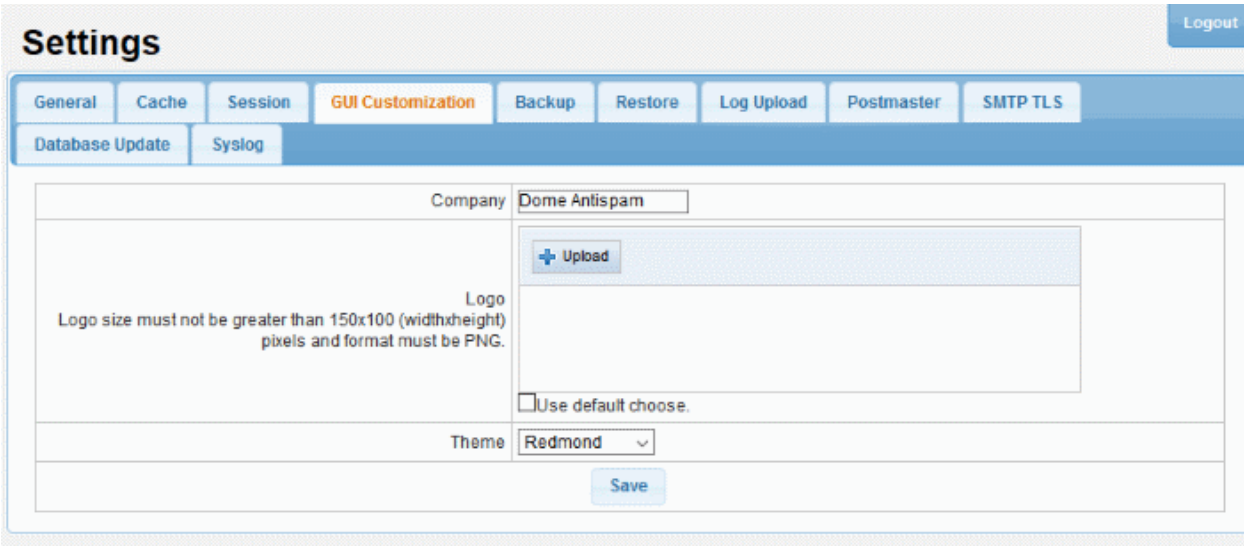


- **Session Timeout Duration:** Determines how many minutes of inactivity should be allowed before all users are automatically logged out.
- **Login Limit:** Enter the maximum amount of users that can login to the portal at the same time.
- Click the 'Save' button to apply your changes.

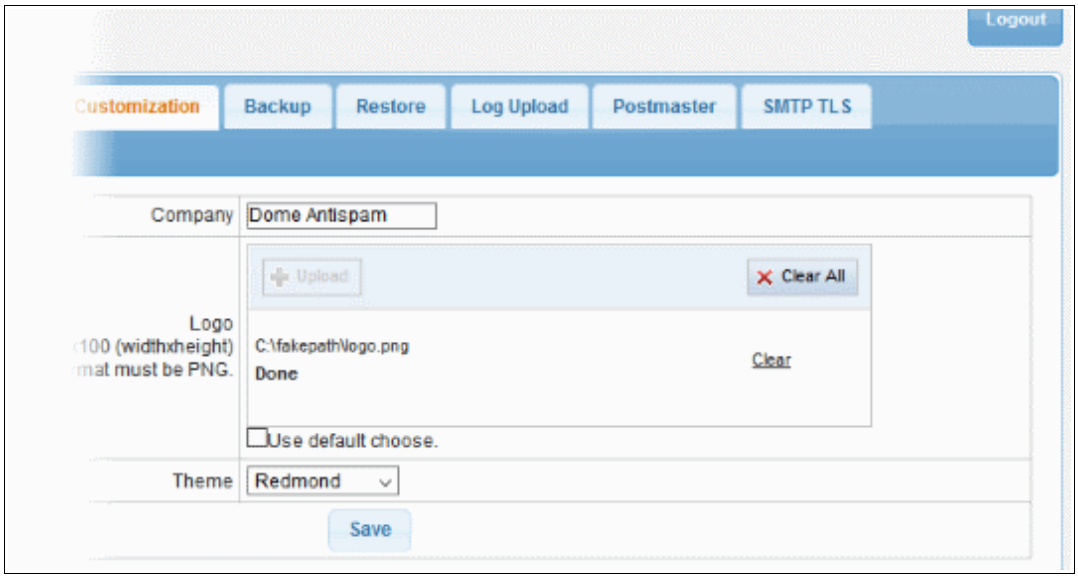
3.3.4 GUI Customization

The 'GUI Customization' tab lets you customize the look and feel of the console. 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'



- **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.

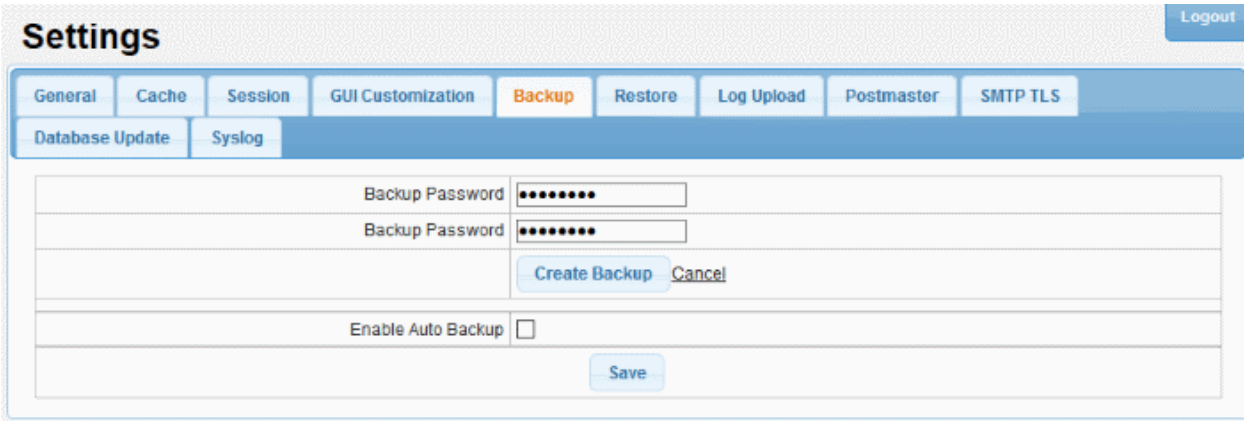


  - To remove the logo, click the 'Clear' link.
  - Click the 'Save' button to upload the logo.
- **Theme:** The 'Themes' drop-down allows you to choose the colors and appearance of the GUI as you prefer *(Default = Redmond Theme).*
- Click the 'Save' button to apply your changes.

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.

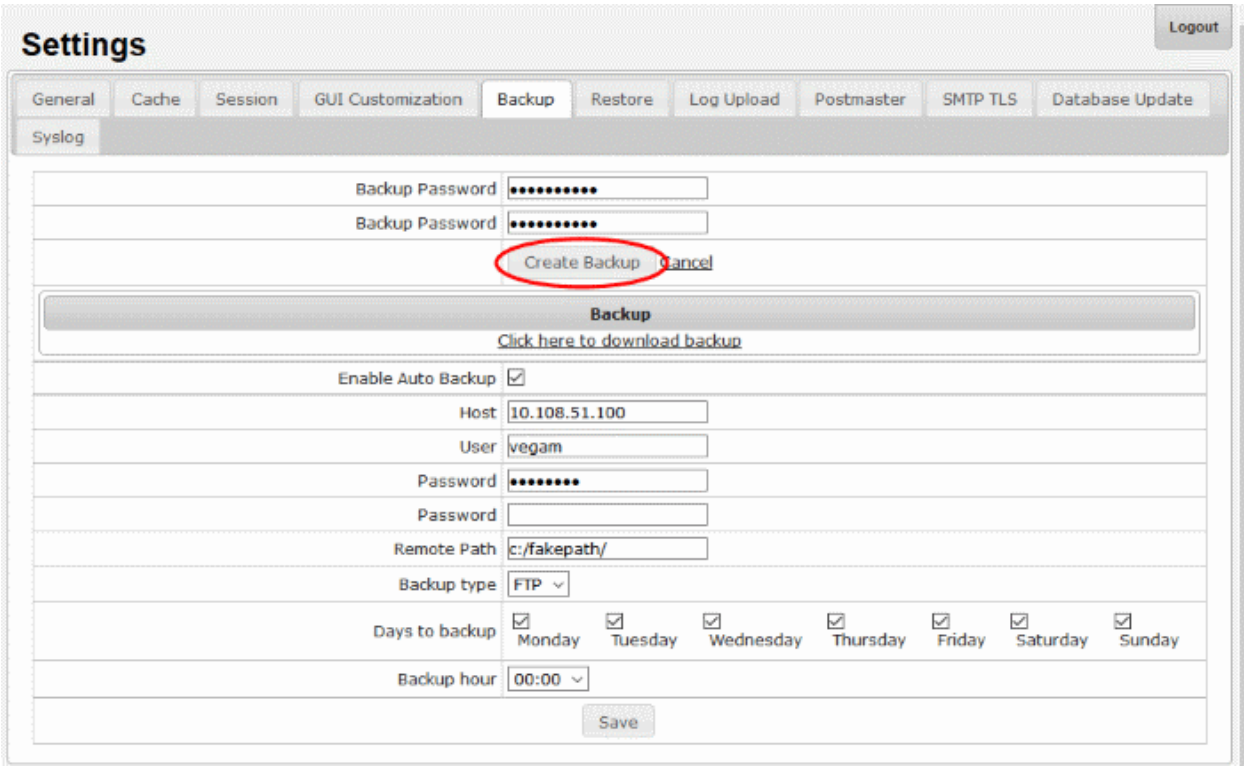
- To open the 'Backup' settings interface, click the 'System' tab on the left menu, then 'Settings' and 'Backup' tab.



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.



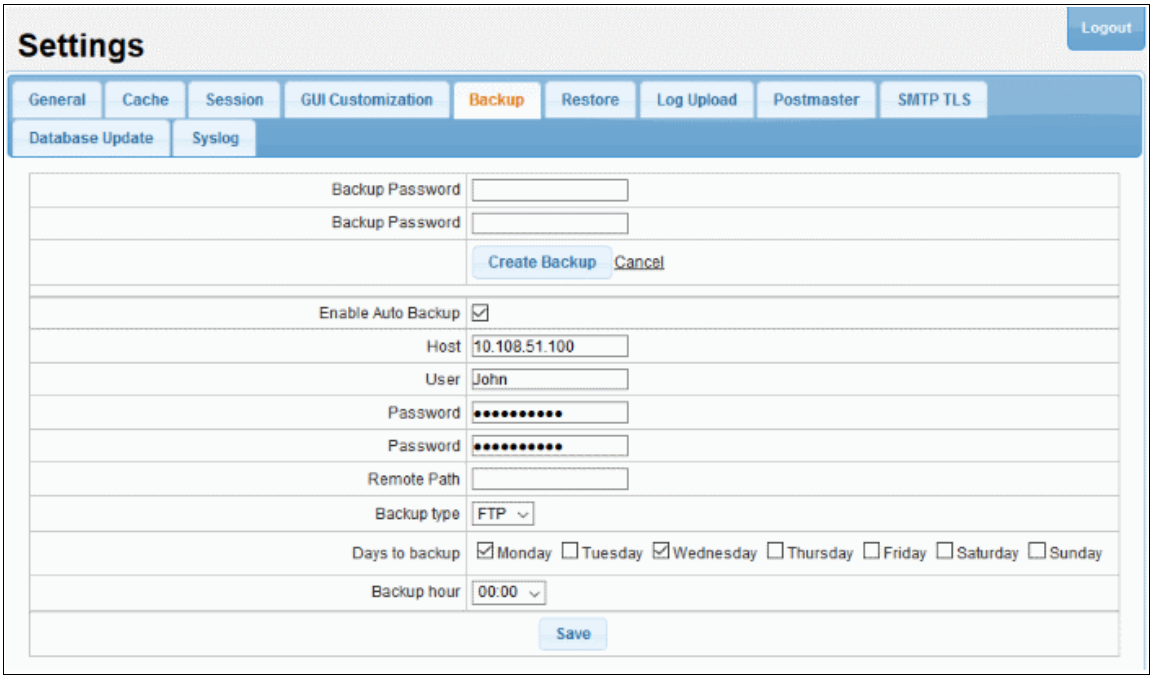
- Click the 'Click here to download backup' link.

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

Scheduled Backup

You can automate the backup process by scheduling the jobs.

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



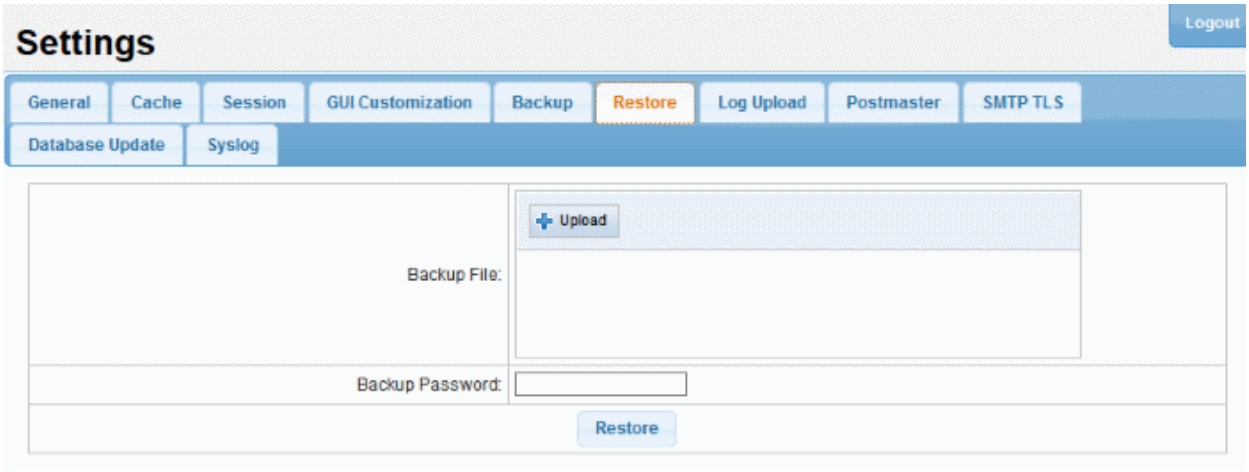
- **Host:** The name or IP of the system where the data should be backed up.
- **User:** The user name of the system
- **Password:** Enter the password to access the system
- **Remote Path:** Enter the remote path of the system including the folder name. Leaving the field blank means the backup will be uploaded to the default FTP folder.
- **Backup type:** Select the backup type from the drop-down. Currently only FTP option is available.
- **Days to backup:** Schedule the backup day(s) from the options.
- **Backup hour:** Select the hour when the scheduled backup should run on the selected backup day(s)

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

3.3.6 System Restore

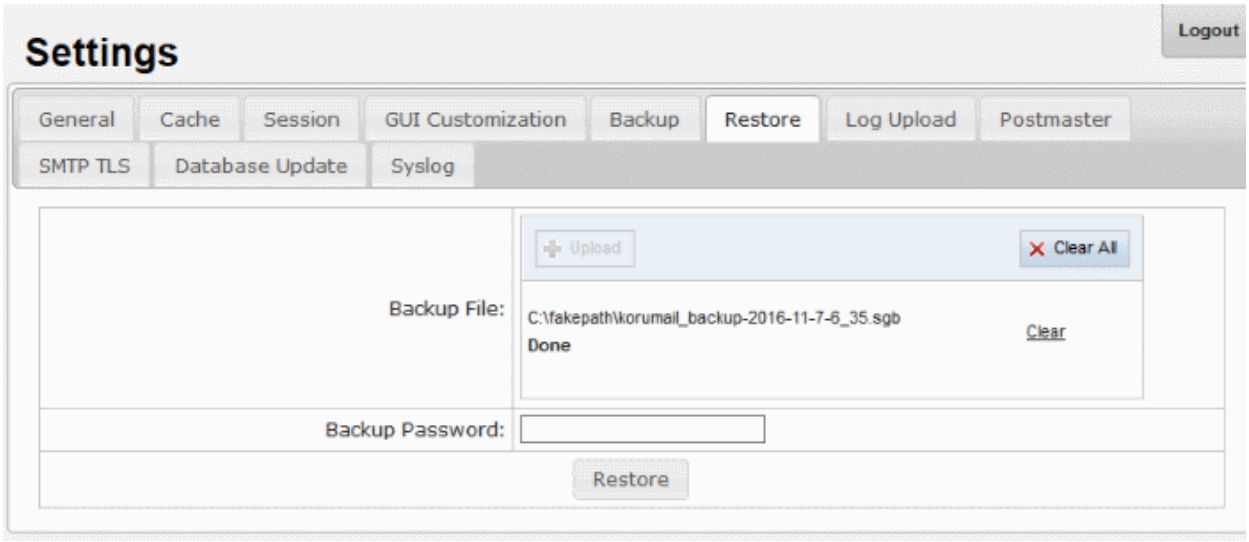
The 'Restore' feature allows you to revert your Dome Antispam configuration and logs to a previous system state. The console will need to be rebooted in order to complete a restore operation.

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

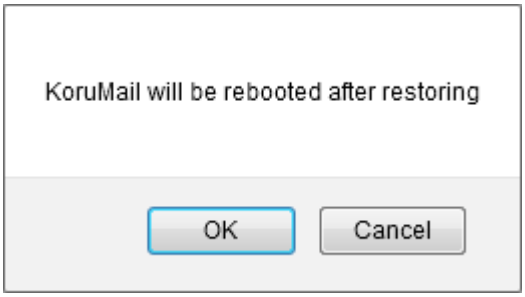


- To restore, click the 'Upload' button, navigate to the location where the backup file is saved and click 'Open'.

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



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

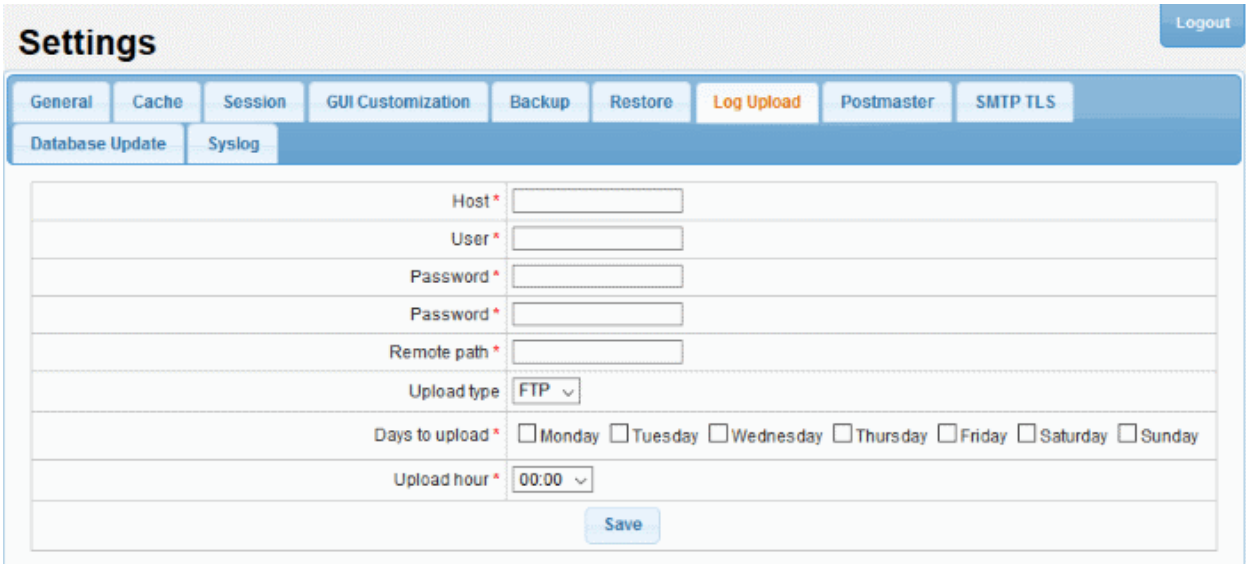


The console has to be rebooted to complete the restore operation. Click 'OK' to confirm.

3.3.7 Log Upload Settings

The 'Log Upload' tab allows you to configure the automated upload of various types of Dome Antispam logs.

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

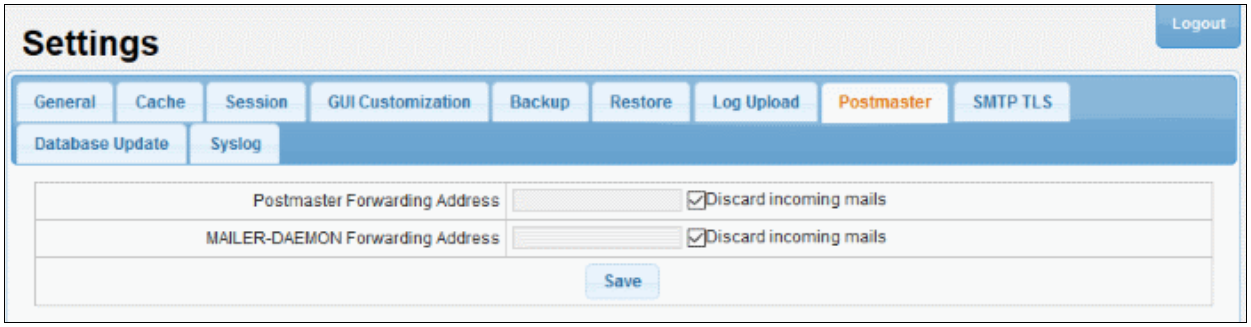


- **Host:** The name or IP of the system where the logs should be uploaded.
- **User:** The user name of the system
- **Password:** Enter the password to access the system
- **Remote Path:** Enter the remote path of the system including the folder name. Leaving the field blank means the logs will be 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 the 'Save' button. The scheduled job will be saved. To change the schedule or the upload location, edit the settings accordingly and click the 'Save' button.

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. Dome Antispam allow administrators to forward these to other addresses and /or reject emails sent to these addresses.

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

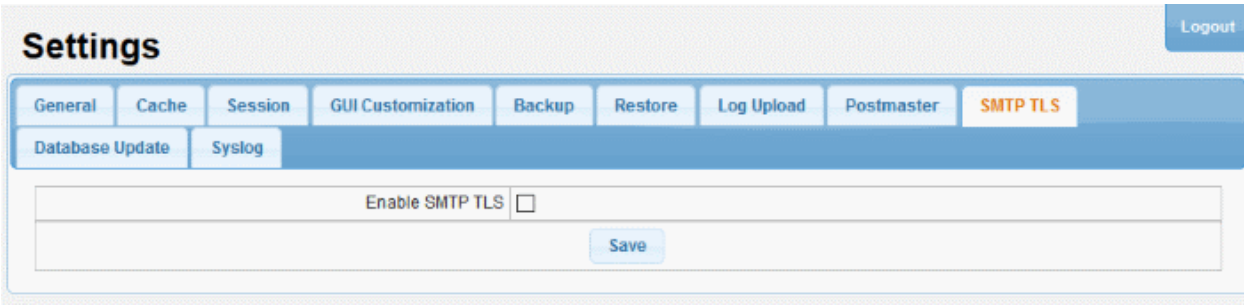


- **Postmaster Forwarding Address:** Enter the forwarding address to which the email to postmaster are directed.
- **MAILER-DAEMON Forwarding Address:** Enter the forwarding address to which the Mailer Daemon notifications are to be directed.
- **Discard incoming mails:** Select the check box if the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

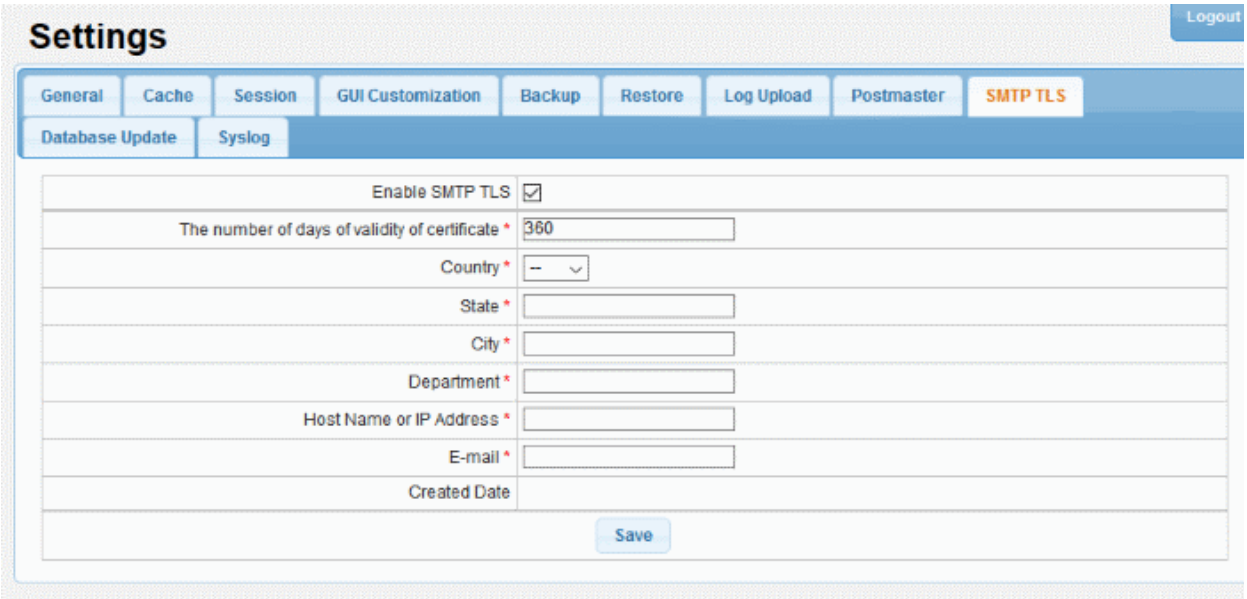
3.3.9 SMTP TLS Settings

The 'SMTP TLS' (Transport Layer Security) area lets you enable encryption for email traffic. A certificate must be installed on your mail server if your enable TLS encryption.

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



- **Enable SMTP TLS:** Enable TLS to encrypt messages transmitted between Mail Transfer Agents (MTAs). Please enter the details of your TLS certificate in the fields provided:



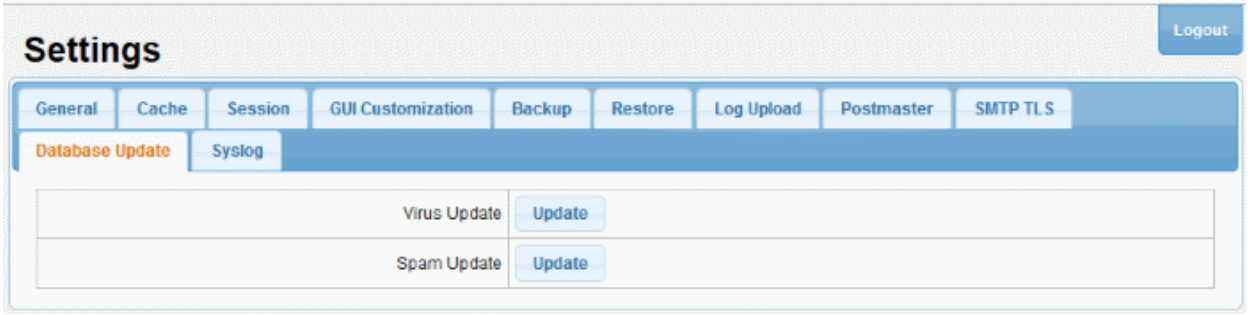
- Click the 'Save' button.

3.3.10 Update Database

Dome Antispam updates virus and spam databases once per day. If required, the databases can be updated

instantly from 'Database Update' tab.

- To open the 'Database Update' settings interface, click the 'System' tab on the left menu then click 'Settings' > 'Database Update'.

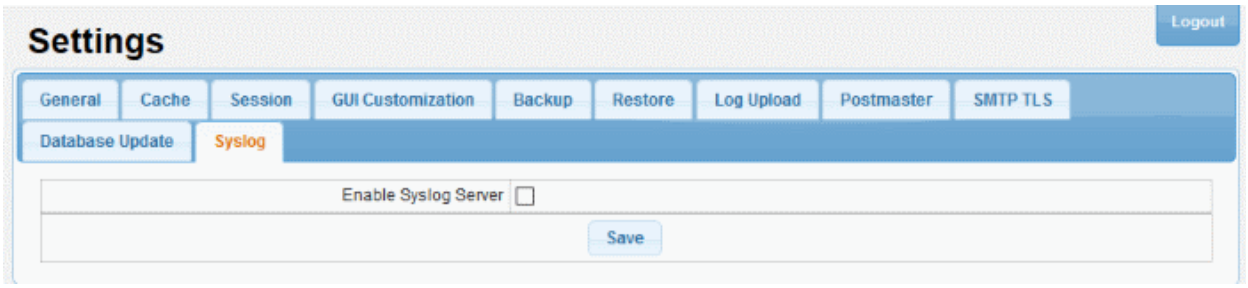


- **Virus Update:** Click the 'Update' button to update the virus database
- **Spam Update:** Click the 'Update' button to update the spam database

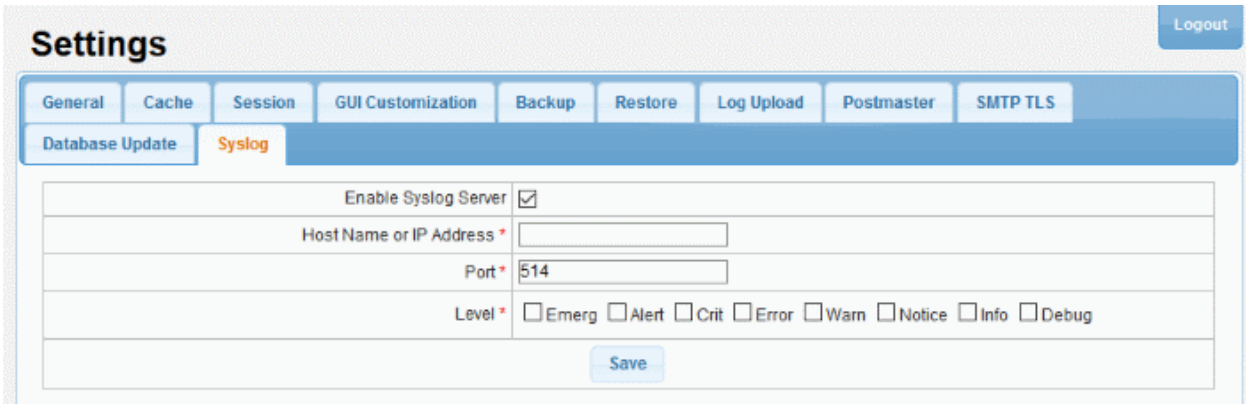
3.3.11 Syslog Server

Dome Antispam has the ability to forward logs pertaining to various operations and configuration changes to a remote Syslog server.

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



- **Enable Syslog Server:** Enable this to store logs on your remote server. Enter your Syslog server details in the fields provided:



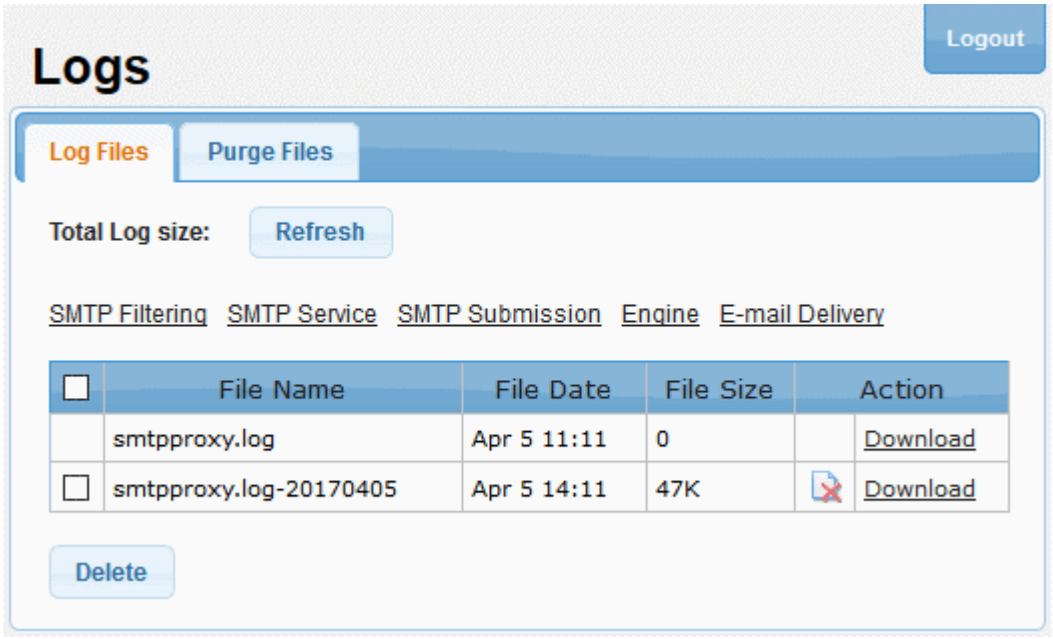
- **Host Name or IP Address**: Enter the host name or the IP address of the remote logging server to which the logs should be passed.
- **Port:** Enter the port number through which the server receives the logs. Default is 514.

- **Level**: Specify the types of logs by severity level that you want to forward to the remote logging server.
- Click the 'Save' button.

3.4 Logs

Dome Antispam 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.

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



The 'Logs' interface has the following tabs:

- Log Files
- Purge Files

3.4.1 Log Files

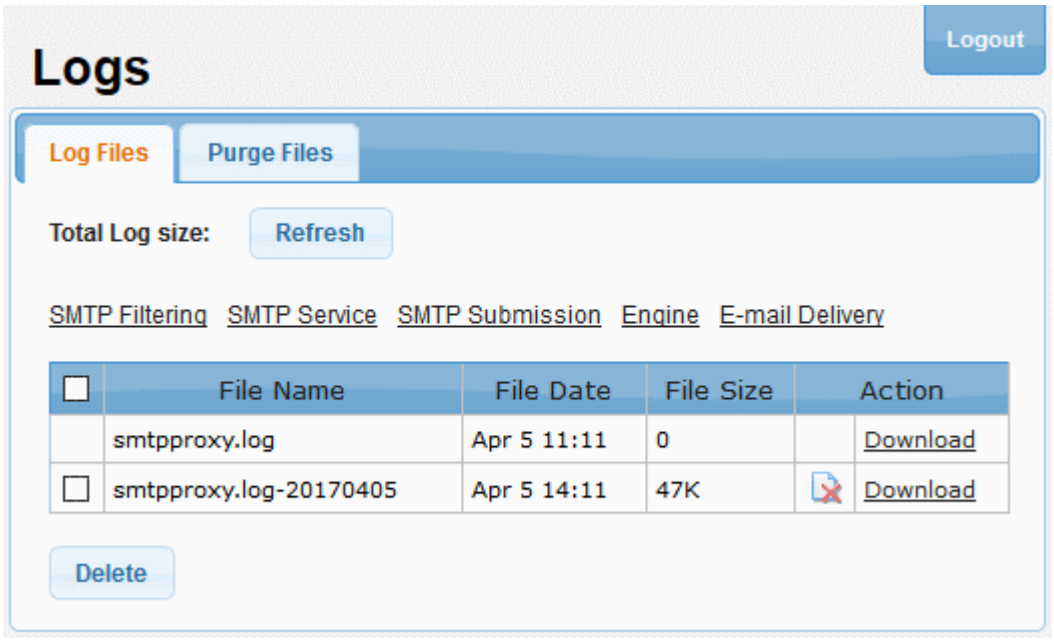
The 'Log Files' tab displays available log files for different activities and connection attempts. These include:

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

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

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

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



- The interface displays the total size of all log files available.
- Clicking 'Refresh' reloads the list to include the latest logs.
- The links above the table enable admins to choose the category of logs they wish to manage.

Log Files - Table of Column Descriptions		
Column Header	**Description**	
File Name	Name of the log file	
File Date	The precise date and time at which the log file was created.	
File Size	The size of the log file.	
Actions		Delete selected logs.
	Download	Download selected logs.

To download a log file

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

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

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

To delete an unwanted log file

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

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

- Click the delete icon in the row of the log you wish to delete.
- Click 'OK' in the confirmation dialog.

To delete several unwanted log files

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

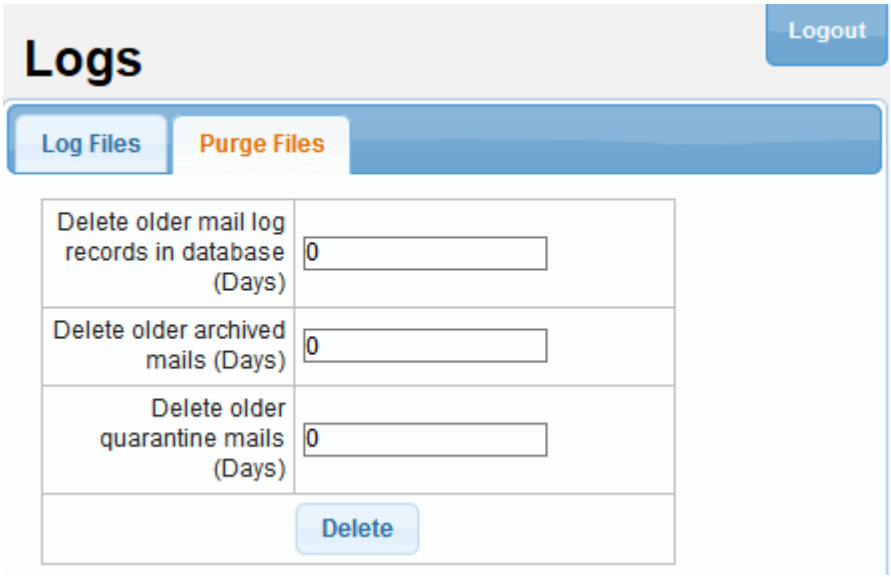
The list of available log files under the chosen category will be displayed.

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

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.

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

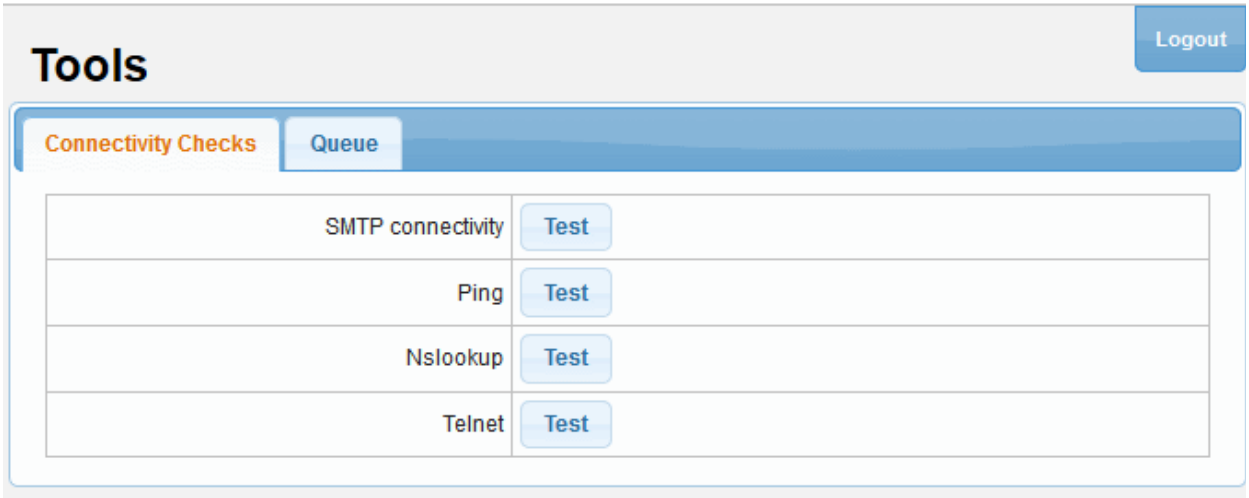


- Delete older mail log records in database (Days) - Specify the number of days to store the log files. The log files older than the days specified here will be automatically deleted.
- Delete older archived mails (Days) - Specify the number of days for which the quarantined mails are to be retained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

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

- To open the 'Tools' interface, click the 'System' tab on the left menu and then click 'Tools' from the sub-menu.



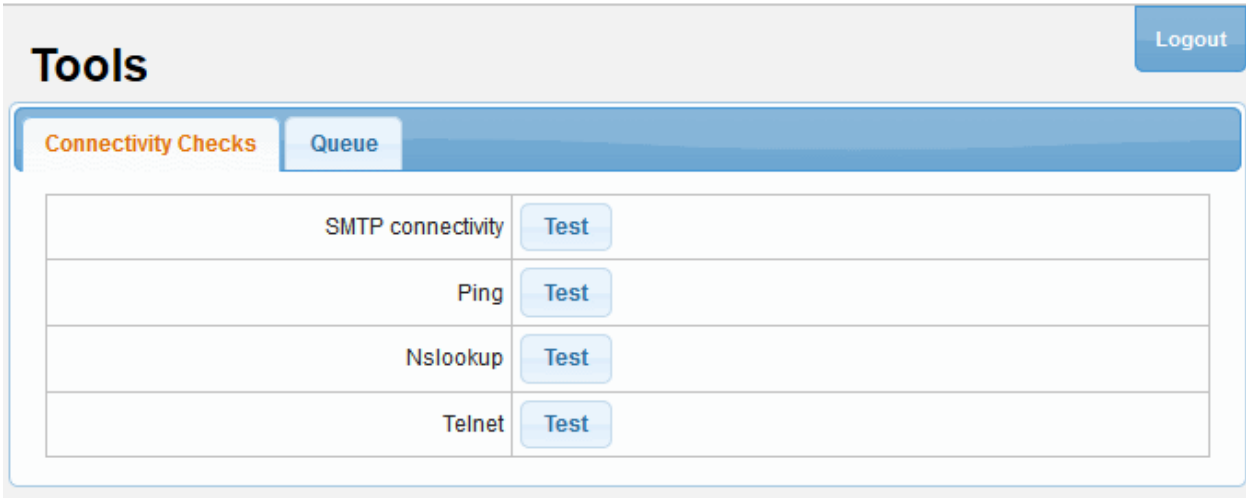
The 'Tools' interface has two tabs:

- Connectivity Checks
- SMTP Queue

3.5.1 Check Connectivity

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

- To open the interface, click the 'System' tab on the left then 'Tools' > 'Connectivity Checks'.

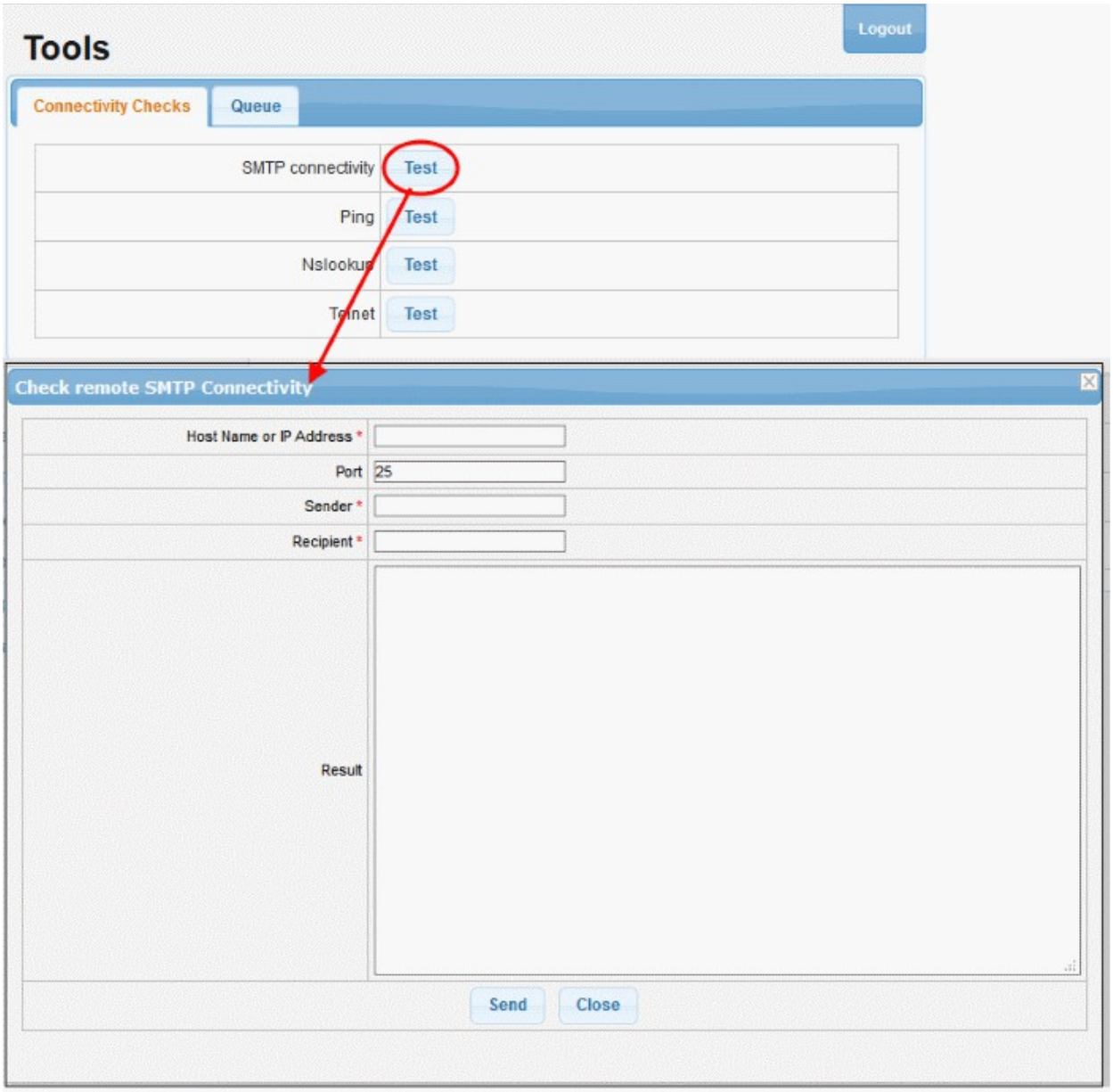


You can check for the following:

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

To check connection to a SMTP server

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



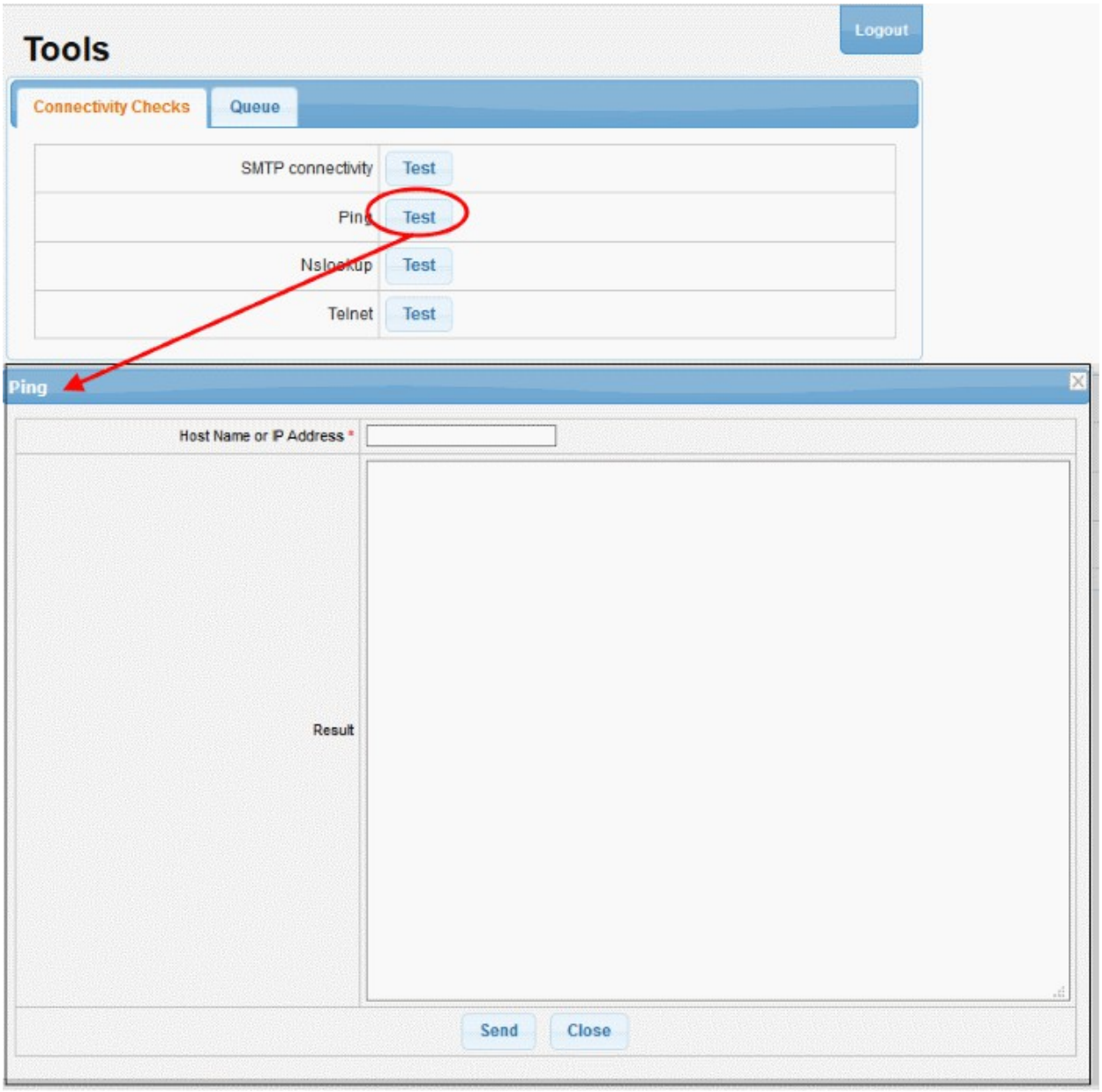
The 'Check remote SMTP Connectivity' interface will appear.

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

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

To check connectivity to a remote host

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



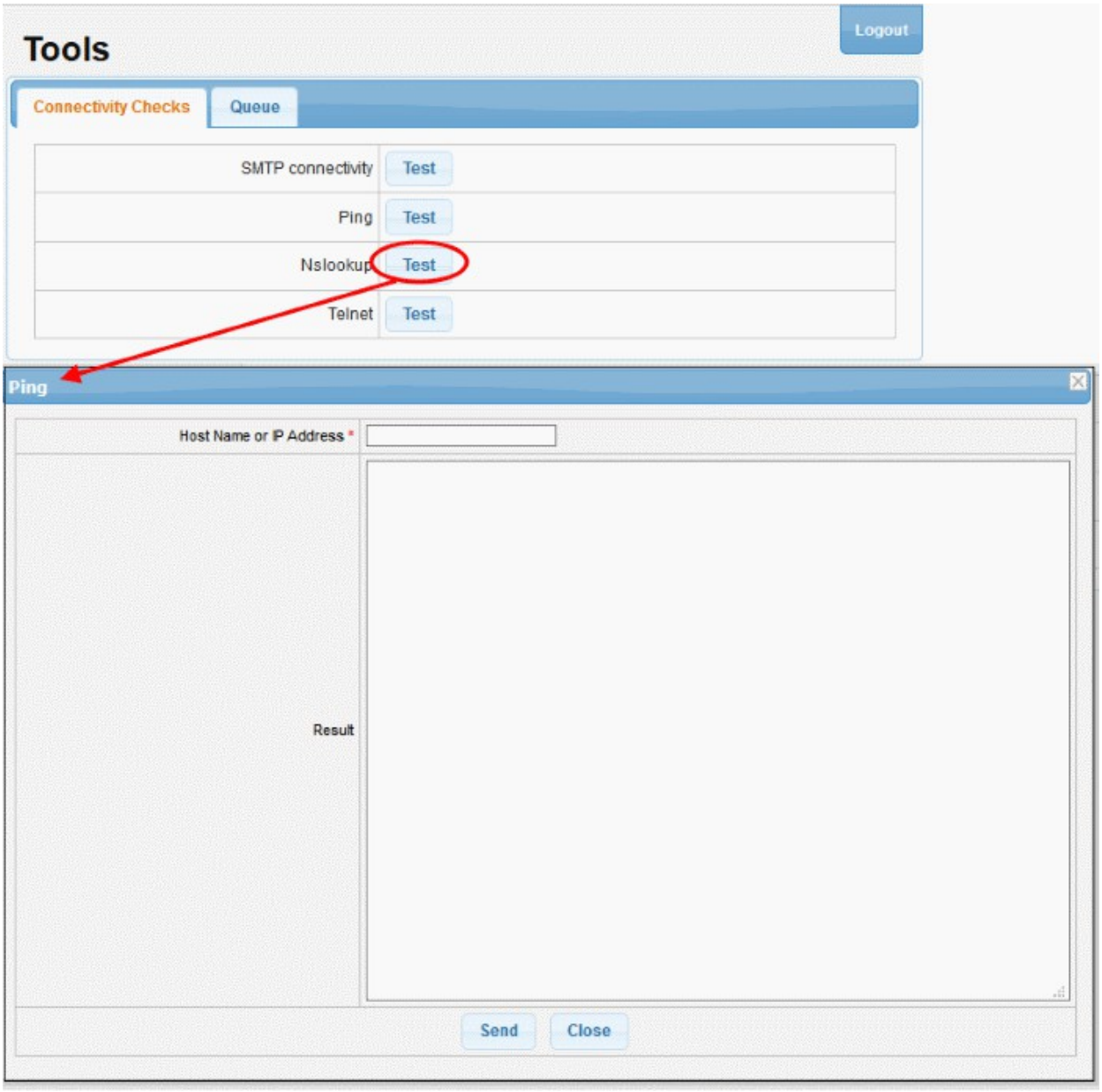
The 'Ping' interface will appear.

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

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

To lookup name server for a remote host

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



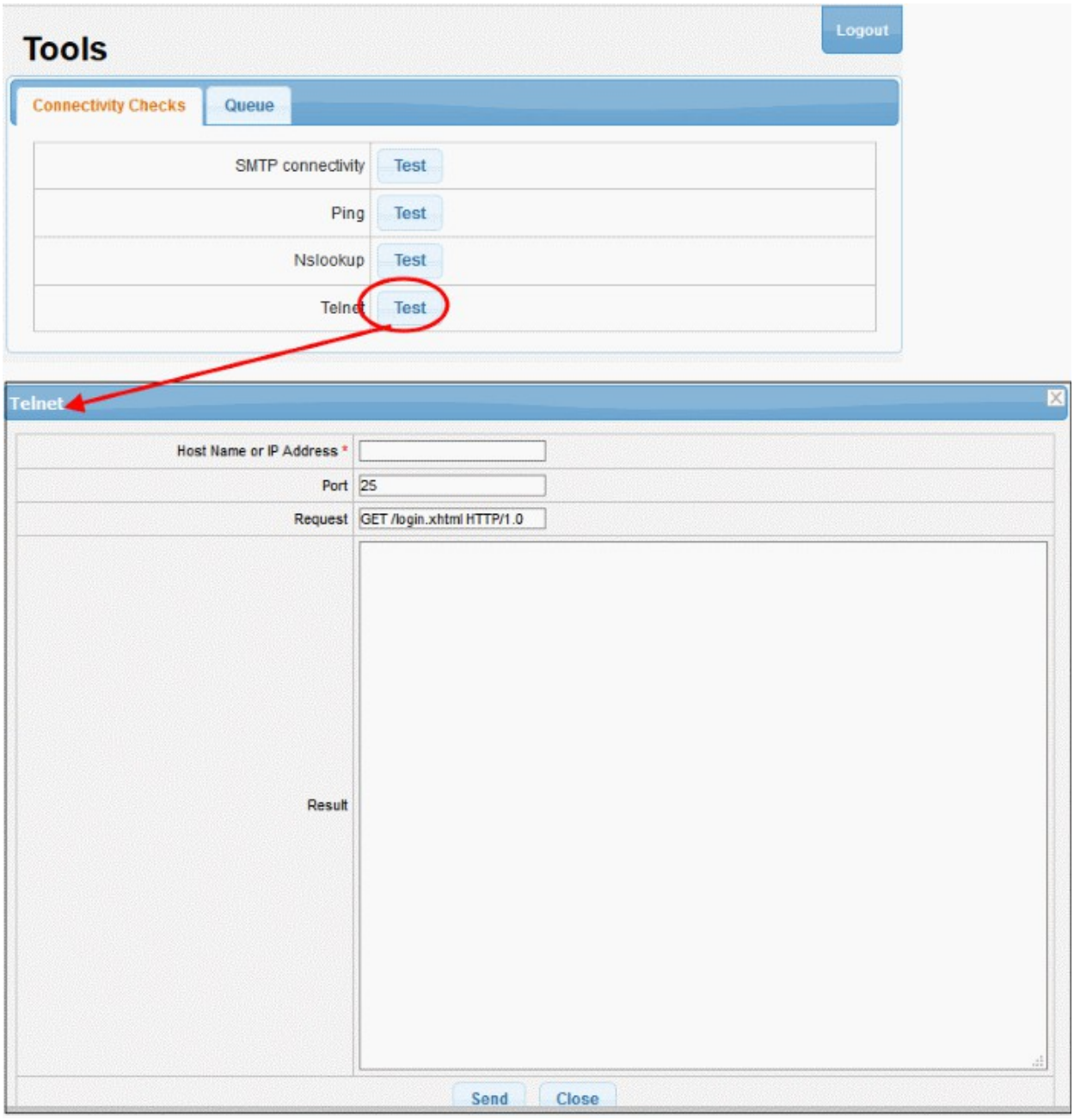
The 'Nslookup' interface will appear.

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

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

To check Telnet connectivity to a remote host

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



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).
- Dome Antispam 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'

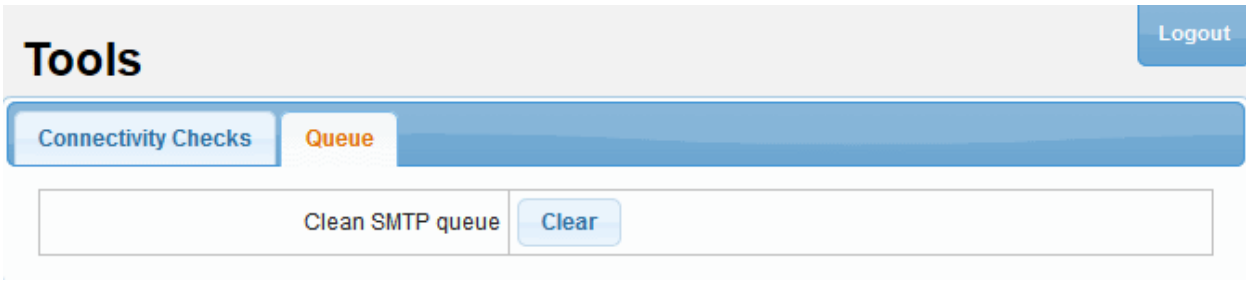
Dome Antispam will send the request to the remote host for checking the Telnet connectivity and display the results in the 'Result' field.

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.

To clear the SMTP queue

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

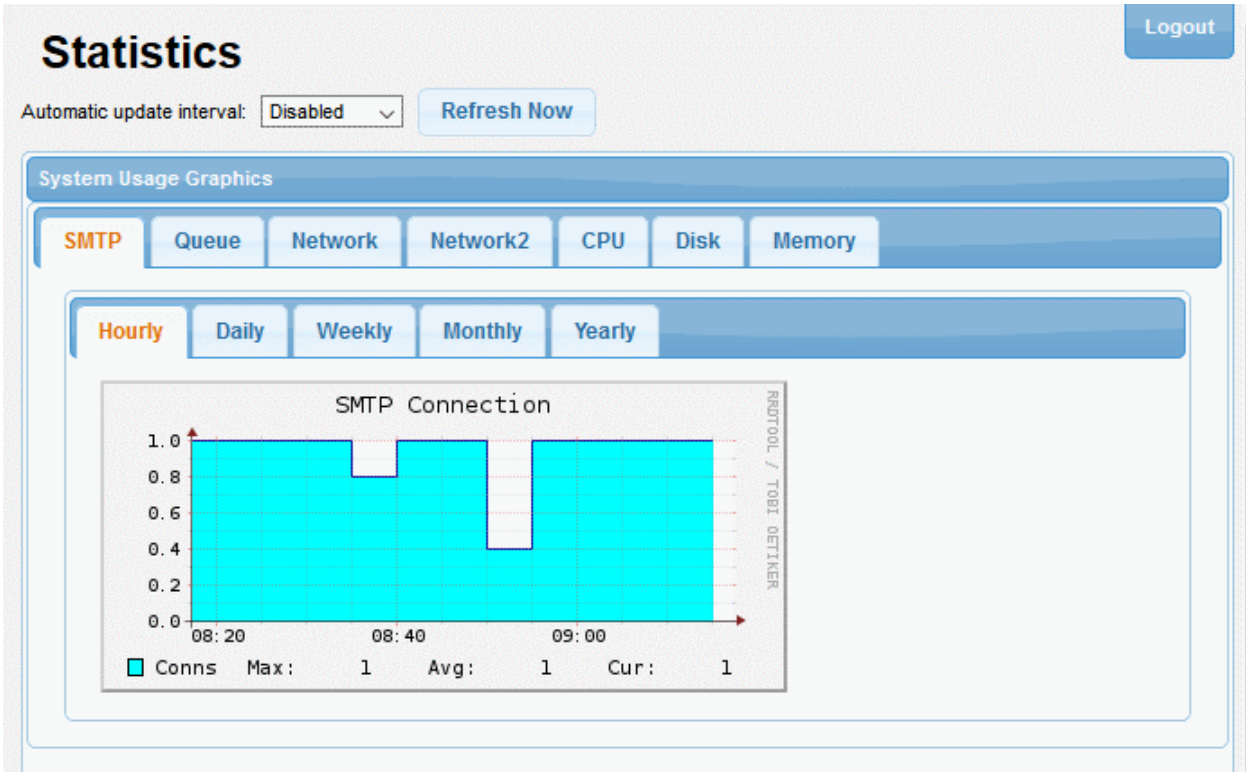


- Click the Clear button beside CLEAN SMTP queue.

3.6 System Usage Statistics

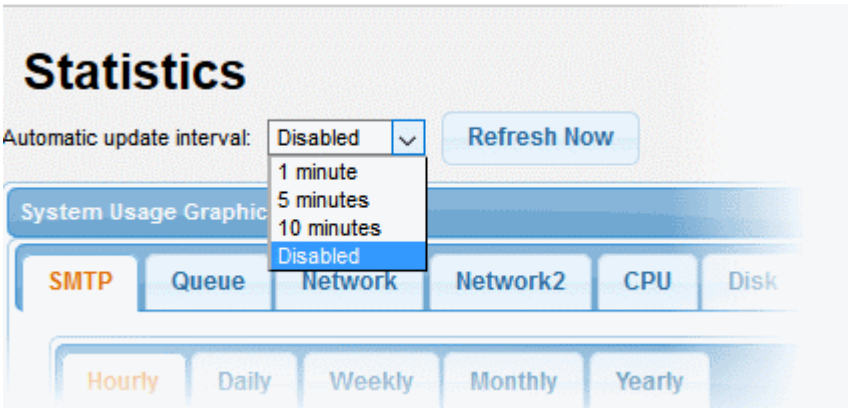
Dome Antispam displays SMTP connection statistics, mail statistics and utilization statistics of hardware and software resources like network, CPU, hard disks and system memory as graphs in the 'Statistics' interface.

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



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

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



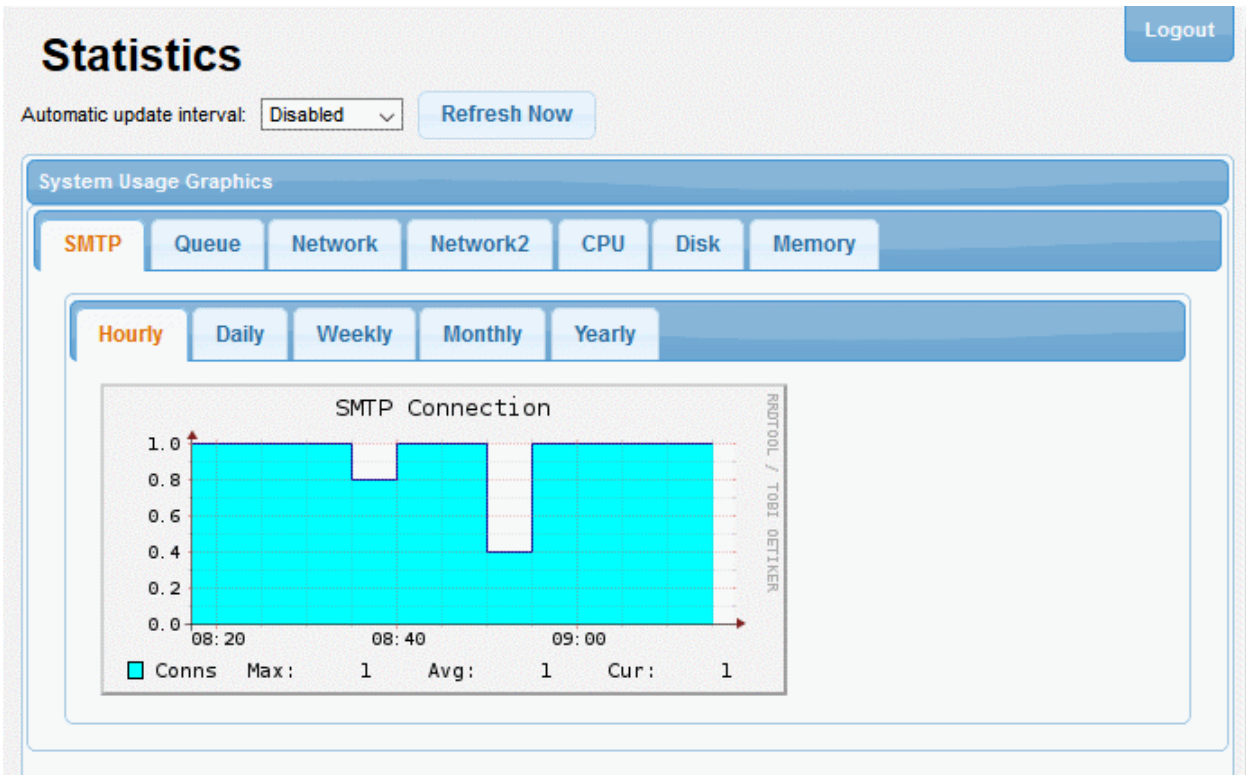
- To instantly update the statistics, click the 'Refresh Now' button.

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

- **SMTP**: A graphical representation of the number of SMTP connections between Dome Antispam 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 Dome Antispam 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:

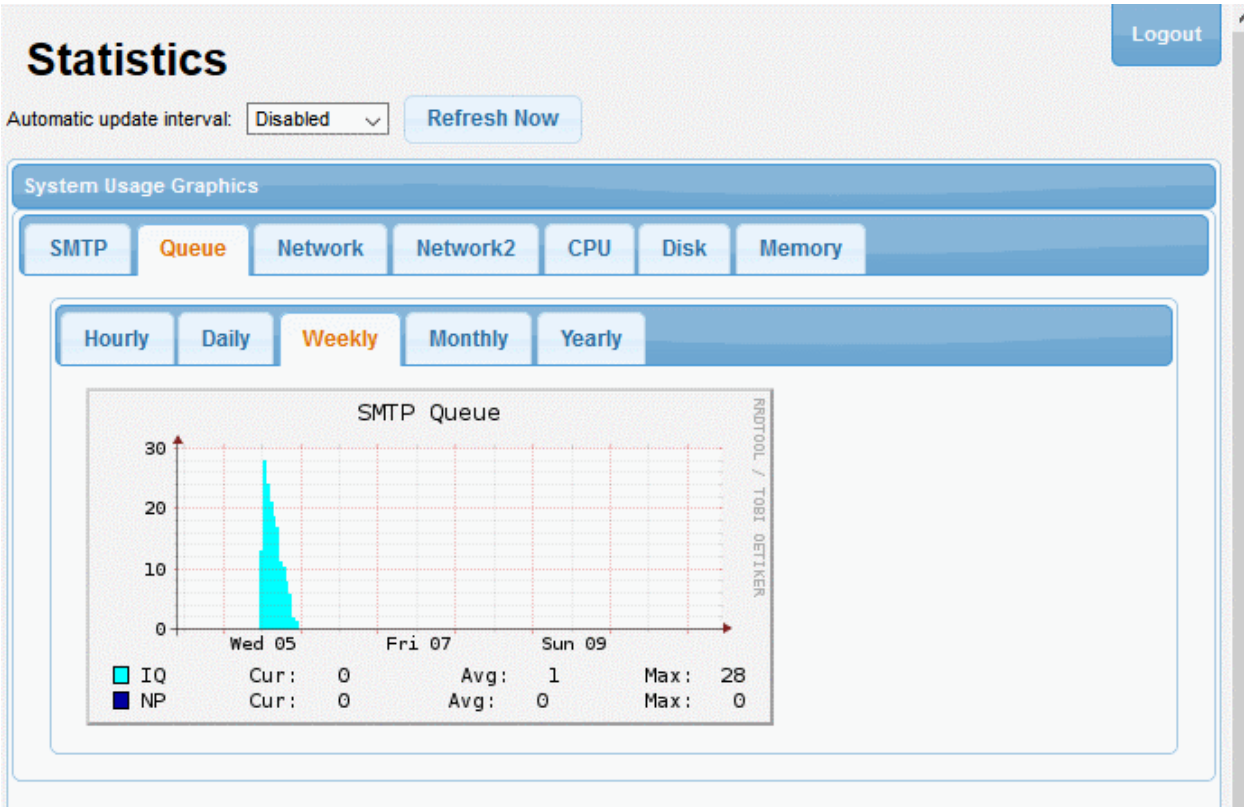


- Hourly - Shows the log of connections for the past one hour
- Daily - Shows the log of connections for the past 24 hours
- Weekly - Shows the log of connections for the past seven days
- Monthly - Shows the log of connections for the past four weeks
- Yearly - Shows the log of connections for the past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

Dome Antispam 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.

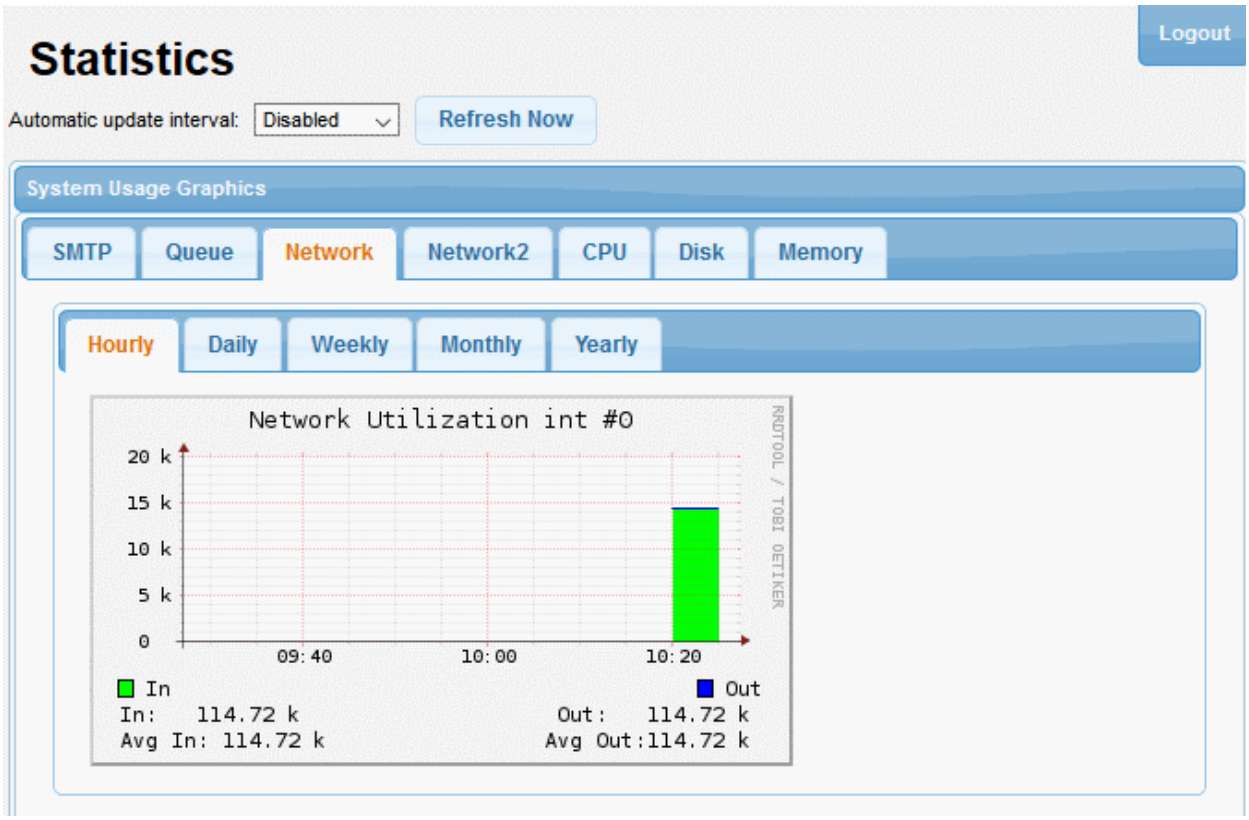


You can choose the time period for which you wish to see the logs from the sub tabs:

- 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

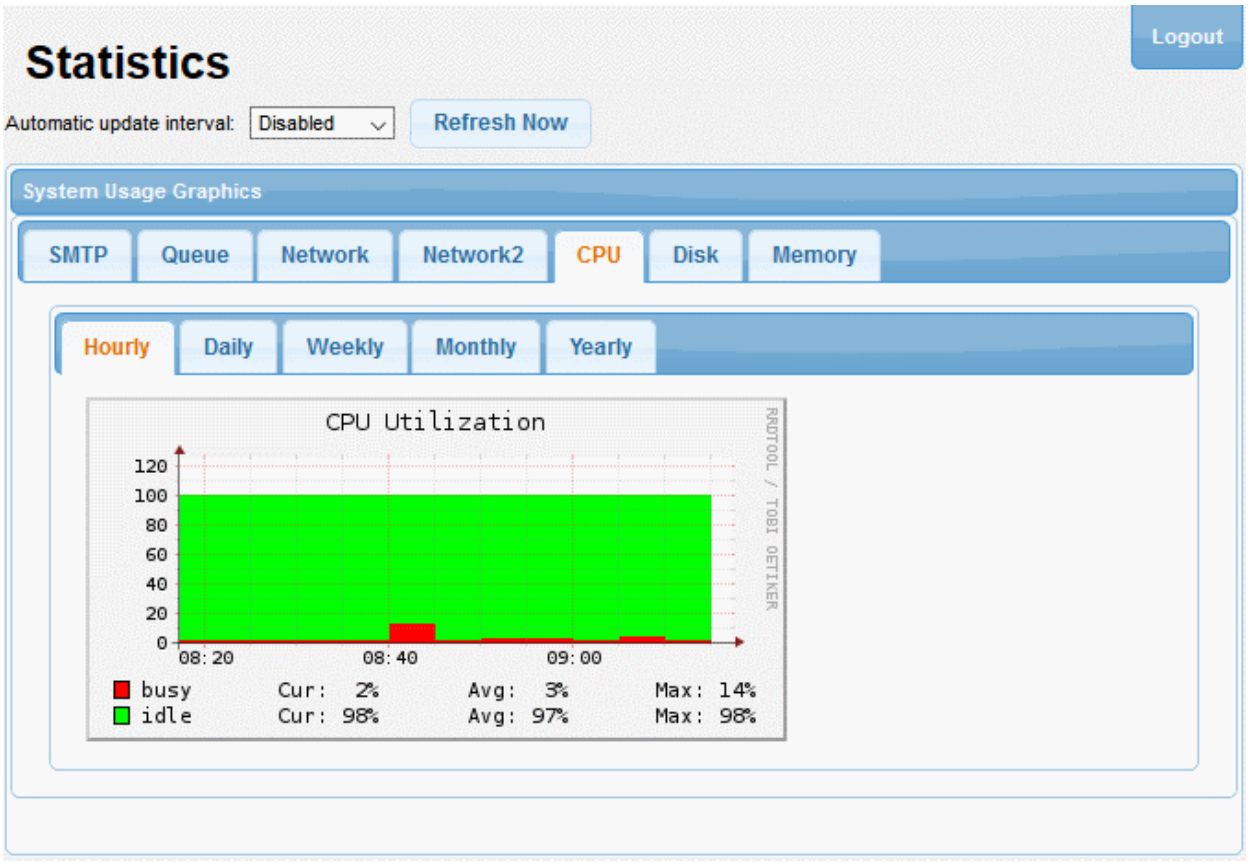
The incoming and outgoing traffic are represented with different colors in the graph.

- 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 Dome Antispam 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

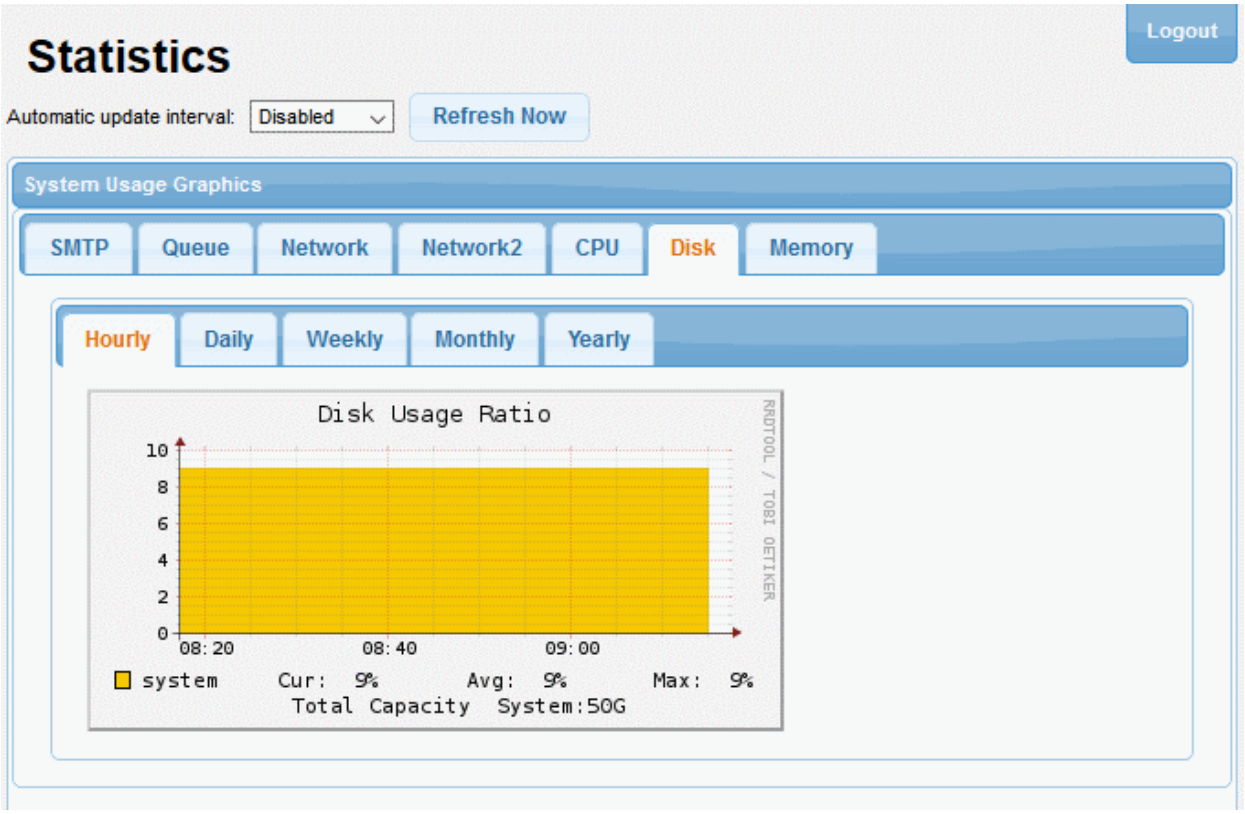
The processes that are responsible for CPU usage are indicated with different colors.

- 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 Dome Antispam, for the period chosen from the sub-tabs.



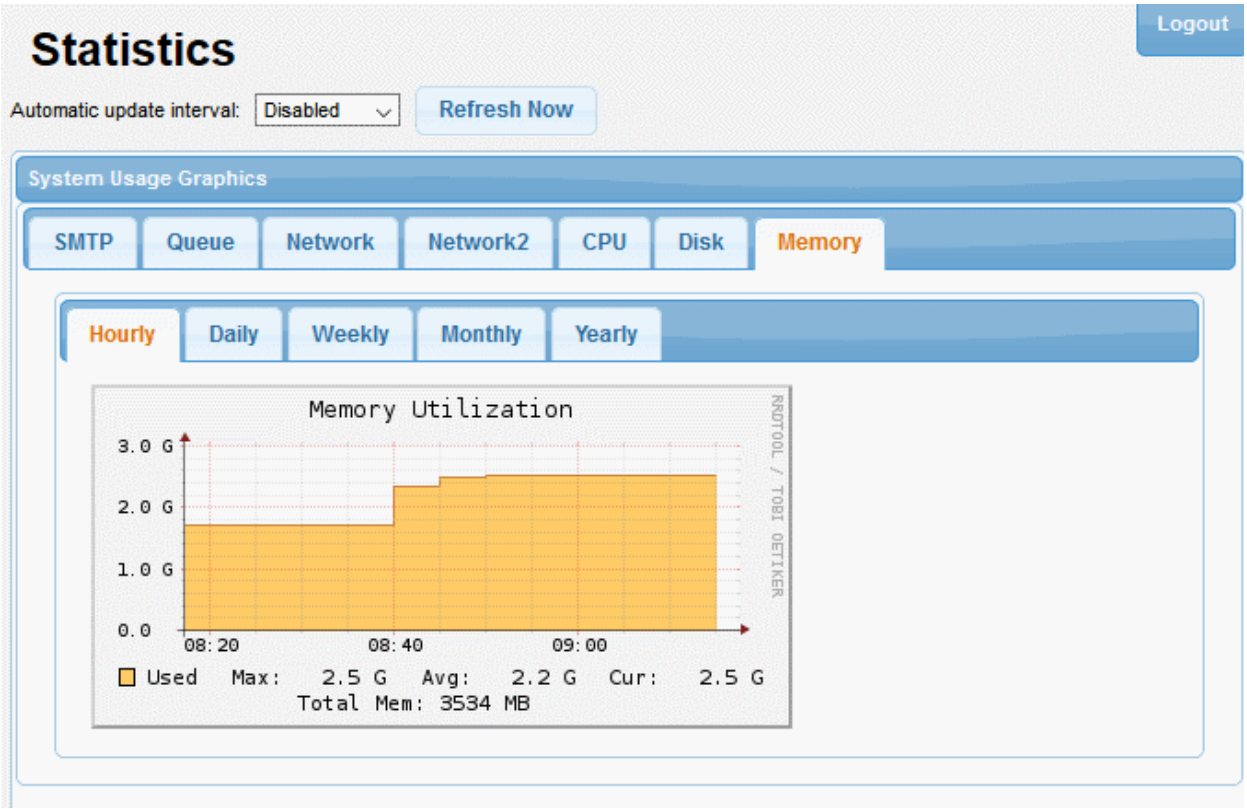
- Hourly - Shows the disk usage for the past one hour
- Daily - Shows the disk usage for the past 24 hours
- Weekly - Shows the disk usage for the past seven days
- Monthly - Shows the disk usage for the past four weeks
- Yearly - Shows the disk usage for the past twelve months

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



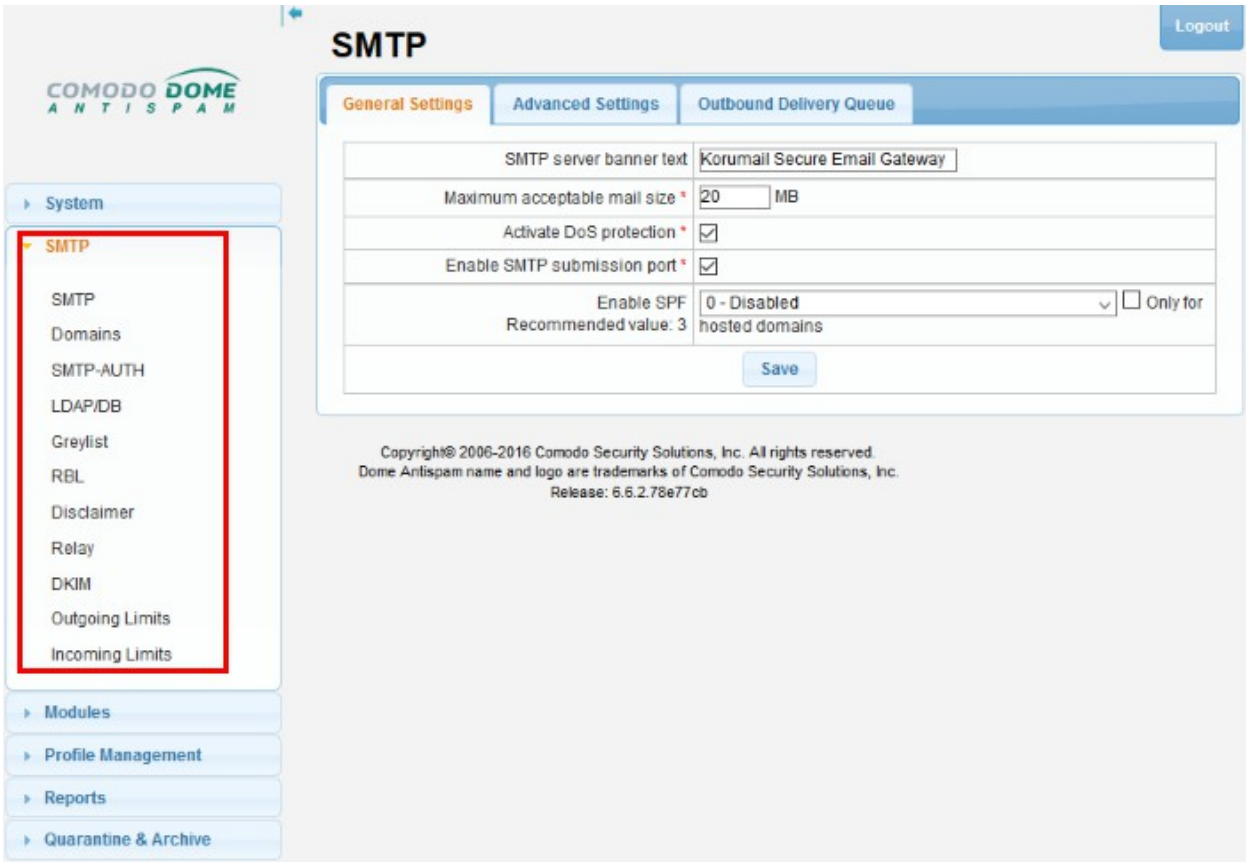
The 'Memory' tab displays a graphical representation of the usage of system memory of Dome Antispam, for the period chosen from the sub-tabs.

- 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.



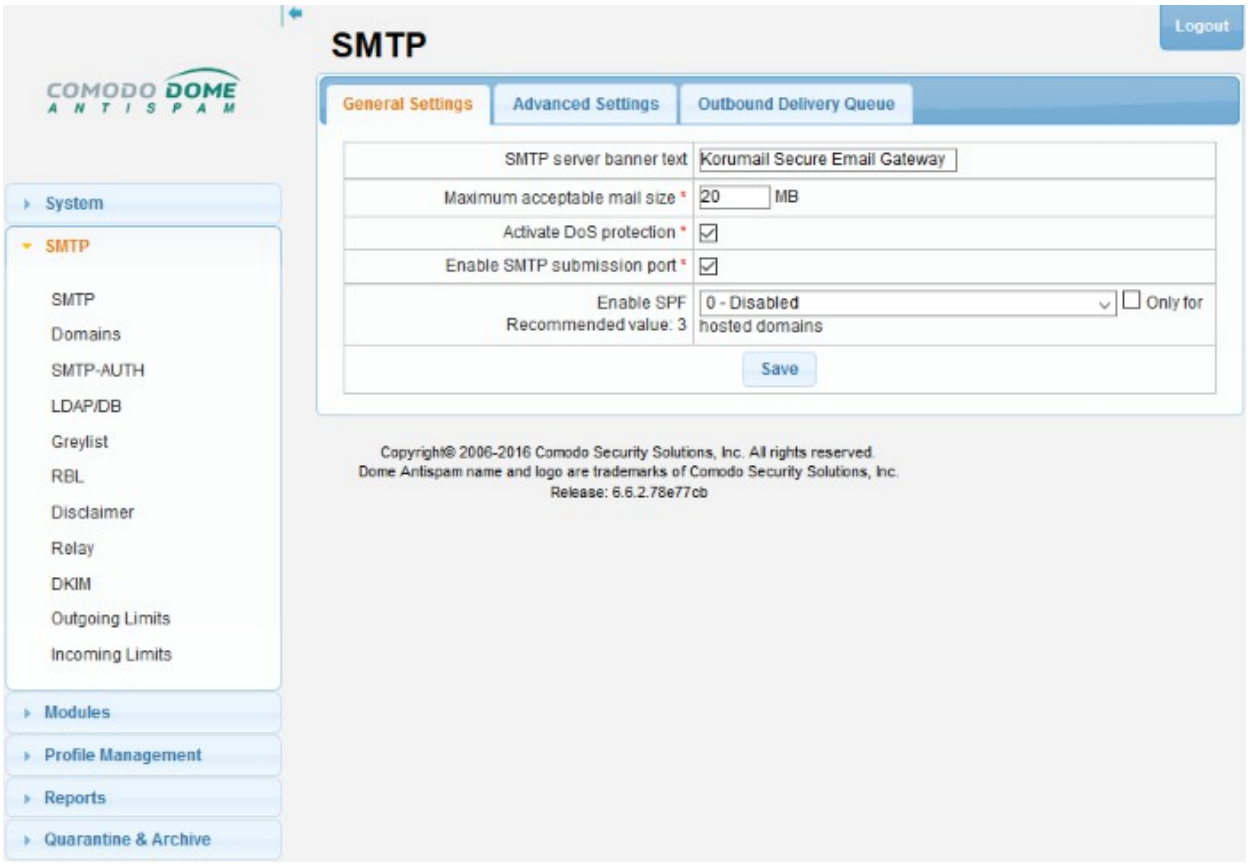
Click the following links for more details:

- SMTP Settings
- Manage Domains
- Dome Antispam SMTP AUTH Connector
- LDAP/Local DB/My SQL User Database
- Greylist
- Managing RBL Servers
- Disclaimer
- SMPT Relay
- DomainKeys Identified Mail (DKIM)
- Outgoing SMTP Limits
- Incoming SMTP Limits

4.1 SMTP (Send E-Mail Protocol) Settings

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

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



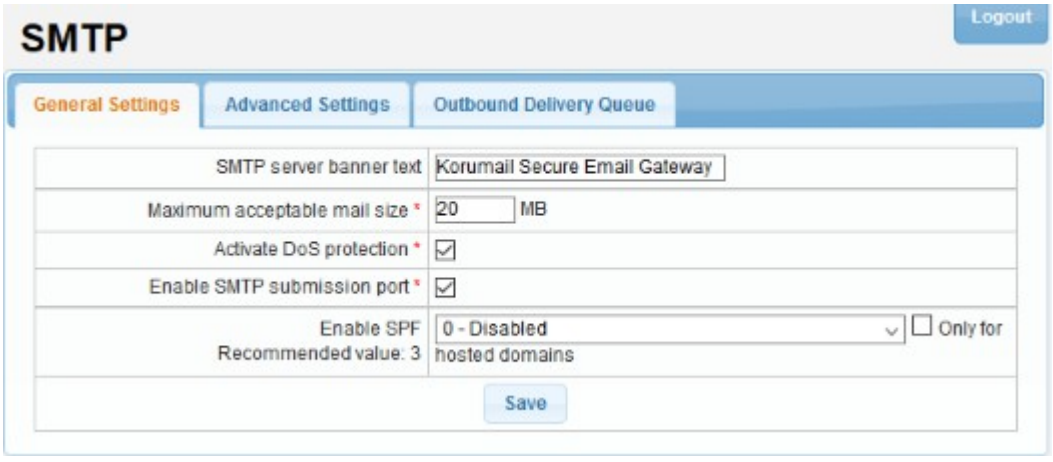
Click the following links for more details:

- General Settings
- Advanced Settings
- Outbound Delivery Queue

4.1.1 General Settings

The 'General Settings' allows administrators to configure banner text, maximum size of outgoing mails, denial of service protection and more.

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



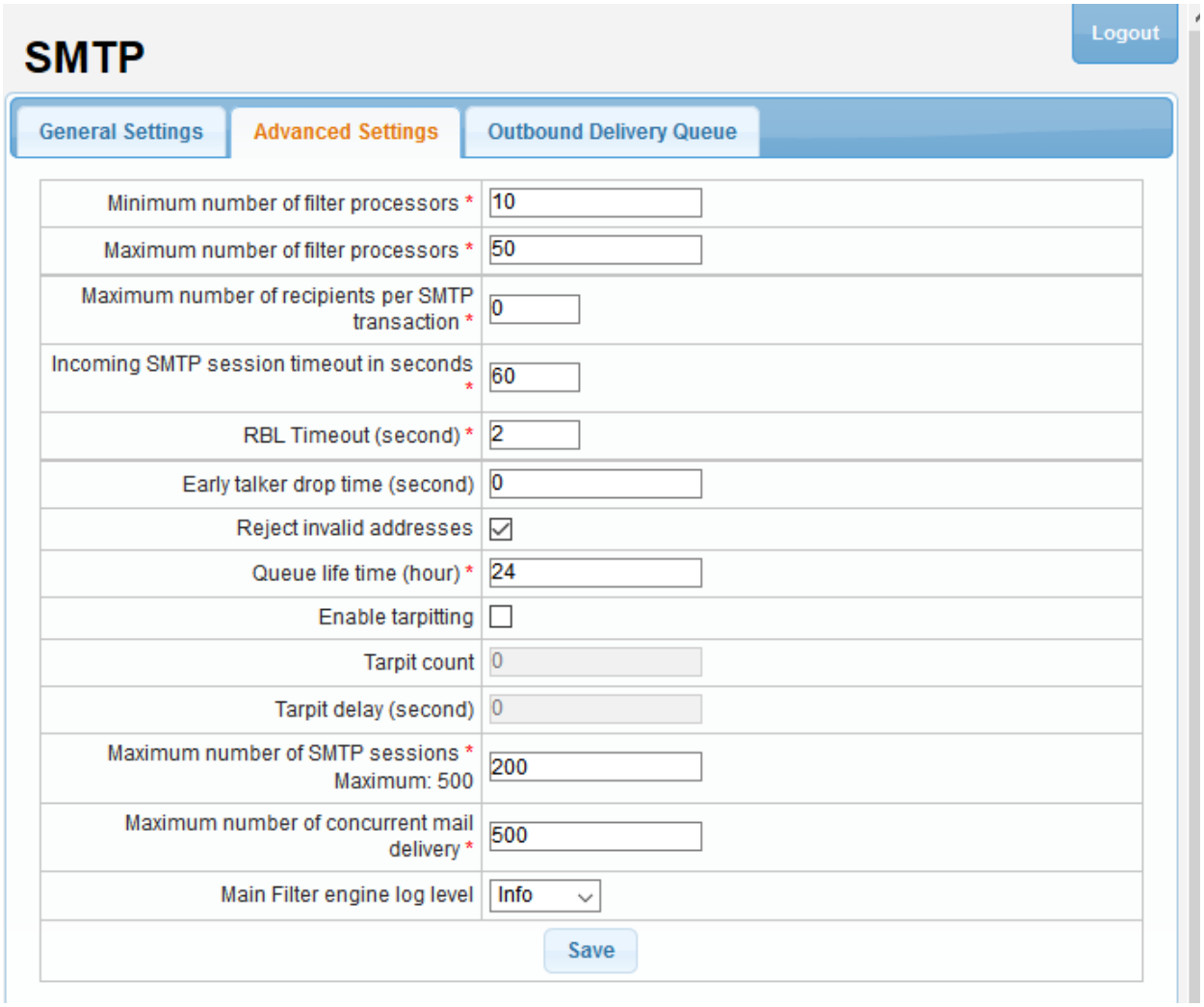
SMTP Settings - General Settings Table of Parameters	
Parameter	**Description**
SMTP server banner text	The welcome message displayed on the SMTP server when connection to Dome Antispam port 25 is established.
Maximum acceptable mail size (MB)	The maximum permitted size of a single email + attachments. 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, Dome Antispam will not accept outgoing messages from unauthenticated sources, thus helping to protect your network and users from spam emails.
Enable SPF	SPF (Sender Policy Framework) is a security standard to block the forgery of sender address. SPF values 1. Just add received-SPF header 2. Return temporary failure in DNS query error 3. If SPF result fails (ban) then reject it (recommended) 4. If SPF result is softfail then reject it 5. If SPF result is neutral then reject it 6. If SPF result is not passed then reject it You can disable SPF by selecting '0' from the list. If the check box 'Only for hosted domains' is selected, then the SPF check will be performed for outgoing mails for domains that are hosted in the network.

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

4.1.2 Advanced Settings

The SMTP 'Advanced Settings' area allows administrators to configure settings such as the minimum and maximum number of processors that the main filtering engine should use, the number of recipients per SMTP transactions and more. Multiple filters run concurrently on incoming mails to improve the performance of Dome Antispam. You can specify the min/max quantity of filters which should be used on a selected domain. You can also specify the maximum number of recipients per SMTP transaction.

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



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. • 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. • 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 Dome Antispam.
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 replys with a HELO or a EHLO command. On receiving this (premature) message before the server sends greetings, then the client could be serving spam. The waiting time of SMTP server to send a greeting message is called Early talker drop time.

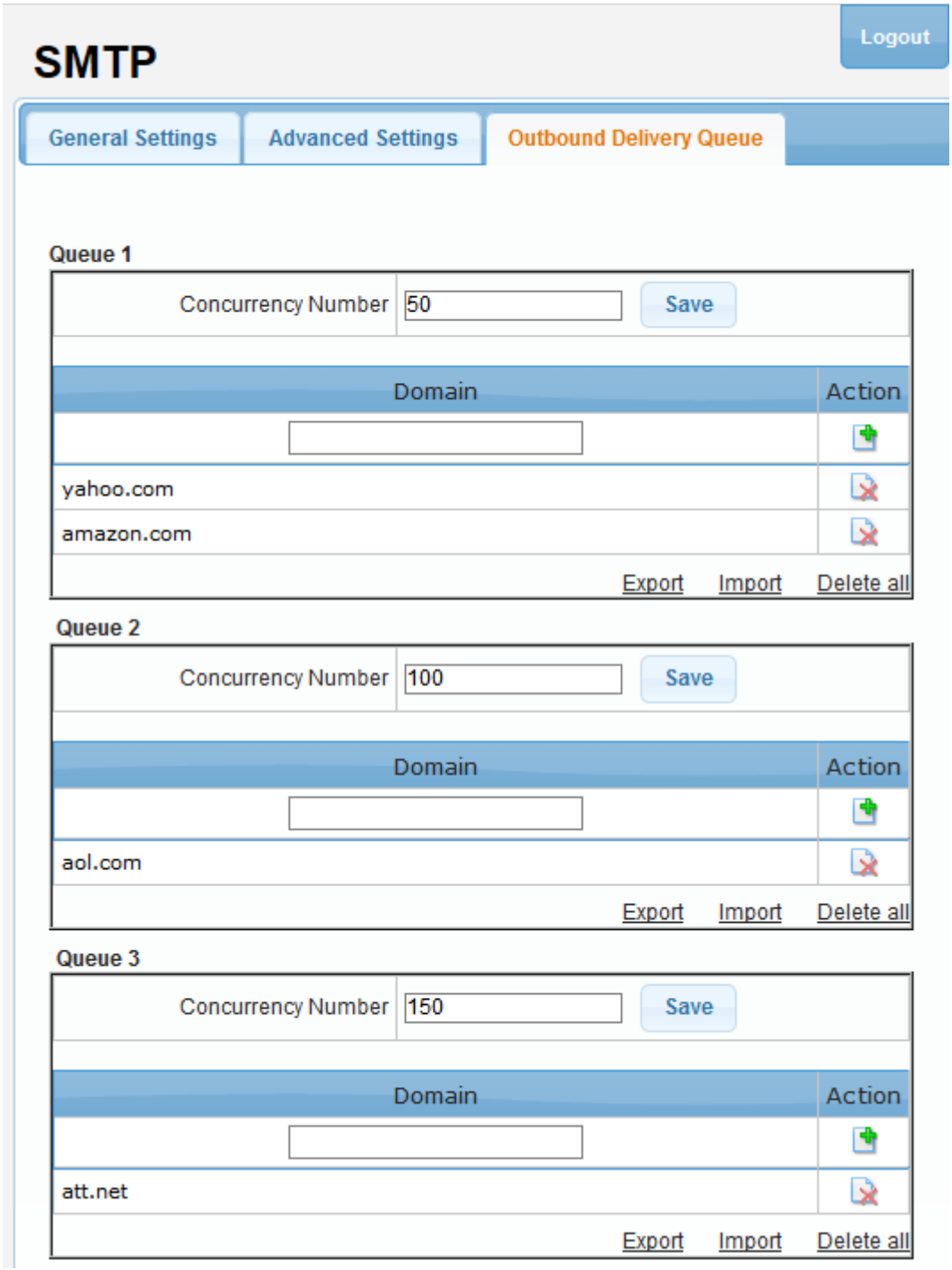
Reject invalid addresses	If enabled, outgoing mails with invalid address will be rejected
Queue life time (hour)	Enter the number of hours that a mail can be queued for delivery before it is bounced.
Enable tarpitting	Tarpitting helps thwart spammers by slowing the transmission of bulk emails. If a spammer sends an email to several recipients on your server during one SMTP session, enabling this feature will slow down the communication. Spammers may stop sending emails to your server if the response to their requests is very slow.
Tarpit count	Tarpitting will become active if the number of recipients exceeds the Tarpit count.
Tarpit delay (second)	The number of seconds that Tarpitting will delay the transmission response
Maximum number of SMTP sessions	Maximum number of concurrent SMTP sessions.
Maximum number of concurrent mail delivery	Maximum number of concurrent messages that can be sent by SMTP server.
Main Filter engine log level	Select the level of main filtering engine event that should be logged. Selecting 'Notset' will log all the levels.

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

4.1.3 Outbound Delivery Queue

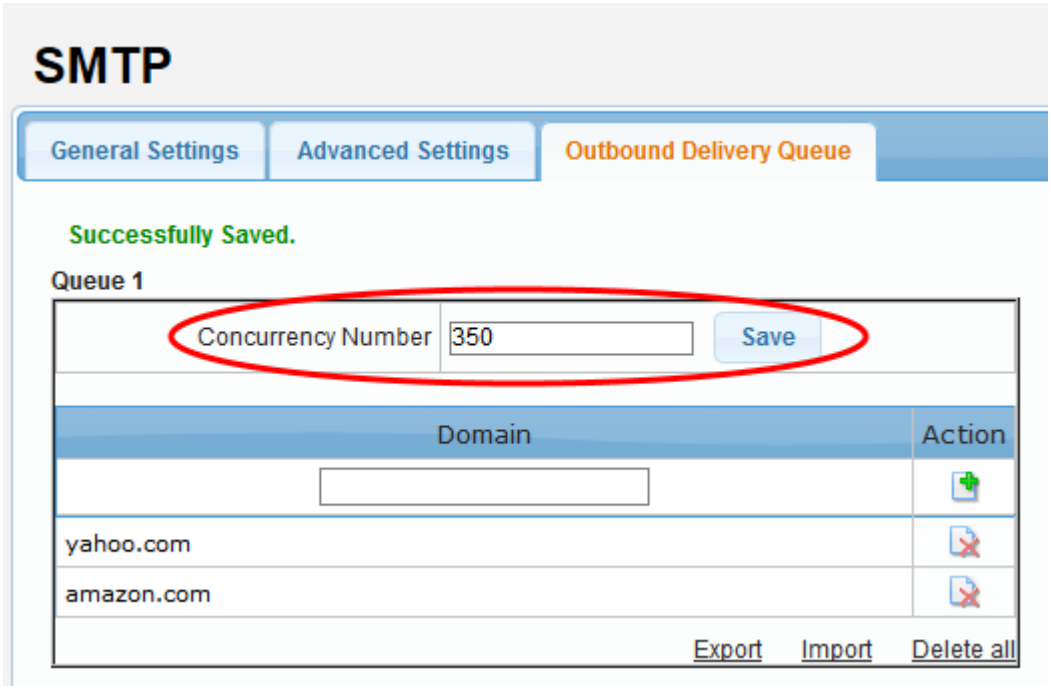
Some domains have restrictions on how many emails can be delivered concurrently from a source. Dome Antispam allows you to queue outbound mails per domain so only a certain number of mails will be delivered at once.

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

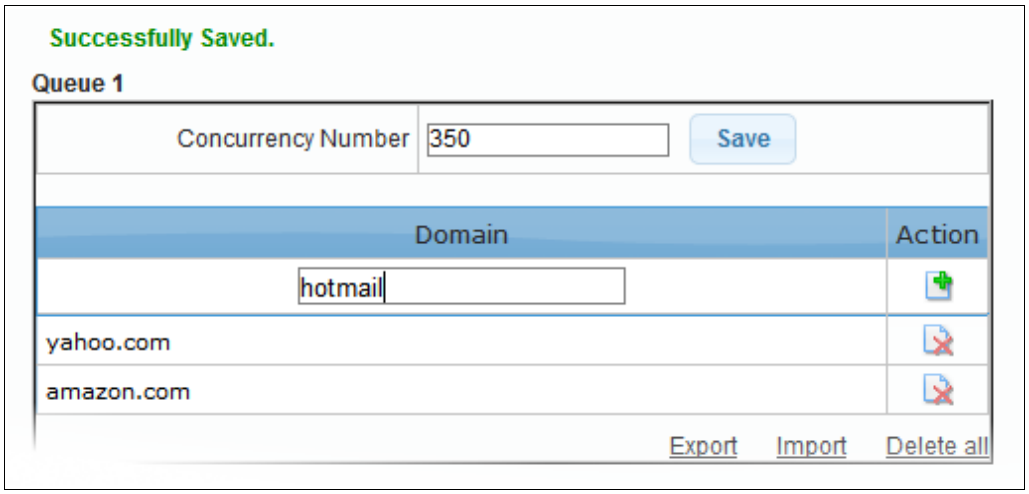


The interface has three preset delivery queue numbers that can be configured according to your organizational needs. The 'Concurrency Number' for each of the queue can be changed.

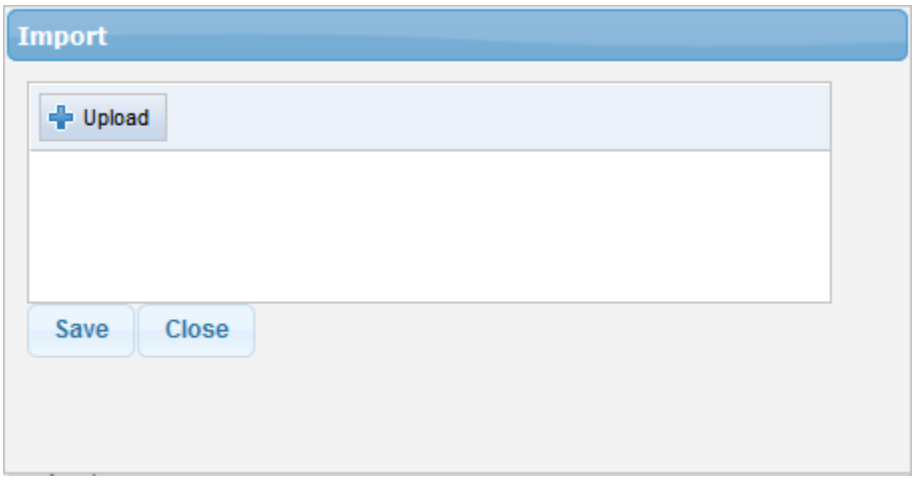
- To set the number of emails that can be sent at a time, enter the number in the 'Concurrency Number' field and click the 'Save' button.



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

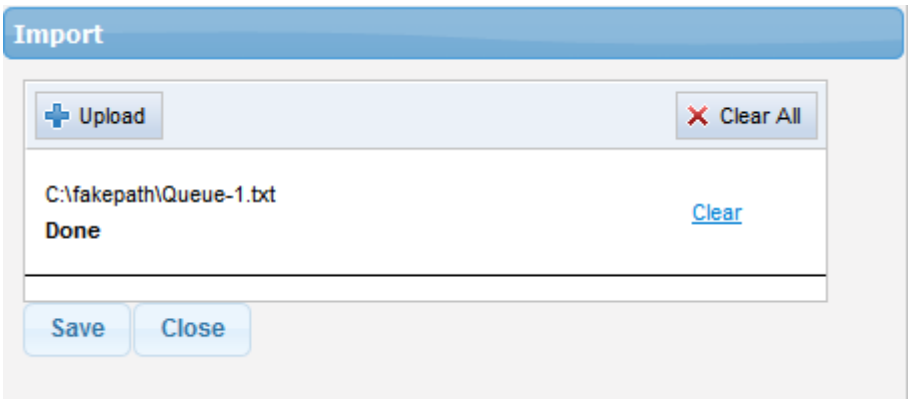


- To remove a domain from the list, click the button beside it.
- To remove all domains from the list, click the 'Delete all' link and confirm the removal in the 'Confirmation Dialog'.
- To save the list of domains in a 'Queue', click the 'Export' link and save it to your system.
- To import a list of 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.

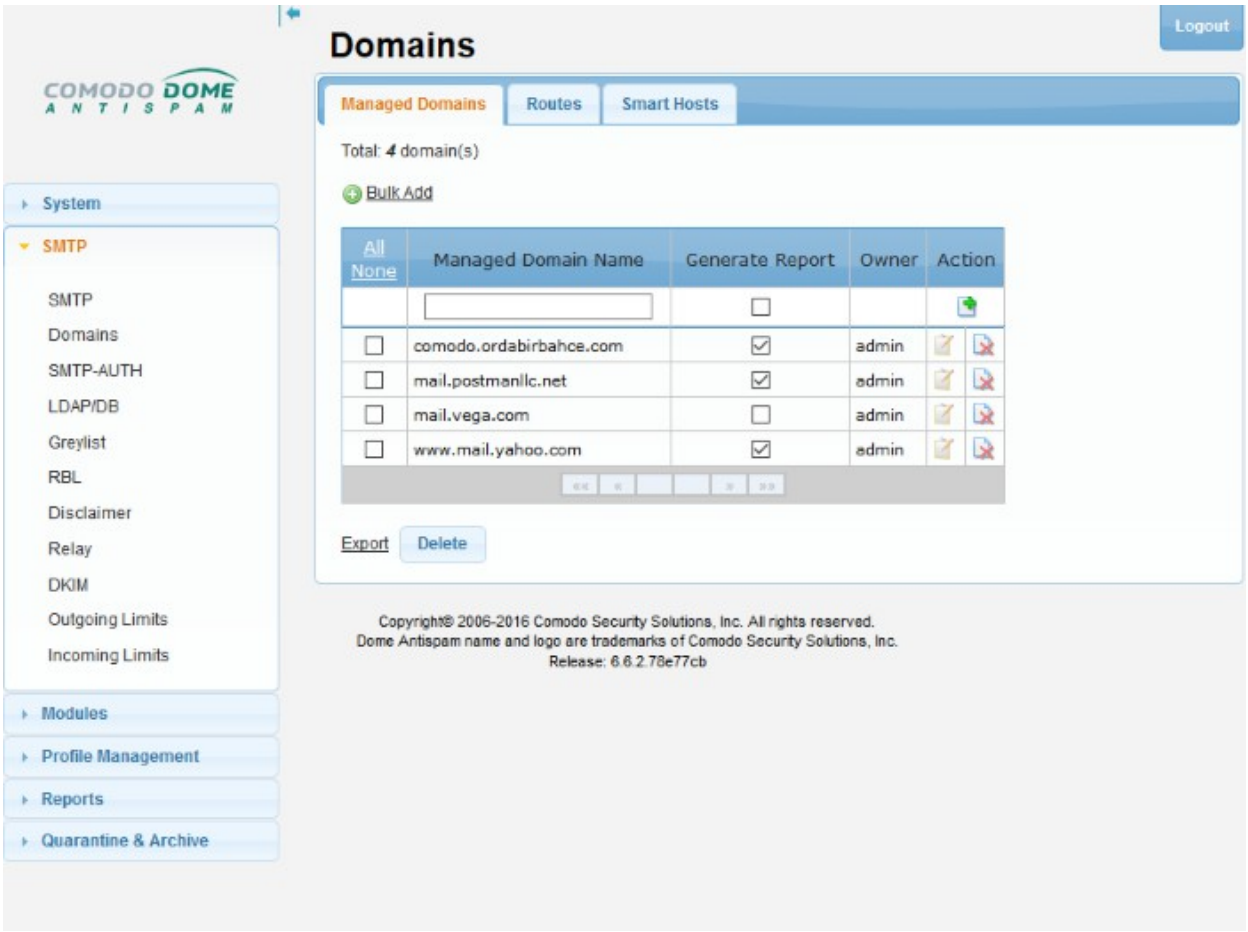


- Repeat the process to add more files.
- To remove a file, click the 'Clear' link beside it.
- To remove all the added files, click the 'Clear All' button at the top right.
- To import the list of domains from the files, click the 'Save' button.

4.2 Manage Domains

The 'Manage Domains' area allows you to add, edit and view the domains you wish to filter. You can also configure routes and SMTP servers and add 'Smart Hosts' for domains so mail is routed to an intermediate or relay server rather than directly to the recipients' server.

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



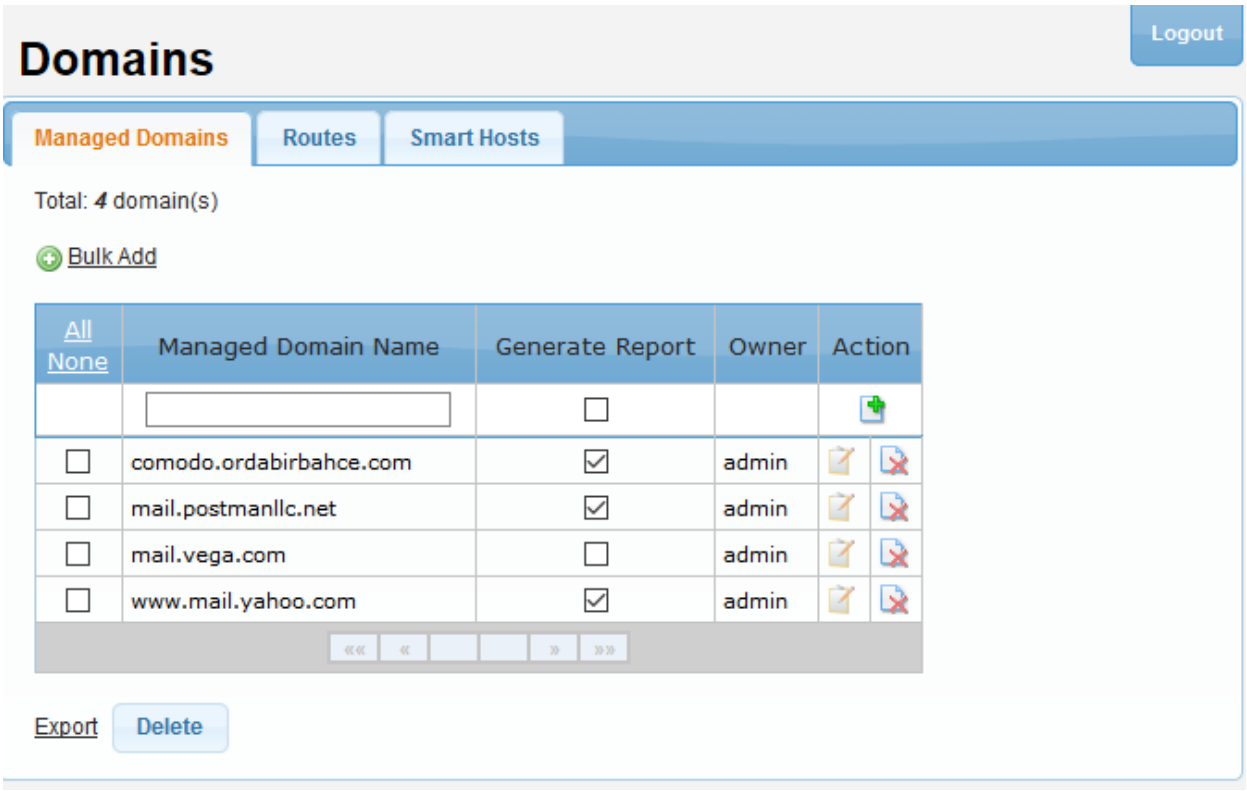
Click the following the links for more details:

- Managing Domain Names
- Managing Domain Routes
- Managing Smart Hosts
- Default Domain Routing

4.2.1 Managing Domain Names

The 'Managing Domain Names' tab allows you to view, add and edit your protected domains.

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



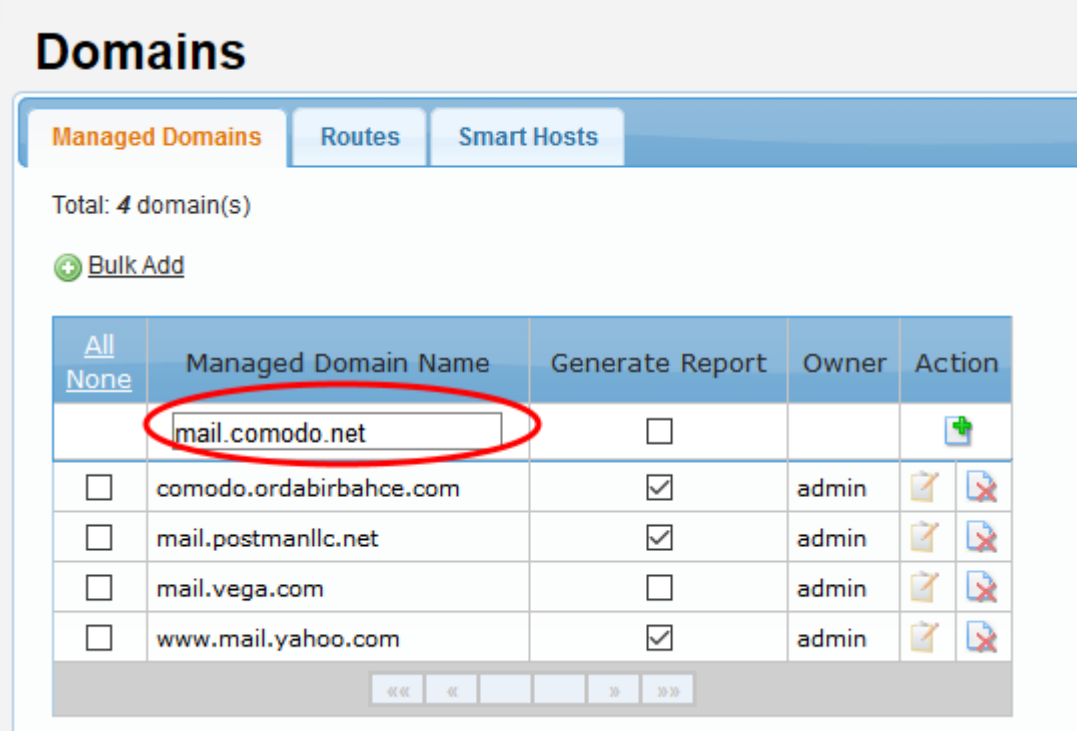
Managed Domains - Table of Column Descriptions		
Column Header	**Description**	
Managed Domain Name	The name of the domain added to Dome Antispam	
Generate Report	If enabled, Dome Antispam displays related email statistics of the selected domain name in 'Domain Reports'	
Owner	The name of the administrator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

The interface allow administrators to:

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

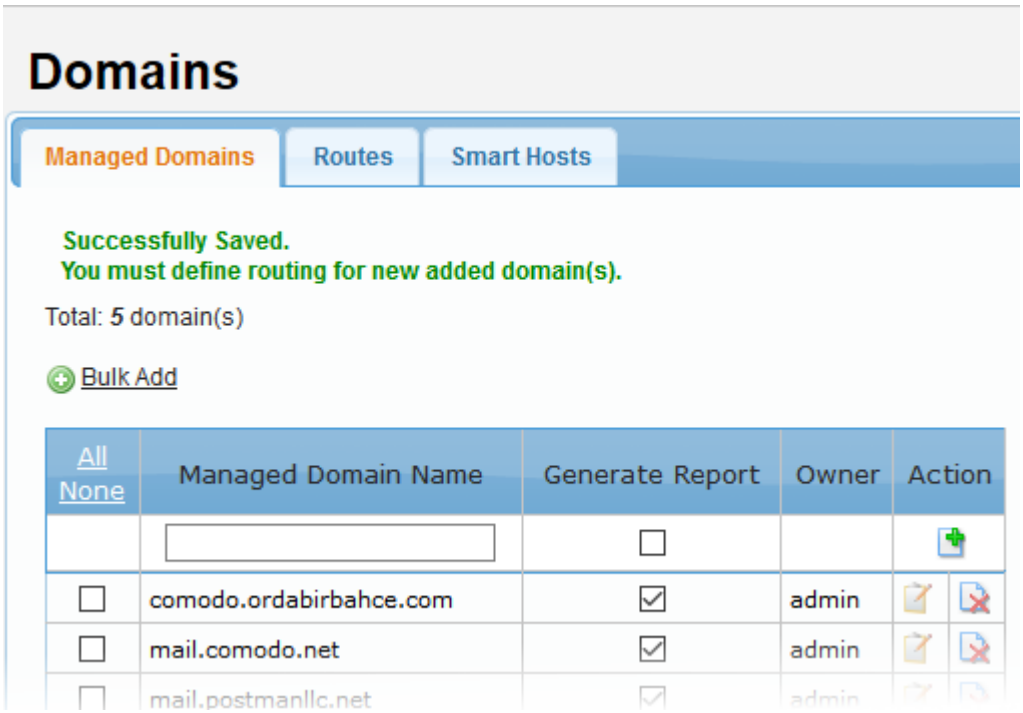
To add a domain name

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



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

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



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

To add multiple domain names

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

same time. For doing this lines must be written in Domain Name; Target IP Address; Port; LDAP name format. If target IP address is left blank no routing is done for this domain name. If port field left blank, port 25 is used as default.

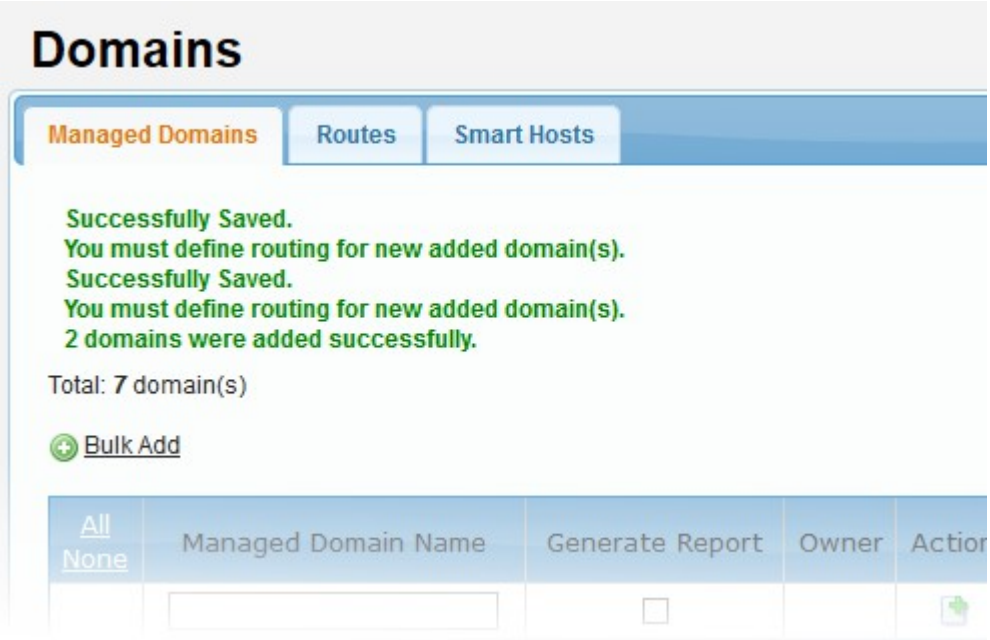
- Click the 'Bulk Add' link in the 'Managed Domains' screen

The 'Bulk Add' screen will be displayed.

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

- Click the 'Add' button.

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

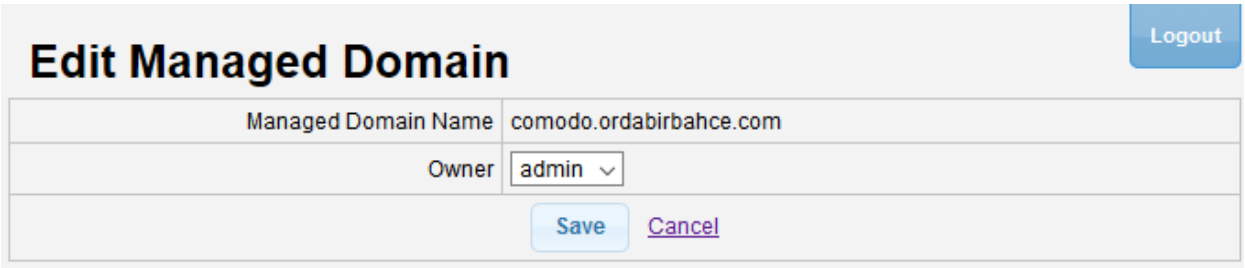


To edit a domain owner

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.

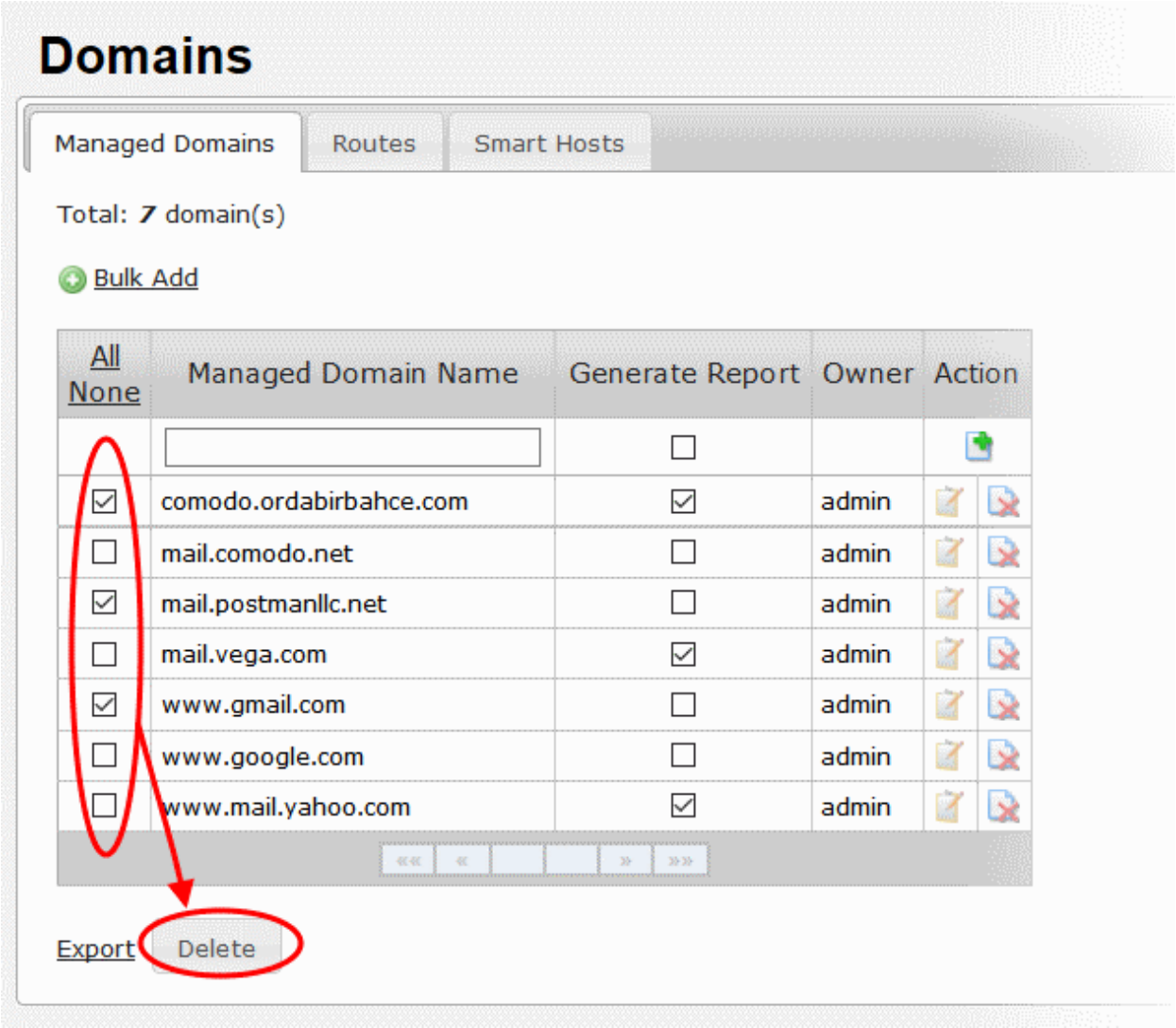
The 'Edit Managed Domain' screen will be displayed.



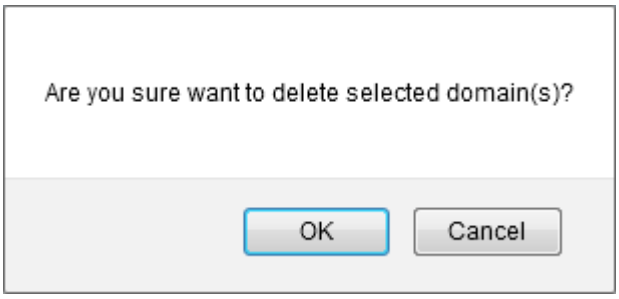
- Select the name that you want to change as the owner from the 'Owner' drop-down
- Click the 'Save' button

To delete domain names

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

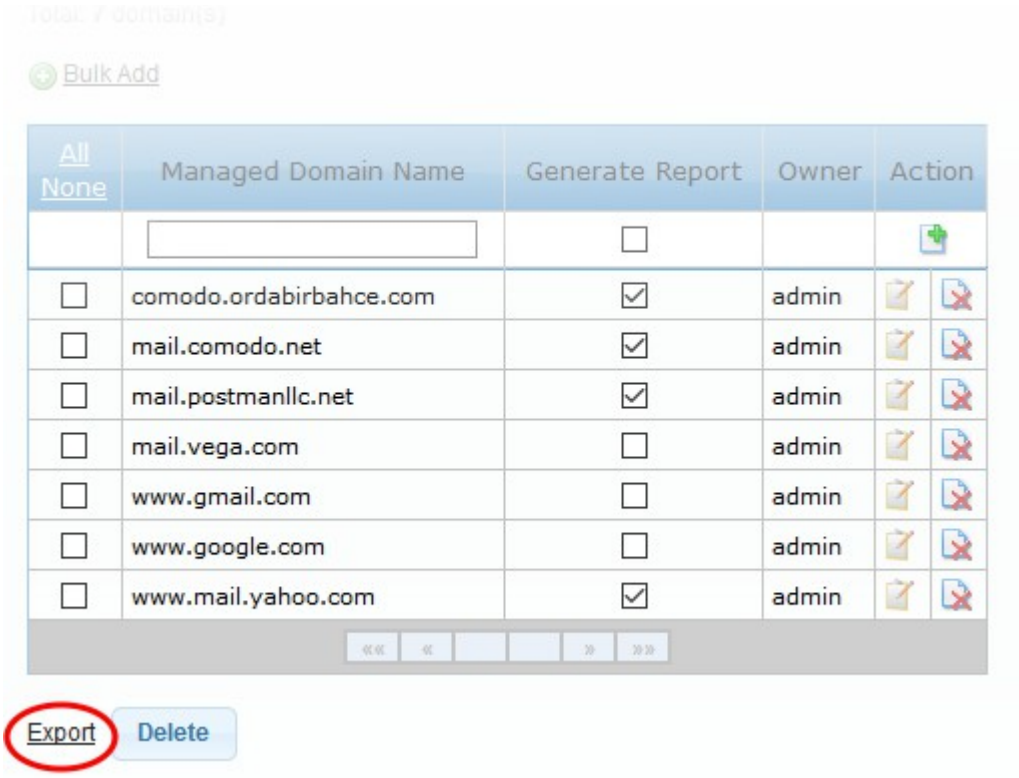


- Click 'OK' to confirm the deletion of the selected domains.

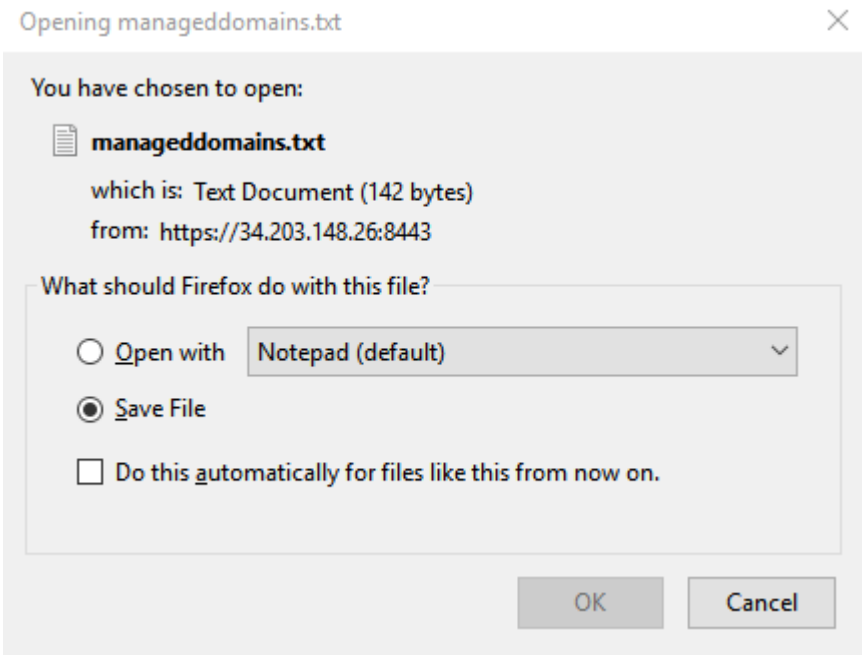


To export the domain names to a file

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



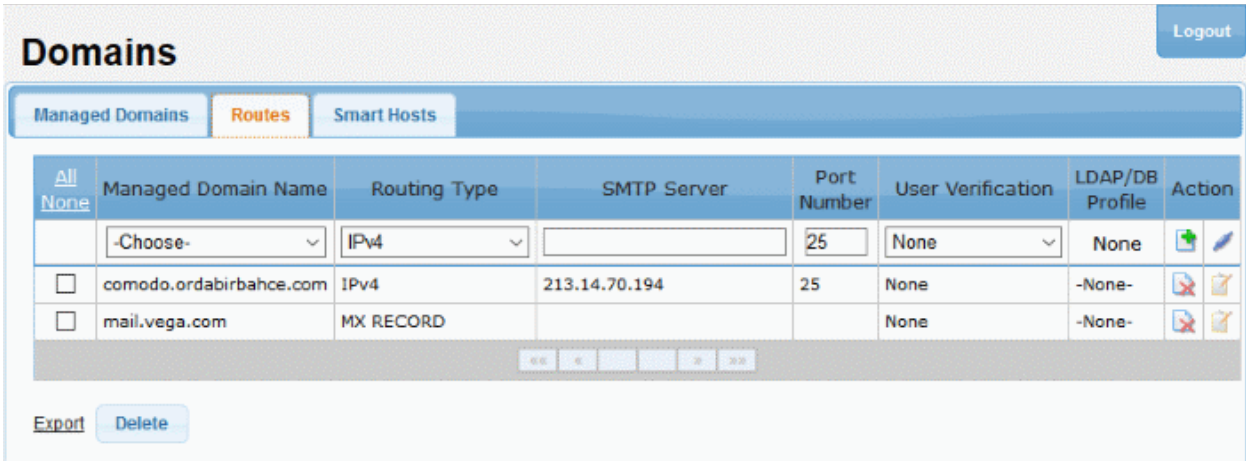
- Click 'OK' to download and save the domains list as a text file to your system.



4.2.2 Managing Domain Routes

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

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



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

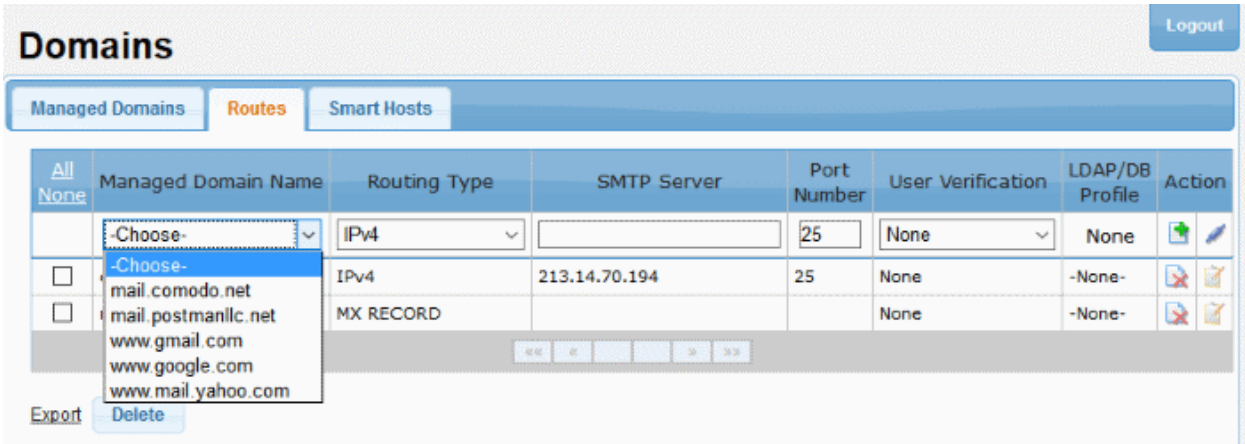
	• LDAP	
SMTP Server	Enter the IP address or the SMTP server name	
Port Number	The port number to which the Dome Antispam should forward the mail	
User Verification	The type of user verification that Dome Antispam should use before forwarding the mails. The options available are: • None • Local User DB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

The interface allow administrators to:

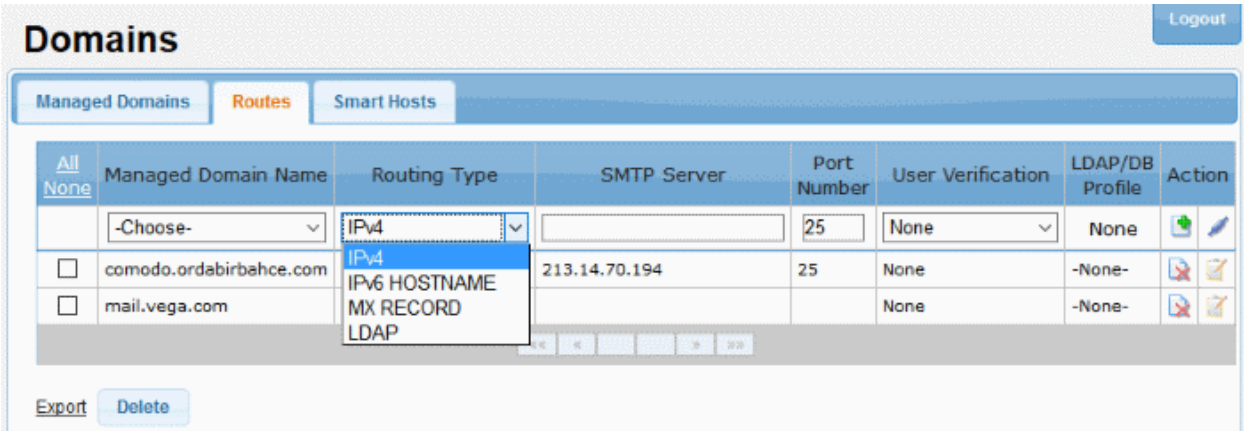
- Configure domain route for the added domains
- Edit a domain route
- Delete domain routes
- Export domain routes

To configure a domain route

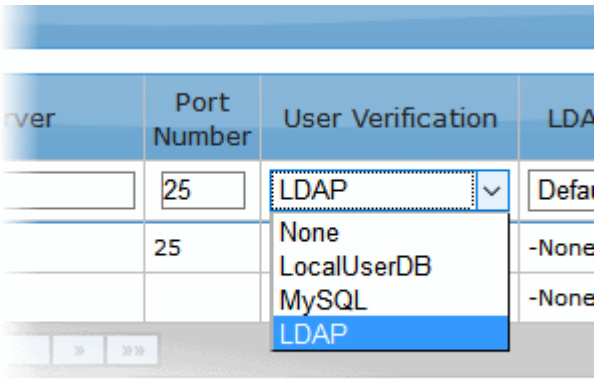
- Click the 'Choose' drop-down and select the added domain for which you want to configure the route.



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



- Enter the server name or IP address of the SMTP server to which Dome Antispam should forward the mails to in the filed under 'SMTP Server'
- Enter the port number to which the Dome Antispam should forward the mail
- Select the verification type that the Dome Antispam should use before forwarding the mails. The options available are: Local User DB, My SQL and LDAP. These are configured in **LDAP/DB** section.
- Depending on the 'User Verification' type chosen, the 'LDAP/DB Profile' column will be populated. If 'LDAP' is chosen as 'User Verification' then the LDAP profiles added in **LDAP/DB** section will be displayed from the drop-down. Select the LDAP profile from the options.



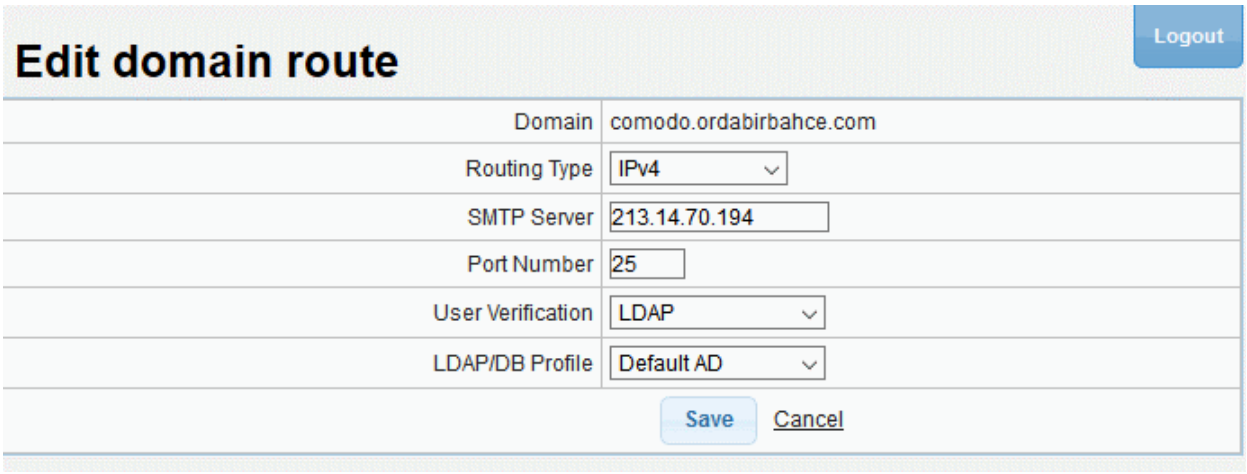
- To check the connectivity between Dome Antispam and the configured remote server, click the button under the 'Action' column header. The connection will be checked and the result displayed at the top.
- To add a domain route to the list, click the button under the 'Action' column header.

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

To edit a domain route

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

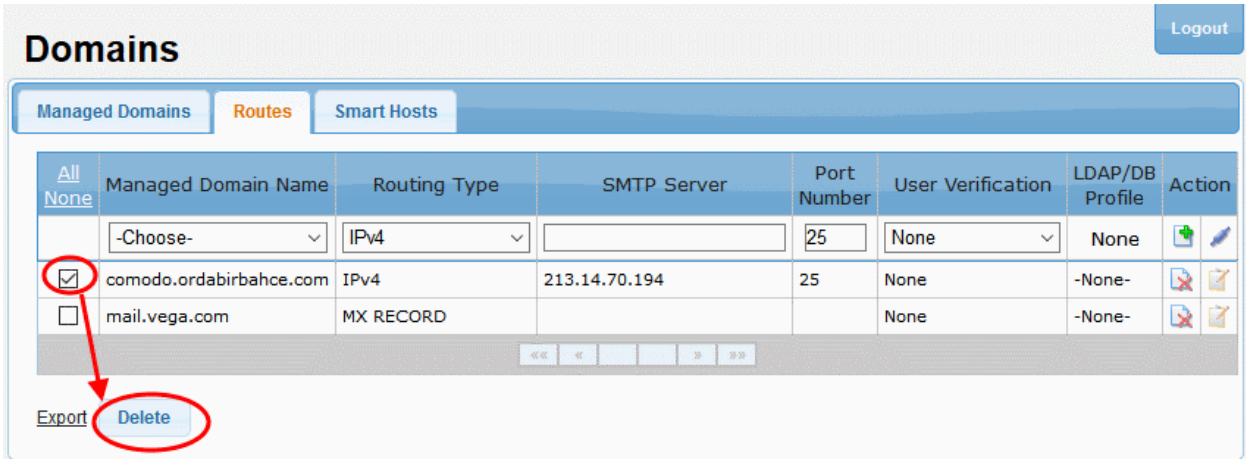
The 'Edit domain route' screen will be displayed.



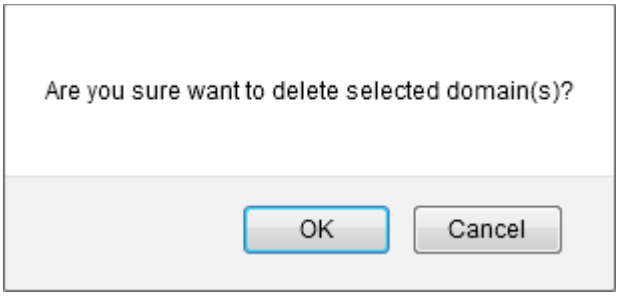
- Edit the required parameters. This is similar to the method explained in the 'Add' section.
- Click the 'Save' button to apply your changes.

To delete domain routes

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

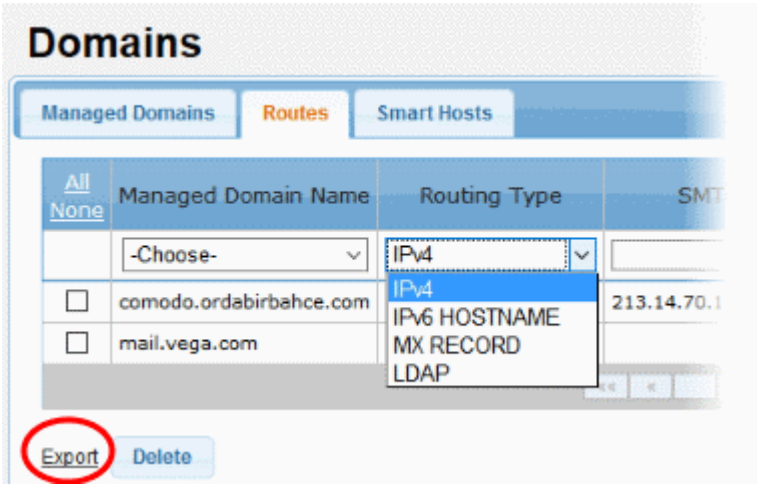


- Click 'OK' to confirm the deletion of the selected domain routes

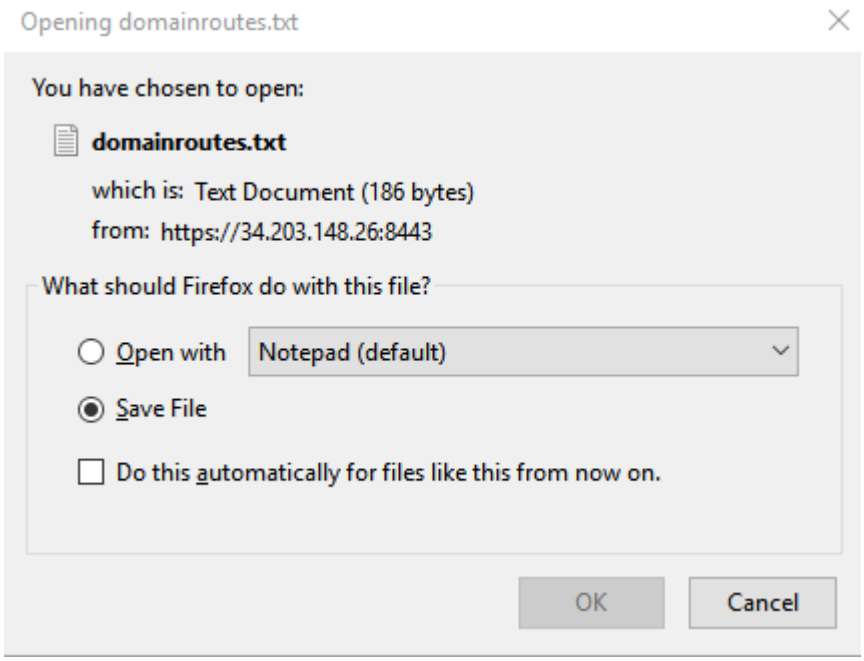


To export the domain routes to a file

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



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

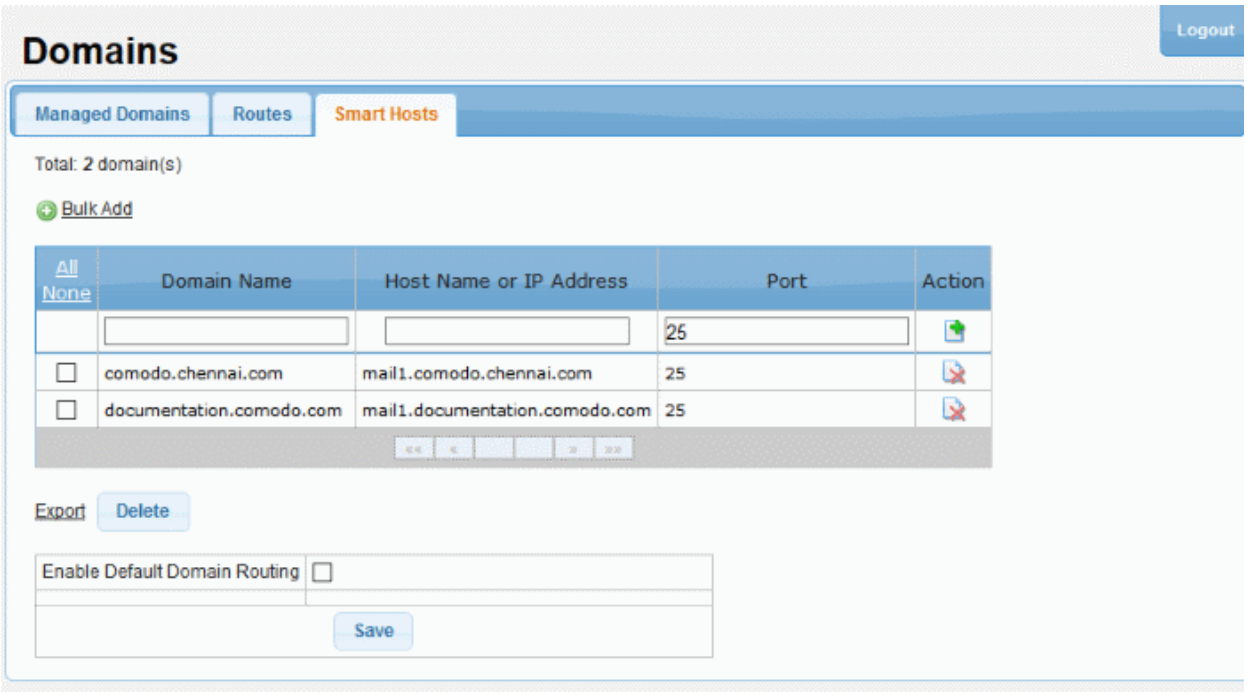


4.2.3 Managing Smart Hosts

Smart Hosts serve as an intermediate mail server that receive mail from an SMTP server and, after applying their own policy, forward them to end user mail boxes. Smart hosts requires authentication from the sender to verify that the sender has privileges to forward mails through the smart host. This is different to an open mail relay that will forward mails directly to the recipient server without authentication. Dome Antispam has the ability to route emails to 'Smart Hosts'. Please note that a domain added under 'Managed Domains' cannot be added for 'Smart Host' routing.

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

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



Smart Hosts - Table of Column Descriptions		
Column Header	**Description**	
Domain Name	The name of the domain added to Dome Antispam	
Host Name or IP Address	Host Name or IP address of the 'Smart Host'	
Port	The port number to which the Dome Antispam 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

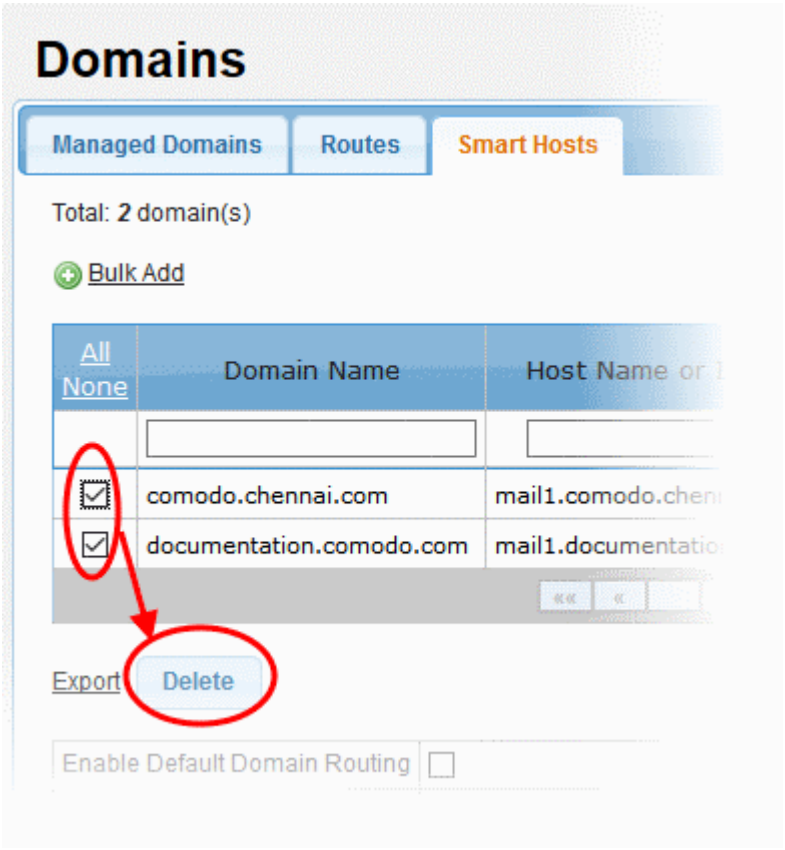
To configure 'Smart Host' route for domains

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

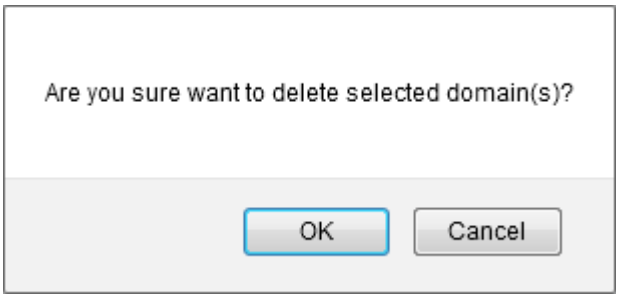
To delete 'Smart Host' route for domains

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

- To delete 'Smart Host' routes, select the check boxes beside them and click the 'Delete' button at the bottom.

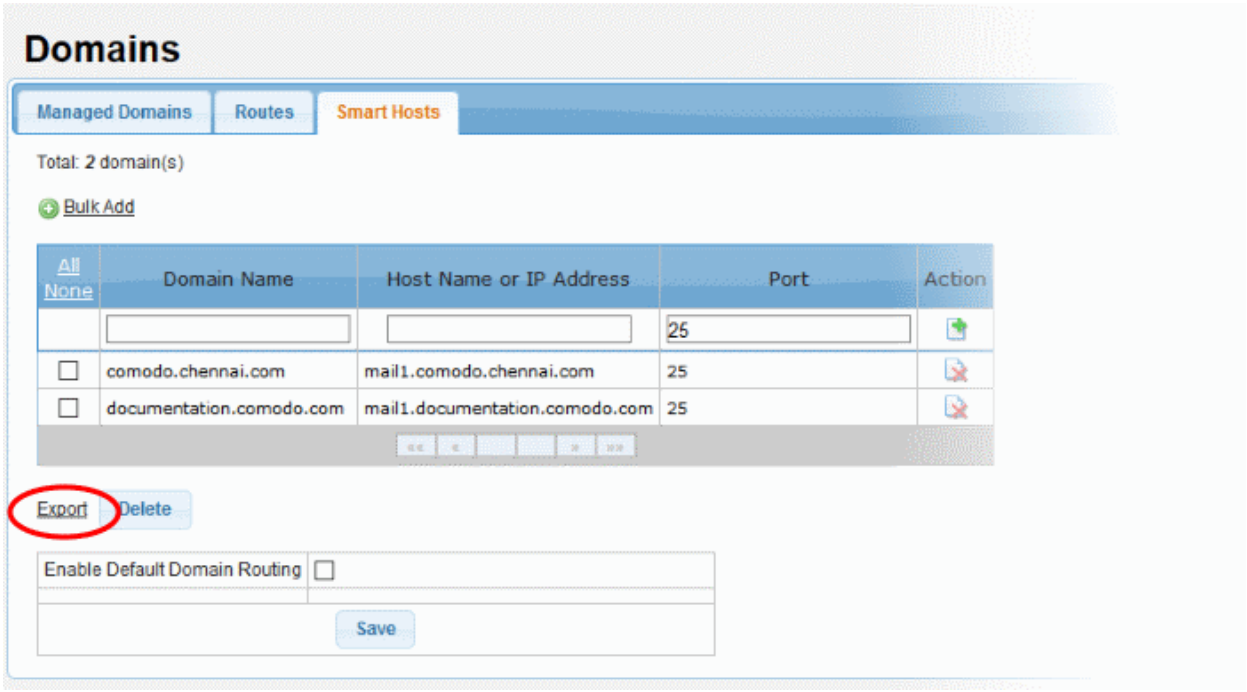


- Click 'OK' to confirm the deletion of the selected 'Smart Host' routes

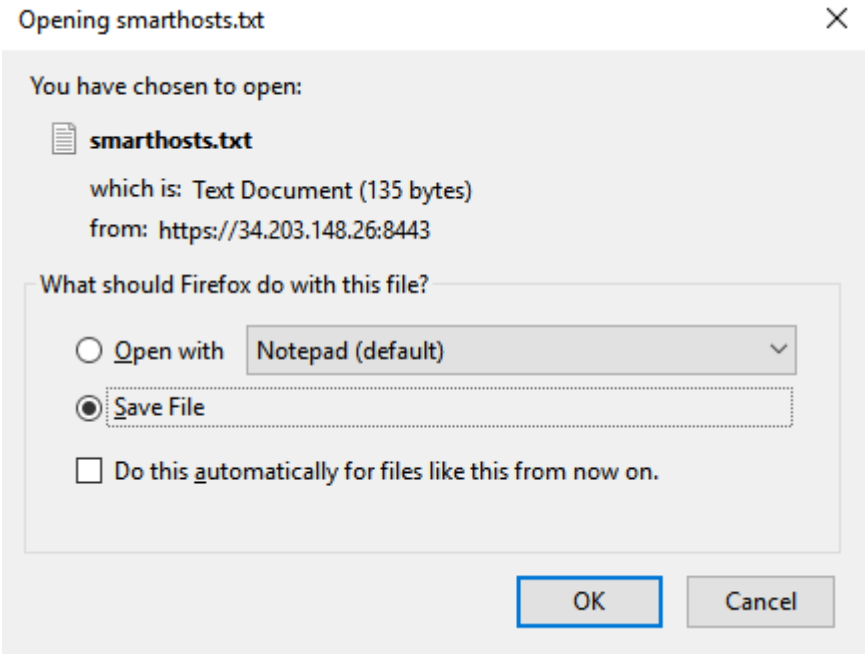


To export 'Smart Host' routes list for domains

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



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

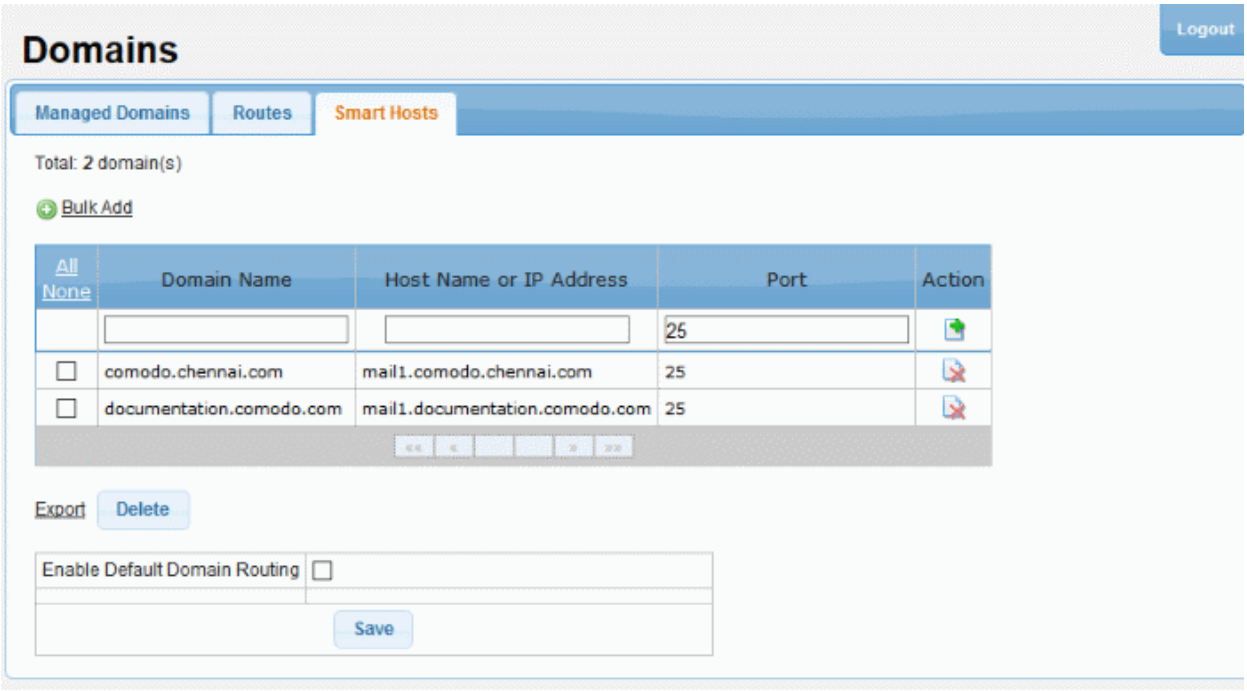


4.2.4 Default Domain Routing

Dome Antispam allows you to configure routing for 'Manage Domains' that are protected by its filtering engine. Refer

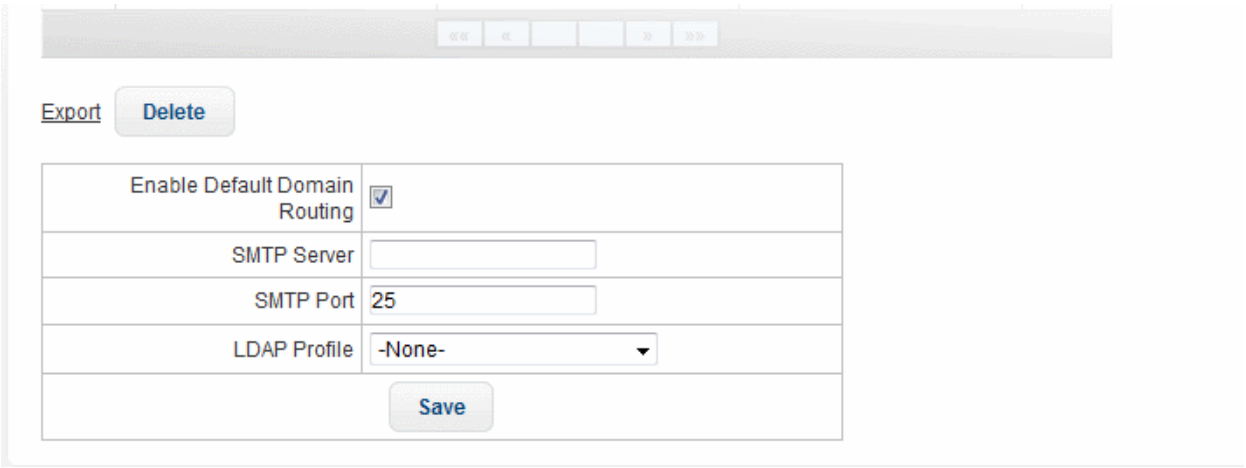
to the section 'Managing Domain Routes' to find out how to configure routing for managed domains. If no routing is configured, then the default domain routing will apply for added domains. The default settings can be configured in the 'Smart Hosts' section.

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



- Select the 'Enable Default Domain Routing' check box

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



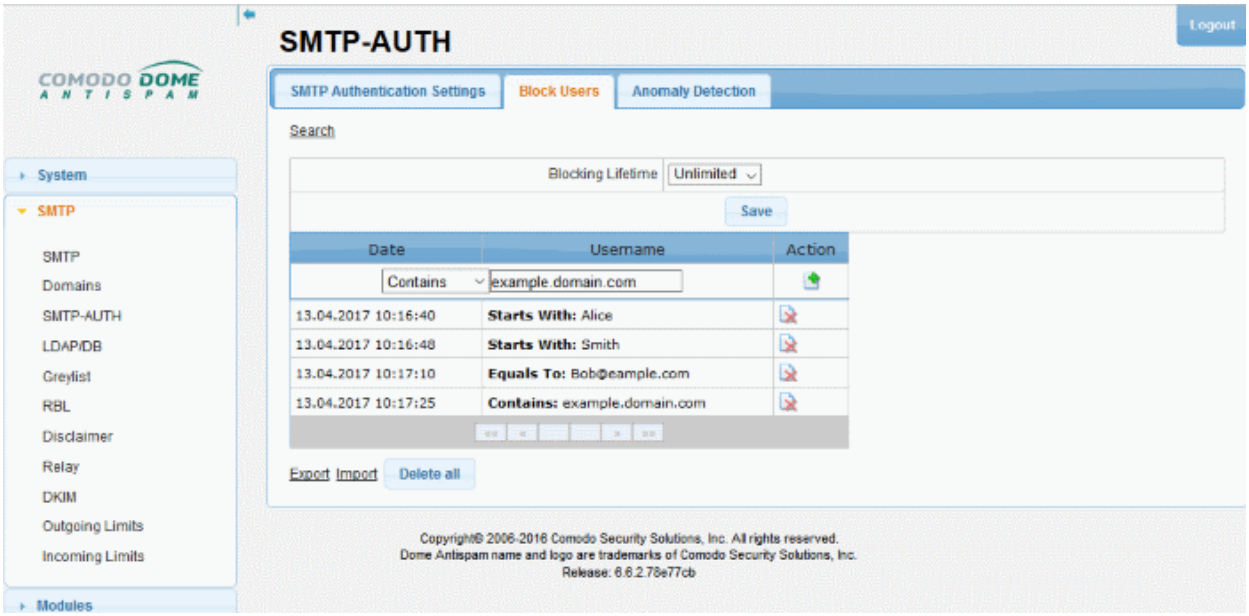
- **SMTP Server:** Enter the server name or IP address of the SMTP server to which Dome Antispam should forward the mails
- **SMTP Port:** Enter the port number to which Dome Antispam should forward the mails
- **LDAP Profile:** Select the LDAP Profile that Dome Antispam should use for user verification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

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

4.3 Dome Antispam SMTP AUTH Connector

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

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



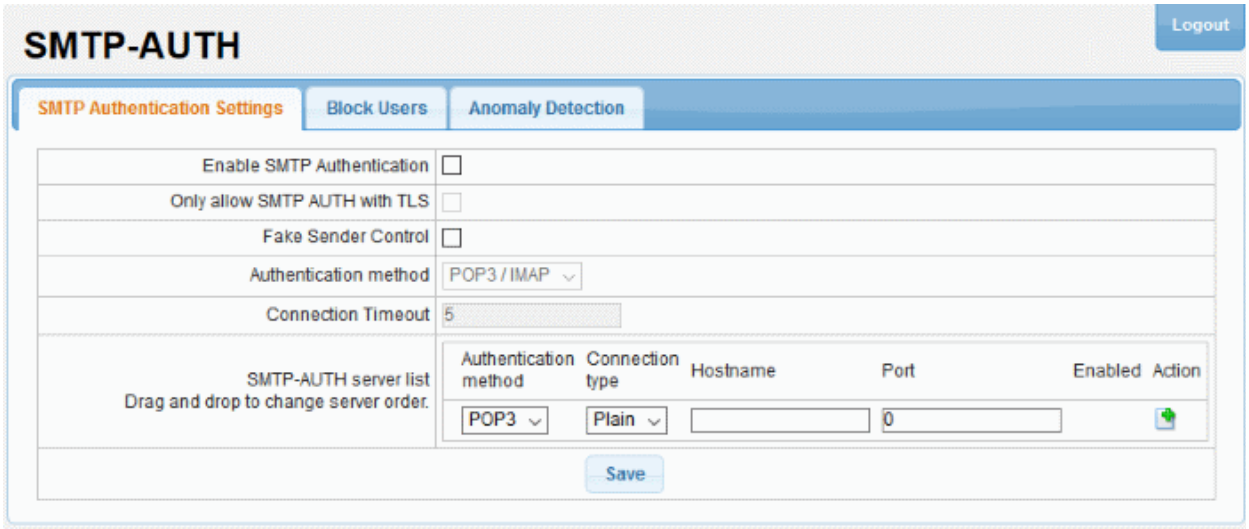
Click the following links for more details:

- SMTP Authentication Settings
- Block Users
- Anomaly Detection

4.3.1 SMTP Authentication Settings

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

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



SMTP 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. Refer to 'POP3/IMAP Authentication Method' and 'LDAP Authentication Method' for details on the respective settings.		
Connection Timeout	Enter the time in seconds during which authentication between the client and the POP3/IMAP/LDAP server must be completed. The user will be prompted to enter credentials again if the time elapses.		
POP3/IMAP Authentication Method			
SMTP-AUTH server list	Authentication method	Select authentication method - either POP3 or IMAP.	
	Connection type	Select the type of connection (clear text or encrypted SSL/TLS).	
	Hostname	Enter the server name or IP address of the SMTP-AUTH server.	
	Port	Enter the port of the server to which Dome Antispam should connect to.	
	Enabled	Activate or disable the server.	
	Action		Click this button to add an SMTP-AUTH server to the list after configuring all parameters.
			Allows 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.		

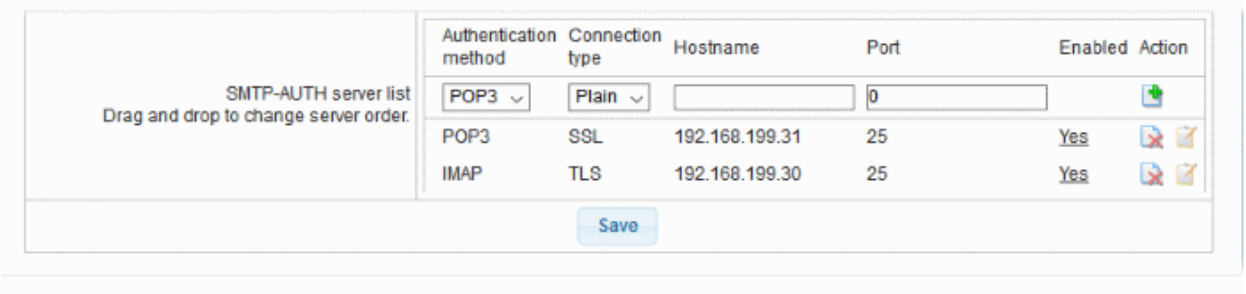
To configure SMTP authentication settings

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

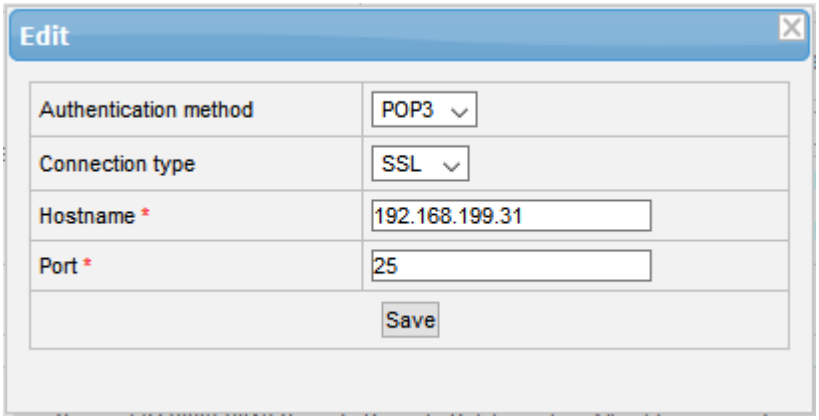
- Enter the time in seconds after which the SMTP Auth session will end.

POP3/IMAP Authentication Method

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



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

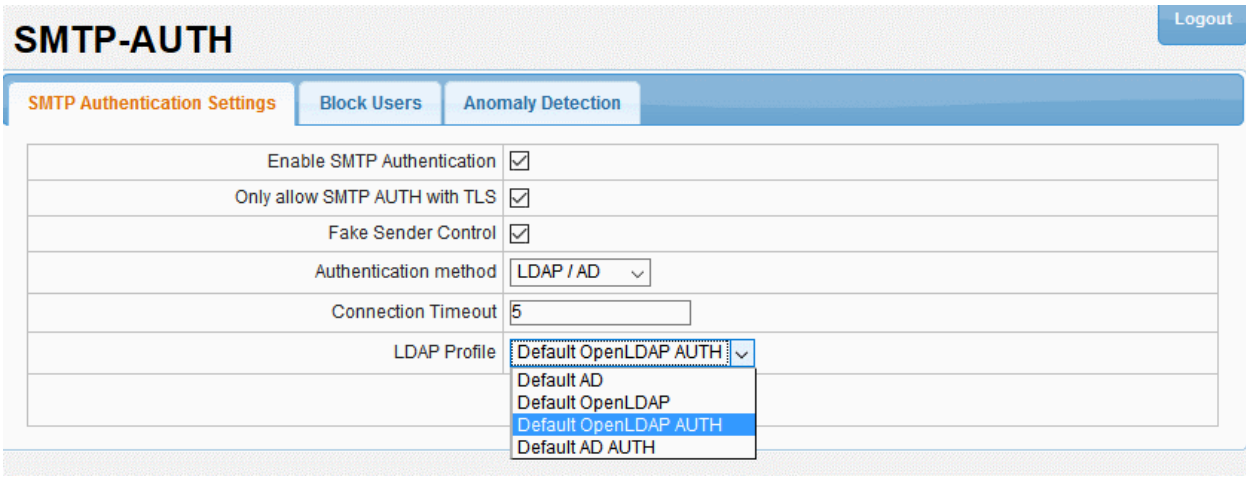


- Edit the parameters as required and click the 'Save' button.
- To delete an auth server from the list, click the button and click 'OK' in the confirmation dialog.

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

LDAP Authentication Method

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

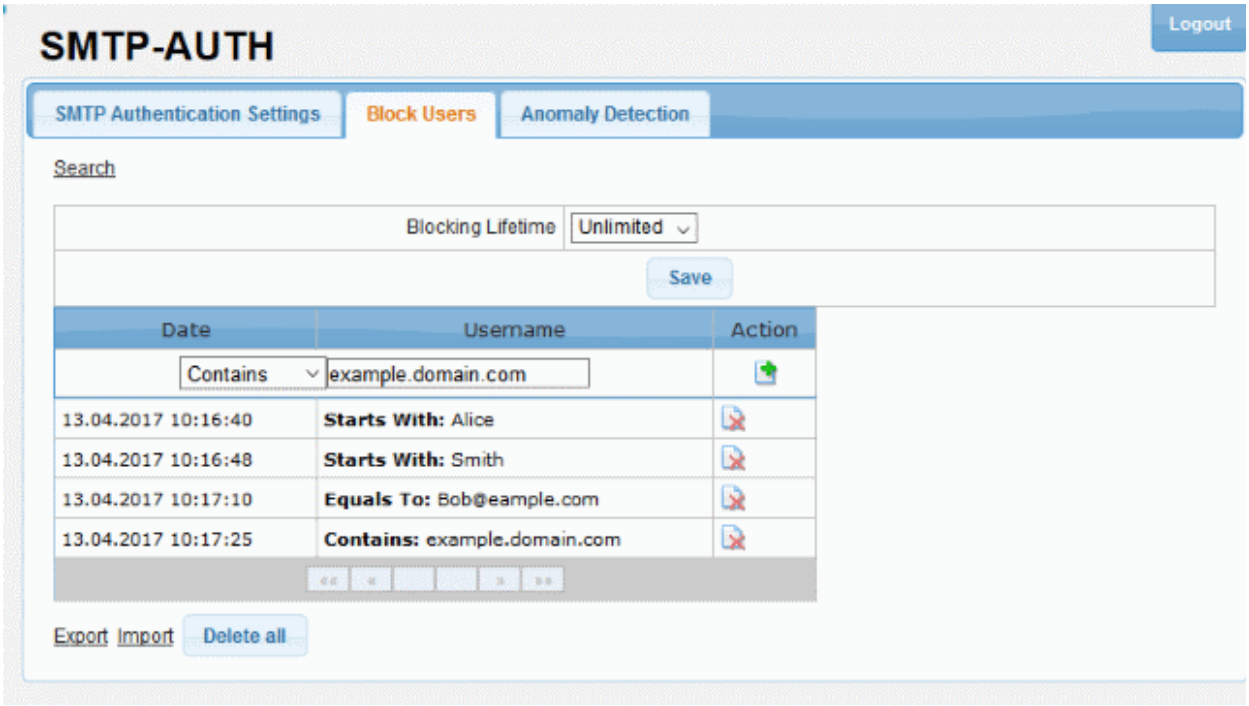


- Click the 'Save' button to apply your changes.

4.3.2 Block Users

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

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



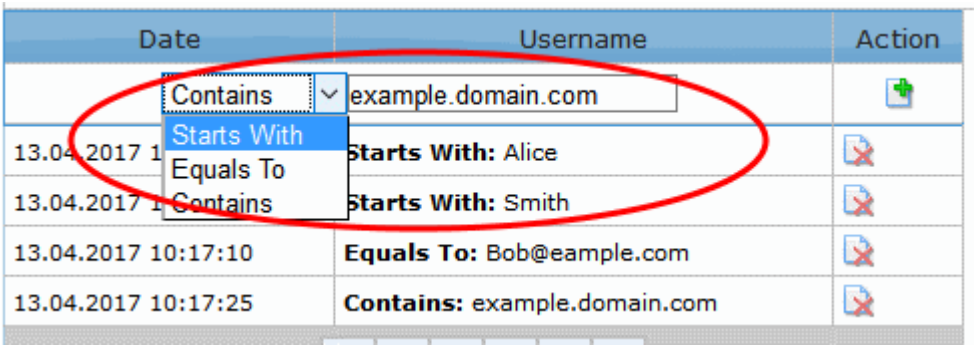
The interface allow administrators to:

- 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

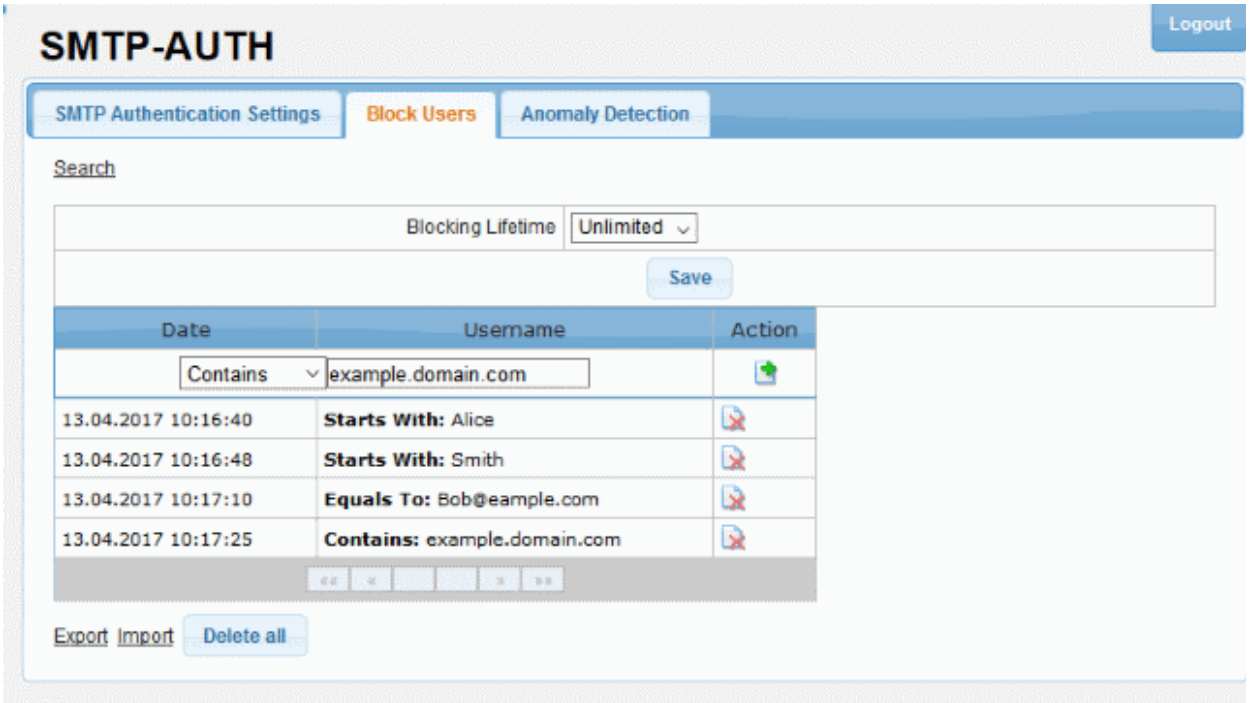
To Add a Blocked User

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

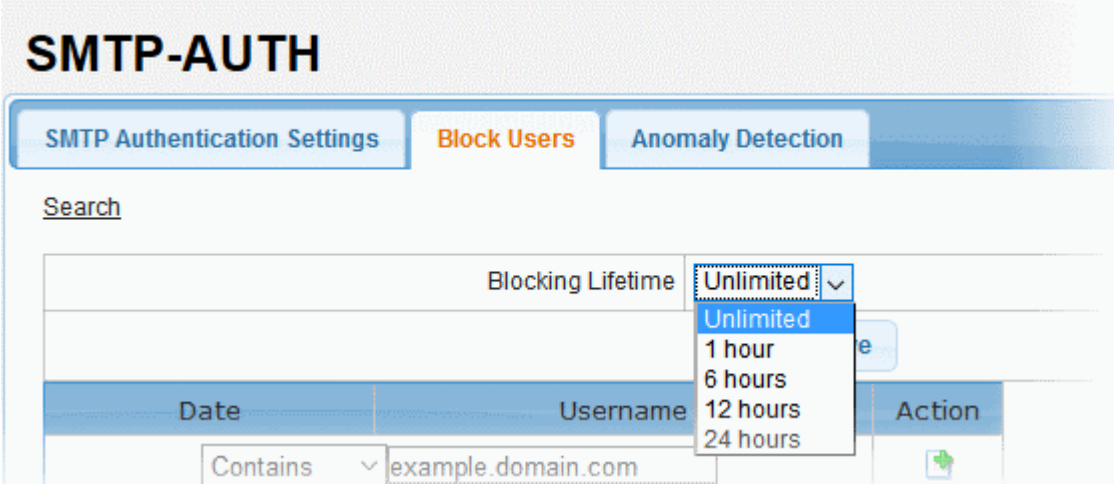


- Click the 'Add' button to apply your choice. The item will be added to the list with the category type displaying on the left side.



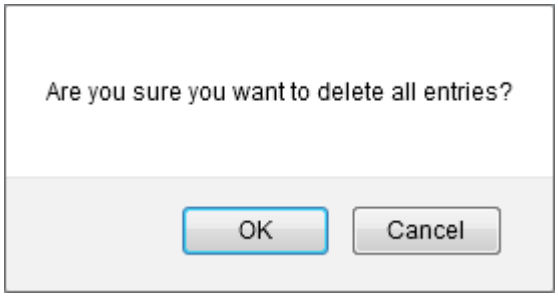
Blocking Lifetime

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'.



To remove users from the blocked list

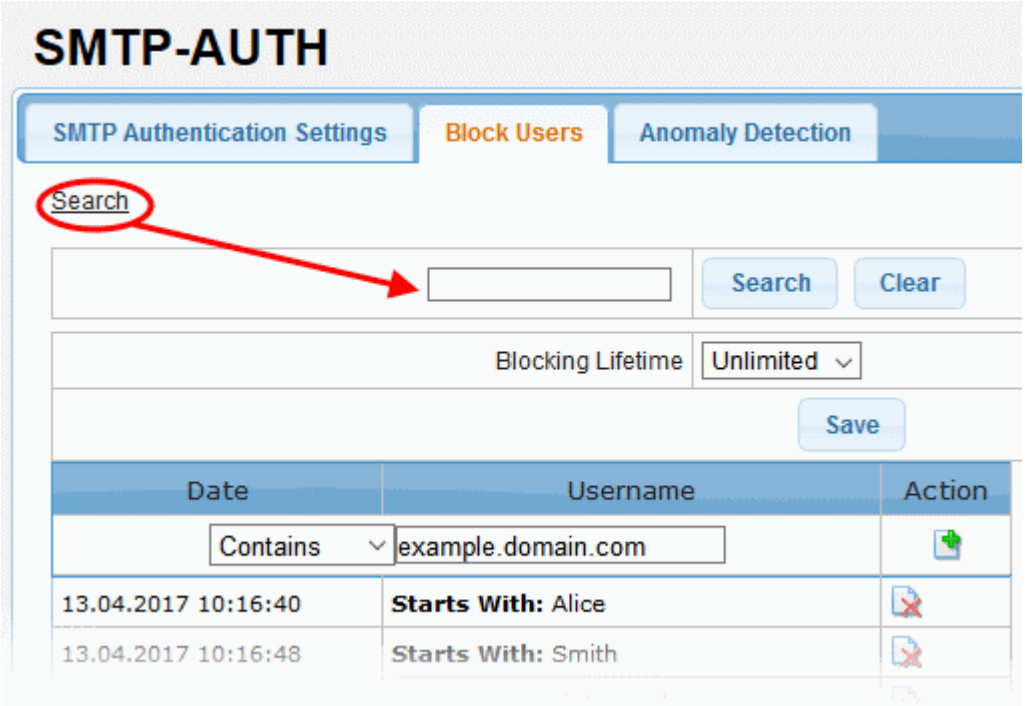
- To remove users one at a time, click the button under the 'Action' column header and confirm the deletion in the 'Confirmation' dialog.
- To delete all the blocked users in the list, click the 'Delete all' button at the bottom.



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

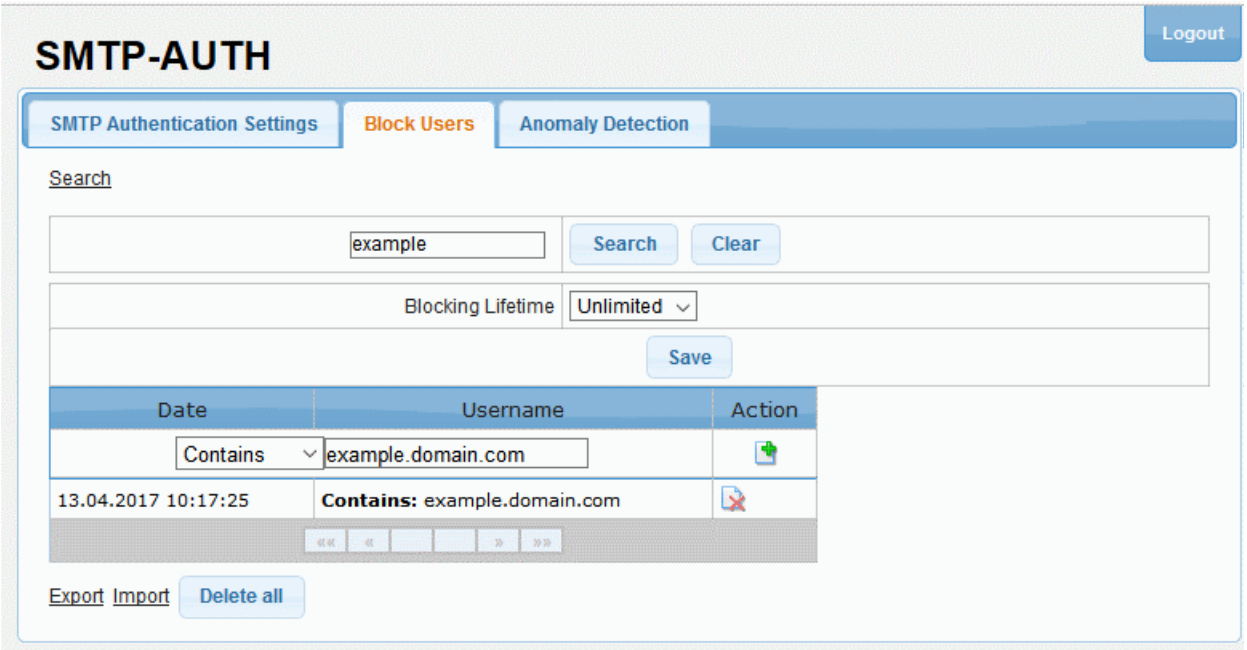
To search for blocked users

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



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

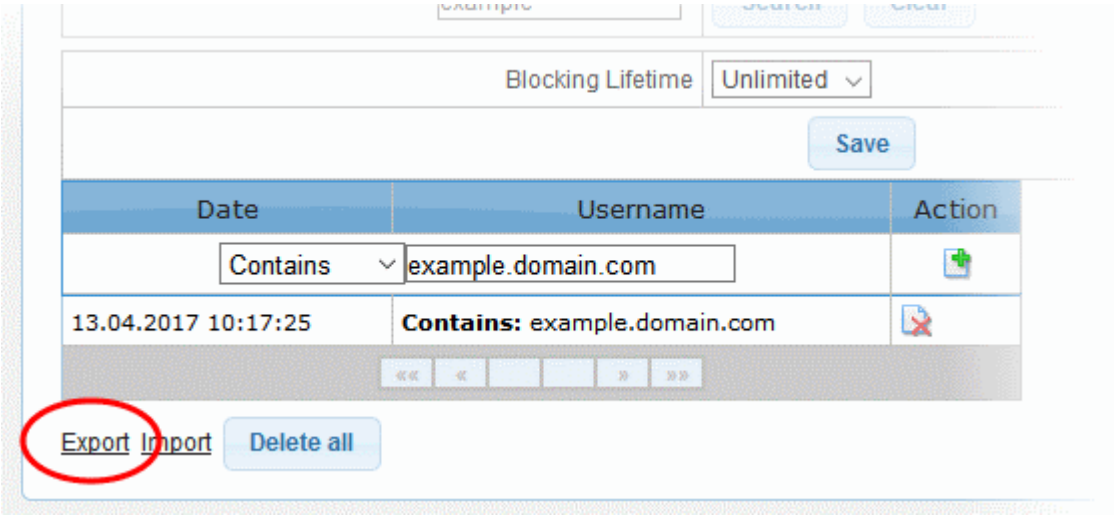
The items that contain the entered search text will be displayed.



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

To export blocked users to file

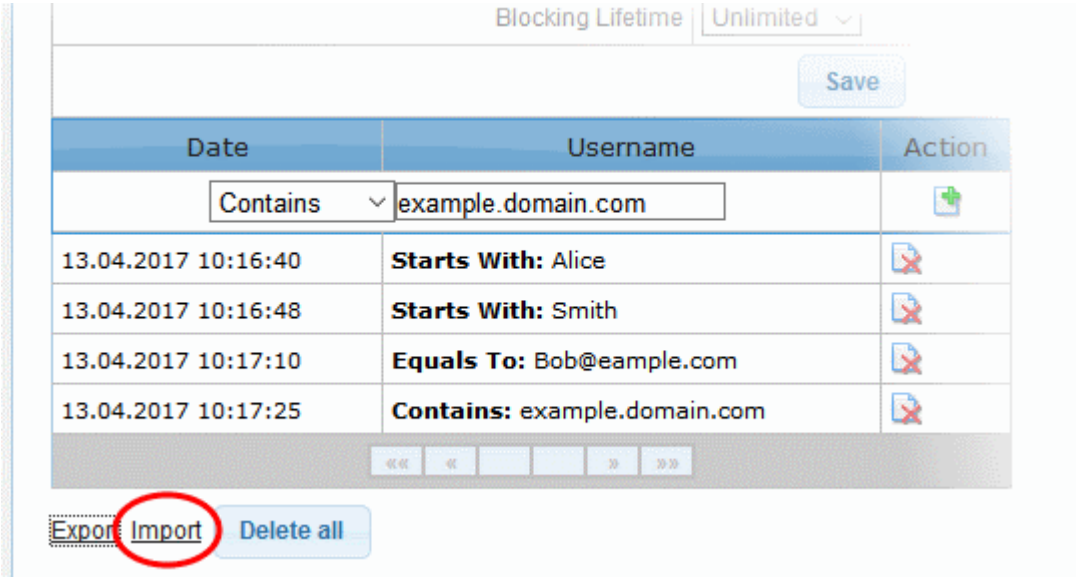
- Click the 'Export' link at the bottom of the screen



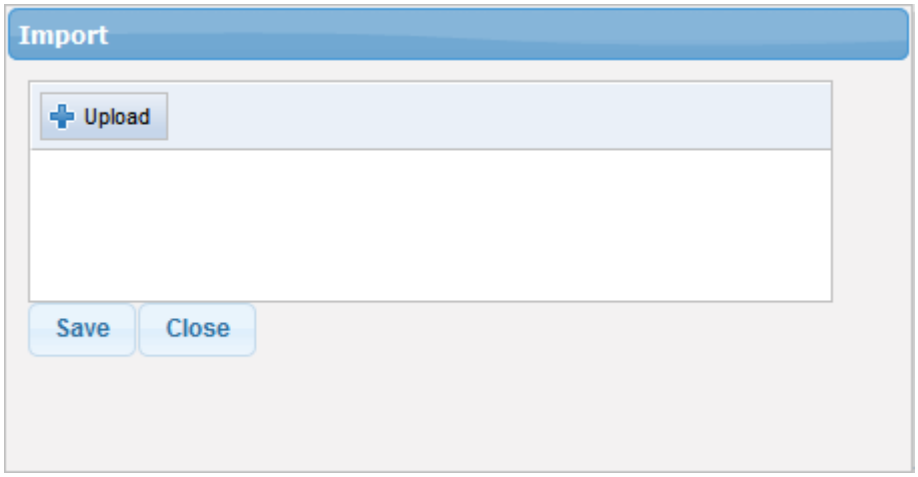
- The user list will be exported as a .txt file. Save the file as required.

To import blocked users from file

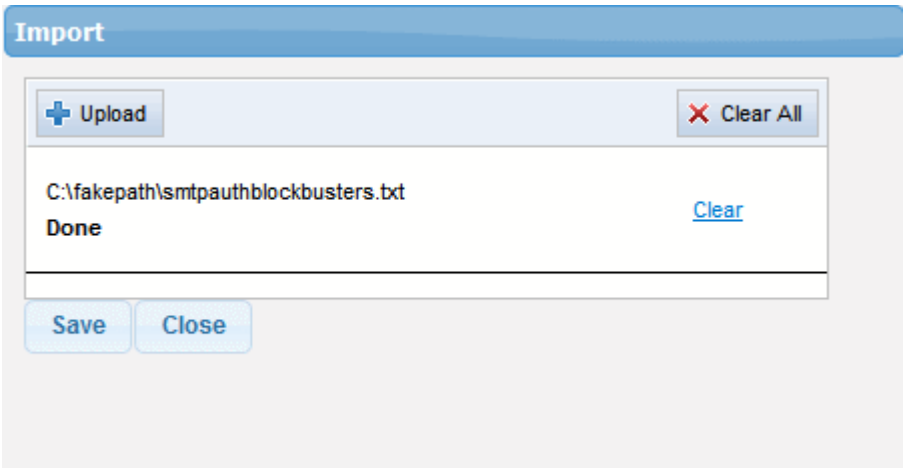
- Click the 'Import' link at the bottom of the screen



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'.

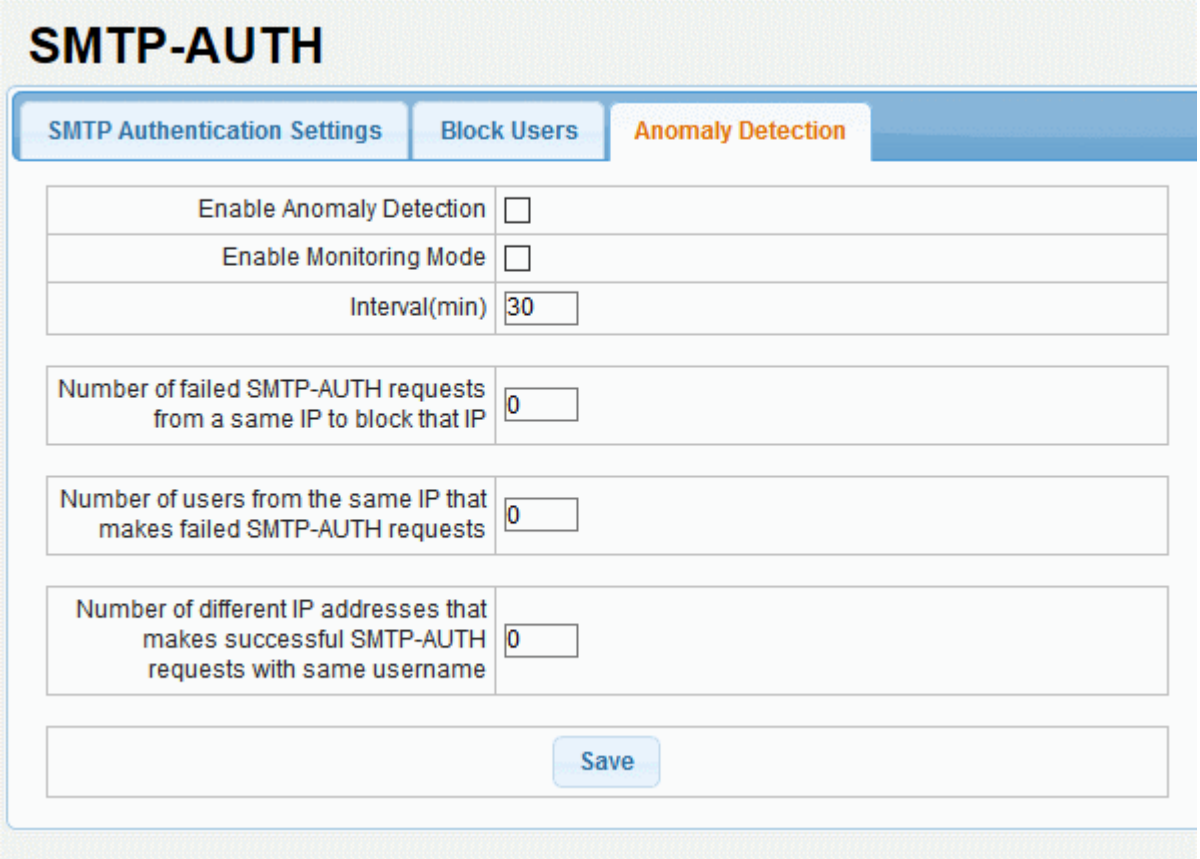


- Repeat the process to add more files.
- To remove a file, click the 'Clear' link beside it.
- To remove all added files, click the 'Clear All' button at top right.
- To finalize the import, click the 'Save' button.

4.3.3 Anomaly Detection

The Anomaly Detection' tab allows you to receive alerts when Dome Antispam detects that a user/email address has sent messages from multiple IP addresses within a set time interval. You can choose to block these users if the outgoing mail IP addresses exceed the number set in this tab. This value cannot be '0'. Set a value between 1 and 10,000 to block users, IP addresses or SMTP Auth requests.

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



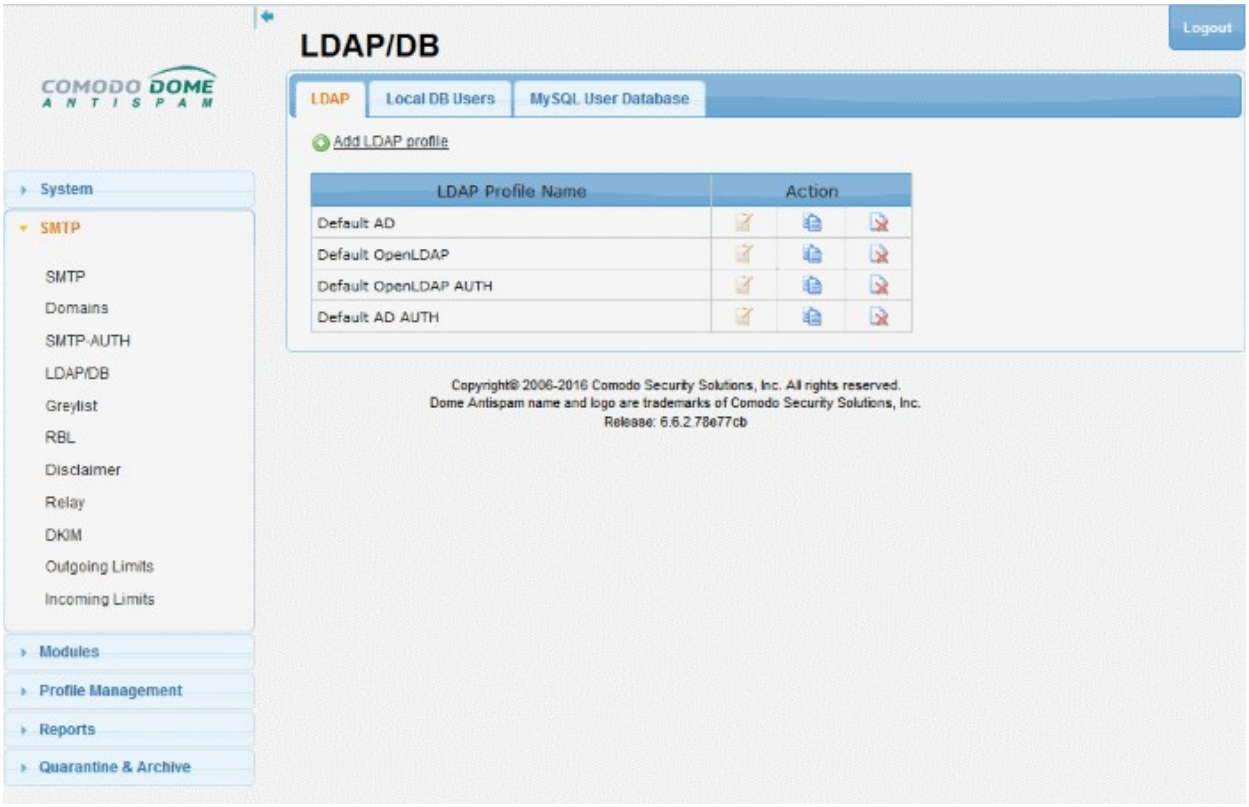
Anomaly Detection Settings - Table of Parameters	
Parameter	**Description**
Enable Anomaly Detection	Enables anomaly detection with the parameters listed directly below this setting. By default this setting is disabled
Enable monitoring mode	If enabled, the SMTP-AUTH controller monitors authorization 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 addresses that makes successful SMTP-AUTH requests with same username	The minimum number of different IP addresses that can make successful SMTP-AUTH requests with the same username. Any request beyond the threshold set will not be processed

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

4.4 LDAP/Local DB/My SQL User Database

Dome Antispam can be configured to check the validity of a recipient before filtering begins so that resources are not wasted on invalid recipients. If the email servers behind Dome Antispam are integrated with LDAP, Local DB and/or MY SQL Database, then Dome Antispam will check the validity of recipients and, if not valid, reject the emails at SMTP level.

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



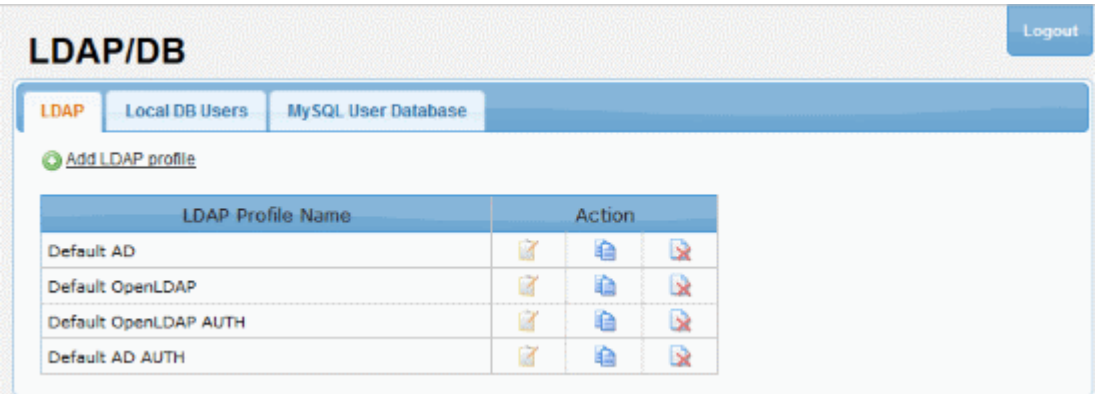
Refer to the following sections for more details:

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

4.4.1 LDAP Profile

The Lightweight Directory Access Protocol, or LDAP, is an application protocol for querying and modifying data using directory services running over TCP/IP. If the email servers behind Dome Antispam are integrated with a directory service via an LDAP profile, Dome Antispam can check whether the recipient is a valid user in the directory. If the recipient is not a valid user then the email is rejected at the SMTP level. This avoids wasting resources by filtering mails 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'.

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



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

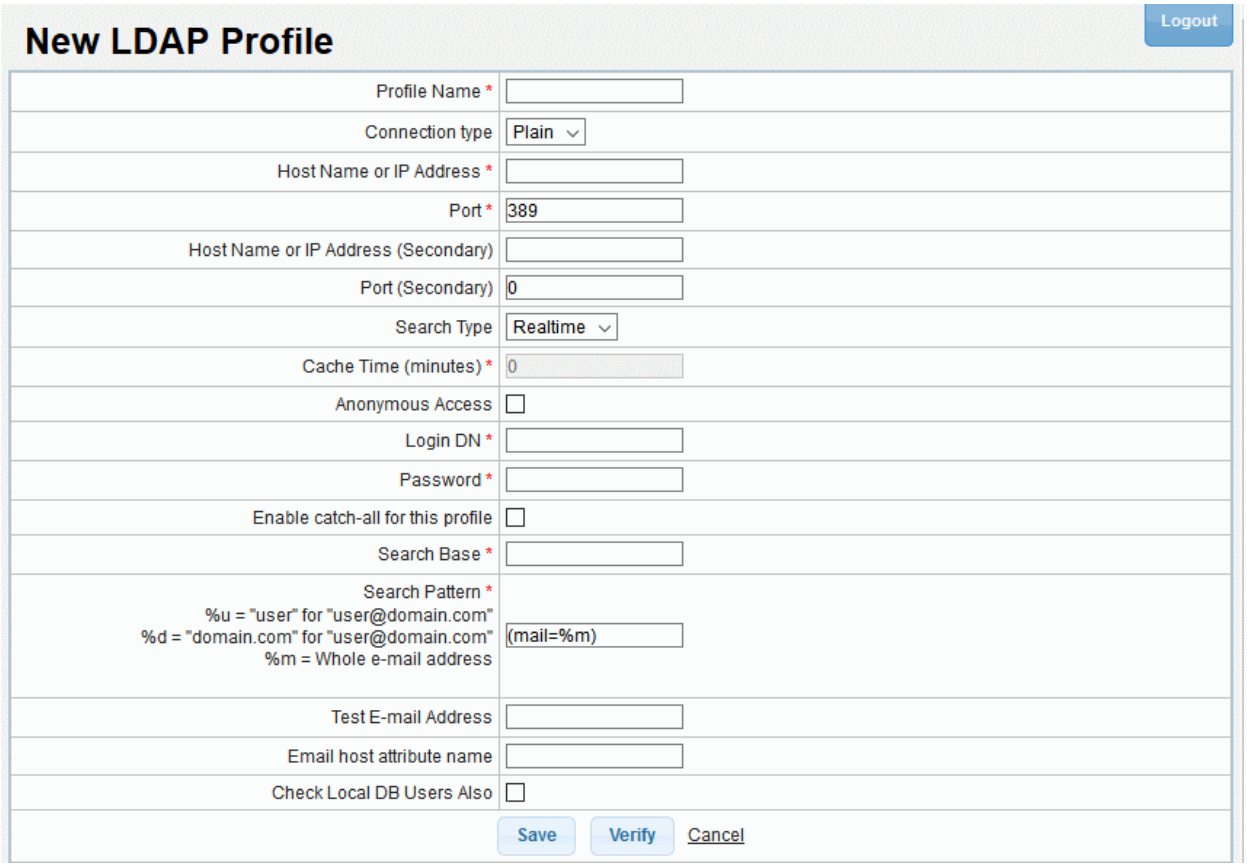
From this screen administrators can:

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

To create a new LDAP profile

You can create a new LDAP profile in two ways:

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



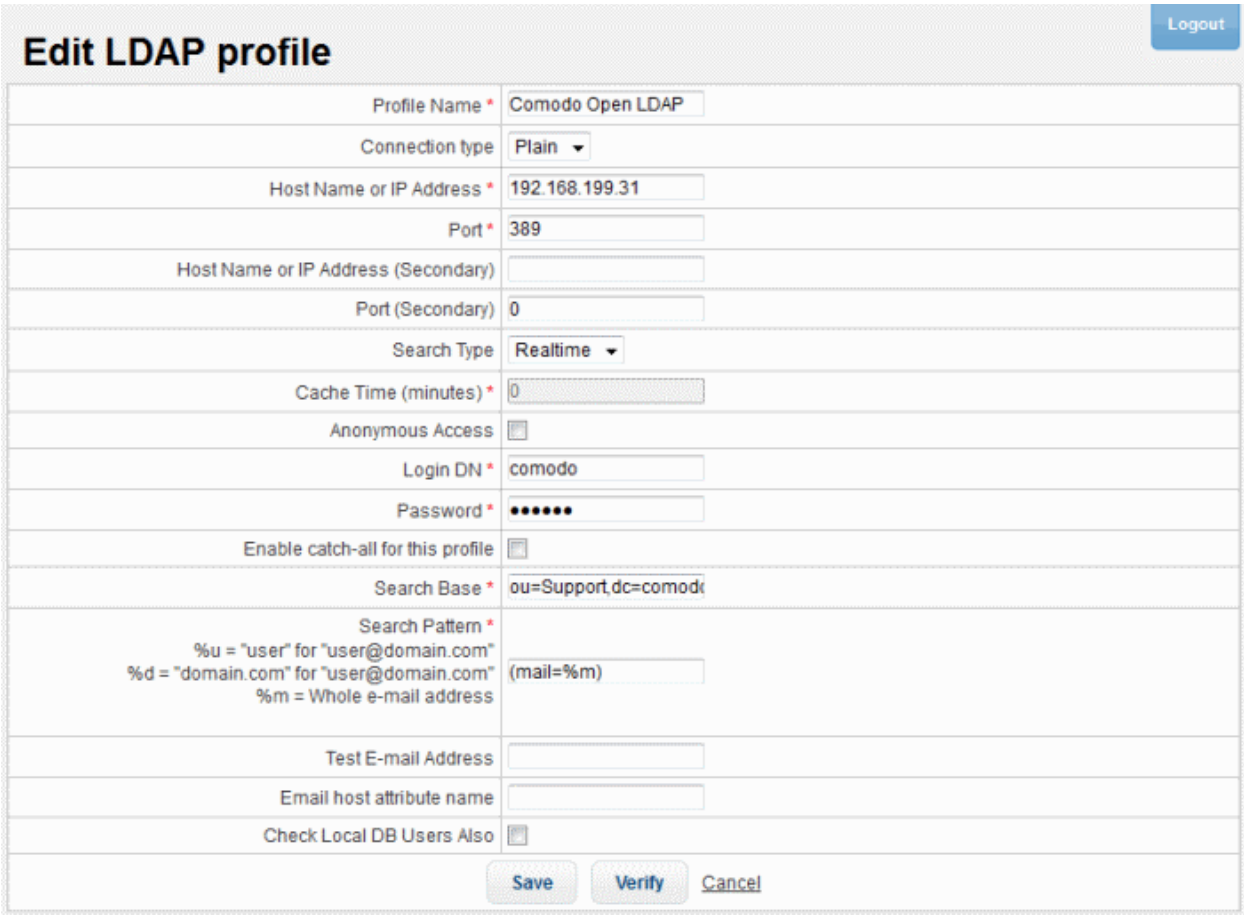
LDAP Profile -Table of Parameters	
Parameter	**Description**
Profile Name	Enter the name of the new LDAP profile
Connection type	Determines how Dome Antispam should connect to the LDAP server. The options available are: • Plain (Not encrypted) • TLS (Encrypted with the TLS protocol. Recommended) • SSL (Encrypted using the SSL protocol. Use if your systems have compatibility issues with TLS)
Host Name or IP Address	Enter the hostname or IP address of the LDAP/Active Directory. Dome Antispam will first check the primary server and will check the secondary server if the primary is not available.
Port	Specify the LDAP server port number. If you use 'Active Directory' then, instead of the default LDAP port 389, port 3826 must be used as Active Directory Catalog port.
Search Type	Select the type of search from the drop-down. The options available are: Realtime - Checks the AD server each time for user validity Cache - Checks the user validity from the system's cache memory and if not available checks the AD server.
Cache Time (minutes)	If the 'Cache' option is enabled as 'Search Type', this field becomes active. Enter the time in minutes the details of users are cached after which they are wiped out.

Anonymous Access	If this feature is enabled, the connection to LDAP server will be created anonymously so that username and password are not required.
Login DN	LDAP username to connect LDAP / Active Directory server.
Password	Enter the LDAP user password.
Enable catch-all for this profile	When this feature is enabled, if the recipient's address is value1-value2-value3@domain.com then Dome Antispam first checks whether this address is registered in LDAP. If it does not find it, it deletes value1 and checks the remaining value2-value3@domain.com address. If it does not find it again then it delete value2 and checks value3@domain.com
Search Base	Specify the search starting criteria to be used in LDAP tree.
Search Pattern	Determines which LDAP attributes will be searched in search base.
Test E-Mail Address	Enter the email address to test the LDAP connection.
Email host attribute name	Enter the mail host attribute name for the LDAP / Active Directory server.
Check Local DB Users Also	Checks for users in Local Data base users list as well.

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

To edit a LDAP profile

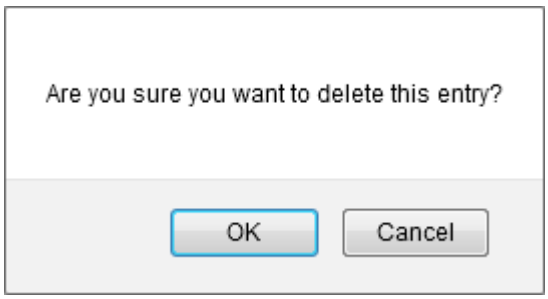
- Click the button beside a LDAP profile that you want to edit.



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

To delete a LDAP profile

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

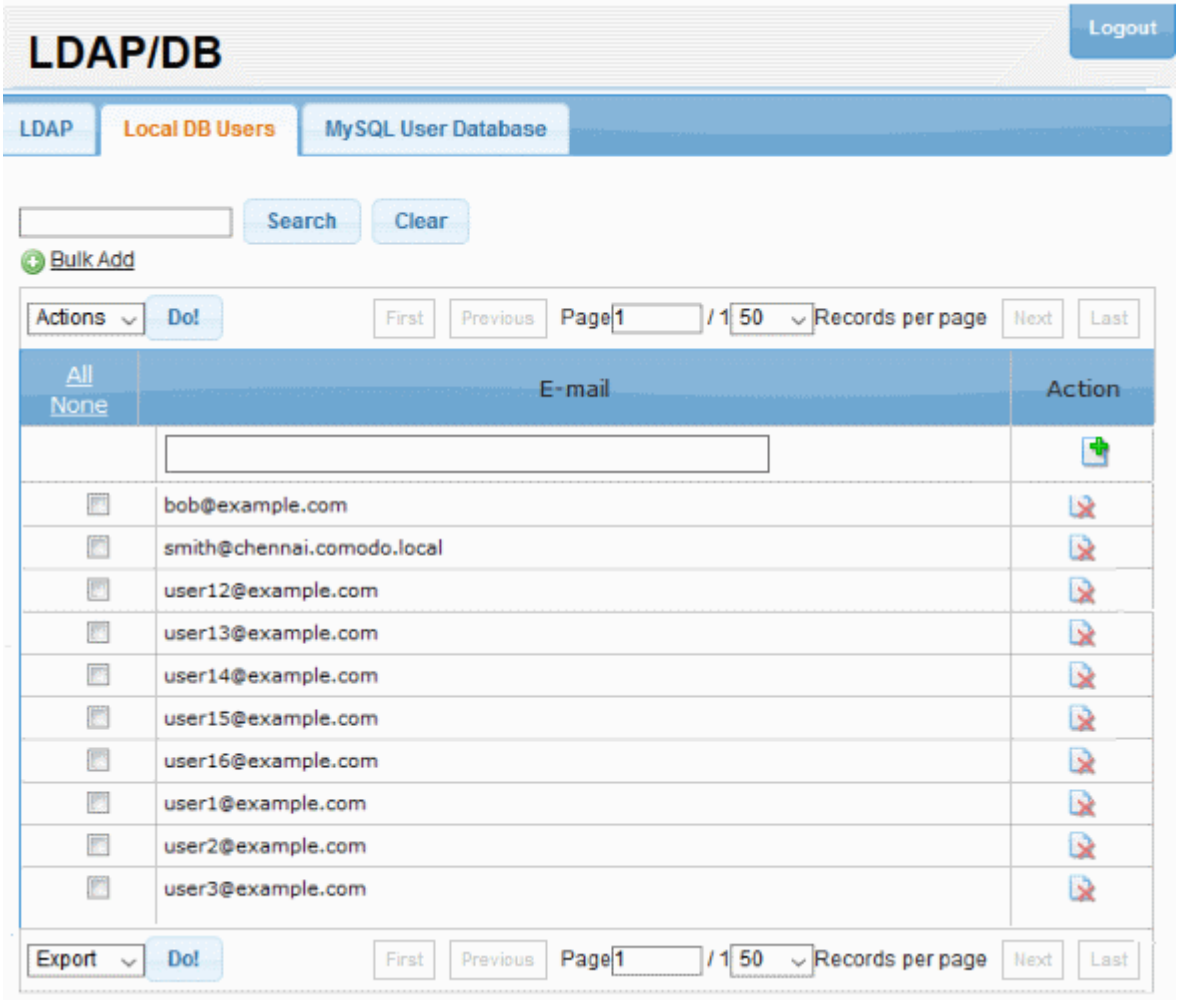


- Click 'OK' to confirm the deletion.

4.4.2 Local DB Users

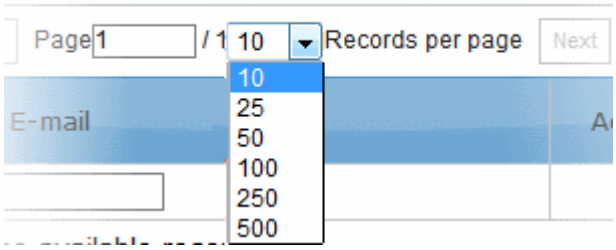
Dome Antispam allows you to add users to its local database for managed domains. This helps to ensure mails to invalid recipients are rejected before the filtering processes is initiated. This helps to conserve the system's resources for better utilization. The users added here are available for selection in interfaces such as 'Managed Domains > Routes'.

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



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

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



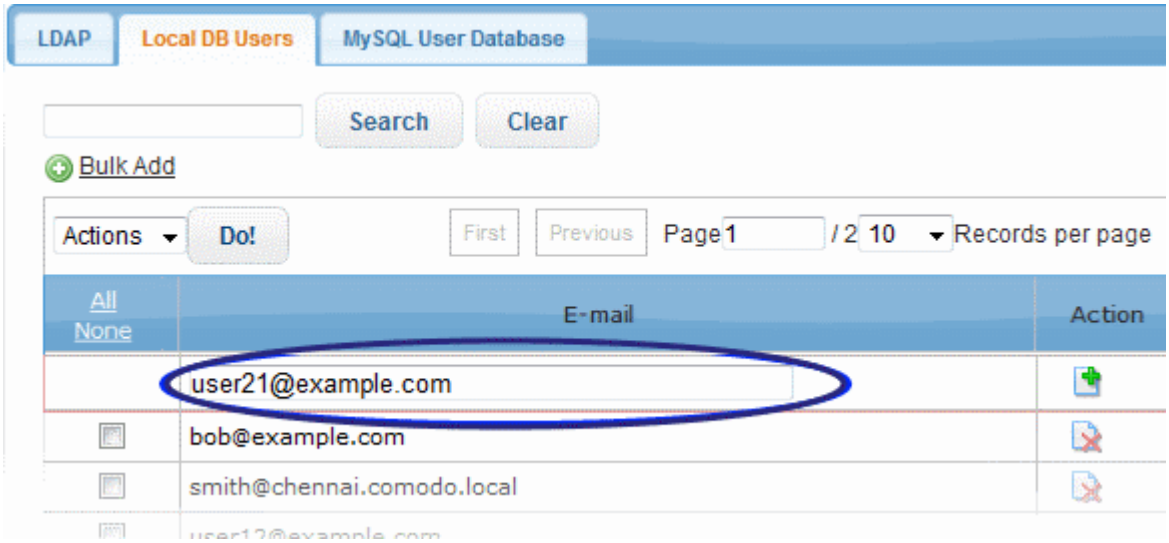
Click the 'First, Previous, Next and Last' buttons to view all the items in the list.

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



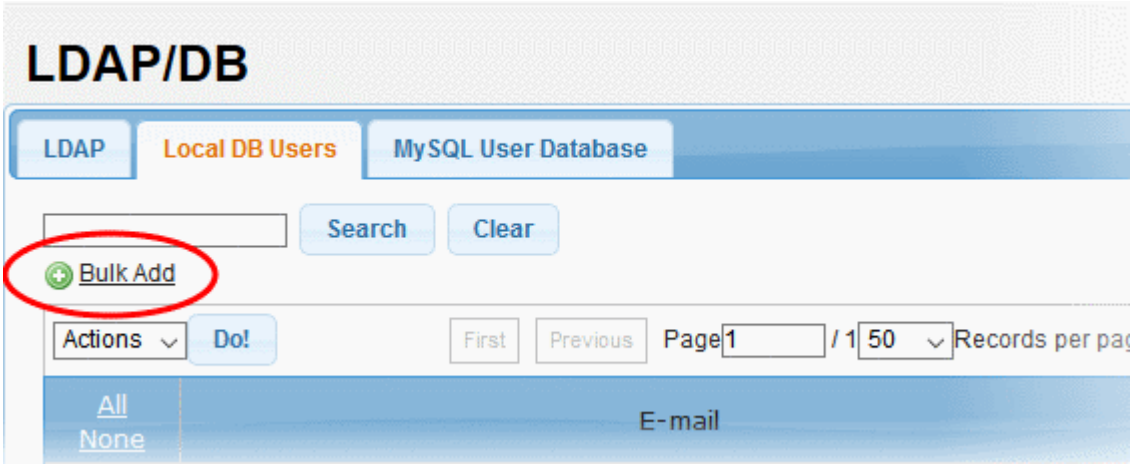
- Click the button under the 'Action' column.

Note: You can add users for managed domains only.

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

To add multiple users

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



The 'Bulk Add' screen will be displayed.

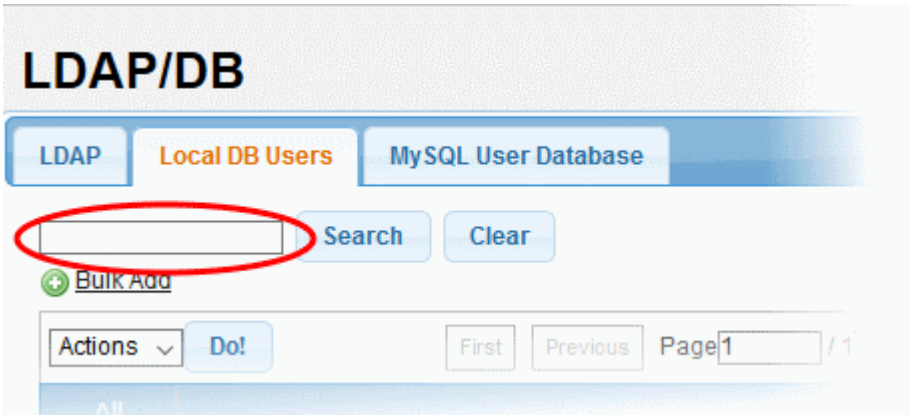
- Enter the users' email addresses each per line. The maximum allowed at a time is 500 users.
- Click the 'Add' button.

Note: You can add users for managed domains only.

The users will be added and displayed in the list.

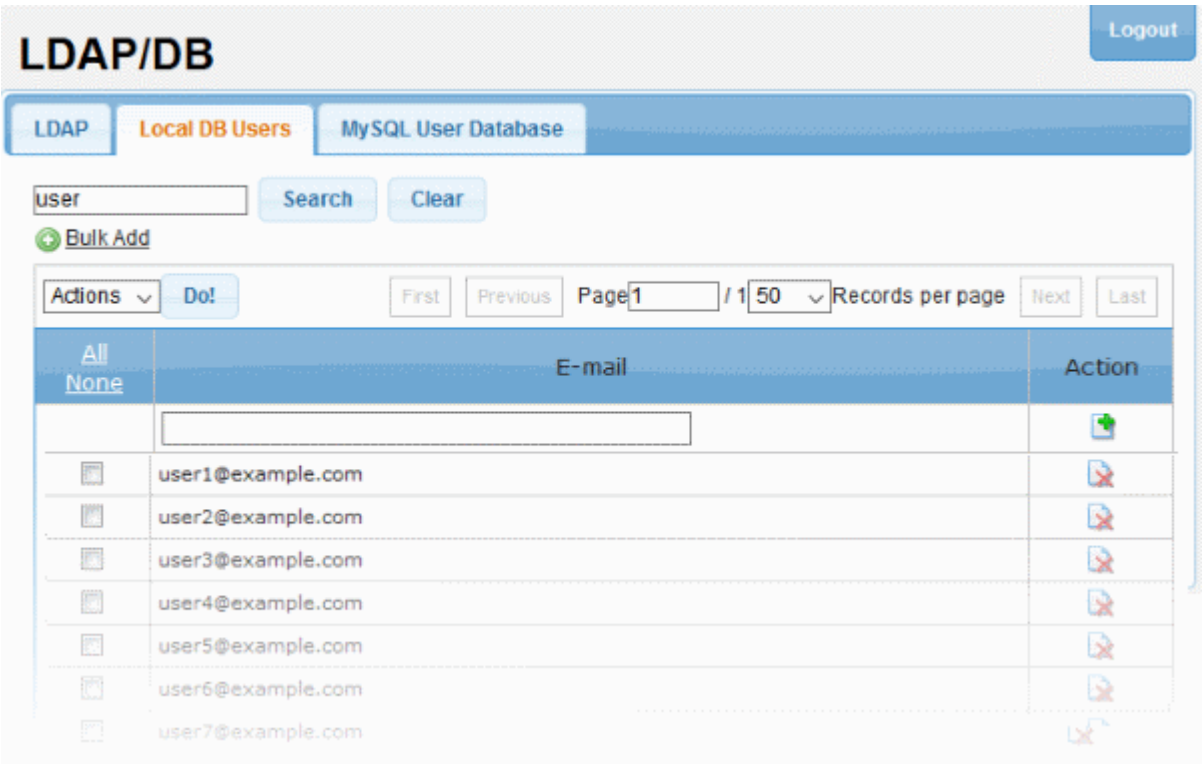
To search for users

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



- Click the 'Search' button.

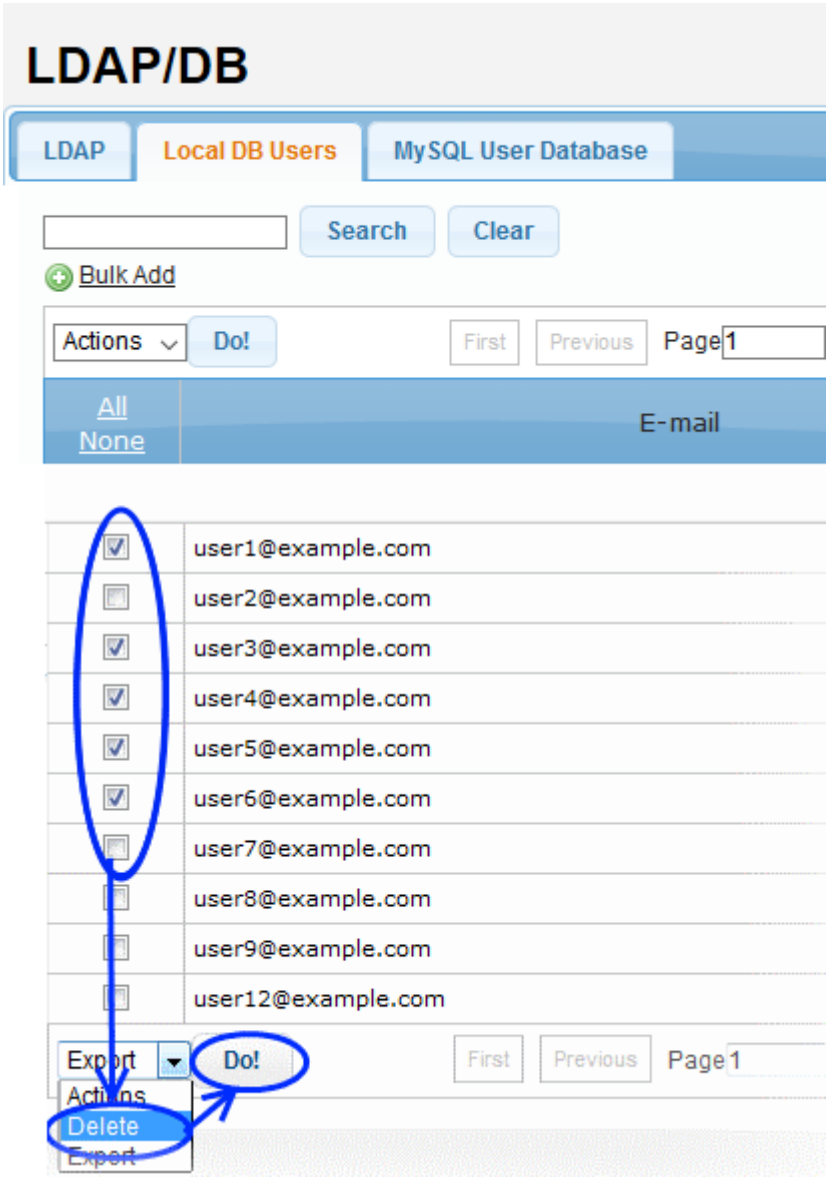
The items that contain the entered search text will be displayed.



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

To delete users

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

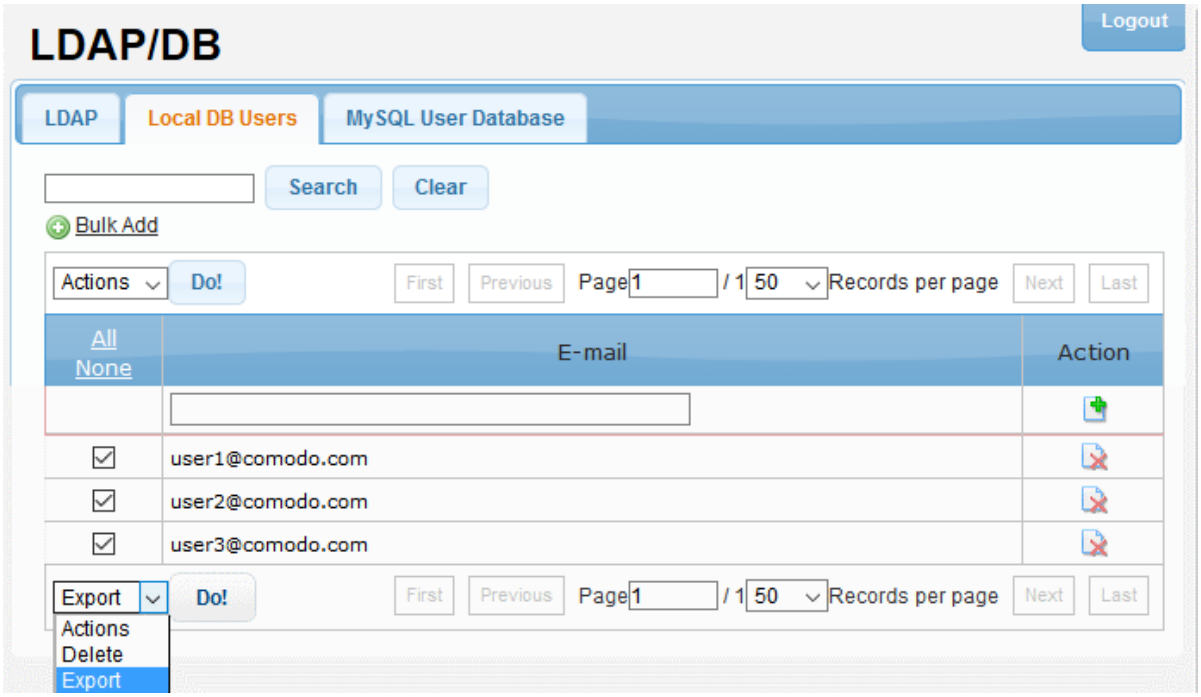


- Select 'Delete' from the 'Actions' drop-down and click the 'Do!' button.

The selected users will be deleted from the list.

To export the user list to a file

- To export users one at a time, click the 'Actions' drop down, and select the 'Export' option.

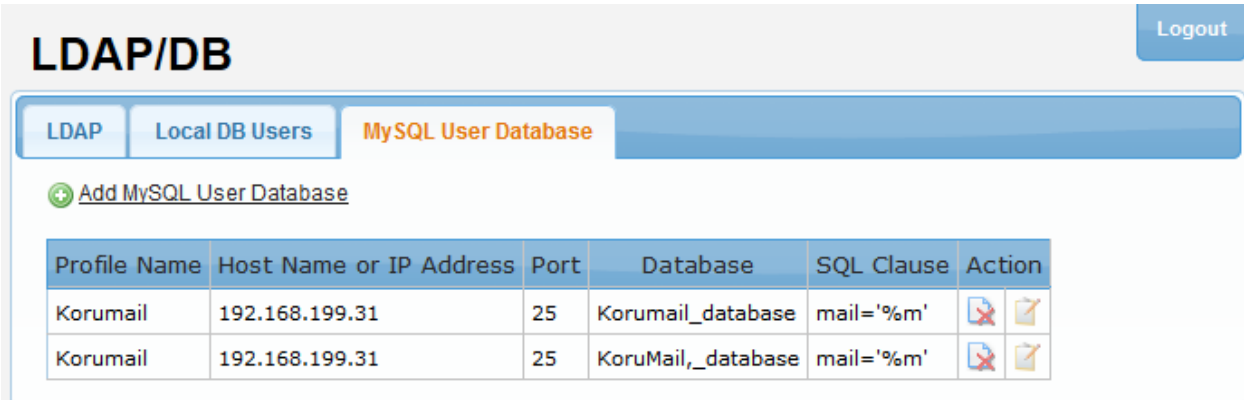


- Click 'Do' to download and save the list as a text file to your system.

4.4.3 My SQL User Database

Dome Antispam 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, Dome Antispam's resources are not wasted. The 'MySQL User Database profiles' added here are available for selection in interfaces such as 'Managed Domains > Routes'.

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



MySQL User Database Profile - Table of Column Descriptions	
Column Header	**Description**
Profile Name	The name of the MySQL User Database profile added to Dome Antispam
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 Dome Antispam connects to.

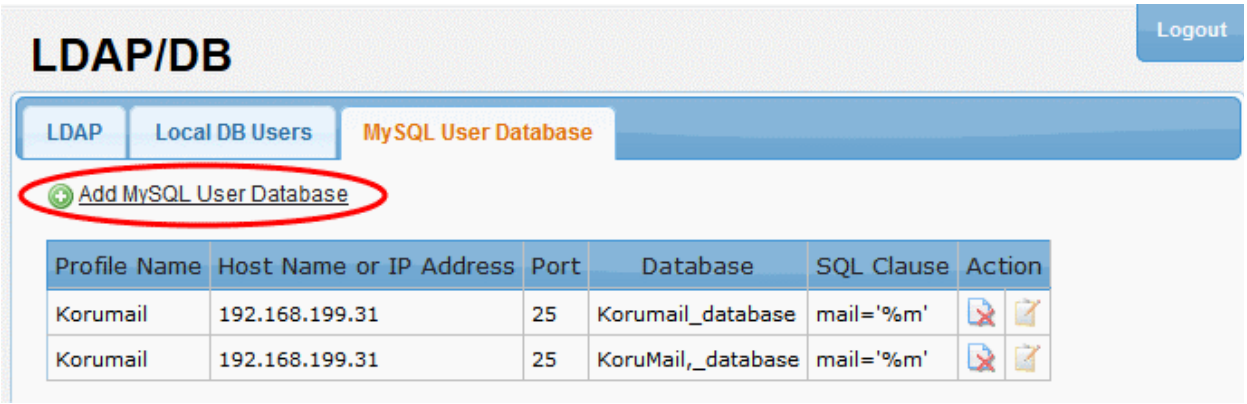
Database	The name of the 'MySQL User Database'.	
SQL Clause	The 'SQL clause' used to fetch the users' details.	
Action		Allows you to edit the details of the 'MySQL' profile
		Allows you to delete a 'MySQL' profile from the list.

From this screen administrators can:

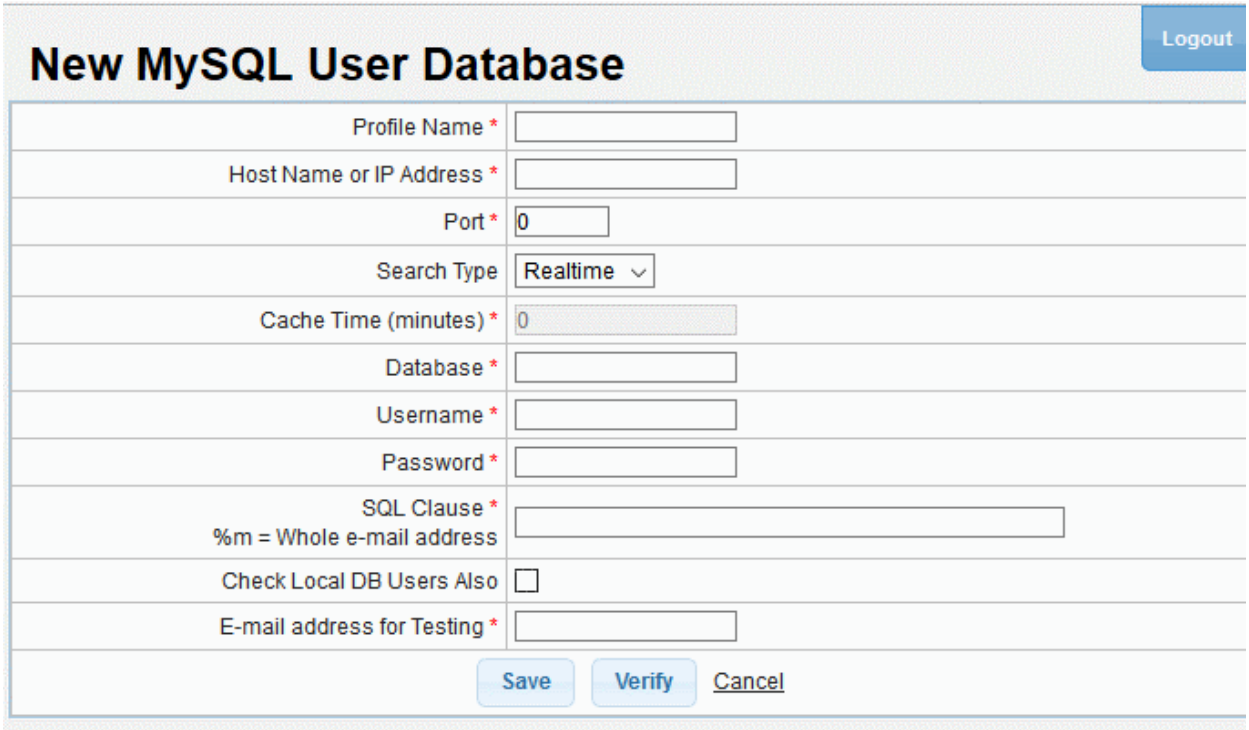
- Add a new MySQL profile
- Edit a MySQL profile
- Delete a MySQL profile

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.



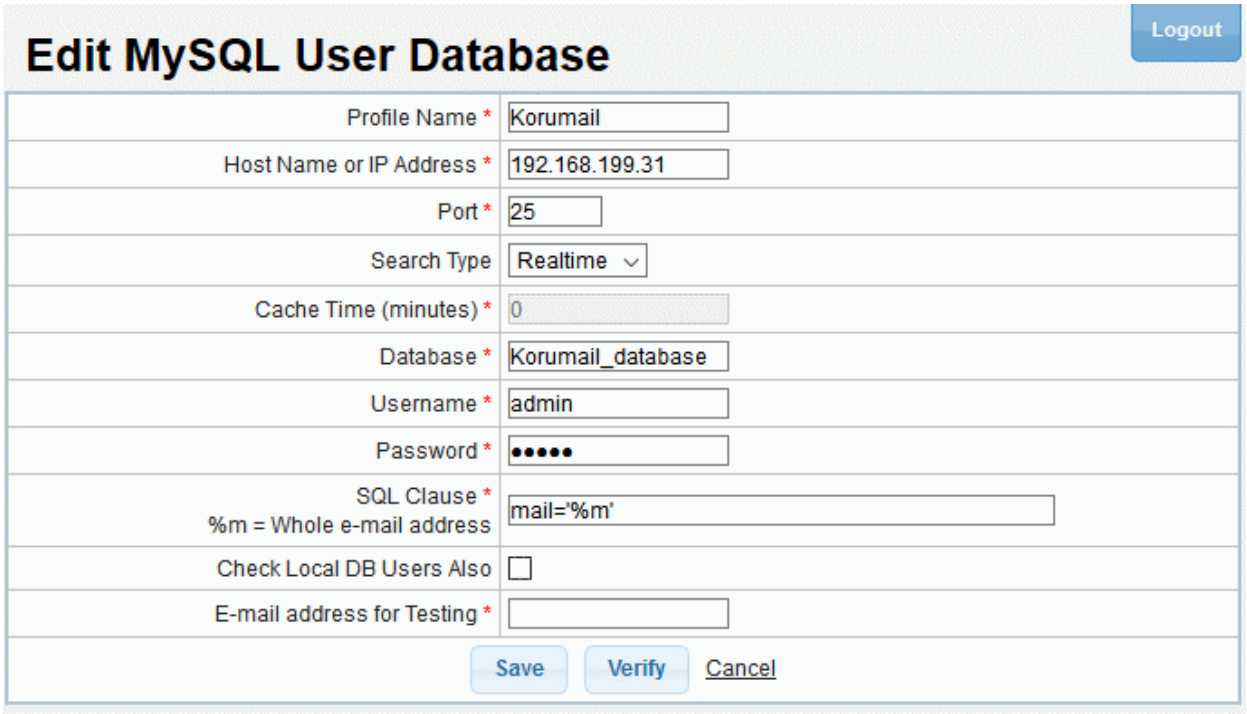
MySQL User Database Profile -Table of Parameters	
Parameter	**Description**
Profile Name	Enter the name of the MySQL profile
Host Name or IP Address	Enter the hostname or IP address of the system where MySQL database is located.
Port	Enter the port number to which Dome Antispam should connect to.
Search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

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

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

To edit a MySQL profile

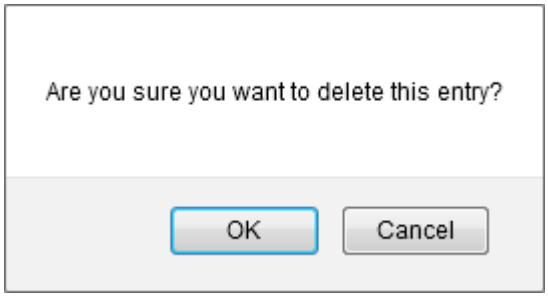
- Click the button beside a 'MySQL' profile that you want to edit.



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

To delete a MySQL profile

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



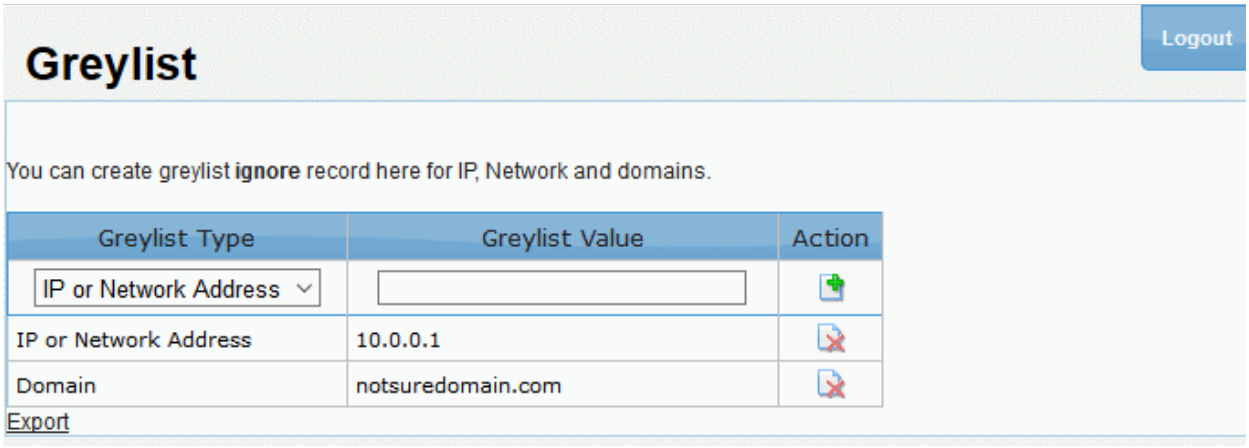
- Click 'OK' to confirm the deletion.

4.5 Greylist

Greylisting is another form of spam control whereby Dome Antispam will temporarily reject any email from senders it does not recognize. Upon receiving this 'try again later' message, legitimate mail servers will indeed try to resend the mail after a delay. Dome Antispam 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 CDAS will accept mail from them on first contact).

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

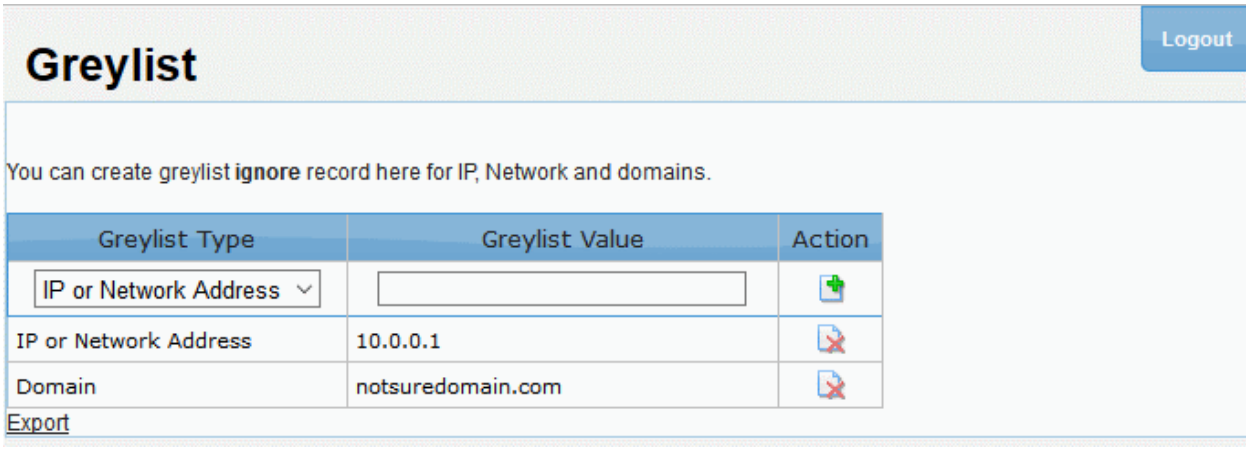


Refer to the next section '**Greylist Ignored IP Addresses/Domains**' for how to add domains, networks and IP addresses to Greylist ignored list.

4.5.1 Greylist Ignored IP Addresses/Domains

Dome Antispam allows you to add IP addresses and domains as exceptions to its greylisting policy. Mail from these addresses will be accepted immediately, without requiring the source mail server to resend. Refer to the previous section, '**Greylist**', if you'd like to read a description of greylisting.

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



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

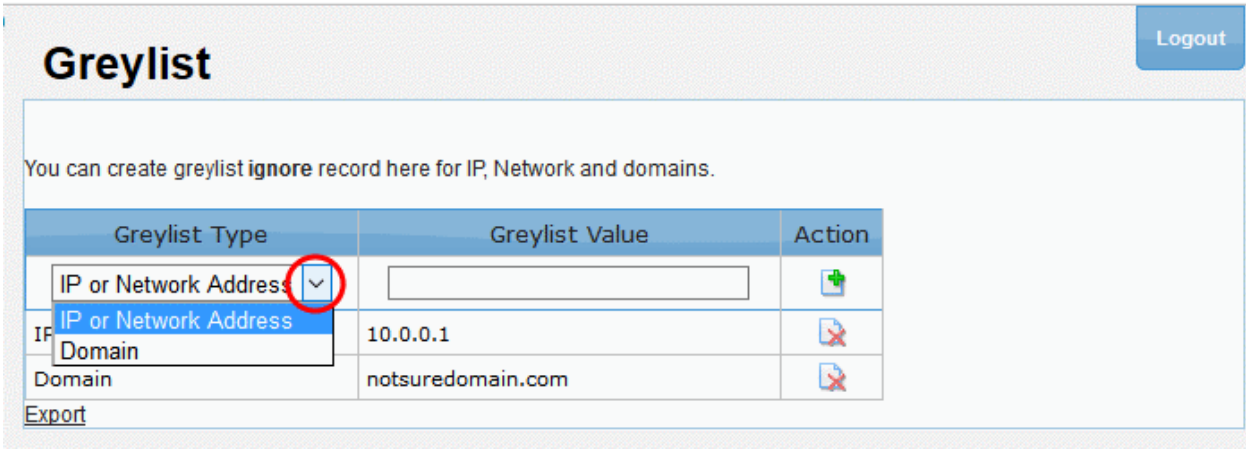
		Allows you to delete a record from the list.

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

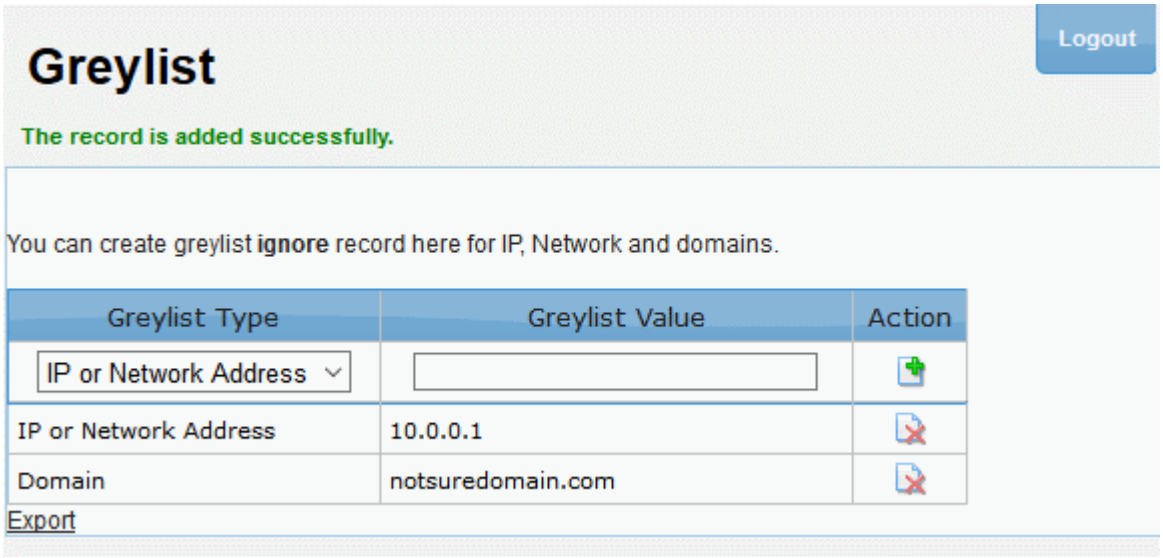
To add a domain name or IP address to Greylist ignore list

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



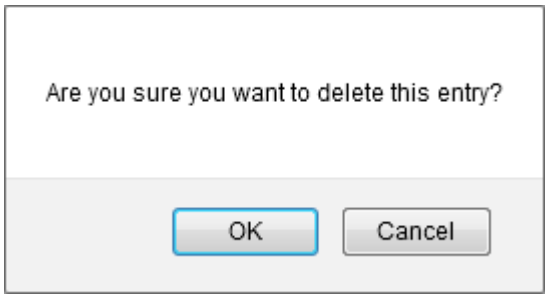
- Type the specific domain name or IP address in the 'Greylist Value' field.
- Click the button under the 'Action' column.

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



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

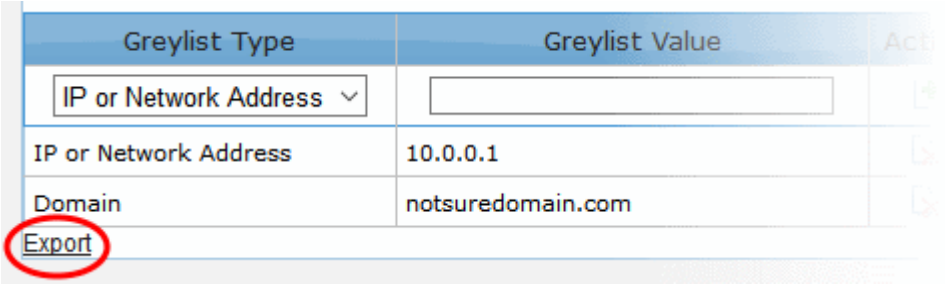
- To delete a domain name/IP address from the Greylist ignore list , click the button under the 'Action' column header.



- Click 'OK' to confirm the deletion.

To export Greylist ignore list to a file

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

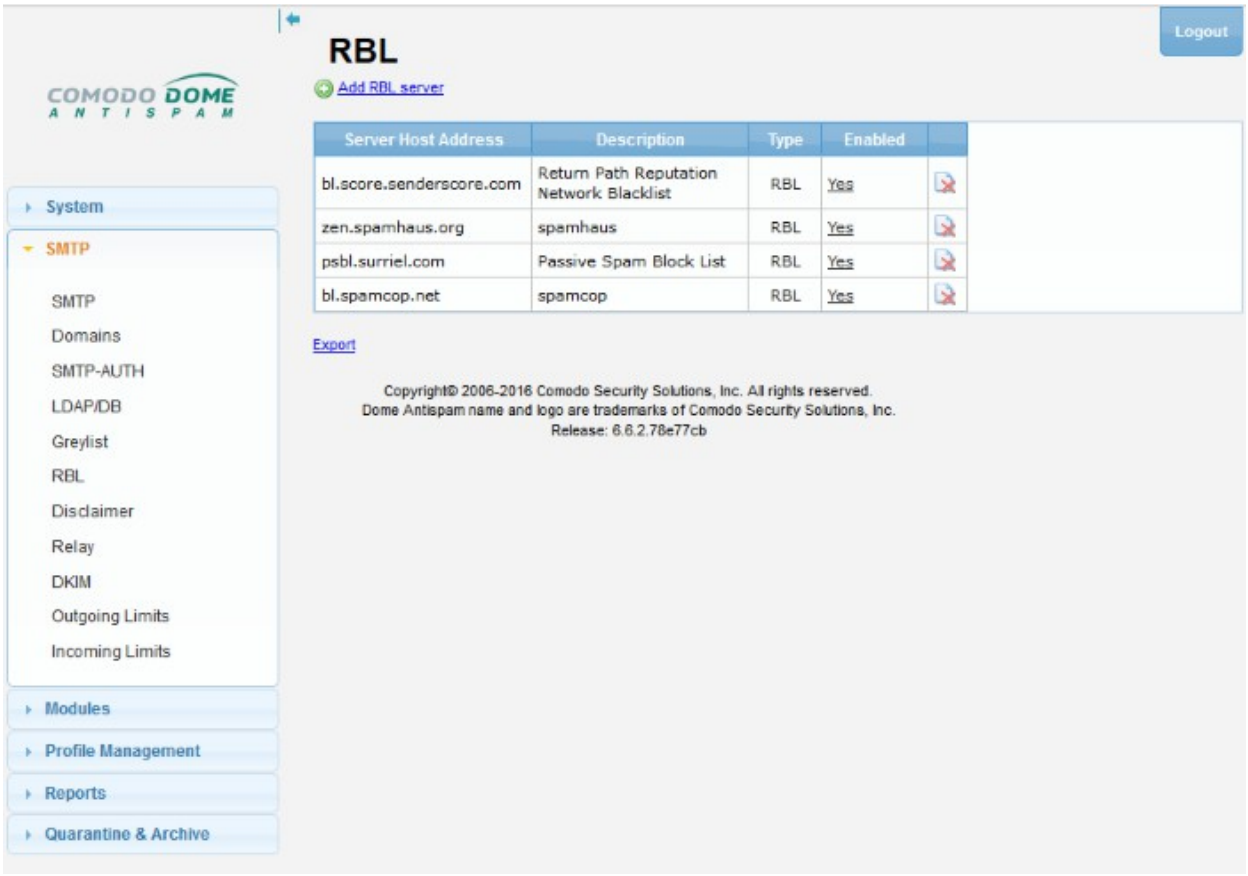


- Save the exported file to your system.

4.6 Managing RBL Servers

A Realtime Blackhole List (RBL) is a list of IP addresses that serve spam, or act as spam relays, or have distributed mails containing viruses. Dome Antispam can block SMTP connections from IP 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.
- To open the 'RBL' screen, click the 'SMTP' tab on the left menu, then click 'RBL'.



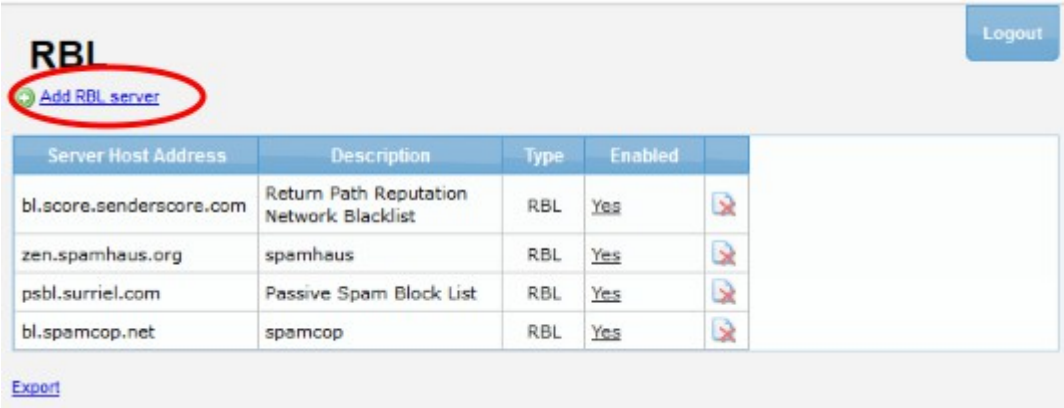
RBL Servers - Table of Column Descriptions		
Column Header	**Description**	
Server Host Address	The address of the RBL server.	
Description	The description provided at the time of adding the RBL server.	
Type	The type of block list selected.	
Enabled	Indicates whether the RBL server is enabled or not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

The interface allow administrators to:

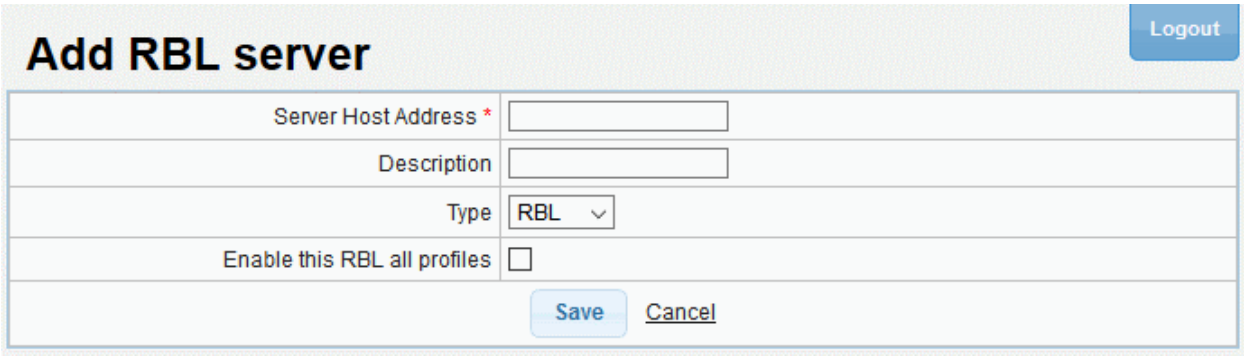
- Add a RBL server
- Enable/disable a RBL server
- Delete a RBL server
- Export RBL server list to a file

To add a RBL server

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



The 'Add RBL server' screen will be displayed:



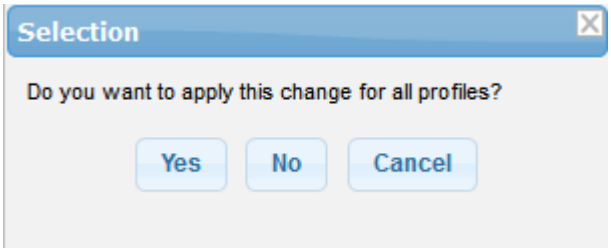
- **Server Host Address:** Enter the address of the RBL server
- **Description:** Enter an appropriate description for the server
- **Type:** Select the type of block list from the options.
  - RBL - Realtime Black Hole Lists
  - SBL - Spamhaus Block List
  - XBL - Spamhaus Exploits List
  - SMTP - Email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

To enable/disable a RBL server

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

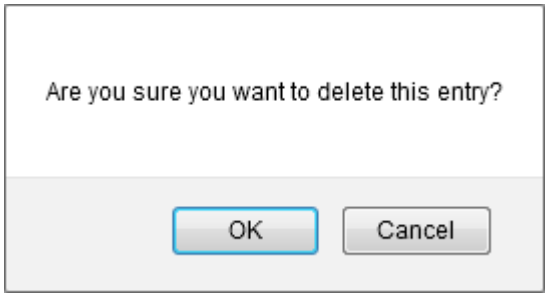
- Click 'Yes' to enable the server for all the profiles.
- Click 'No' to enable the server for the current profile.

The RBL servers can be enabled/disabled independently also for the profiles available in Dome Antispam. Refer to the section '**Profile Management**' for more details.



To delete a RBL server

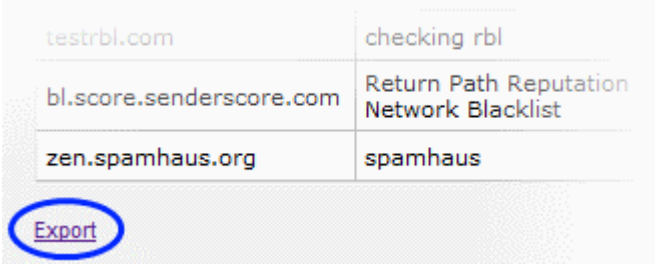
- To delete a RBL server from the list , click the button.



- Click 'OK' to confirm the deletion.

To export RBL server list to a file

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

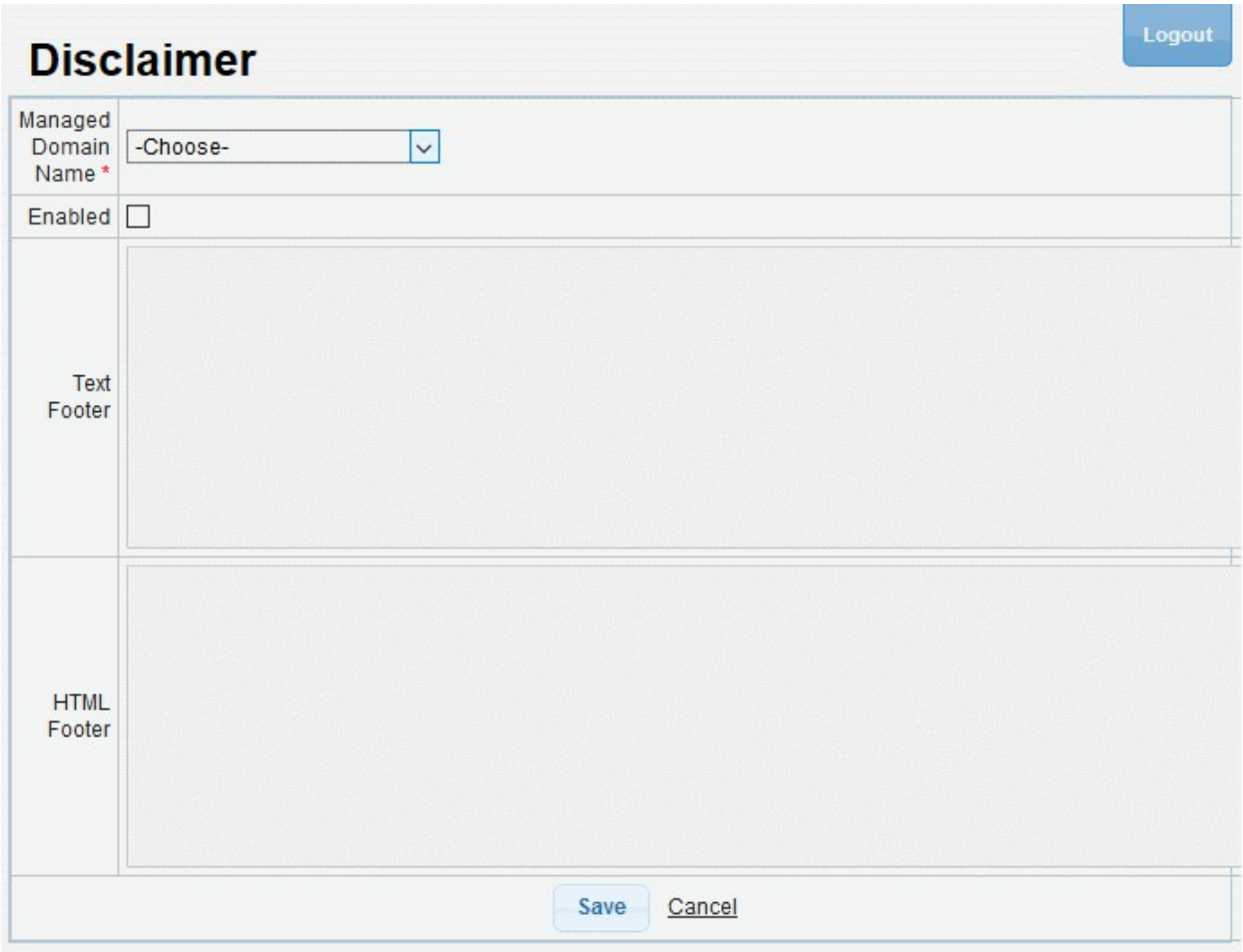


- Download and save the list as a text file to your system.

4.7 Disclaimer

Dome Antispam 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 used to enter the disclaimer content for the selected domain and the 'HTML Footer' can be used to enter corporate messages.

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



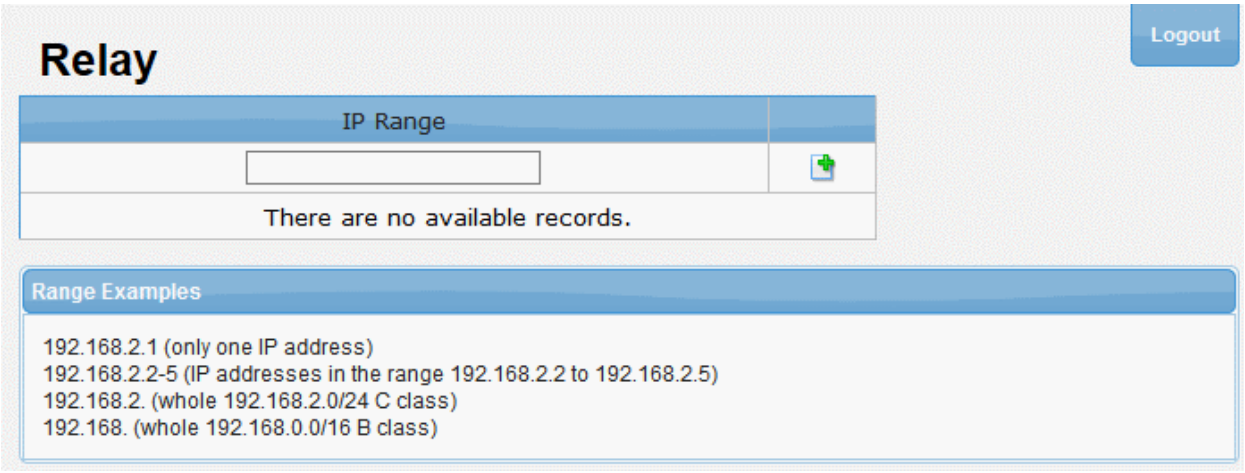
- **Managed Domain Name:** Select the managed domain from the drop-down for which you want to add a disclaimer.
- **Enabled:** If selected, the messages will be inserted in the outgoing mails of the domain.
- **Text Footer:** Enter the disclaimer content in this field.
- **HTML Footer:** Enter content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

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

4.8 SMPT Relay

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

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

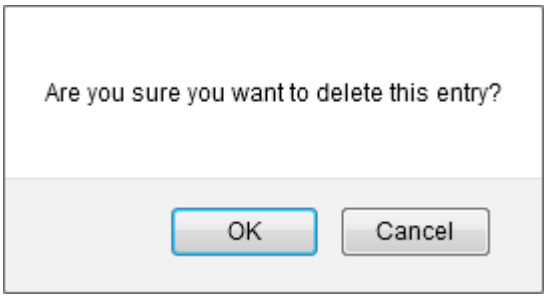


The screen allows you to add a single IP address, a range of IP addresses or a IP address class range.

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

The IP address will be added and displayed.

- To remove an address, click the click the button.

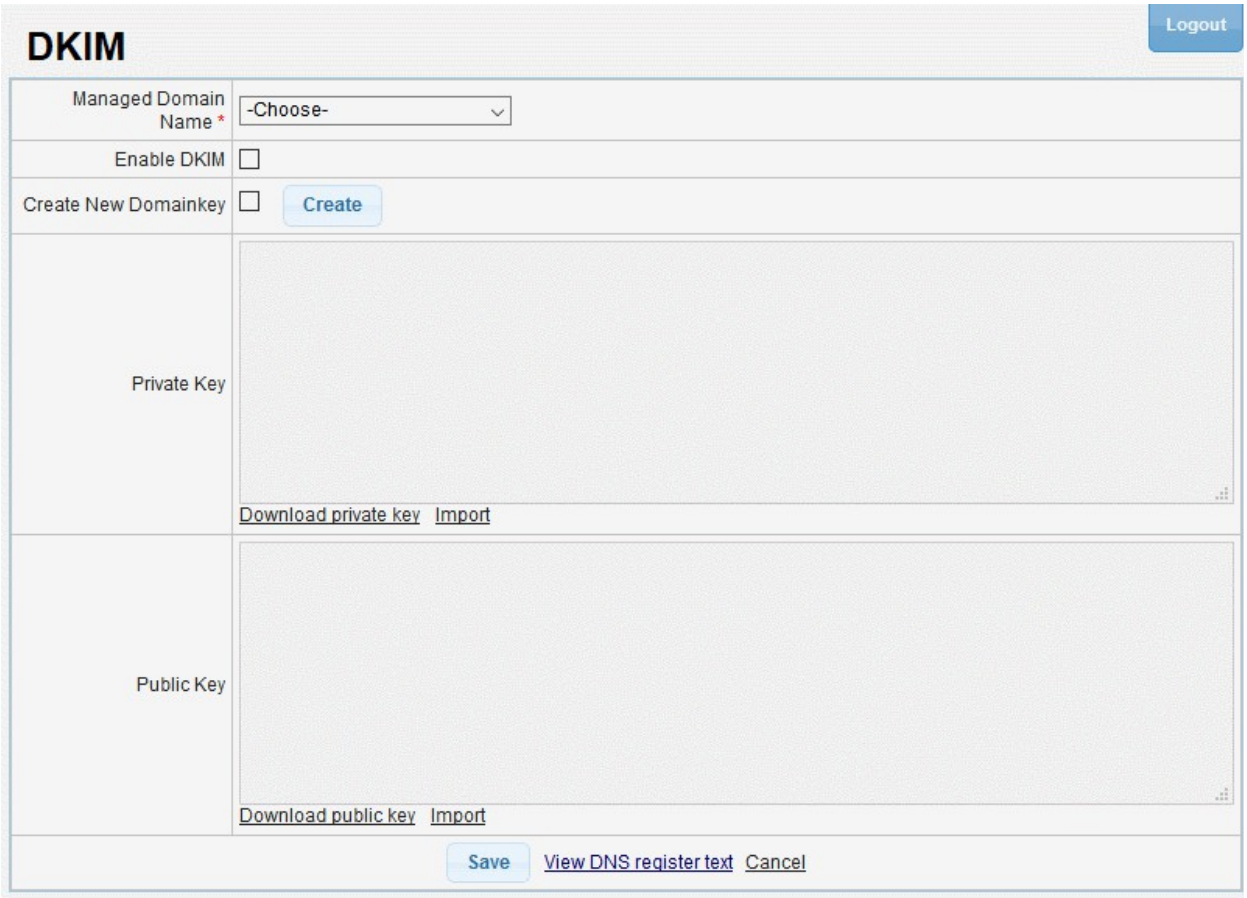


- Click 'OK' to confirm the deletion.

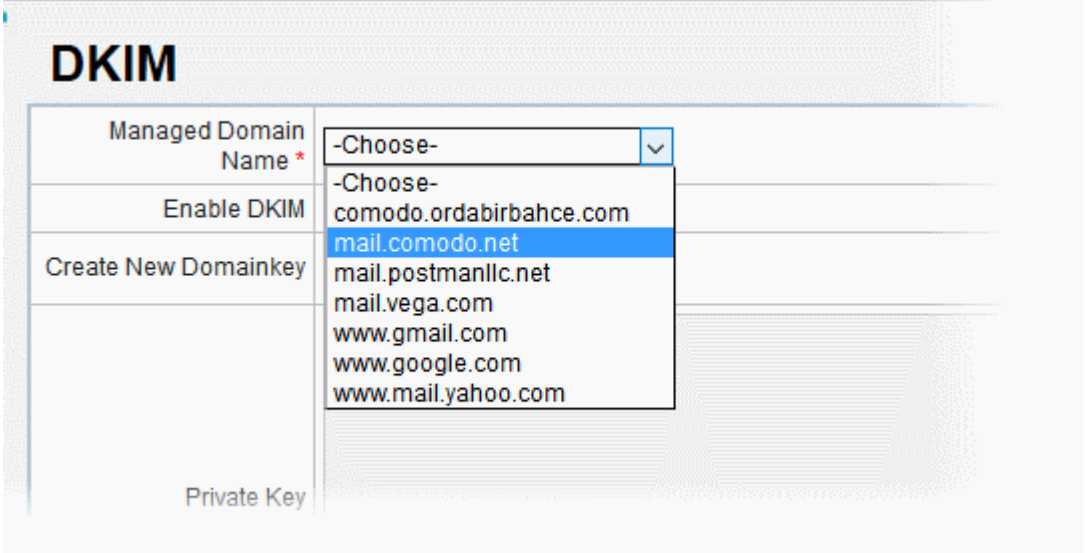
4.9 DomainKeys Identified Mail (DKIM)

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

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

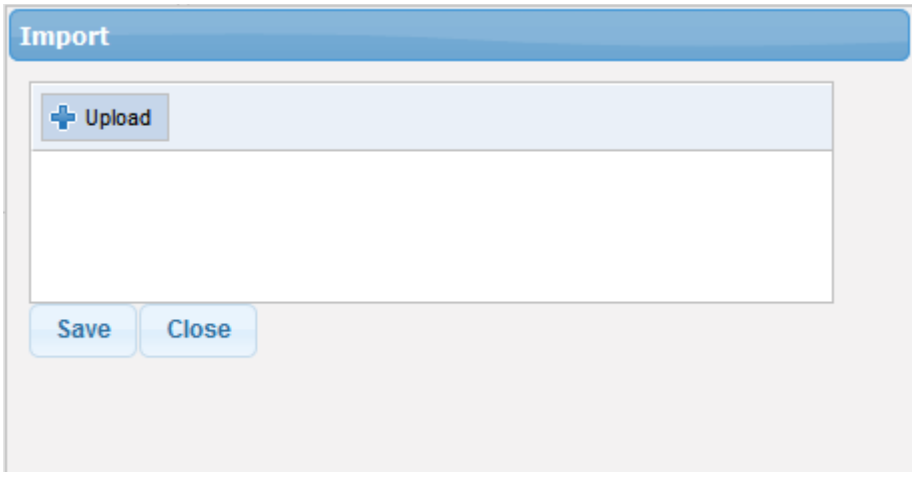


- Select the domain from the drop-down for which you authenticate with DKIM

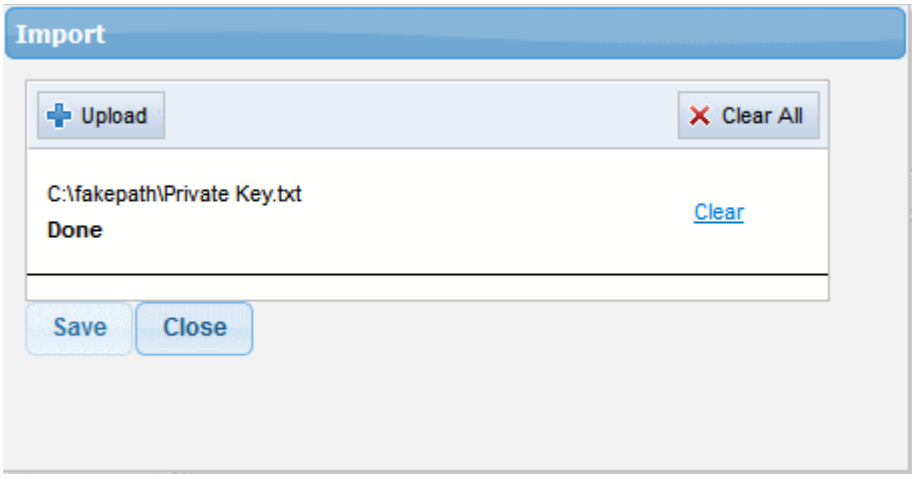


If you have the domain key that needs to be associated with your mails, then follow the steps below:

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



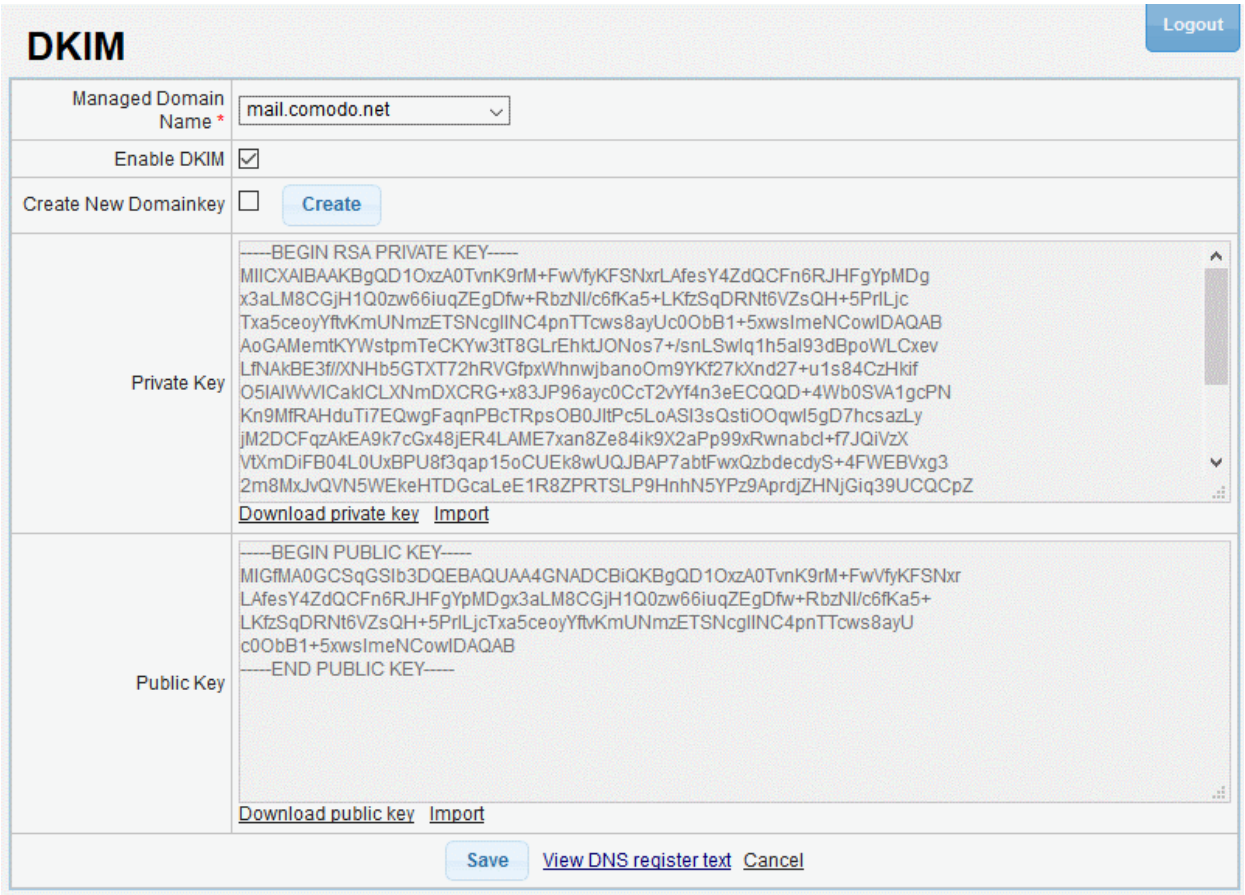
- Click the 'Upload' link, navigate to the location where the private key for the selected domain is saved and click 'Open'



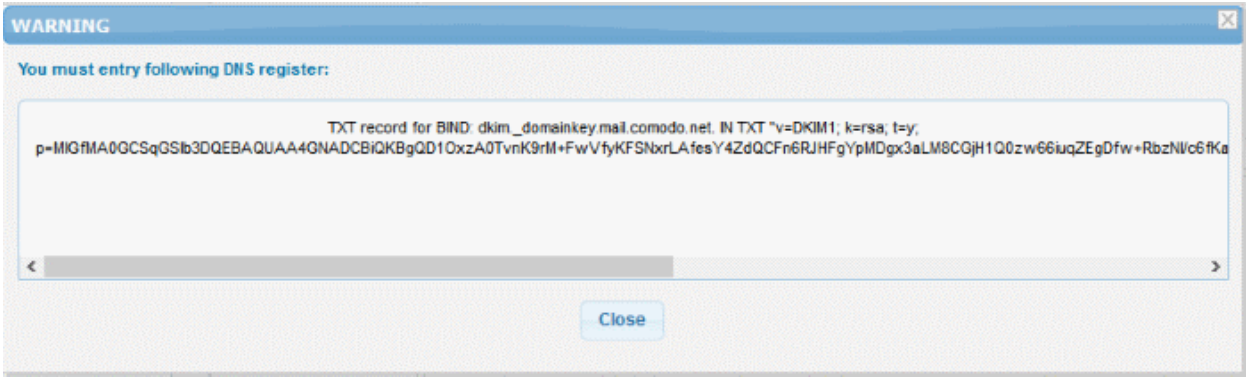
- To remove the selected file from the field, click 'Clear'
- To upload the private key, click the 'Save' button.
- Repeat the above steps to upload the public key.
- To download and save the private and public keys, click the respective download links.

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

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



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

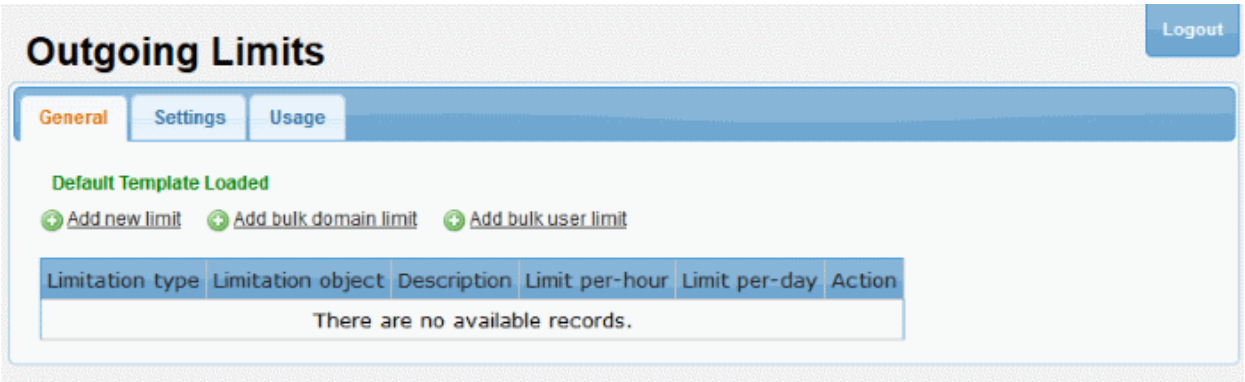


You can view and copy the details of domain key anytime by clicking the 'View DNS register text' link at the bottom. For more details about how to update the DNS record, refer to your domain or web hosting documentation.

4.10 Outgoing SMTP Limits

Dome Antispam allows you to set limits for outgoing mails for users as well as for domain names. Dome Antispam can be configured to allow only a certain number of outgoing mails per hour and per day. The interface allows you to add domains or usernames individually or in bulk.

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



The interface allows administrators to:

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

Configuring outgoing limits for domains and users

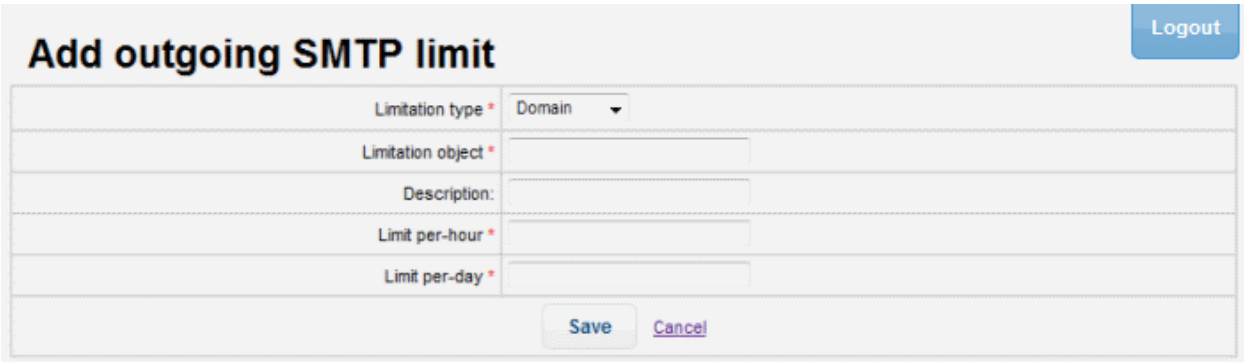
To configure outgoing limits for domains and users:

- Click the 'General' tab

Outgoing Limits: 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

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



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

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

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

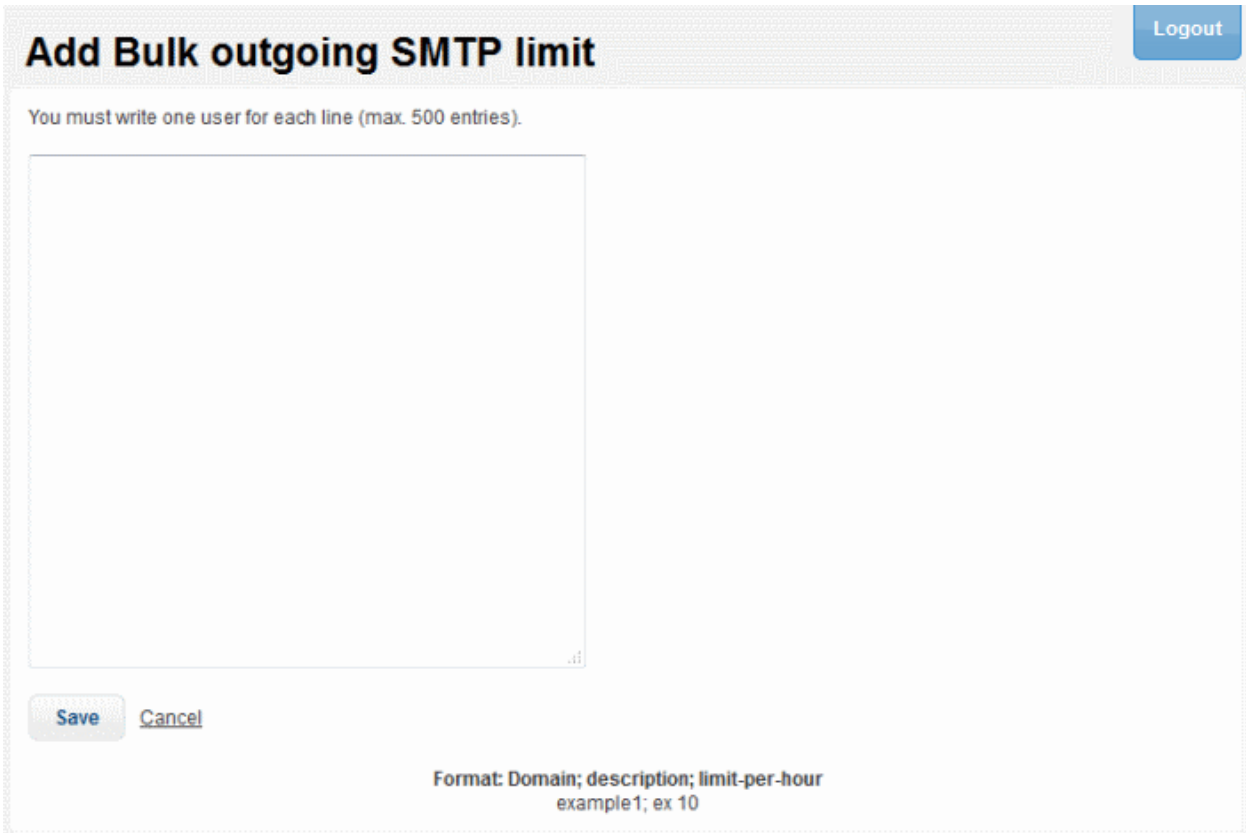
The 'Add Bulk outgoing SMTP limit' screen will be displayed.

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

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

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

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

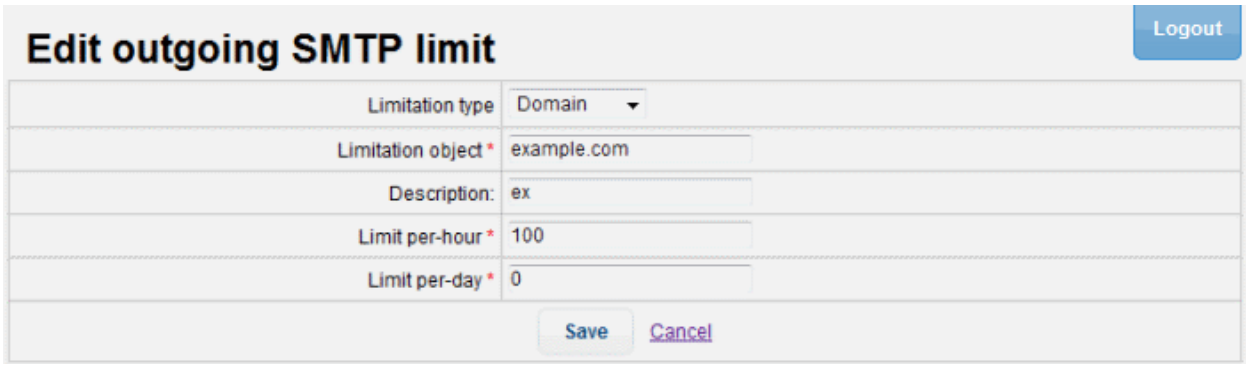


- Enter the limitation for each user per line as per the format shown in the screen.
- Click the 'Save' button to apply your changes.

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

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

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



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

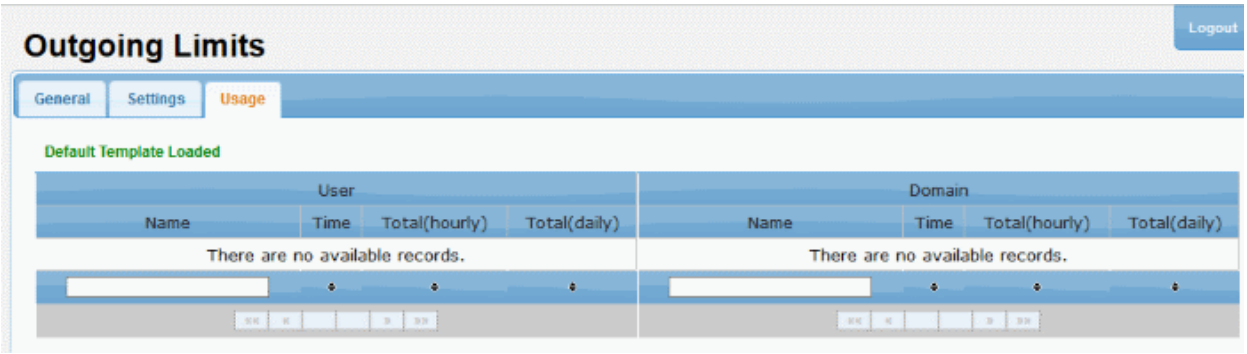
Outgoing Limits: Settings - Table of Parameters	
Parameter	**Description**
SMTP AUTH is enabled by user name limit for outgoing email	If enabled, SMTP AUTH is required for outgoing mails sent by users who are configured in the 'General' tab to send limited mails.
Enable the Limit for From Addresses	If 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	If enabled, the address of the sender must match the SMTP-AUTH username

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

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

Viewing outgoing mail usage details for domains and users

The 'Usage' tab allows 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.

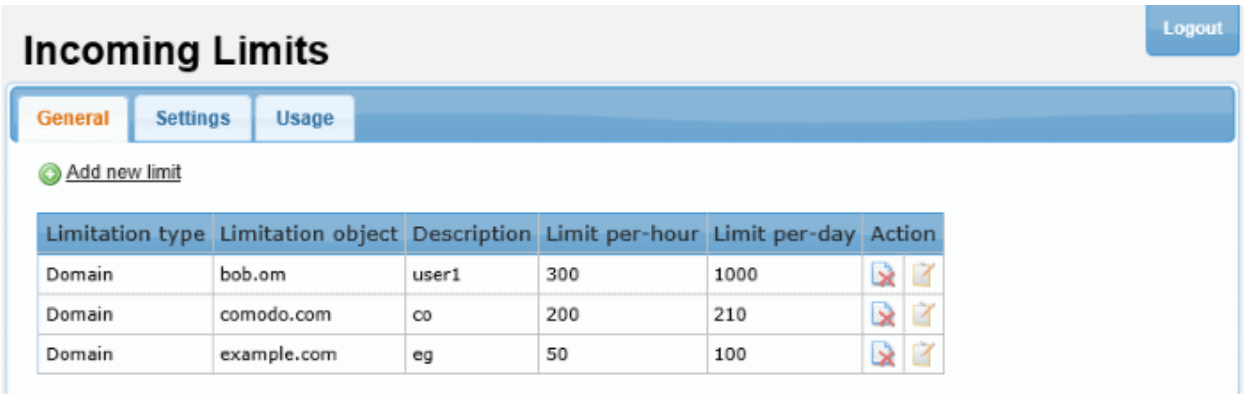
To search for a particular recipient, enter the first few letters of the recipient's name in either the 'User' or 'Domain' search field:

- 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

Dome Antispam allows you to set limits for incoming mails for users as well as for domain names. Dome Antispam can be configured to allow only a certain number of incoming mails per hour and per day. The interface allows you to add domains or usernames individually or in bulk.

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



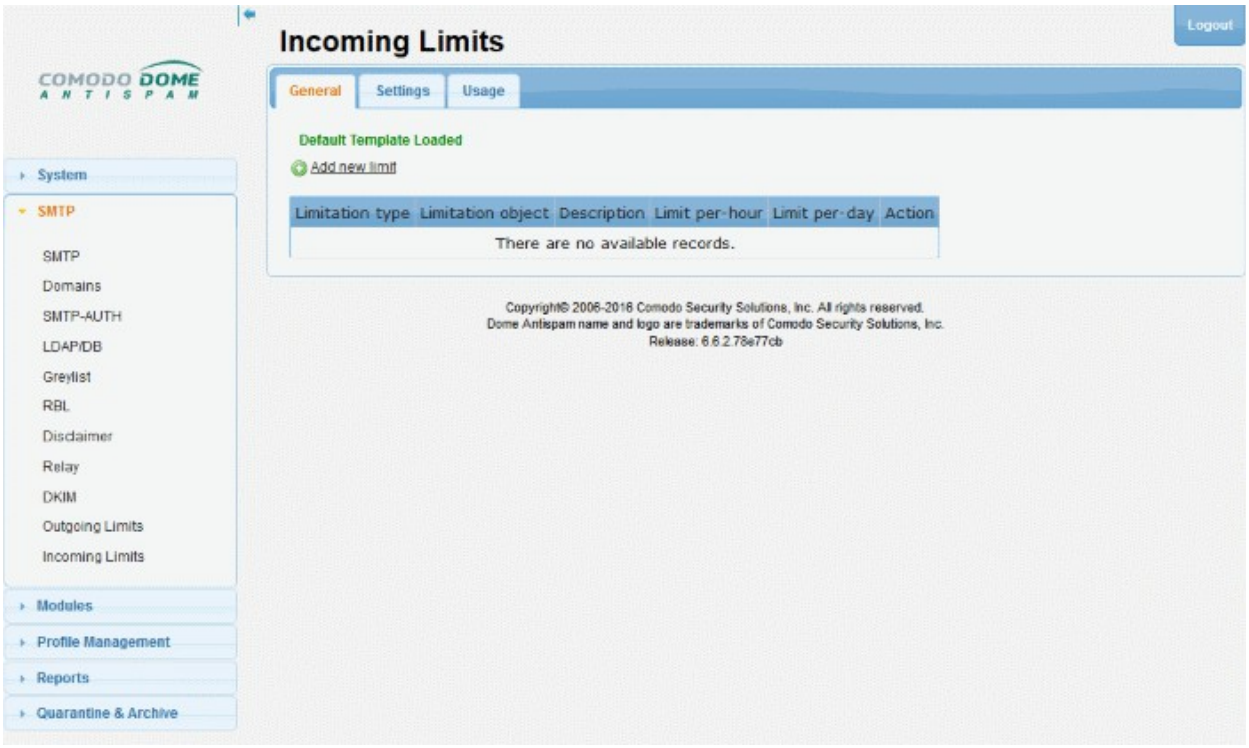
The interface allows you to:

- 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

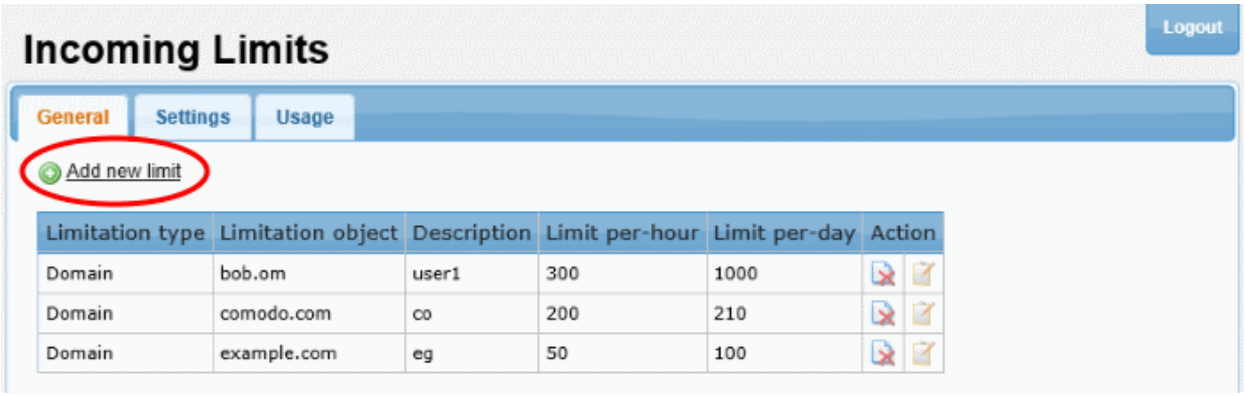
To configure incoming limits for domains and users:

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



Incoming Limits: General - Table of Column Descriptions		
Column Header	**Description**	
Limitation Type	Indicates whether the limitation is for a domain or user	
Limitation Object	The details of the domain or the user	
Description	The description for the limitation	
Limit per-hour	Indicates the number of incoming mails allowed per hour	
Limit per-day	Indicates the number of incoming mails allowed per day	
Action		Allows 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



The 'Add Incoming Limit' screen will be displayed.

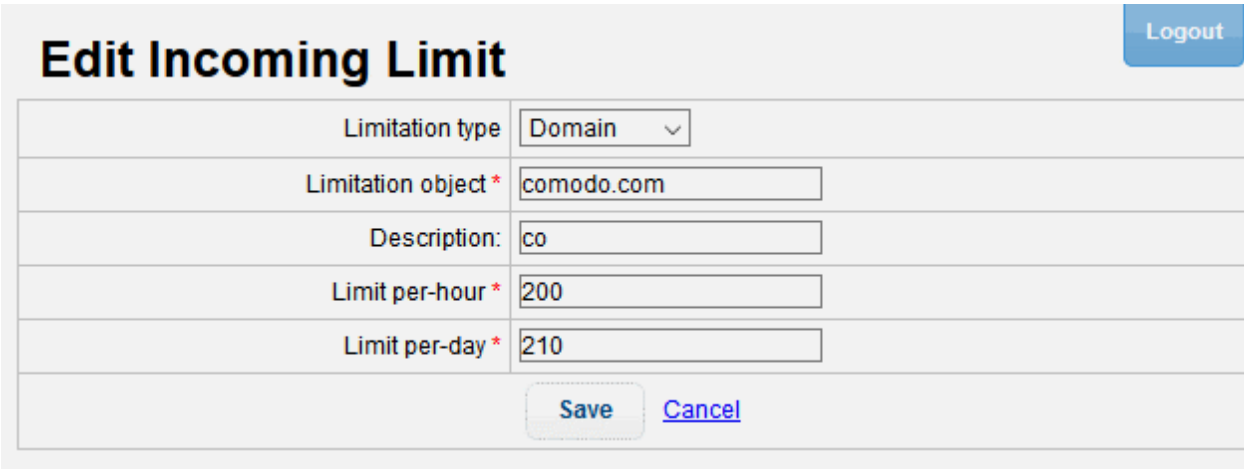
- **Limitation type:** Select whether you want to configure the limit for a domain or user from the drop-down
- **Limitation object:** Enter the name of the domain or username depending on your 'Limitation type' selection
- **Description:** Enter an appropriate description for the limitation
- **Limit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

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

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

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

The 'Edit Incoming Limit' screen will be displayed.



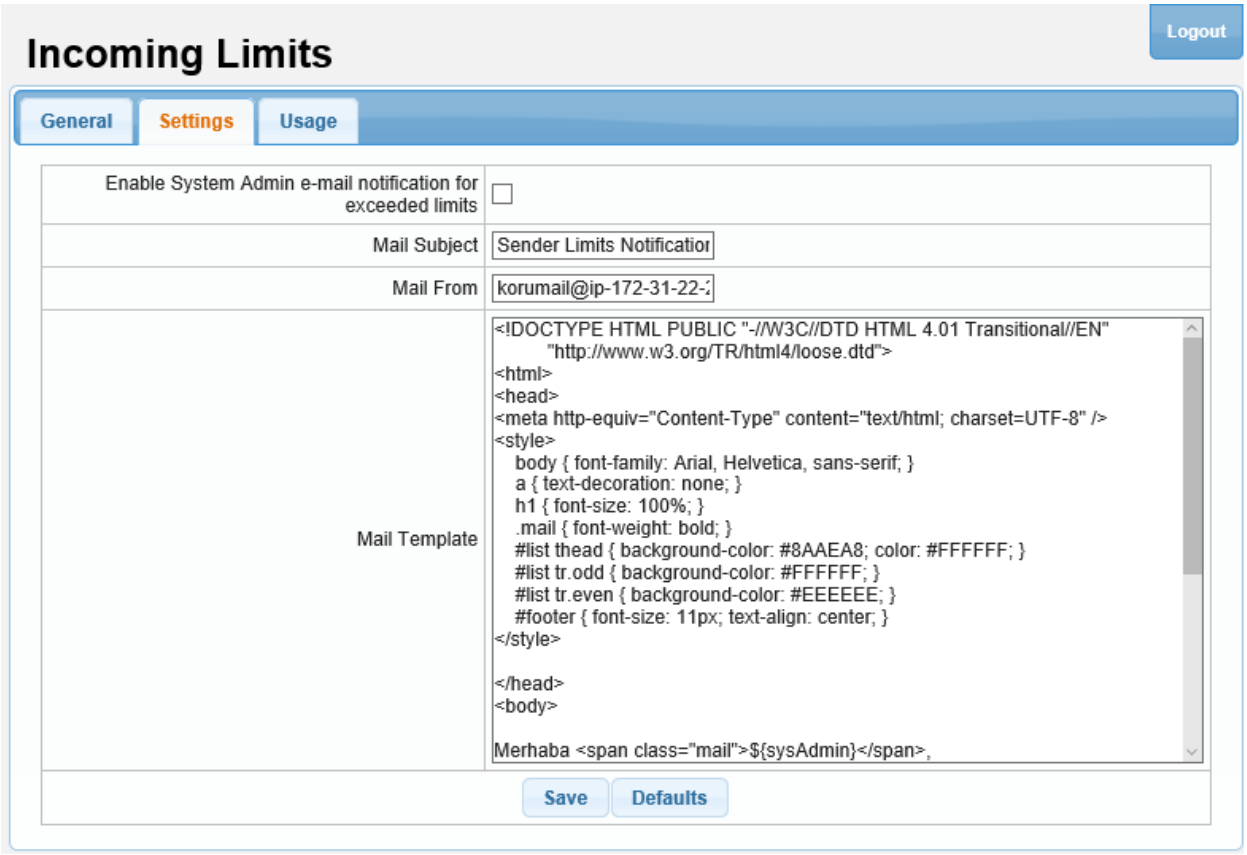
The screen is similar to the 'Add Incoming Limit' interface. Refer to the section for 'Configuring incoming limits for domains and users' for more details.

Configuring Incoming limits settings

The 'Settings' tab in the 'Incoming Limits' screen allows you to configure the settings such that the Dome Antispam 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 Dome Antispam console by default.

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



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

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

Viewing incoming mail usage details for domains and users

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

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,

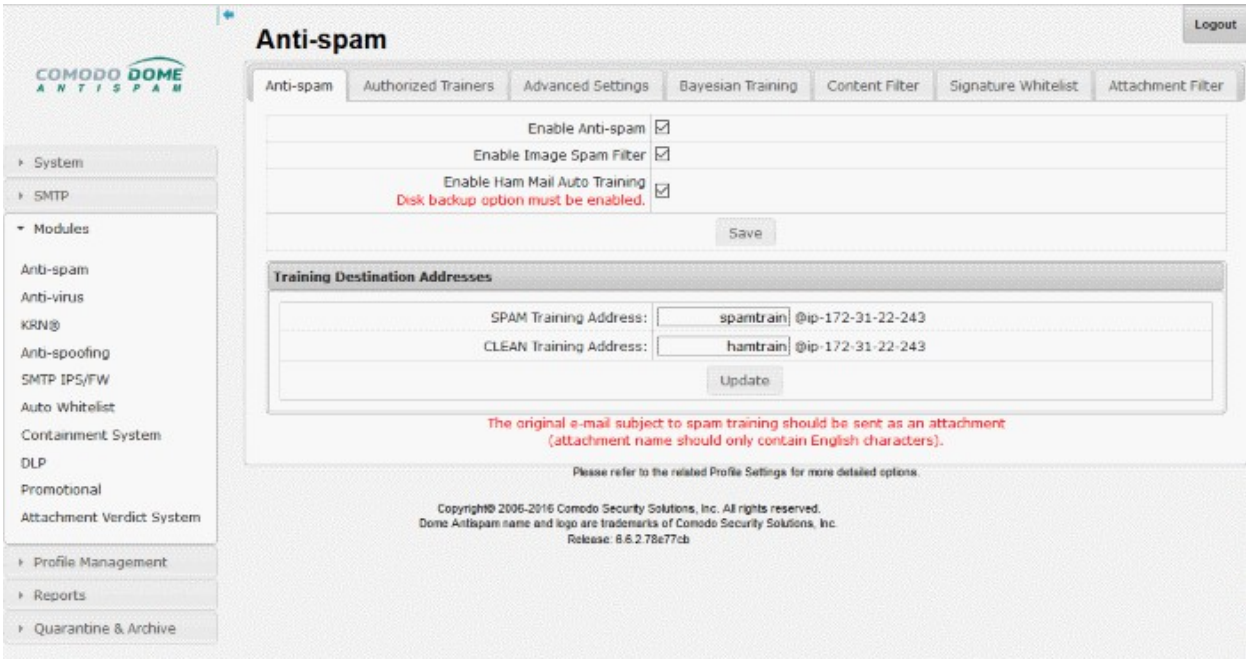
- Enter the first few alphabets of the recipient's name, in the usage details of 'User' and 'Domain'.

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



Click the following links for more details:

- Anti-spam
- Anti-Virus
- Reputation Network (KRN)
- Anti-Spoofing
- SMTP IPS/FW
- Auto Whitelist
- Data Leak Prevention (DLP)
- Promotional
- Attachment Verdict System

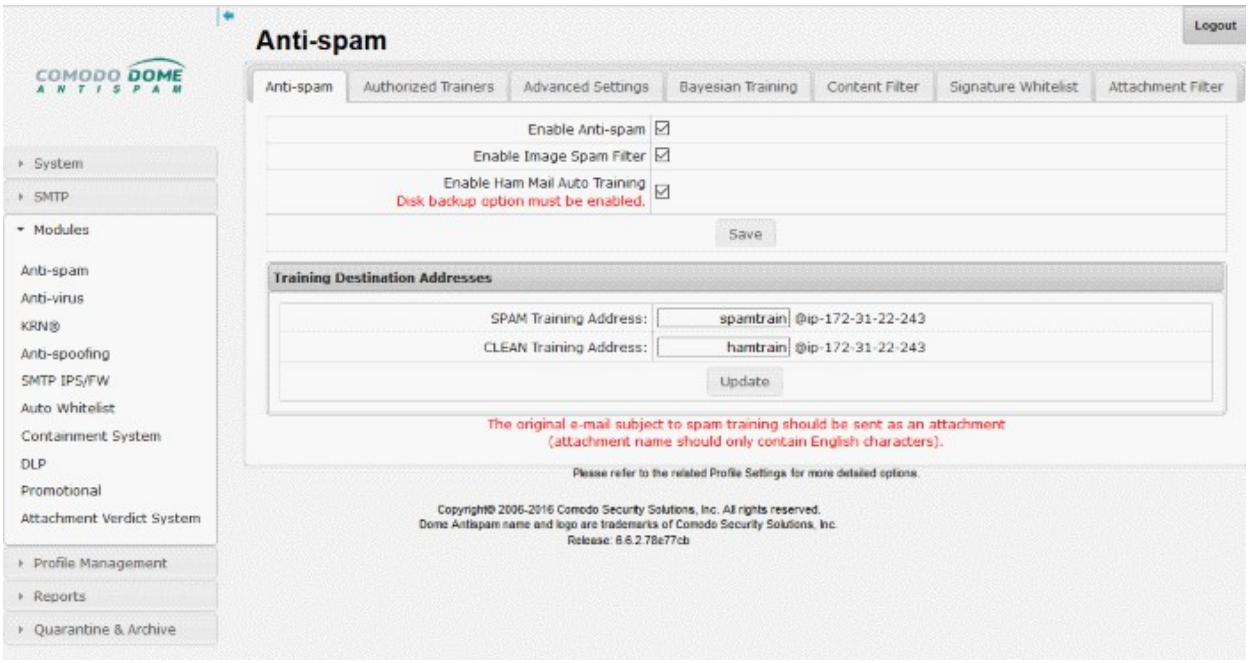
5.1 Anti-spam

The Anti-spam module allows you to configure general and advanced settings, define authorized persons who can submit mail for spam training, upload material for Bayesian Spam and HAM training, and add content filters.

Bayesian spam filtering is a statistical technique of email filtering. It makes use of a naive Bayes classifier to identify spam emails. Dome Antispam uses our huge anti-spam database to accurately assign a spam-probability score to each message. Depending on this score the email is categorized as 'OK' (default = 40 points or below), 'Probable Spam' (default = 40-50 points), 'Spam' (default = 50-100 points) or 'Certainly Spam' (default = 100 points and above).

The anti-spam module must be enabled in order to activate the anti-spam parameters specified in profile settings. Refer to the 'Profile Management' section for more details about profile settings.

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



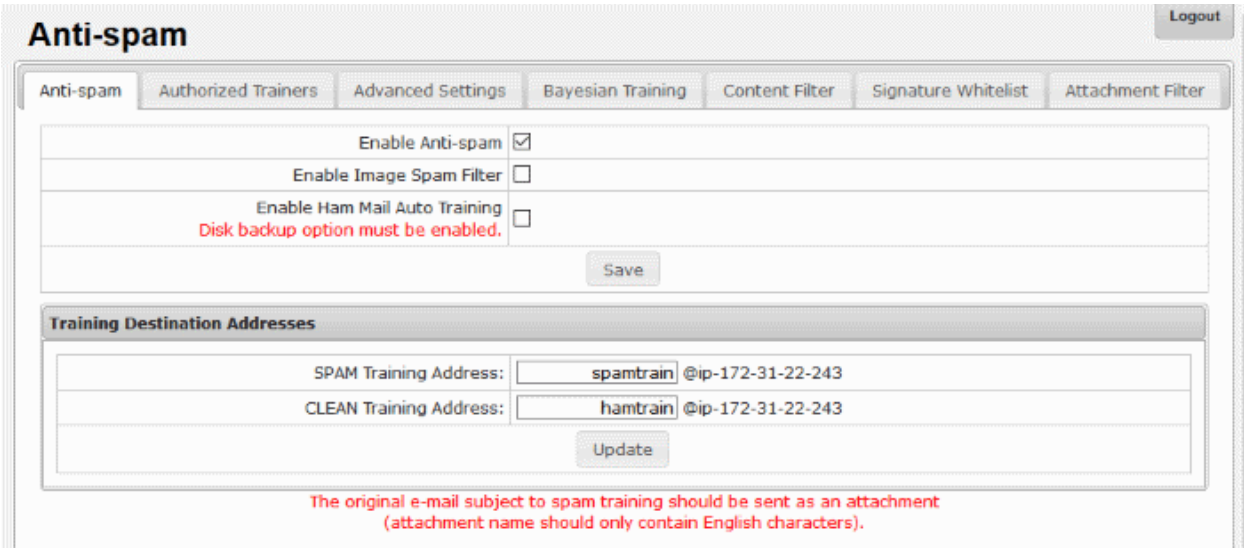
Refer to the following sections for more details:

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

5.1.1 Anti-spam General Settings

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

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



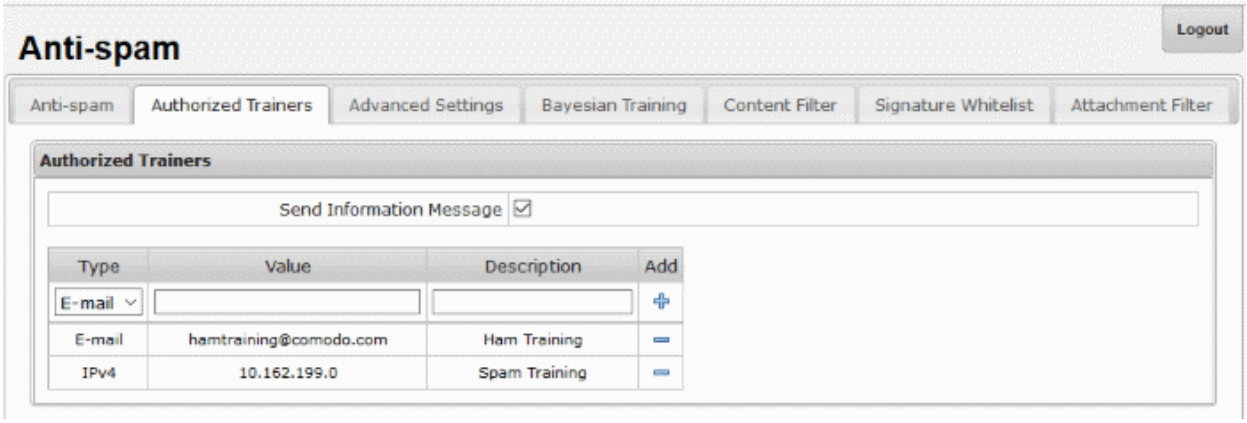
Anti-spam General Settings - Table of Parameters	
Parameter	**Description**
Enable Anti-spam	Select this to activate the anti-spam filtering engine. The anti-spam parameters specified in the profile settings will be activated only if this setting is enabled here. Refer to the '**Profile Management**'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

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

5.1.2 Authorized Trainers

Allows you to define the sources from which spam training emails can be sent. Submitting sample spam emails to Dome Antispam allows the system to learn, adapt and protect against new spam types. Training content sent from any other source will not be accepted by Dome Antispam.

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



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***)

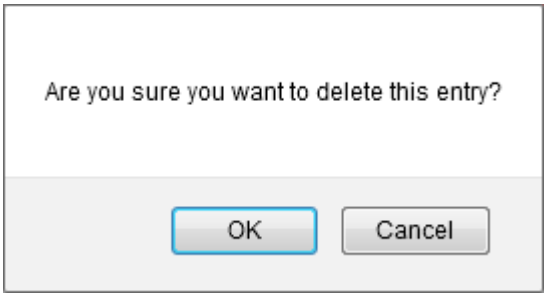
To add an authorized trainer

- 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.

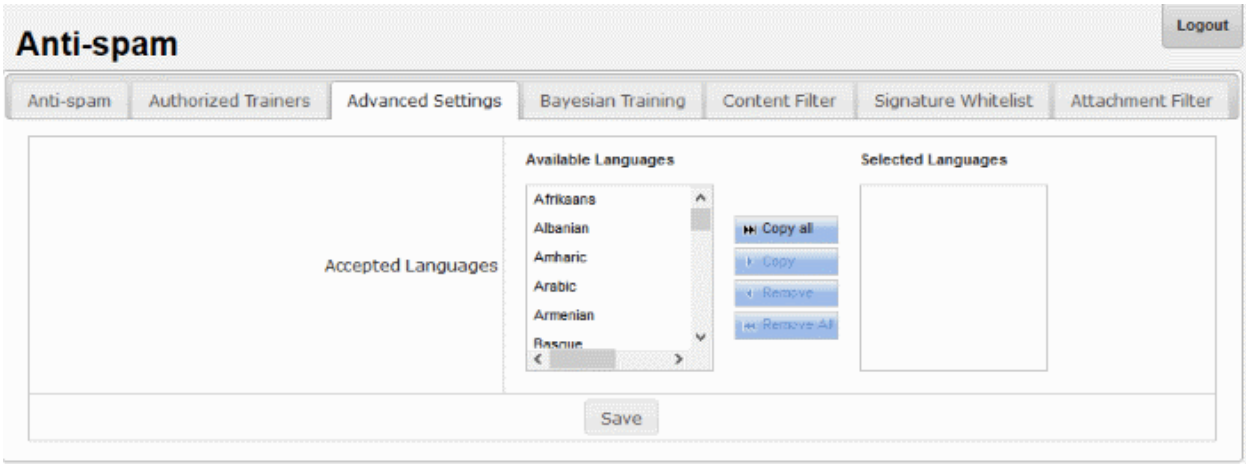


- Click 'OK' to confirm the removal of an authorized trainer.

5.1.3 Advanced Anti-spam Settings

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

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



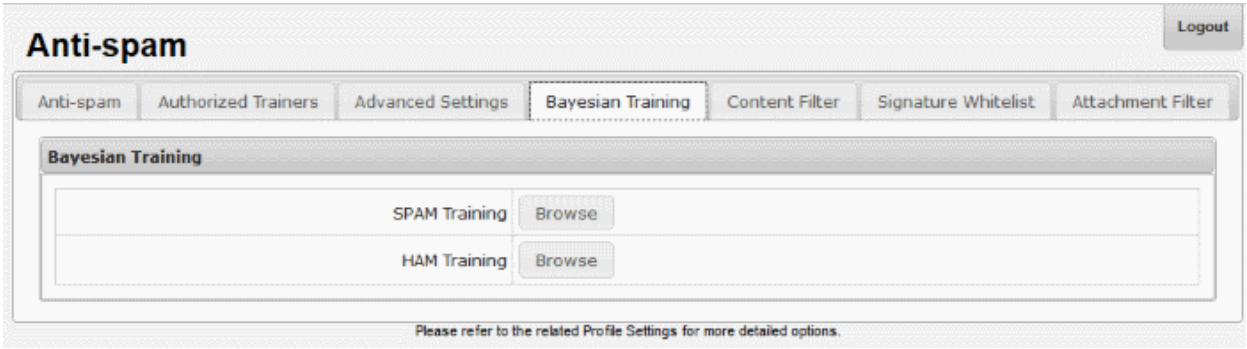
- **Accepted Languages:** The languages for which the Bayes spam engine should analyze the emails for spam. By default, a set of predefined languages is selected. To remove a language from the list, select it and click the 'Remove All' button. To move a language to the right side, select it and click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

Click the 'Save' button to apply your changes.

5.1.4 Bayesian Training

The Bayesian spam engine in Dome Antispam can be trained to identify spam and clean emails, you can upload content from the 'Bayesian Training' screen. It allows to upload both spam and safe content for training.

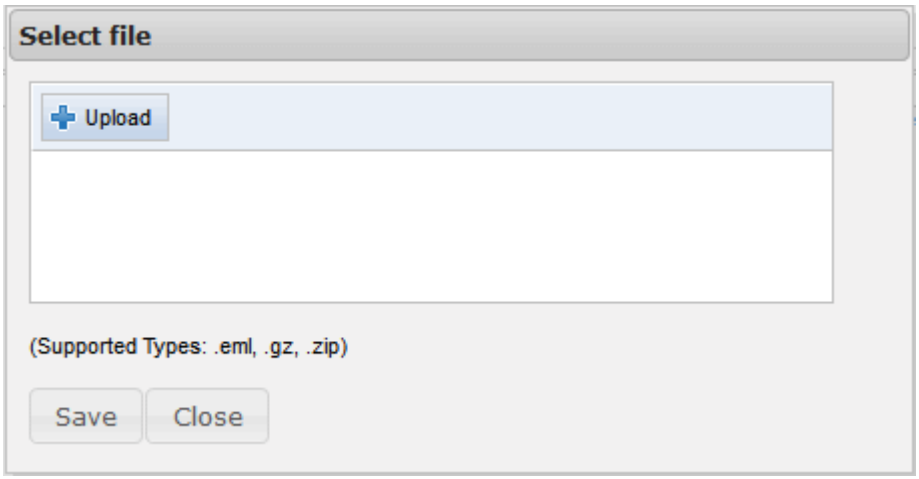
- To open the 'Bayesian Training' screen, click the 'Bayesian Training' tab in the Anti-spam interface.



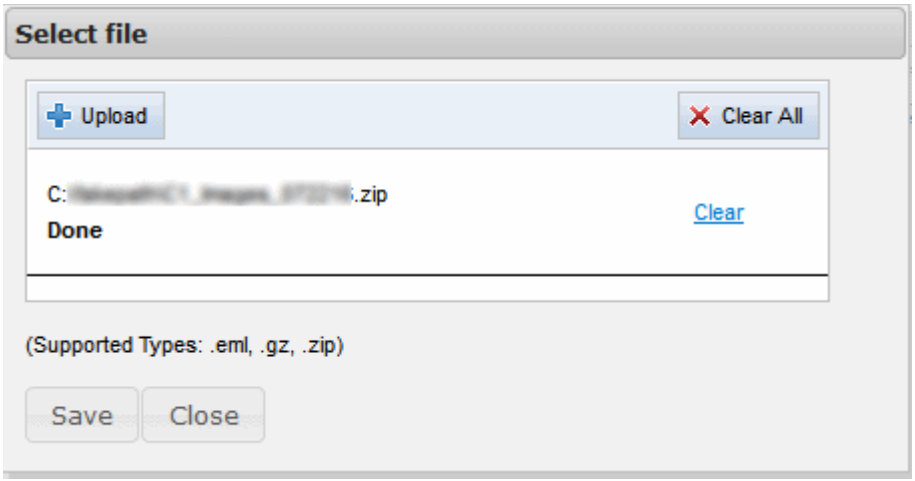
- **SPAM Training:** Allows to upload spam content to train the Bayesian spam engine
- **HAM Training:** Allows to upload safe content to train the Bayesian spam engine

To upload content

- Click the 'Browse' button



- Click the 'Upload' button, navigate to the location where the content is saved and click 'Open'. (Note: Only .eml, .gz and .zip file formats are supported)

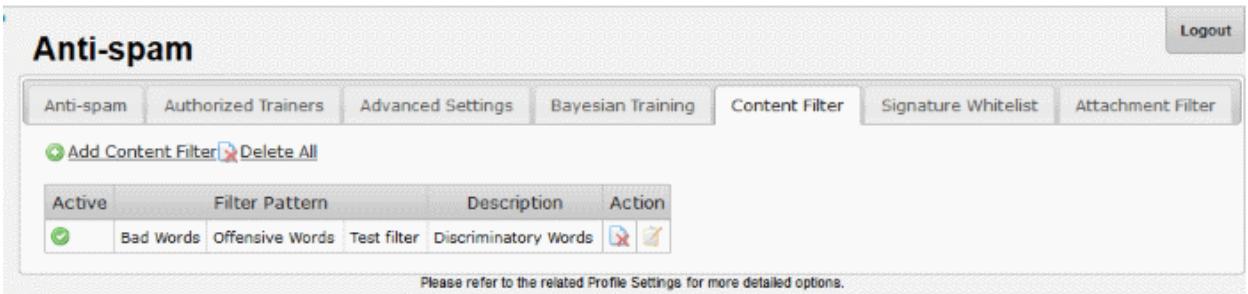


- Repeat the process to add more files
- To remove a file from the list, click the 'Clear' link beside it
- To remove all the files from the list, click the 'Clear All' button at the top
- To upload the files, click the 'Save' button

5.1.5 Content Filter

Dome Antispam's content filter can detect words or patterns of words in the body of emails then mark those messages as spam.

- To open the 'Content Filter' screen, click the 'Content Filter' tab in the Anti-spam interface.



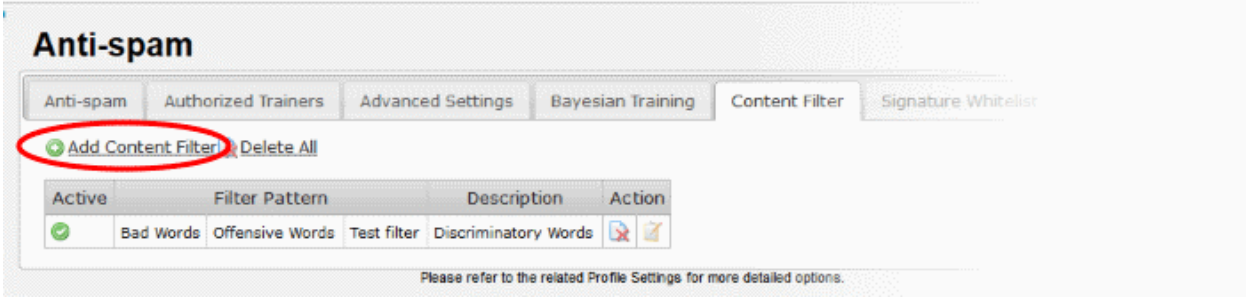
Content Filter - Table of Column Descriptions		
Column Header	**Description**	
Active	Indicates whether the 'Content Filter' is enabled or disabled	
Filter Pattern	Displays the details of the filter pattern.	
Description	The description for the added 'Content Filter'	
Action		Allows you to delete a filter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

The interface allows administrators to:

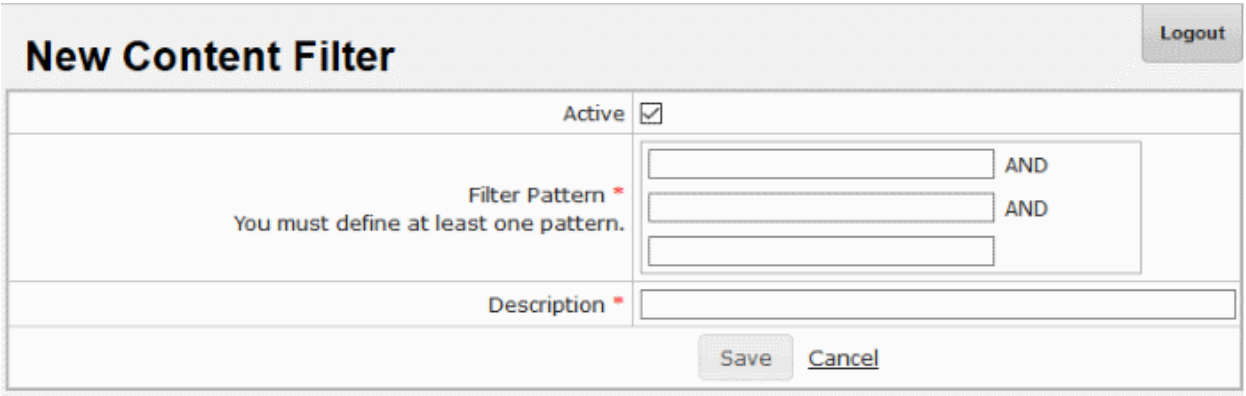
- Add a new content filter
- Edit a content filter
- Delete a content filter

To add a new content filter

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



The 'New Content Filter' screen will be displayed.



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

Click the 'Save' button. The newly added filter will be listed in the screen.

To edit a content filter

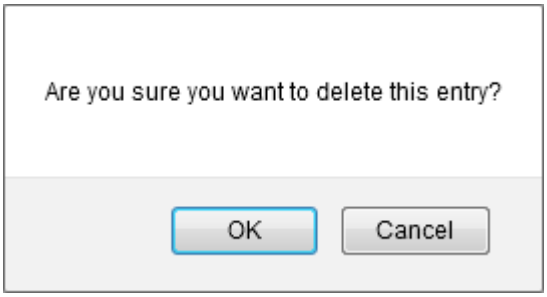
- Click the button beside a filter that you want to edit.

The 'Edit Content Filter' screen will be displayed.

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

To delete a content filter

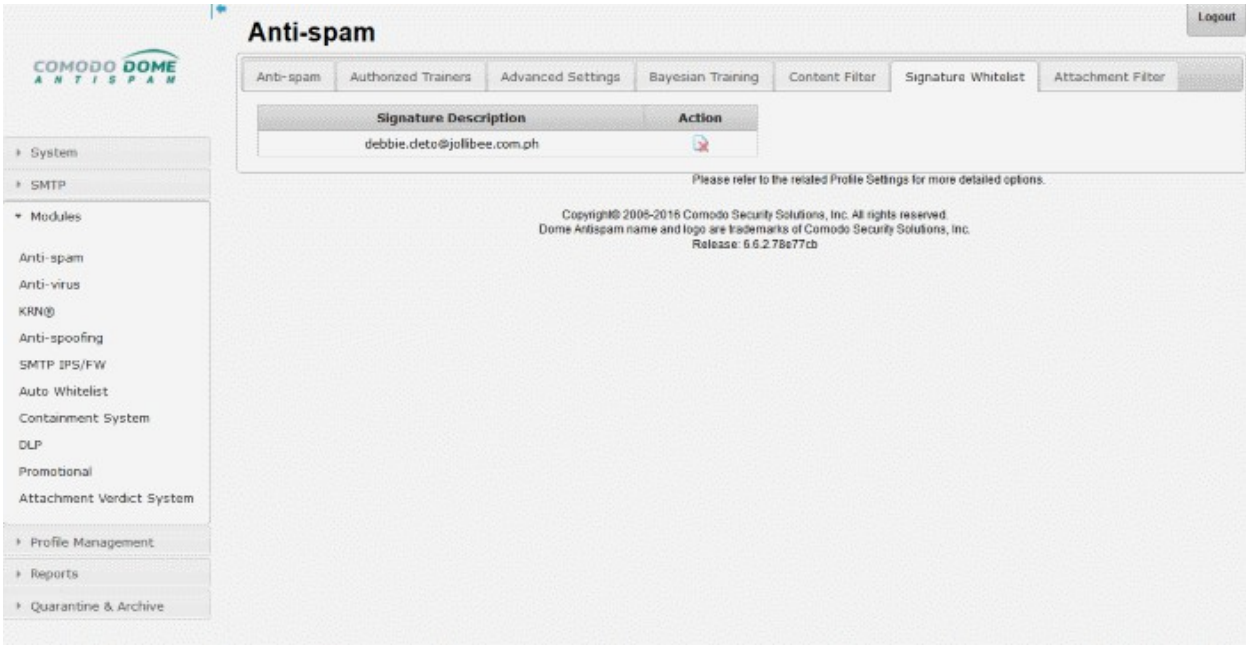
- Click the button beside a filter that you want to remove



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

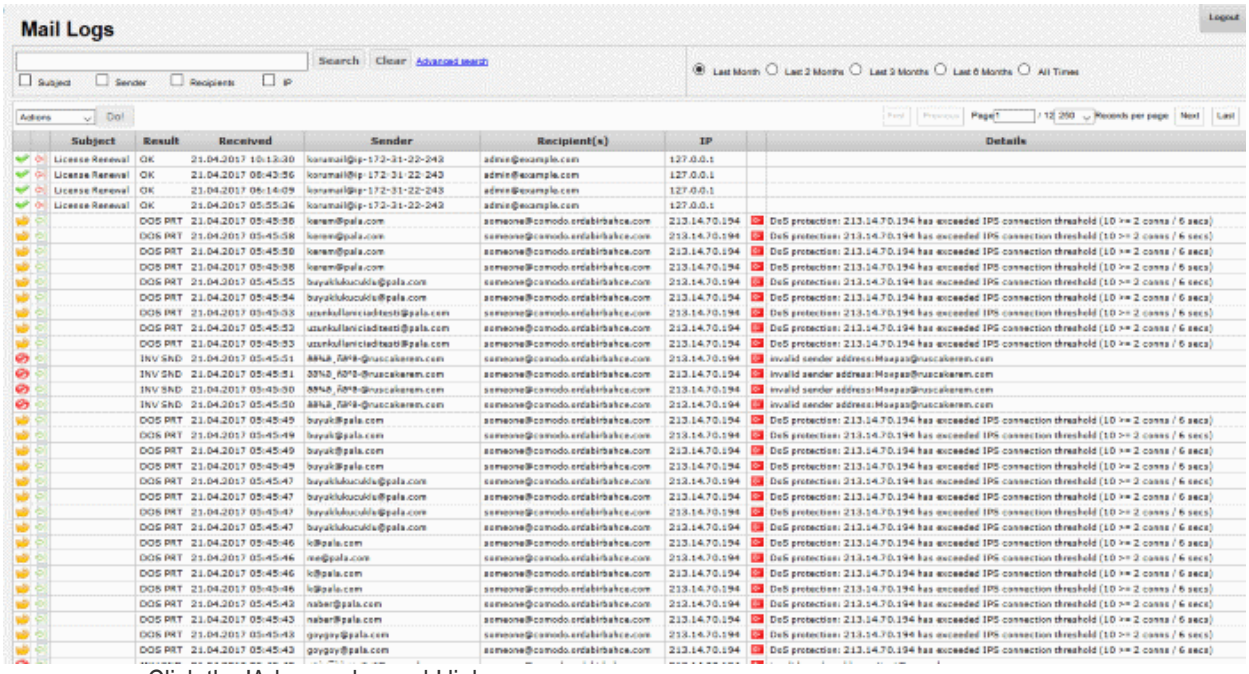
5.1.6 Signature Whitelist

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

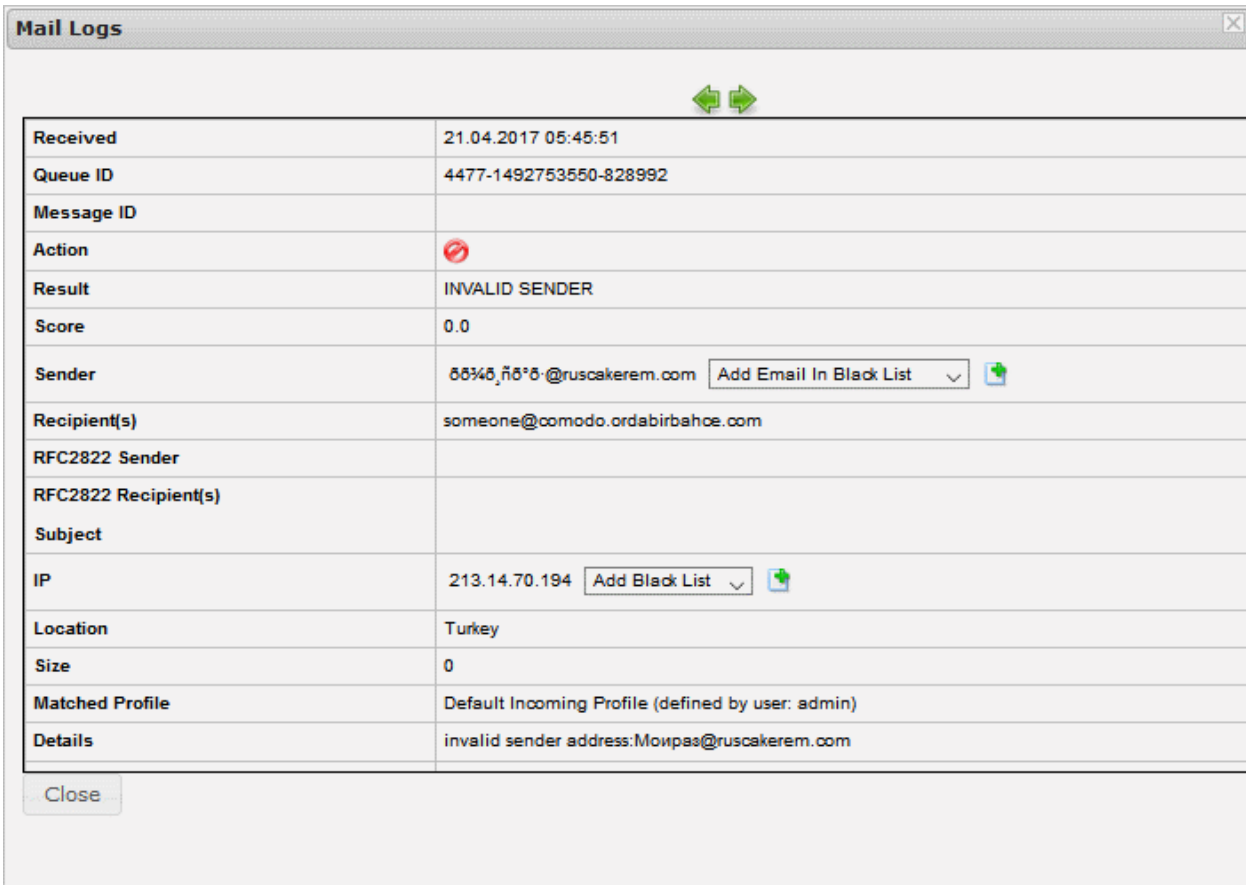


To whitelist emails in 'Mail Logs':

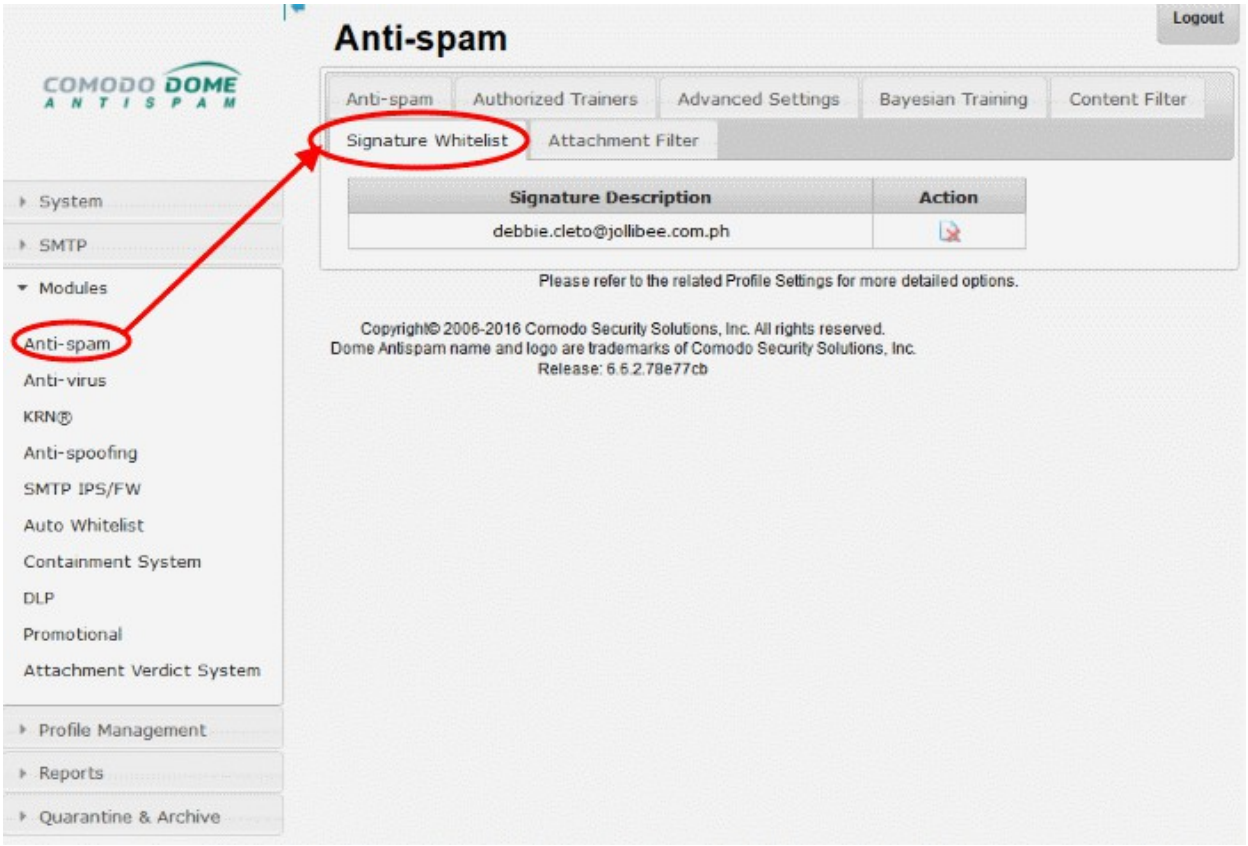
- Click 'Mail Logs' from reports menu.



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



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

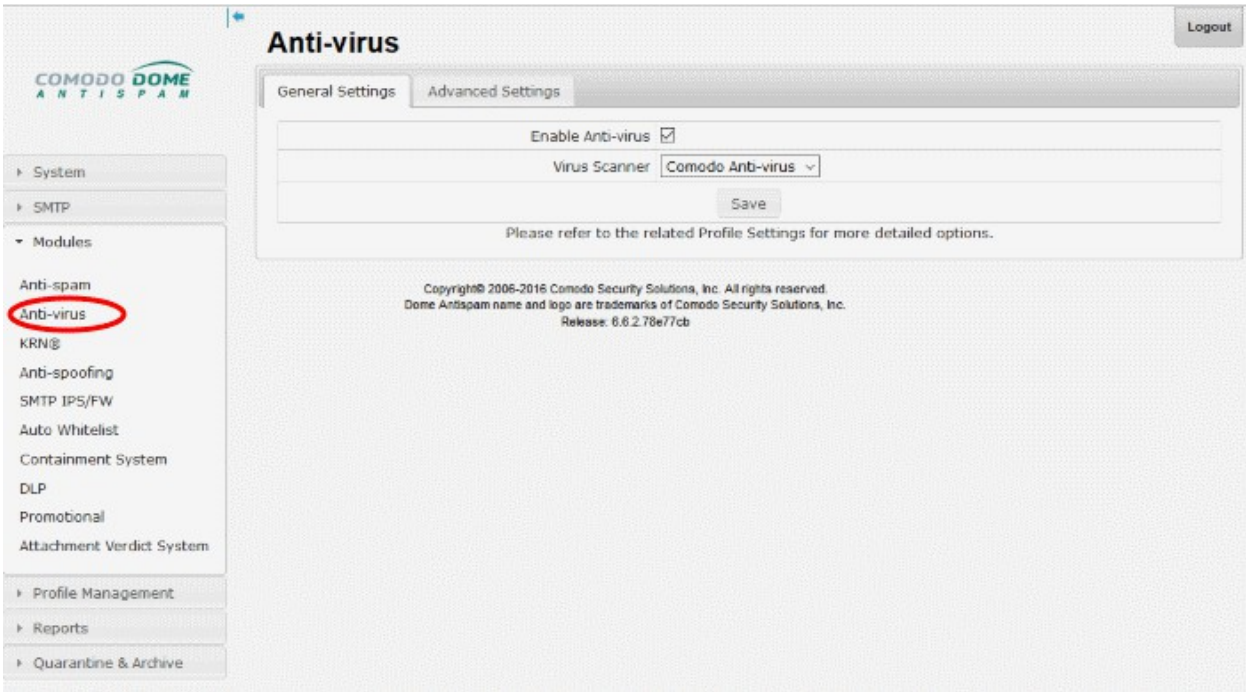


The email will automatically populate in the 'Signature Whitelist' tab in Anti-spam' module.

5.2 Anti-Virus

Dome Antispam is capable of virus scanning of all emails that pass through its engine. Dome Antispam includes built-in Comodo AntiVirus program and you have the option to select Comodo's AV program. The anti-virus module must be enabled in order to activate the anti-virus parameters specified in profile settings. Refer to the 'Profile Management' section for more details about profile settings.

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



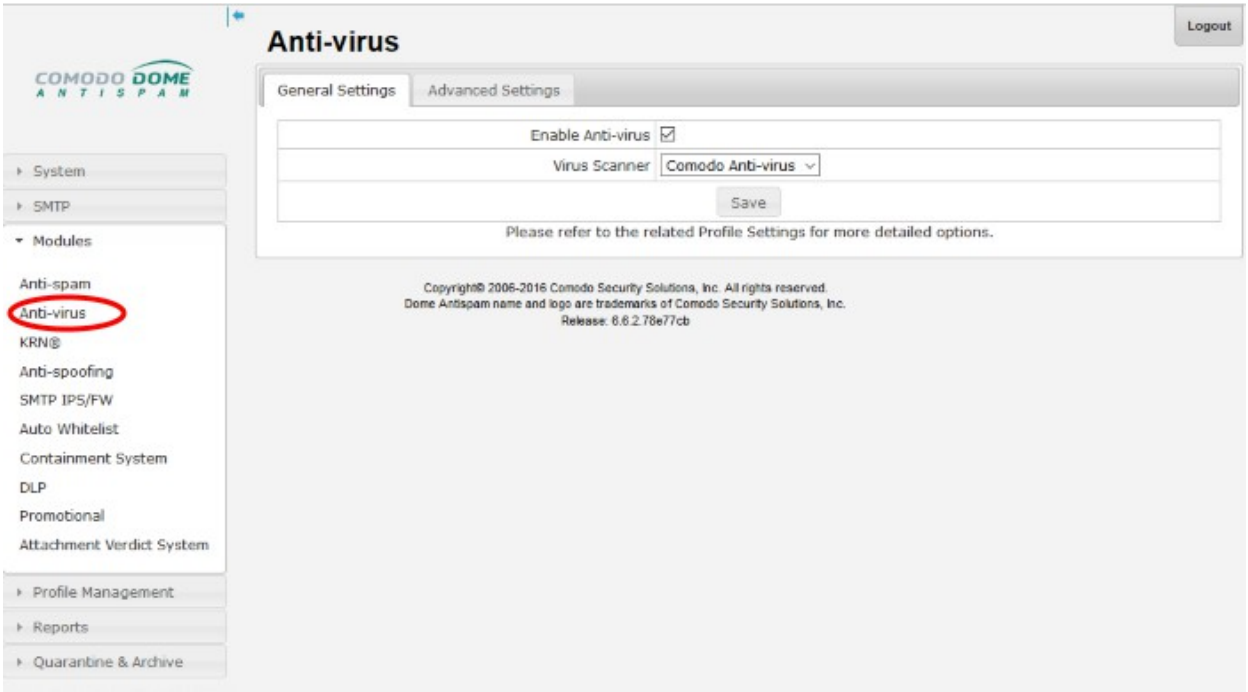
Refer to the following sections for more details:

- Anti-Virus General Settings
- Advanced Anti-Virus Settings

5.2.1 Anti-Virus General Settings

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

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



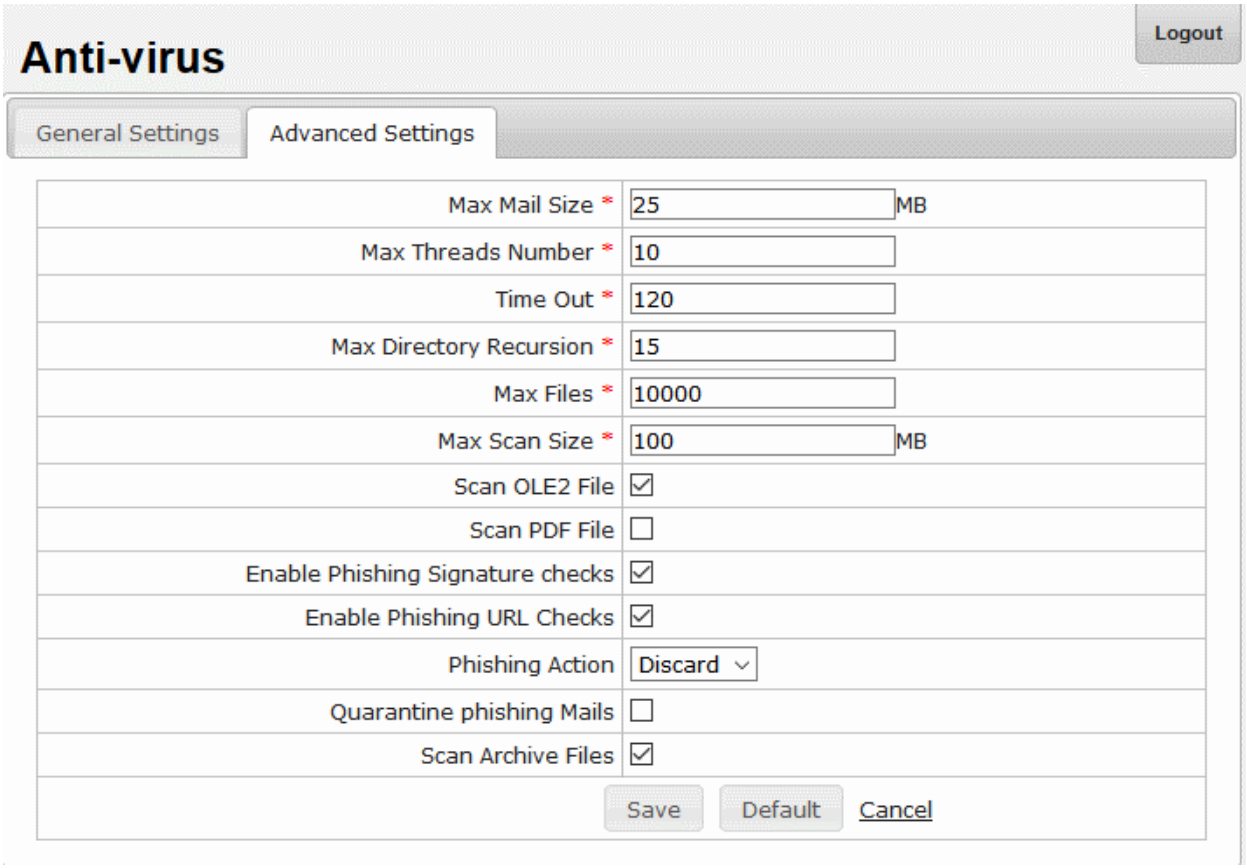
Anti-virus General Settings - Table of Parameters	
Parameter	**Description**
Enable Anti-virus	Select this to active the anti-virus scanning engine. The anti-virus parameters specified in the profile settings will be activated only if this setting is enabled here. Refer to the 'Profile Management' section for more details about profile settings.
Virus Scanner	Select the AV program from the drop-down that should be used for scanning the emails. The AV program available for selection is Comodo AV.

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

5.2.2 Advanced Anti-Virus Settings

The 'Advanced Settings' screen allows you to set the maximum size of email that should be scanned, the number of mail threads, the maximum number of files and more. Please note that if the maximum size is surpassed then the antivirus filter for the particular email will not be applied.

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



Anti-virus Advanced Settings - Table of Parameters	
Parameter	**Description**
Max Mail Size	The maximum size of email that should be scanned.
Max Threads Number	The maximum number of email threads in a email that should be scanned.
Time Out	The AV scanning time in seconds for an email.
Max Directory Recursion	Maximum number of sub-directories or nested archives that will be scanned. If an archive contains more than this threshold then the attachment will be blocked.
Max Files	Maximum number of files that can be scanned within an archive or email.
Max Scan Size	Maximum amount of data (specified value set) scanned for each input file. Archived files are scanned till the Antivirus scanner reaches the set value.
Scan OLE2 File	If enabled, AV scan is run for OLE2 file formats.
Scan PDF File	If enabled, AV scan is run for PDF file formats.
Enable Phishing Signature checks	If enabled, AV scanner checks for phishing 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, AV scanner quarantines phishing emails. These emails can be accessed by

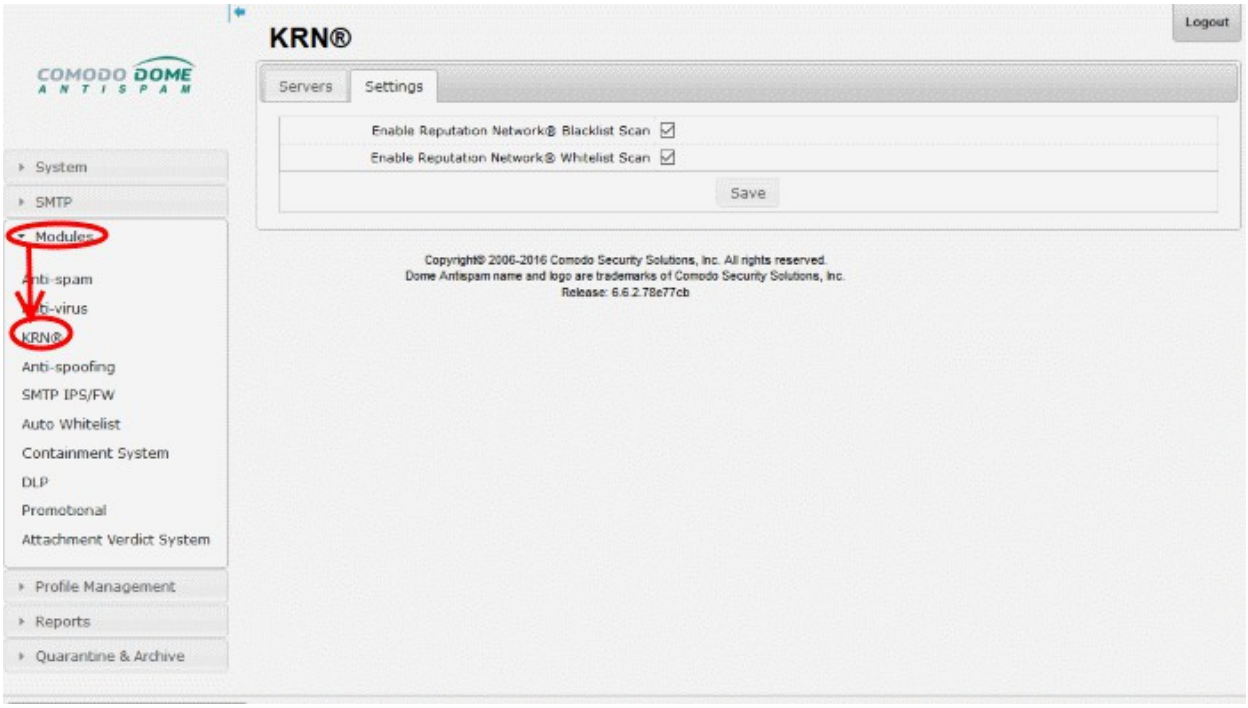
	users through Webmail interface.
Scan Archive Files	If enabled, archived mails will also be scanned. The type of mails that should be archived and its related settings are configured in profile settings. Refer to the 'Profile Management' section for more details about profile settings.

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

5.3 Reputation Network (KRN)

Reputation Network is an IP reputation scoring system developed by Comodo. It not only includes traditional features such as real-time IP blacklists (RBL) but also has 'whitelist' and 'greylisting ignore' features. The whitelisting feature means emails that come from trusted sources which will be permitted and helps to reduce false-positive rates.

- To open the 'KRN®' interface, click the 'Modules' tab on the left, then click 'KRN®'



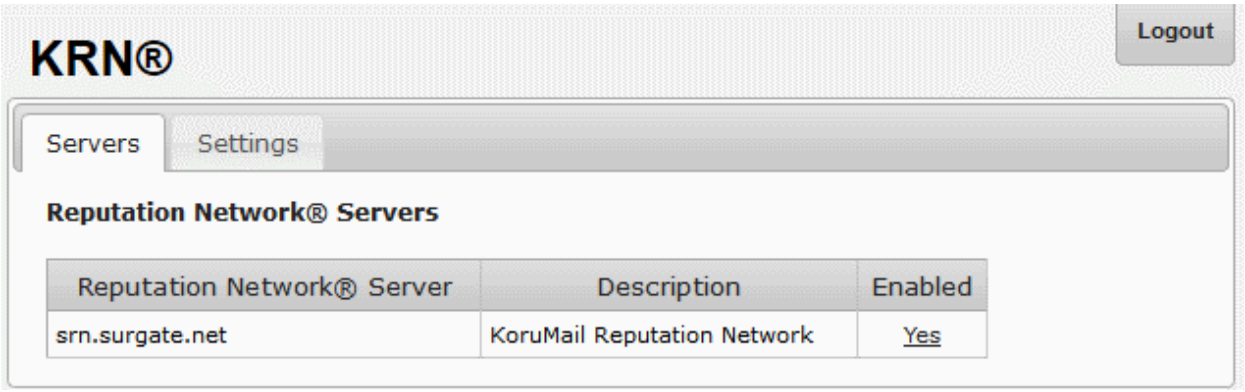
The interfce allows administrators to:

- Enable / disable a KRN server
- Configure KRN settings

To enable / disable a KRN server

A newly added KRN server will be in enabled status by default.

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



KRN Settings

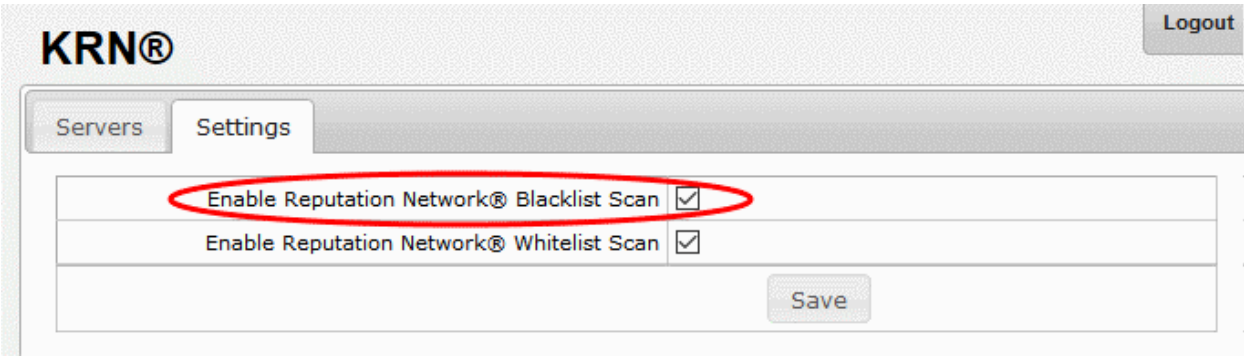
The KRN settings interface allows you to enable/disable KRN Blacklist and Whitelist scan. The KRN Blacklist and Whitelist scan in the KRN module must be enabled in order to activate the KRN parameters specified in profile settings. Refer to the 'Profile Management' section for more details about profile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

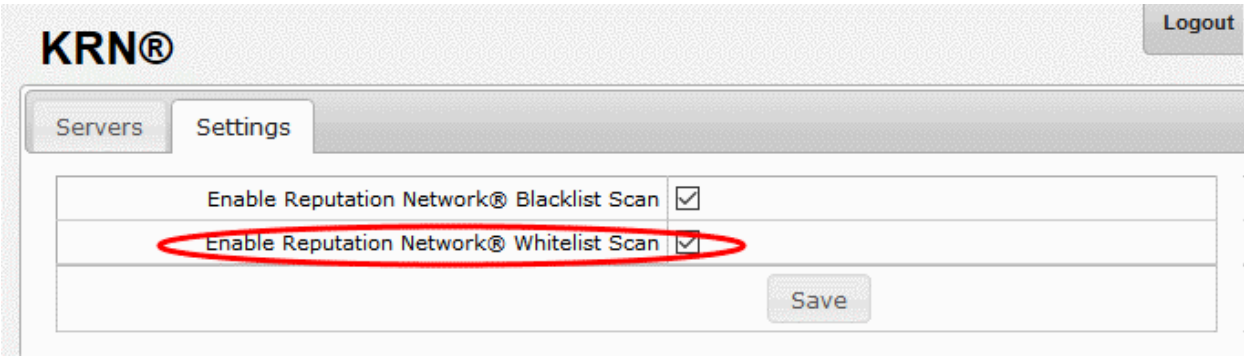
- Click the 'Settings' tab in the KRN®' interface



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

To enable / disable KRN whitelist scan

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

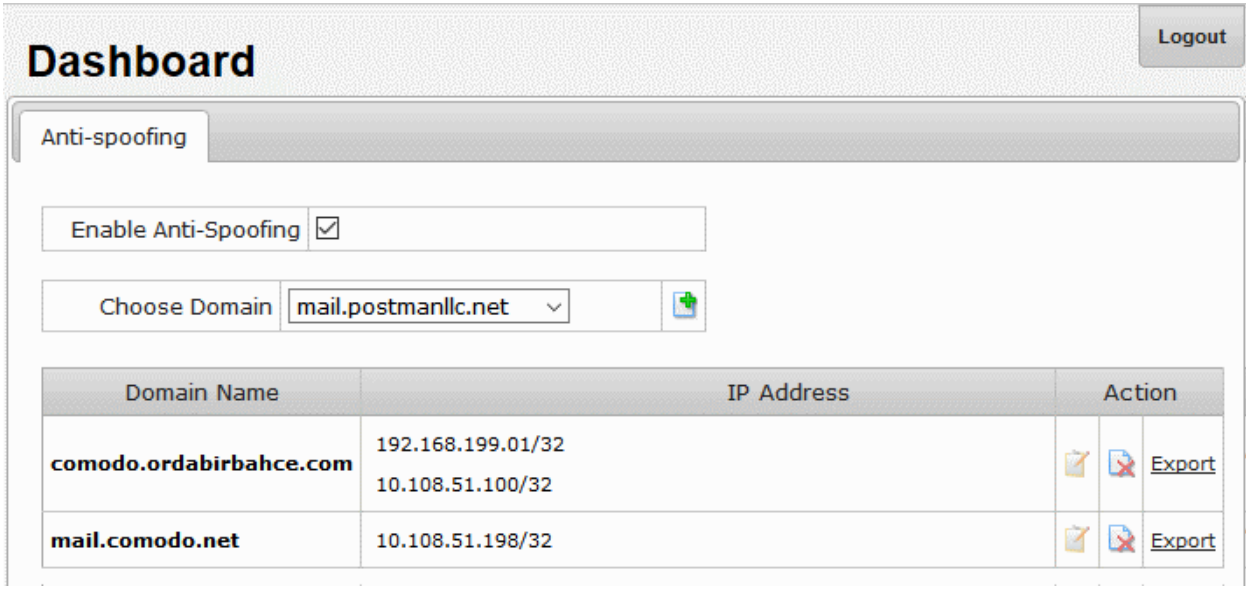


- Select / deselect the 'Enable Reputation Network® Whitelist Scan' check box to activate or deactivate the KRN whitelist scan
- Click the 'Save' button to apply your changes.

5.4 Anti-Spoofing

Email spoofing is a technique used to forge email headers so that the message appears to originate from a source other than the true sender. Email spoofing is possible because SMTP (Simple Mail Transfer Protocol) being the main protocol used in sending emails, does not include an authentication mechanism. The 'Anti-Spoofing' feature in Dome Antispam 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. Dome Antispam allows you to add a range of IP addresses for a protected domain, which an MTA (Mail Transfer Agent) can look up to confirm whether an email is being sent from an authorized server.

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



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

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

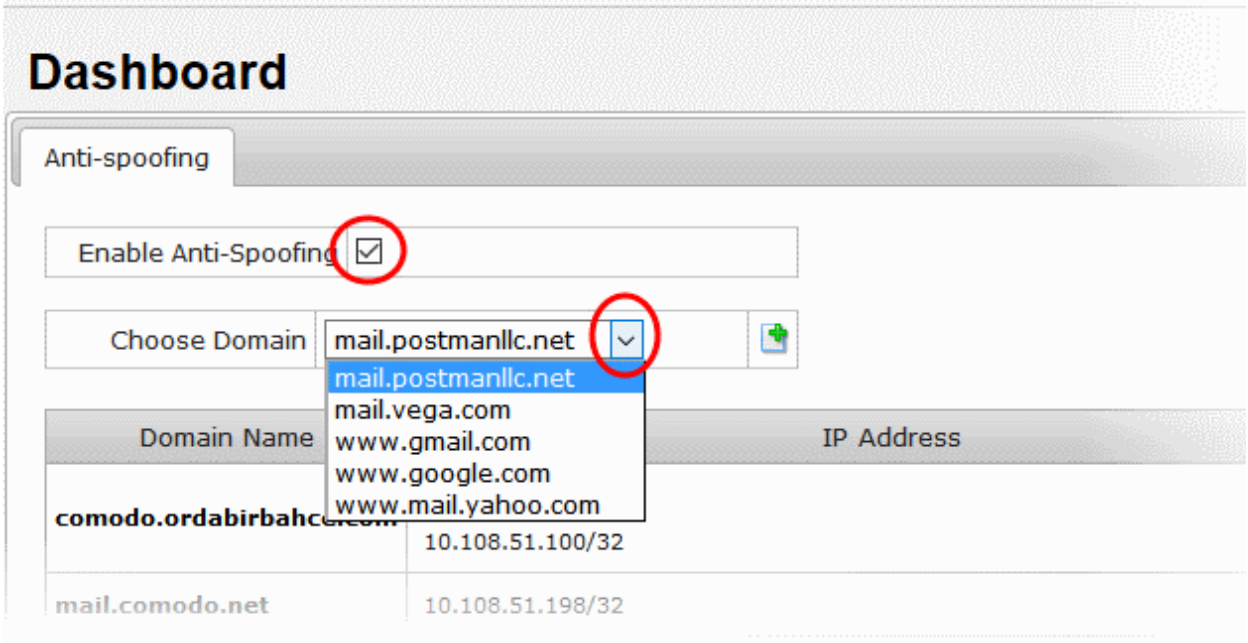
The interface allows administrators to:

- 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

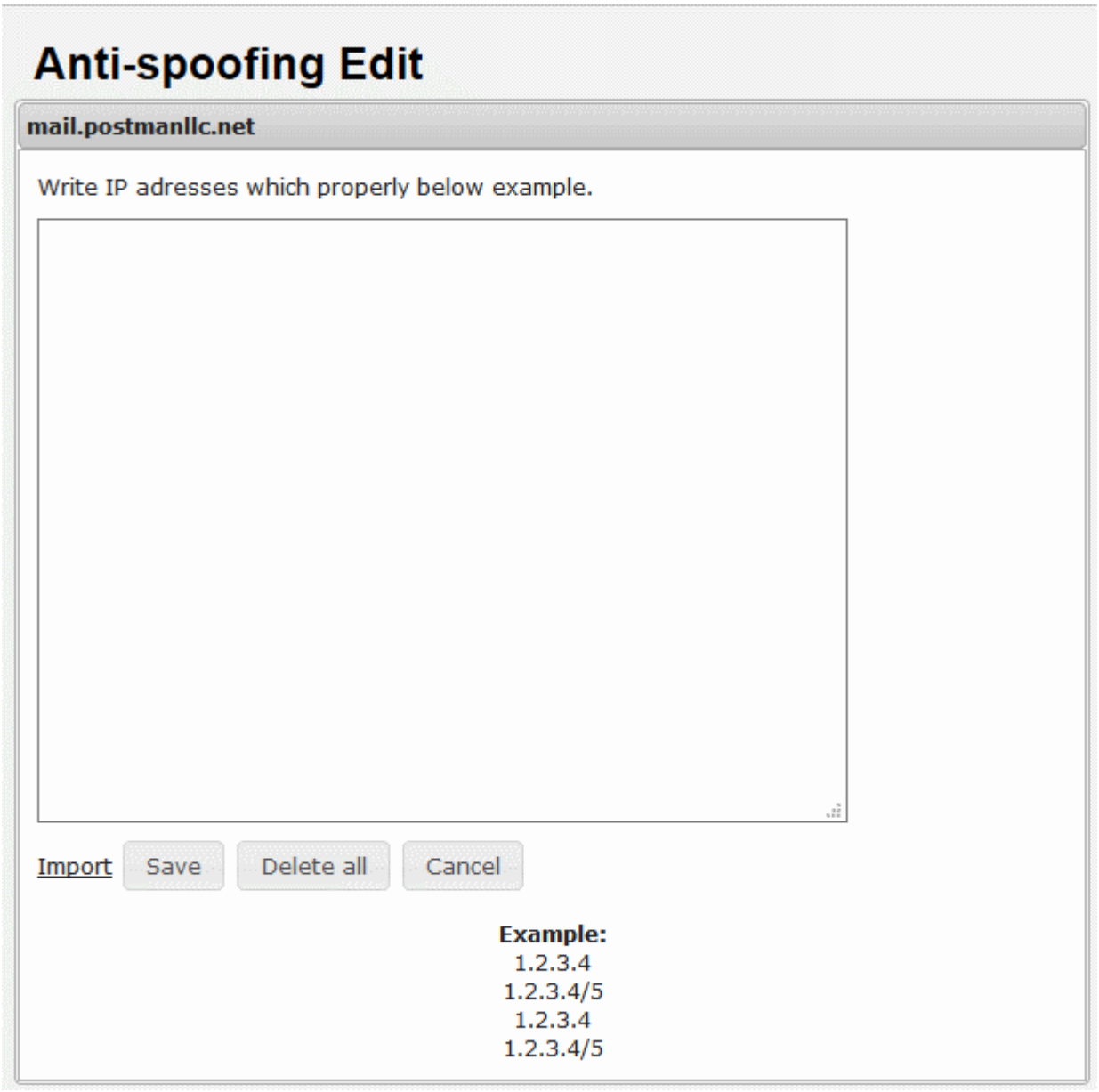
To add an IP range for a domain

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

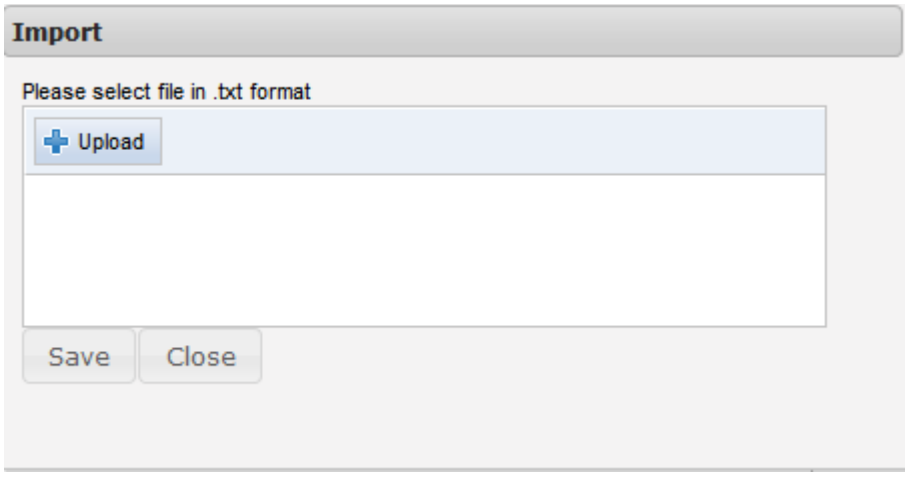


- Click the button

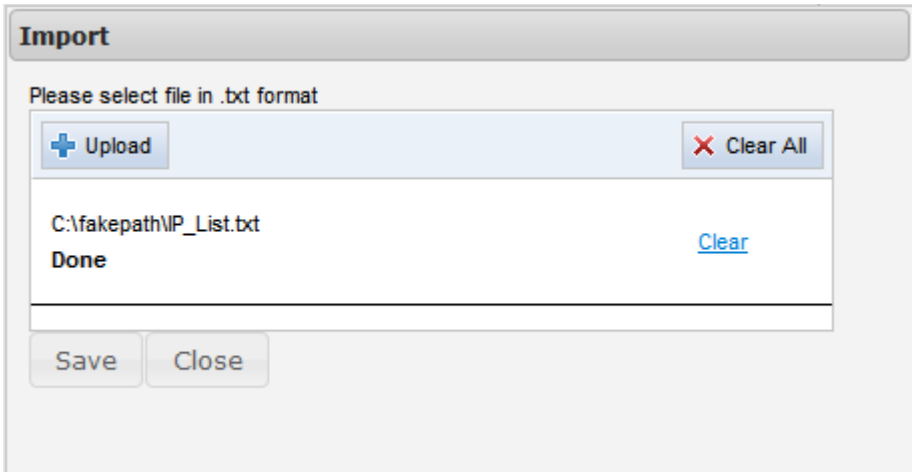
The 'Anti-spoofing Edit' screen will be displayed.



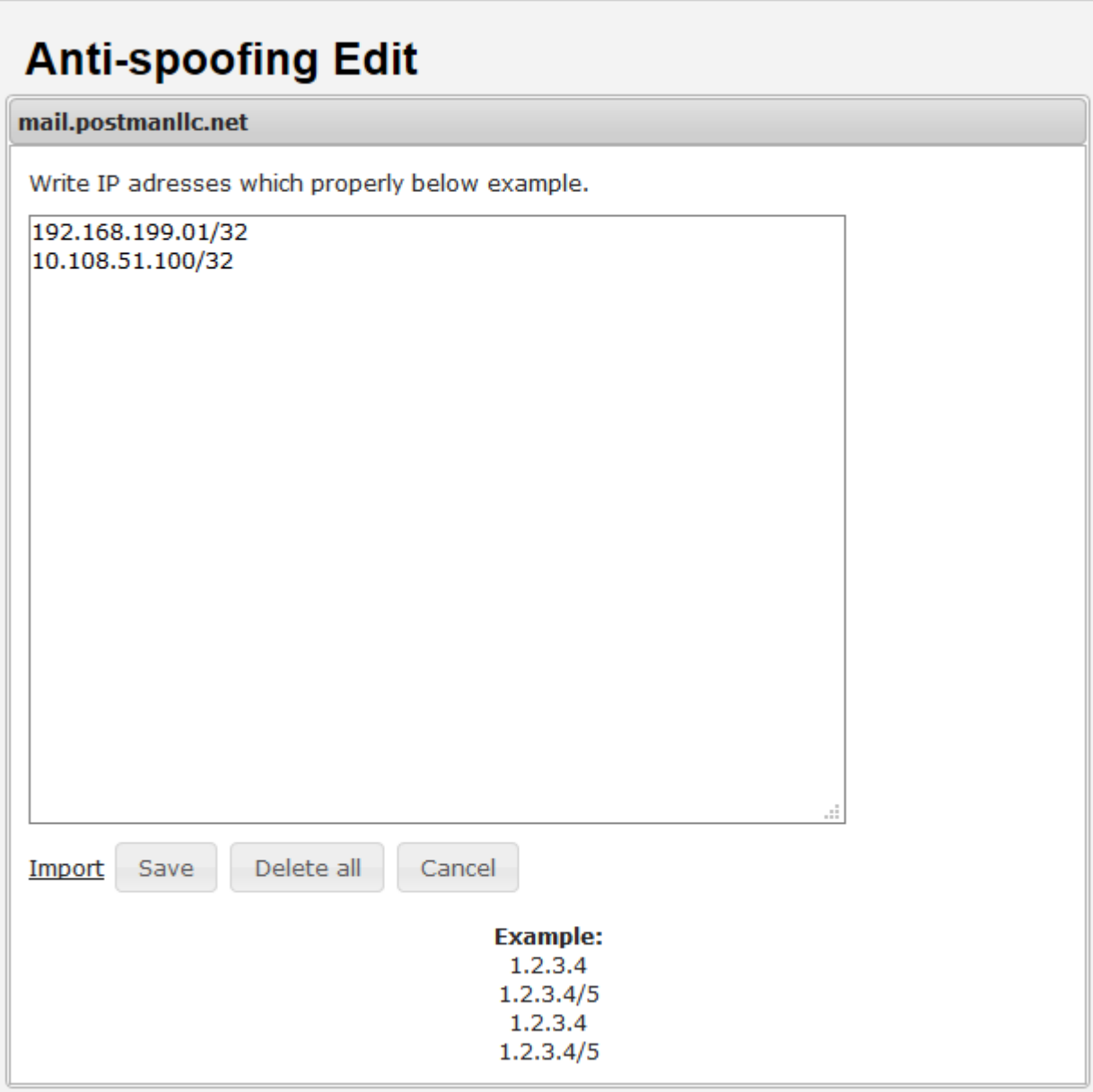
- To add the IP range manually, enter the address each per line in the field and click the 'Save' button.
- To import from a saved file, click the 'Import' link



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



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



- 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.

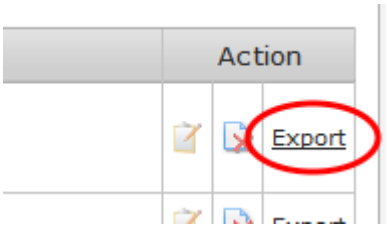
- Edit the address as required and click the 'Save' button.

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



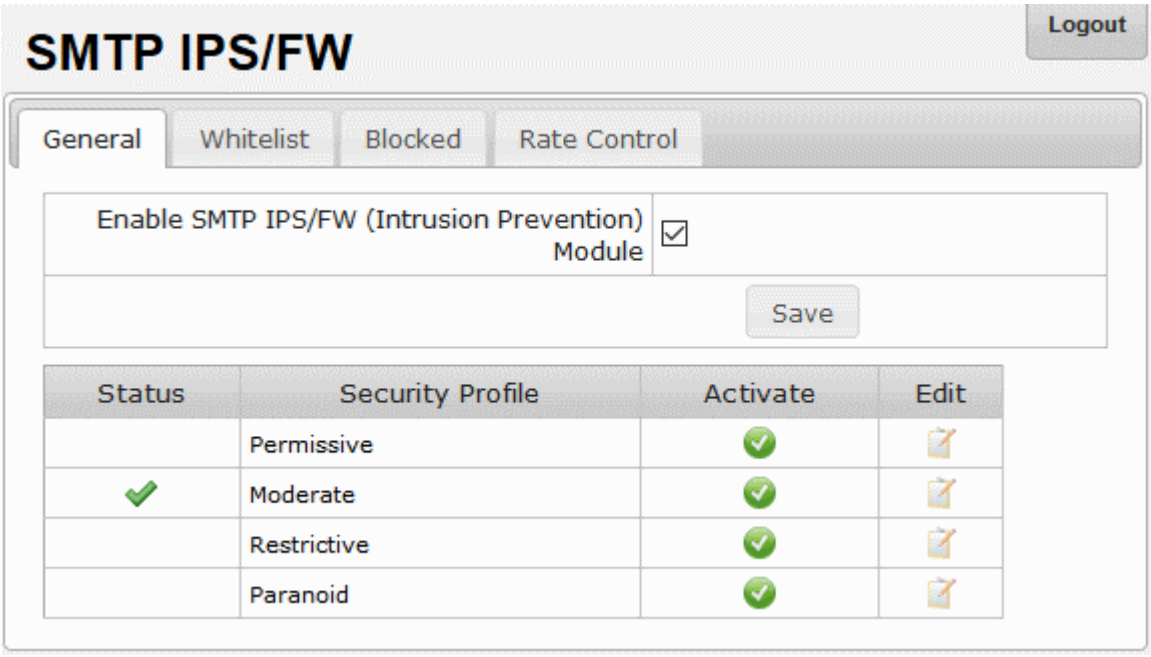
- The SPF IP list will be downloaded as a text file to your system.

5.5 SMTP IPS/FW

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

The module also allows you to define Whitelist and Blocked rules to better control the spam mails. The Rate Control feature, a subset of DoS protection system, allows you to control how many connections are allowed within the specified time from the same IP address.

- To open the 'SMTP IPS/FW' interface, click the 'Modules' tab on the left, then click 'SMTP IPS/FW'.



Refer to the following sections for more details.

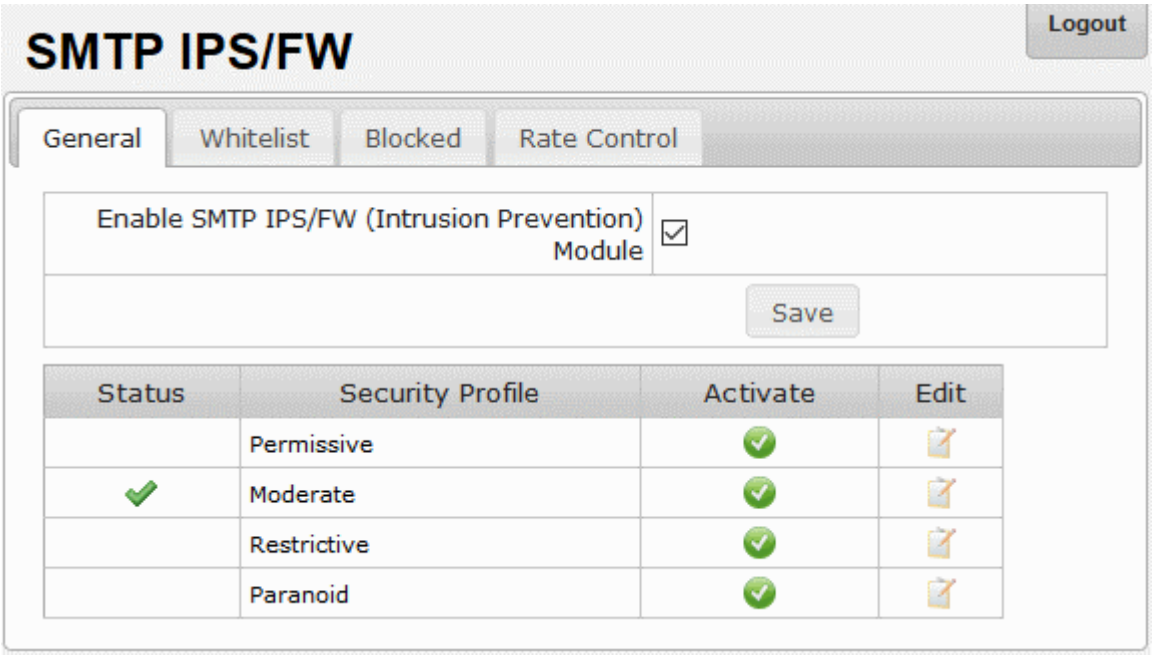
- SMTP IPS General Settings
- Whitelist IP Addresses
- Blocked IP Addresses
- Rate Control

5.5.1 SMTP IPS General Settings

The 'General' tab in the SMTP IPS/FW module allows you to enable/disable the Intrusion Prevention System (IPS) and configure a security profile for Dome Antispam. The IPS allows Dome Antispam to control the number and rate

of SMTP connections from any single IP address. This helps to detect and block spam/denial-of-service attacks and aids traffic management.

- To open the 'IPS General Settings' interface, click the 'General' tab in the 'SMTP IPS/FW' screen.



- SMTP IPS/FW (Intrusion Prevention) Module: Select the check box to activate the module so as to apply the security profile.

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

IPS General Settings - Table of Column Descriptions		
Column Header	**Description**	
Status	Indicates whether the security profile is activated	
Security Profile	The name of the security profile. The name cannot be edited. There are four security profiles - 'Permissive', 'Moderate', 'Restrictive' and 'Paranoid'. Each one has default settings provided according to their respective security levels.	
Activate	Click this button to enable a profile. Please note that only one security profile can be active at a time.	
Edit		Allows you to edit the parameters of a security profile.

The interface allows you to:

- Activate a security profile
- Edit the parameters of a security profile

To activate a security profile

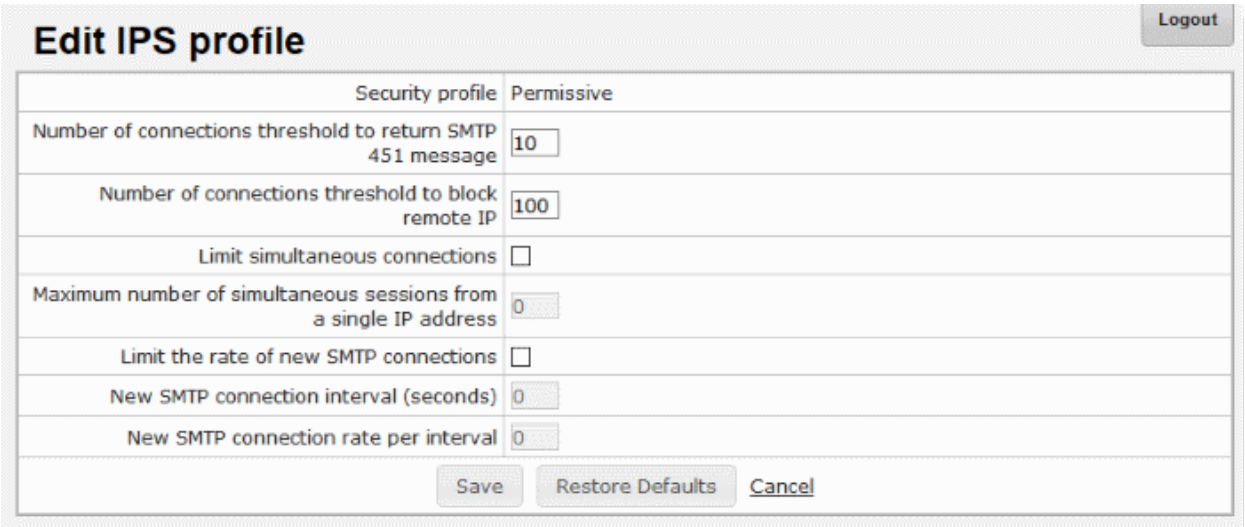
- Click the button under the 'Activate' column in a security profile row that you want to enable. Please note that only one security profile can be active at a time.

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.



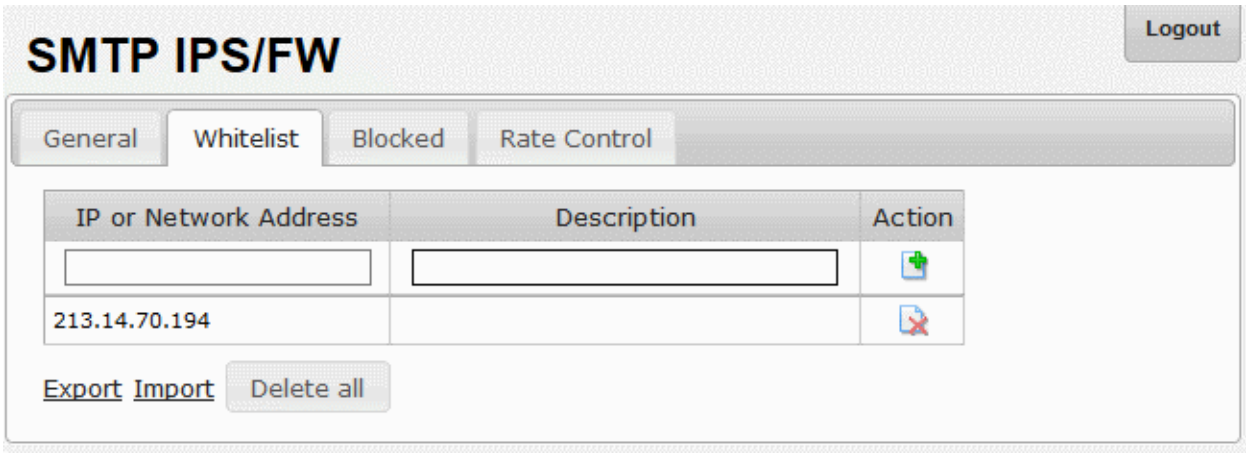
IPS Profile - Table of Parameters	
Parameter	**Description**
Security profile	The name of the predefined profile
Number of connections threshold to return SMTP 451 message	• Maximum number of SMTP connections before Dome Antispam will refuse further connections and will send out a 451 'bounce-back' email to the sender. If you wish to unblock this sender, please contact support@comodo.com to whitelist or unblock the IP.
Number of connections threshold to block remote IP	Maximum number of remote connections allowed before Dome Antispam's built in firewall blocks the exceeding connections.
Limit simultaneous connections	If enabled, instant SMTP connections are limited from a single IP as per the maximum number of simultaneous sessions allowed.
Maximum number of simultaneous sessions from a single IP address	Maximum number of sessions that can be opened by a single IP address after limiting instant SMTP connections.
Limit the rate of new SMTP connections	If enabled, the parameters 'New SMTP connection interval' and 'New SMTP connection rate' can be specified to set limitations on new SMTP connections.
New SMTP connection interval (seconds)	The time between a new connection and the previous connection.
New SMTP connection rate per interval	Maximum number of new SMTP connections in specified interval.

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

5.5.2 Whitelist IP Addresses

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

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



Whitelist Settings - Table of Column Descriptions		
Column Header	**Description**	
IP or Network Address	The details of IP or networked addresses that are whitelisted.	
Description	The description provided for the IP/Network address.	
Action		Allows 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.

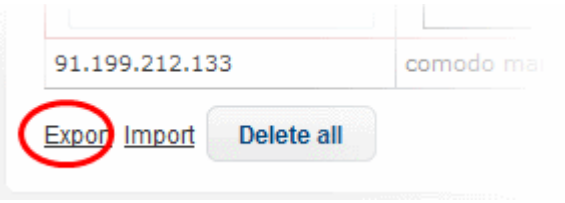
The address will be added and listed as whitelisted.

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 the 'Delete all' button below to remove all the whitelisted addresses from the list and click 'OK' in the confirmation screen.

To export the whitelisted network or IP address details

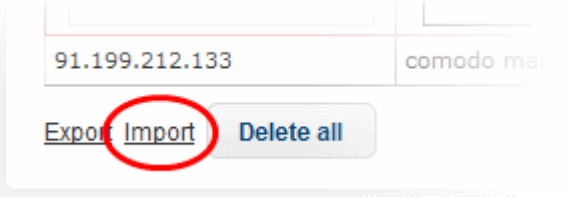
- Click the 'Export' link at the bottom of the screen



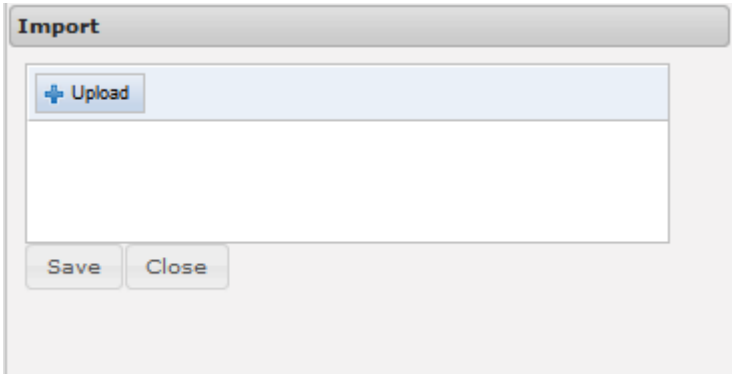
- The list will be exported in .txt format.

To import lists of whitelisted network or IP addresses from files

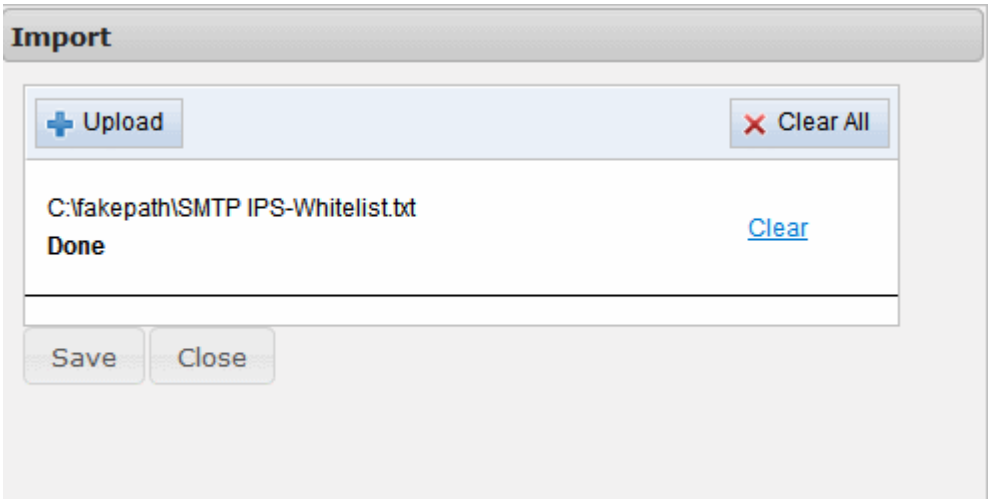
- Click the 'Import' link at the bottom of the screen



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



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

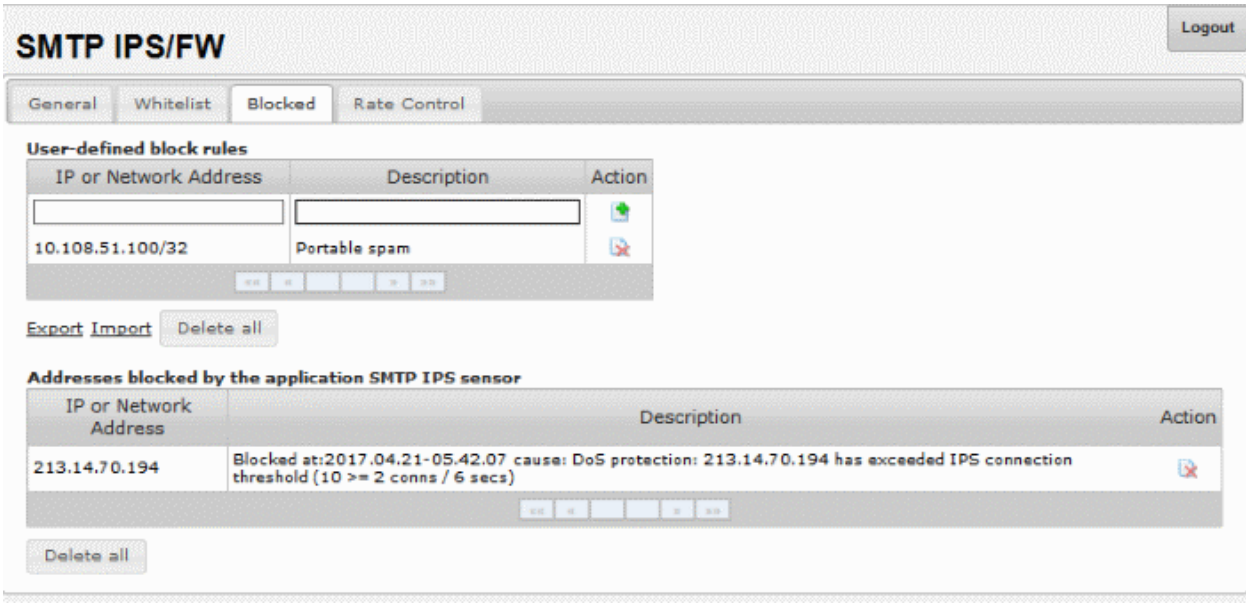


- To remove a file from the list, click the 'Clear' link beside it.
- To remove all the files, click the 'Clear All' button at the top.
- Click the 'Save' button.

5.5.3 Blocked IP Addresses

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

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



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

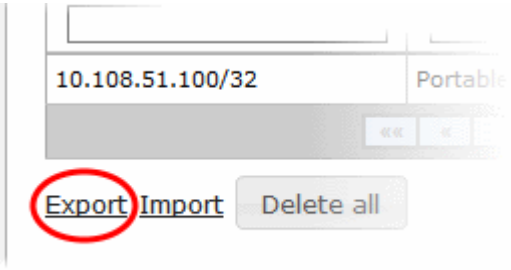
To add a network or IP address to be blocked

- 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.

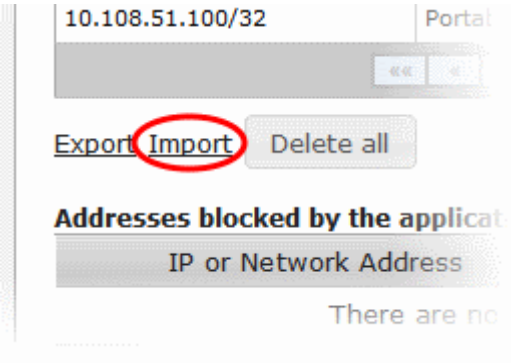


To export the blocked network or IP address details

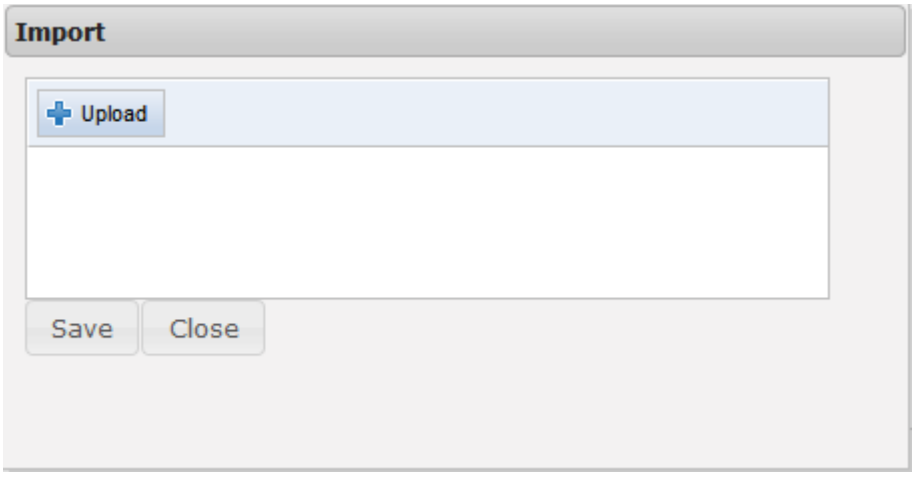
- Click the 'Export' link at the bottom of the screen
- The list will be exported as a text file.

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

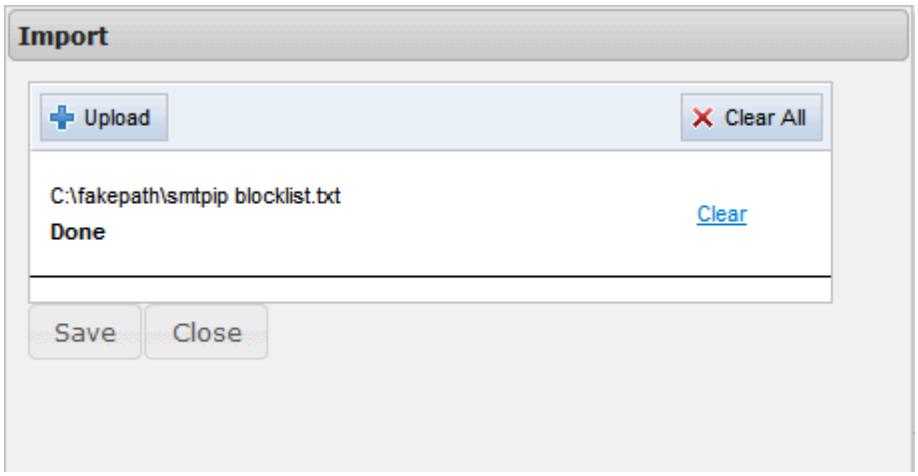
- Click the 'Import' link at the bottom of the screen



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



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

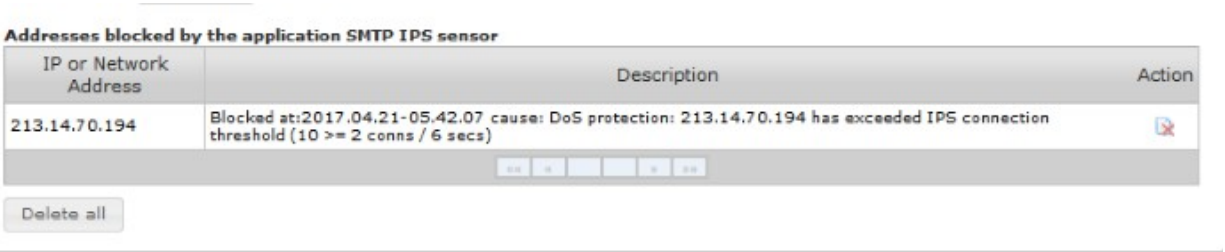


- To remove a file from the list, click the 'Clear' link beside it.
- To remove all the files, click the 'Clear All' button at the top.
- Click the 'Save' button.

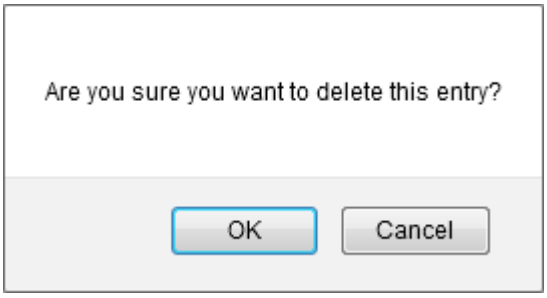
To delete an automatically blocked network or IP address by SMTP IPS sensor from the list

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

- In the 'Addresses blocked by Dome Antispam SMTP IPS sensor' table, click the button beside an address that you want to delete.



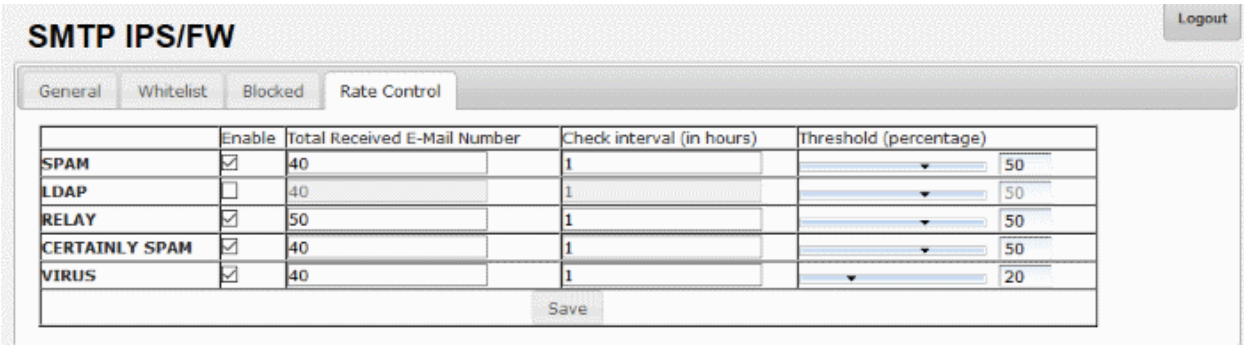
- Click 'OK' in the confirmation screen



5.5.4 Rate Control

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

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



Rate Control Settings - Table of Column Descriptions	
Column Header	**Description**
Category	SPAM - Mails that are categorized as spam LDAP - Verification of LDAP users. When incoming mails are for users that are not in LDAP, the originating IP address will be blacklisted. For example, if the number of mails is set as 50, and the threshold percentage as 50%, then if from a source if the number of mails for non LDAP users exceeds 25 within the check interval, then the source will be blacklisted RELAY - IPs from which mails can be sent by users who are not available on the mail server. CERTAINLY SPAM - Mails that are categorized as definite spam. VIRUS - Mails that are categorized as with virus
Enable	Activate or disable the Rate Control for a mail category
Total Received Email Number	Enter the number of mails in a particular category that will be checked during the time specified in the 'Check interval' column.
Check interval (in hours)	Enter the time in hours for the specified number of mails to be checked for a category.
Threshold (percentage)	Enter or use the slider to set the threshold percentage for the 'Rate Control' to be applied for a category. For example, if the number of email is set as 60 for a category,

	then a 50% threshold means that when the number exceeds 30, then the originating IP address will be blocked.

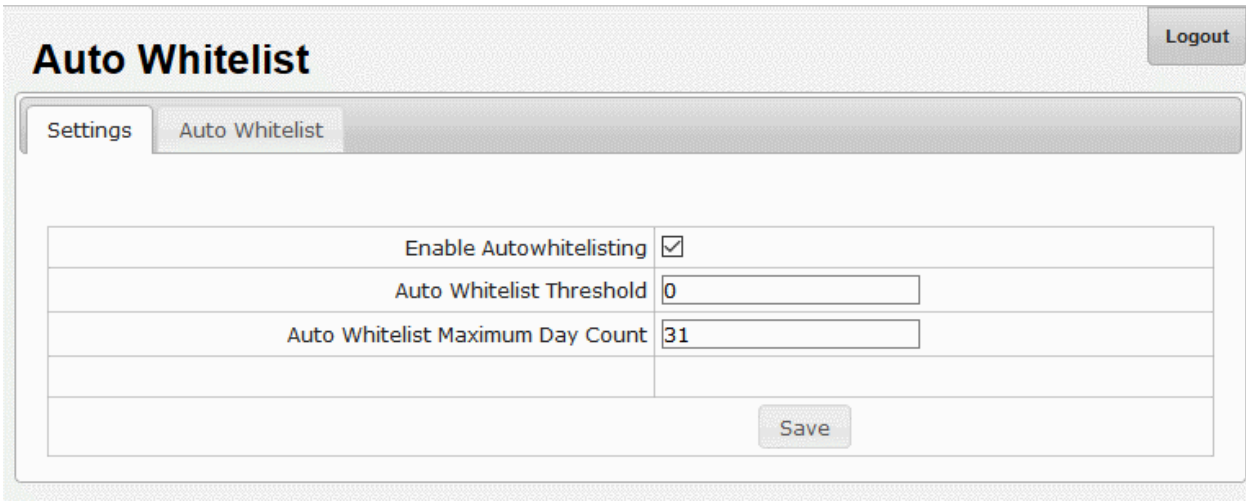
- Click the 'Save' button to apply your changes.

5.6 Auto Whitelist

Dome Antispam allows administrators to automatically whitelist incoming and outgoing mails to and from specific email addresses. The 'Auto Whitelist' module must be enabled to activate the whitelisting of addresses specified in the profile settings. Refer to the '**Profile Management**' section for more details about profile settings.

Auto Whitelist Settings:

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

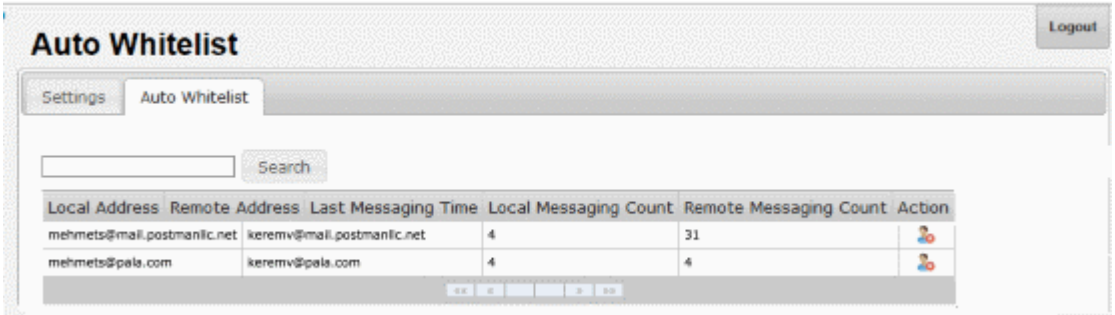


- **Enable Autowhitelisting:** Allow whitelisting of incoming and outgoing emails. This option is disabled by default
- **Auto Whitelist Threshold:** The number of mails to sender that will be whitelisted
- Click 'Save' to apply your changes.

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

Auto Whitelist details

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

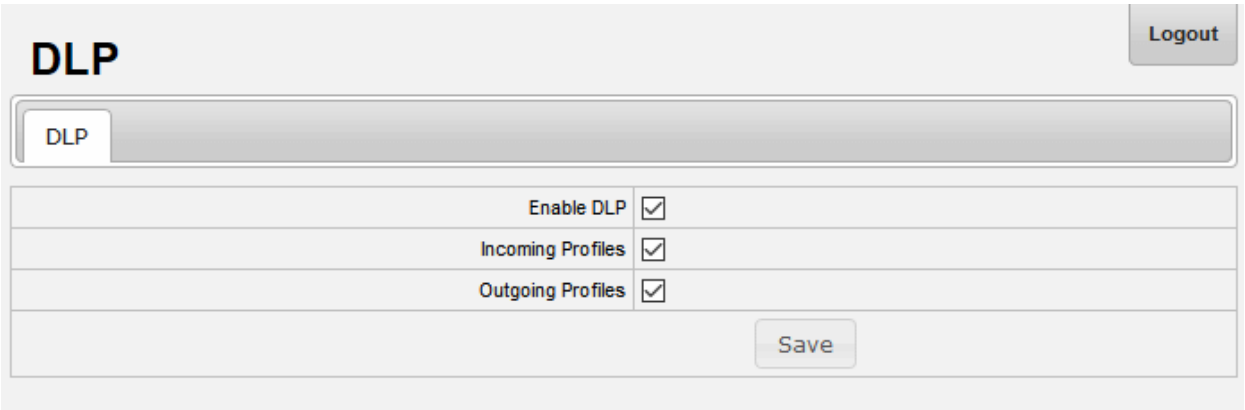


Auto Whitelist - Table of Column Headers	
Column Header	**Description**
Local Address	The recipient's email address
Remote Address	The sender's email address
Last Messaging Time	The time of the most recent sent or received mail
Local Messaging Count	The number of mails received
Remote Messaging Count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

5.7 Data Leak Prevention (DLP)

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

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



- **Enable DLP:** Select the check box to display the 'Incoming Profiles' and 'Outgoing Profiles' check boxes.
- **Incoming Profiles:** Select the check box to apply the DLP profile parameters to incoming mails
- **Outgoing Profile**: Select the check box to apply the DLP profile parameters for outgoing mails. This option is deselected by default.

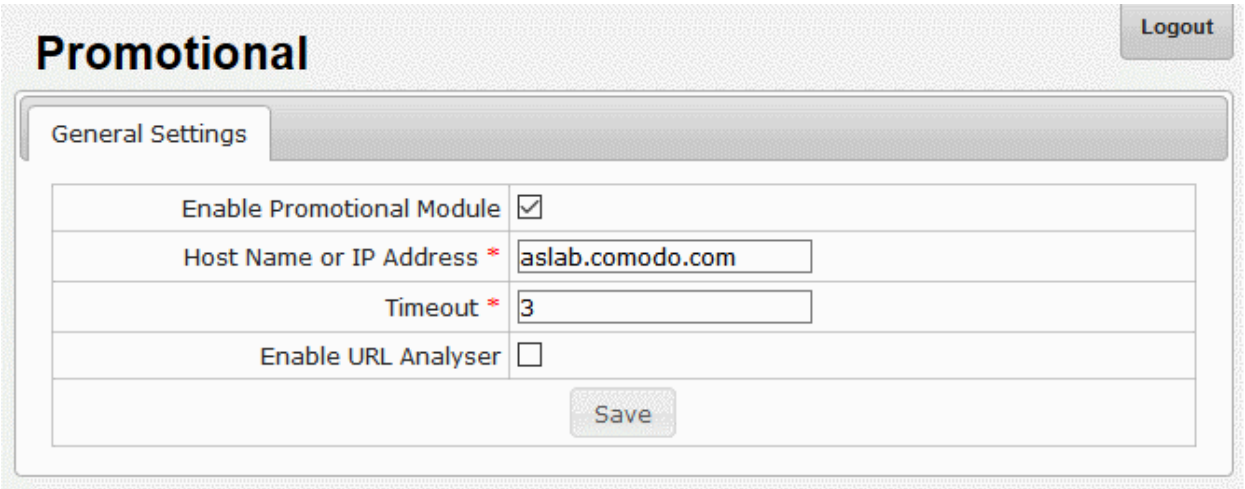
Refer to the 'Profile Management' section for more details about profile settings.

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

5.8 Promotional

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

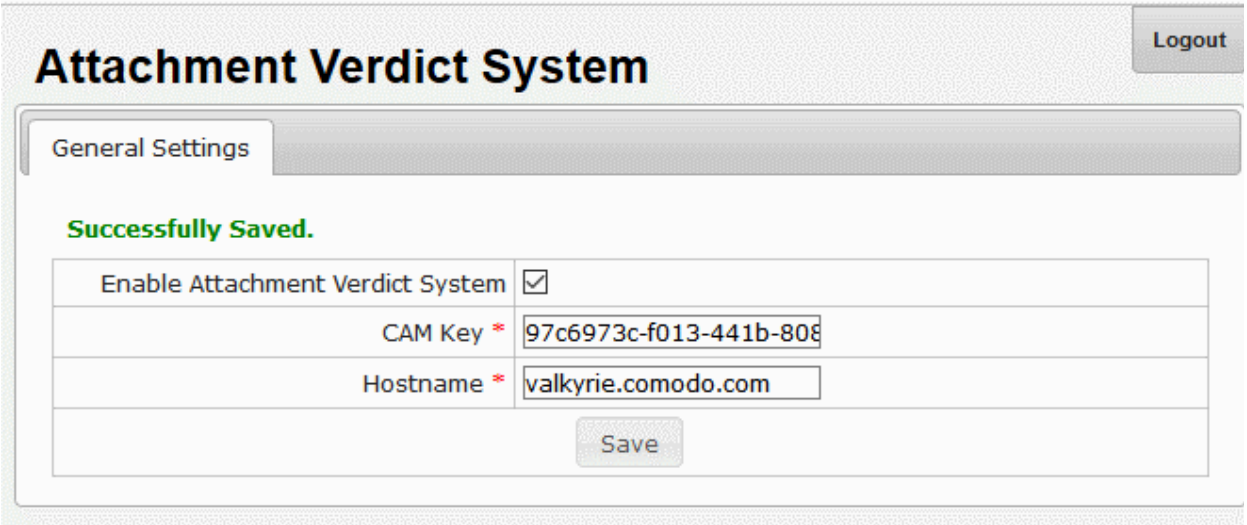
- To open the 'Promotional' interface, click the 'Modules' tab on the left, then click 'Promotional'.



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

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

5.9 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.

- To open the attachment verdict settings area, click Modules > Attachment Verdict System.

Attachment Verdict System - Table of Column Headers	
Column Header	**Description**
Enable Attachment Verdict	If enabled, Dome Antispam will automatically check the trust rating of Windows

System	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 Dome Antispam product to avail a license key.
Hostname	Hostname of the file attachment verdict system. This is set to the Comodo Valkyrie server by default. Only change this if you have established a different server with Comodo support.

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

6 Profile Management

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

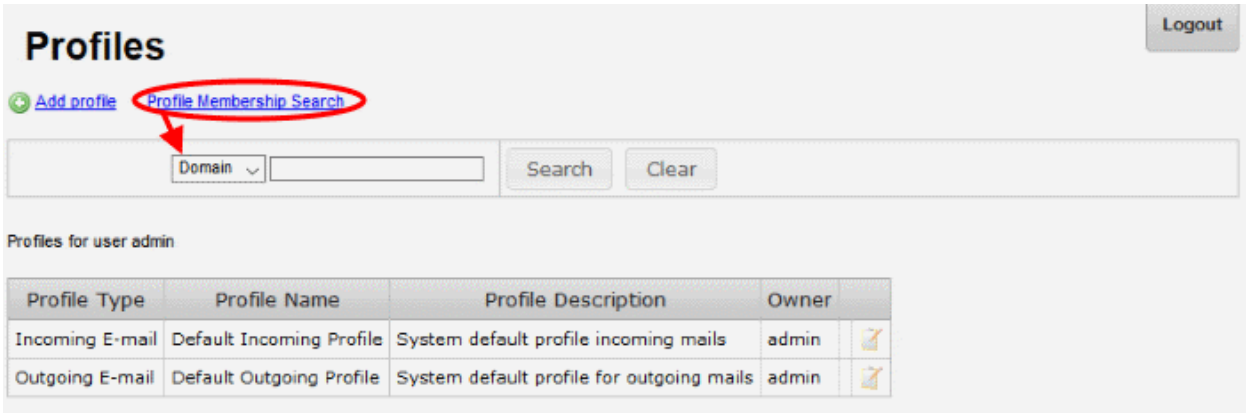
To open the 'Profiles' interface, click the 'Profile Management' tab on the left, then click 'Profiles'

Profiles - Table of Column Headers		
Column Header	**Description**	
Profile Type	The type of profile whether incoming or outgoing	
Profile Name	The name of the profile. The name of default profiles will be auto filled.	
Profile Description	The description provided for the profile	
Owner	The name of the group to which the profile creator belongs	
Action		Allows you to delete a profile. The default incoming or outgoing profile wil apply to the domains and / or users beloning to a profile when it is deleted.

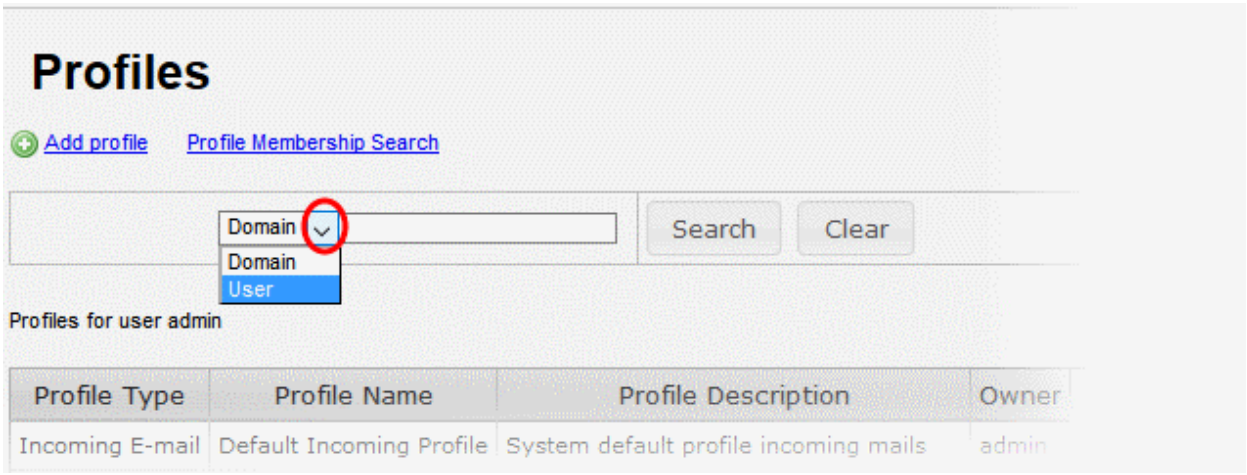
		Allows you to edit the settings in a profile.

Search Option

Click the 'Profile Membership Search' link at the top to search for a profile that is applied to domain and / or users.



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



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

The profile applied for the entered details will be displayed.

- To remove the details in the search field, click the 'Clear' button.
- To remove the search field, click the 'Profile Membership Search' link again.

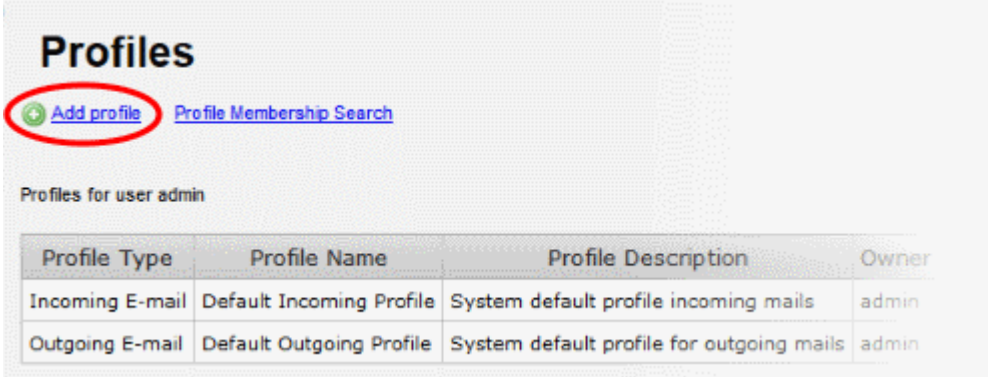
The 'Profiles' interface allows administrators to:

- Add and Confgure a New Profile
- Edit a Profile
- Delete a Profile

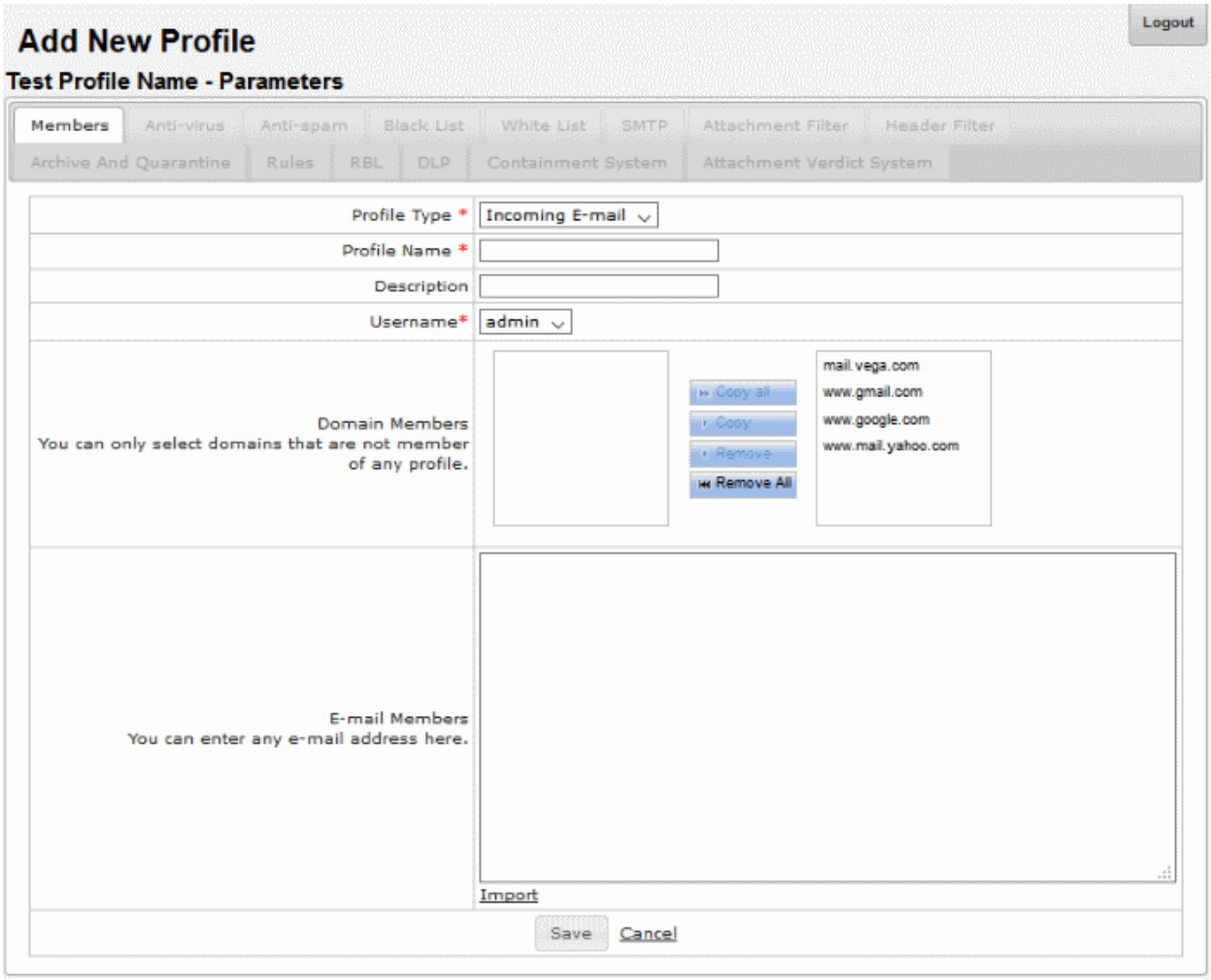
6.1 Adding and Configuring a New Profile

Profiles allow you to determine how Dome Antispam's anti-spam, anti-virus engine and other filtering mechanisms should behave for incoming / outgoing mails belonging to protected domains and / or users. The items that can be set in a profile include Anti-virus, Anti-spam, SMTP, Attachment Filter, Black List, White List, Header Filter, Archive and Quarantine, Data Leak Prevention (DLP) and Realtime Blackhole List (RBL).

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



The 'Add New Profile' screen will be displayed:

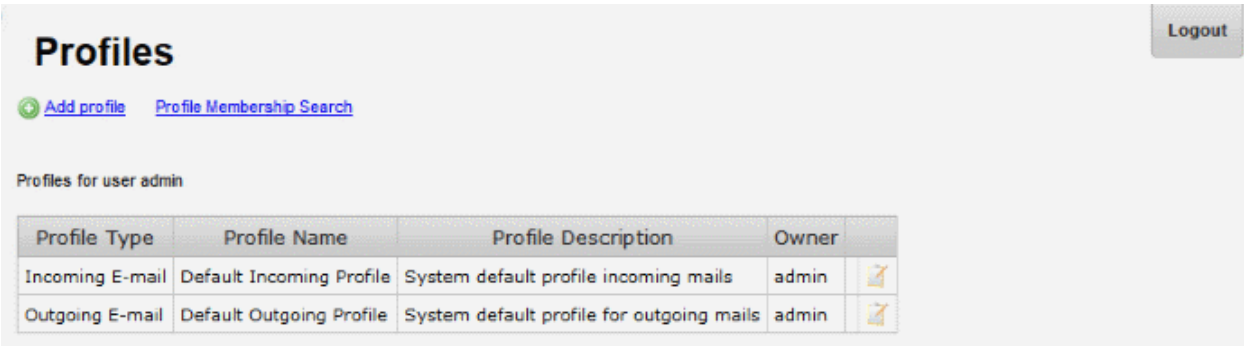


Profiles - Table of Parameters	
Parameter	**Description**
Profile Type	Select whether you want the profile to apply to incoming mails or outgoing mails
Profile Name	Enter a name for the profile
Description	Provide an appropriate description for the profile
Username	Select the username of the person who is adding the profile. Only users with appropriate privileges will be listed.
Domain Members	Allows administrators to add domains to the profile. • 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. • 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	Allows administrators to add users to the profile. • 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	Allows you to add users to the profile by importing them from a saved file. The same limitations mentioned above apply to imported users.

- Click the 'Save' button

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

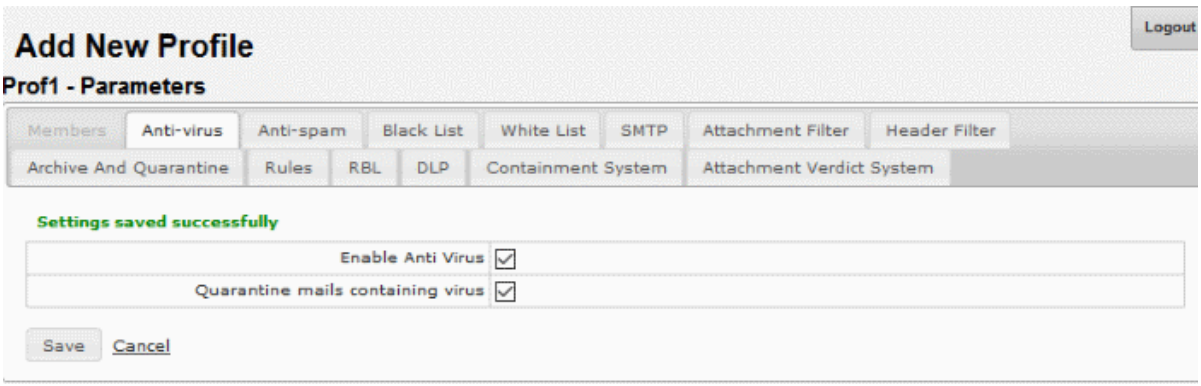


The interface allows administrators to configure profile parameters for:

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

Anti-virus

- Click the 'Anti-virus' tab

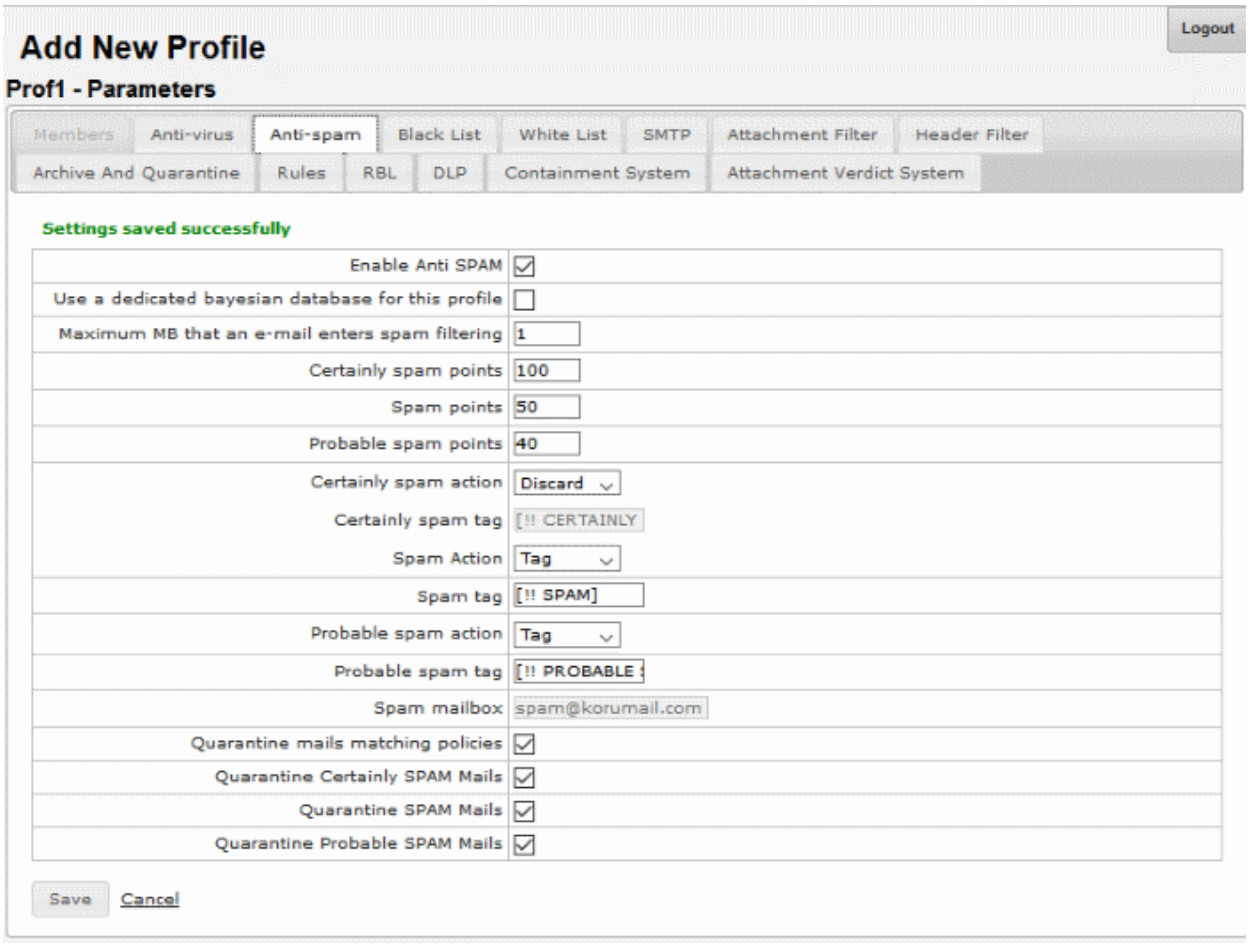


- **Enable Anti Virus:** Select the check box to enable the anti-virus engine for this profile. Please note the 'Anti-virus' module should be enabled for this parameter to become active.
- **Quarantine mails containing virus:** Mails detected with viruses will be quarantined. Users can log into the 'Quarantine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

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

Anti-spam

- Click the 'Anti-spam' tab.



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

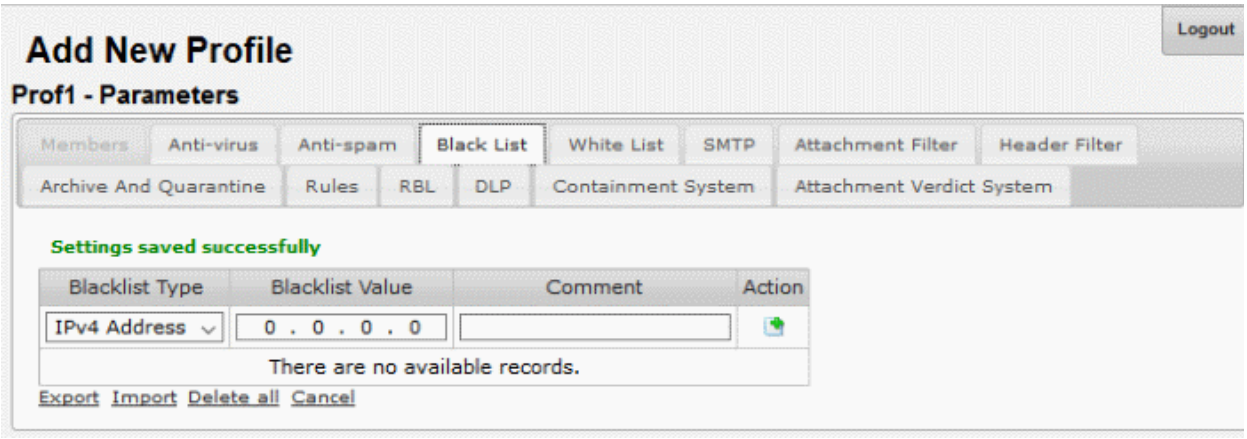
Spam points	Enter a value between 1 and 100 that will classify an email as spam. Suggested values are between 51 - 89 points.
Probable spam points	Enter a value between 1 and 100 that will classify an email as probable spam. Suggested values are between 40 - 50 points.
Certainly spam action	Select the action that has to be taken for emails that are categorized as definitely spam. The options available are: • **Tag** - The email will be sent to the recipient with a tag as entered in the next field 'Certainly spam tag' • **Forward** - The mail will be forwarded to a mail box defined in the 'Spam mailbox' field • **CC** - The mail will be sent to the recipient and a copy will be sent to a mail box defined in the 'Spam mailbox' field • **Discard** - The mail will be quarantined. Daily notifications will be sent to user with details of quarantined emails. The user can view the email using the Quarantined Email web interface. • **Reject** - The mail will be rejected and a reject command will be sent to the sender mail server.
Certainly spam tag	Enter the tag text for emails that are categorized as definitely spam
Spam Action	Select the action that has to be taken for emails that are categorized as spam. The options available are: • **Tag** - The email will be sent to the recipient with a tag as entered in the next field 'Spam tag' • **Forward** - The mail will be forwarded to a mail box defined in the 'Spam mailbox' field • **CC** - The mail will be sent to the recipient and a copy will be sent to a mail box defined in the 'Spam mailbox' field • **Discard** - The mail will be quarantined. Daily notifications will be sent to user with details of quarantined emails. The user can view the email using the Quarantined Email web interface. • **Reject** - The mail will be rejected and a reject command will be sent to the sender mail server.
Spam tag	Enter the tag text for emails that are categorized as spam
Probable spam action	Select the action that has to be taken for emails that are categorized as probable spam. The options available are: • **Tag** - The email will be sent to the recipient with a tag as entered in the next field 'Probable spam tag' • **Forward** - The mail will be forwarded to a mail box defined in the 'Spam mailbox' field • **CC** - The mail will be sent to the recipient and a copy will be sent to a mail box defined in the 'Spam mailbox' field • **Discard** - The mail will be quarantined. Daily notifications will be sent to user with details of quarantined emails. The user can view the email using the Quarantined Email web interface. • **Reject** - The mail will be rejected and a reject command will be sent to the sender mail server.

Probable spam tag	Enter the tag text for emails that are categorized as probable spam
Spam mailbox	Enter the email address to which the forwarded and CCed spam emails configured in the 'Spam action' drop-down will be sent.
Quarantine mails matching policies	If enabled, emails that are matching the configured profile will be quarantined.
Quarantine Certainly SPAM Mails	If enabled, emails that are categorized as definitely spam will be quarantined.
Quarantine SPAM Mails	If enabled, emails that are categorized as spam will be quarantined.
Quarantine Probable SPAM Mails	If enabled, emails that are categorized as probable spam will be quarantined.

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

Black List

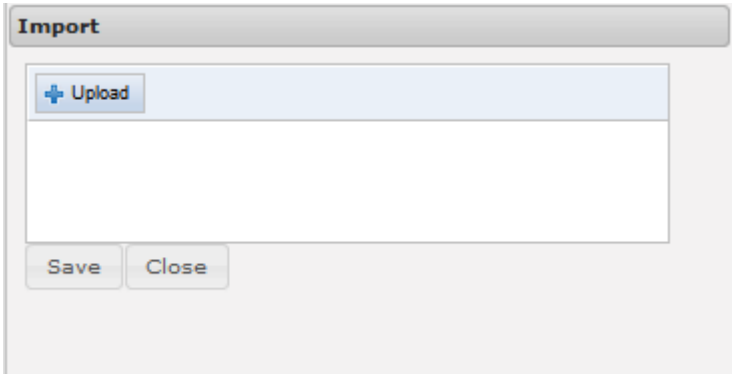
- Click the 'Black List' tab.



Profiles: Black List Settings - Table of Column Descriptions	
Column Header	**Description**
Blacklist Type	Select the type of source that has to be blacklisted. The options available are: • IPv4 Address • IPv6 Address • E-mail • Domain • IPv4 Network • IPv6 Network
Blacklist Value	Enter the details for the type of blacklist selected in the first column.

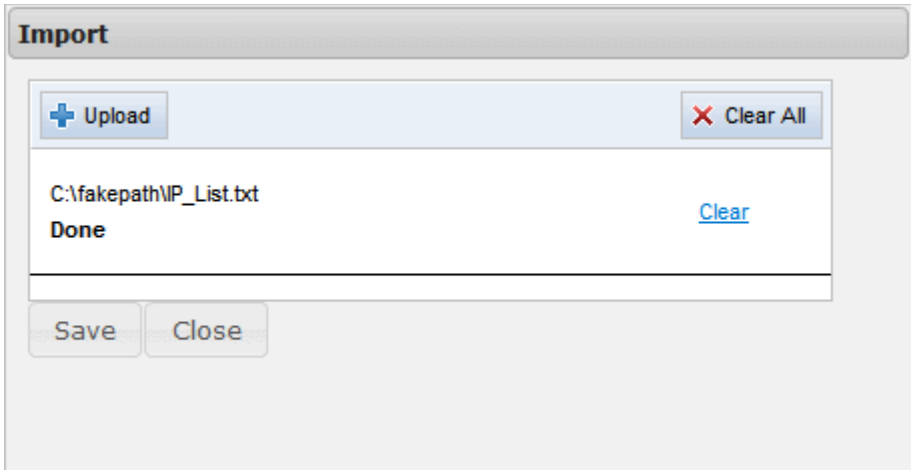
Comment	Provide an appropriate description for the blacklisted source	
Action		Allows you to add a blacklist type after filling the fields in the row
		Allows you to delete a blacklist type from the list

- 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.

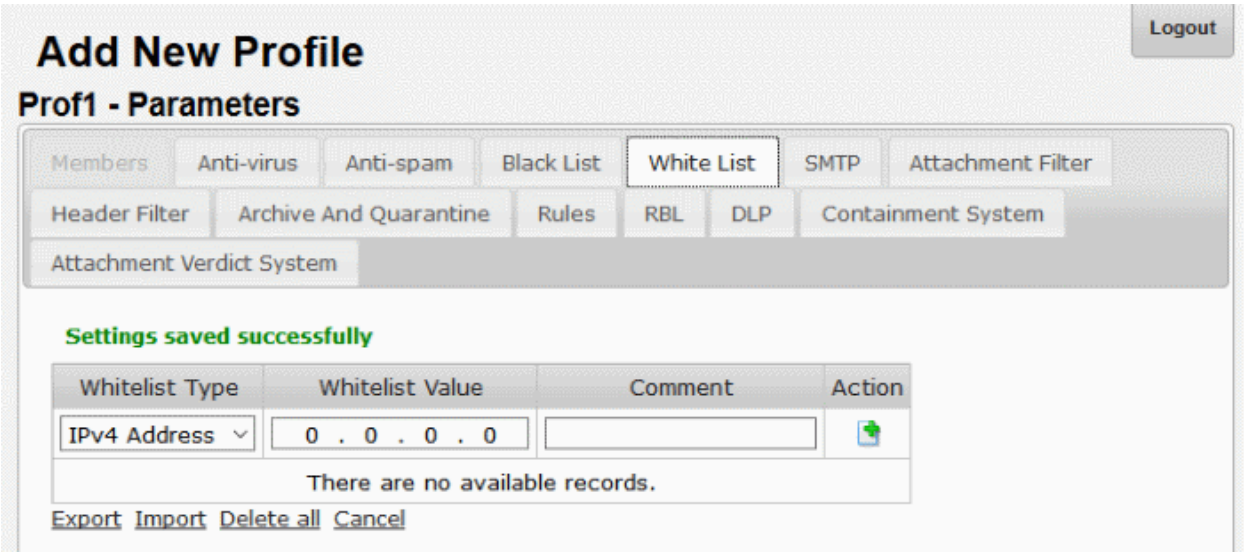


- Repeat the process to add more files.
- To remove a file, click the 'Clear' link beside it.
- To remove all the added files, click the 'Clear All' button at the top right.
- To import the list from the files, click the 'Save' button.

- To delete a blacklist type from the list, click the button under the 'Action' column header and click 'OK' in the confirmation screen.
- To remove all the blacklisted sources, click the 'Delete all' link and click 'OK' in the confirmation screen.

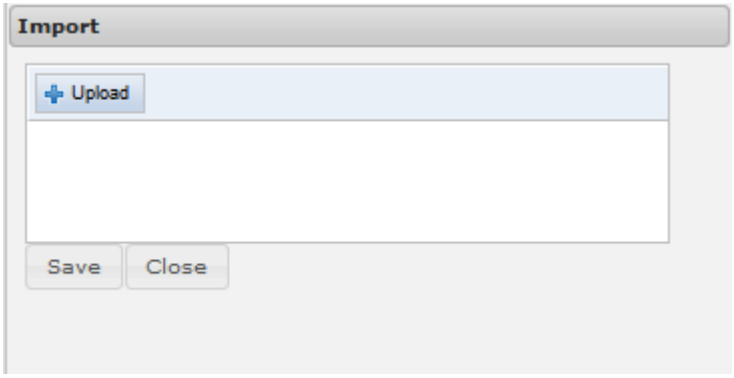
White List

- Click the 'White List' tab.



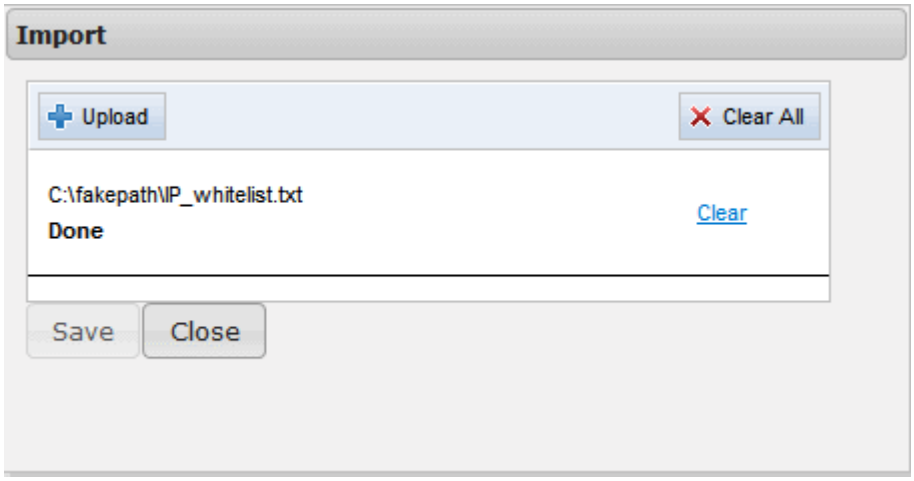
Profiles: White List Settings - Table of Column Descriptions		
Column Header	**Description**	
Whitelist Type	Select the type of source that has to be whitelisted. The options available are: • IPv4 Address • IPv6 Address • E-mail • Domain • IPv4 Network • IPv6 Network	
Whitelist Value	Enter the details 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 the 'Upload' button, browse to the location where the file is saved and click 'Open'.

The file will be added.

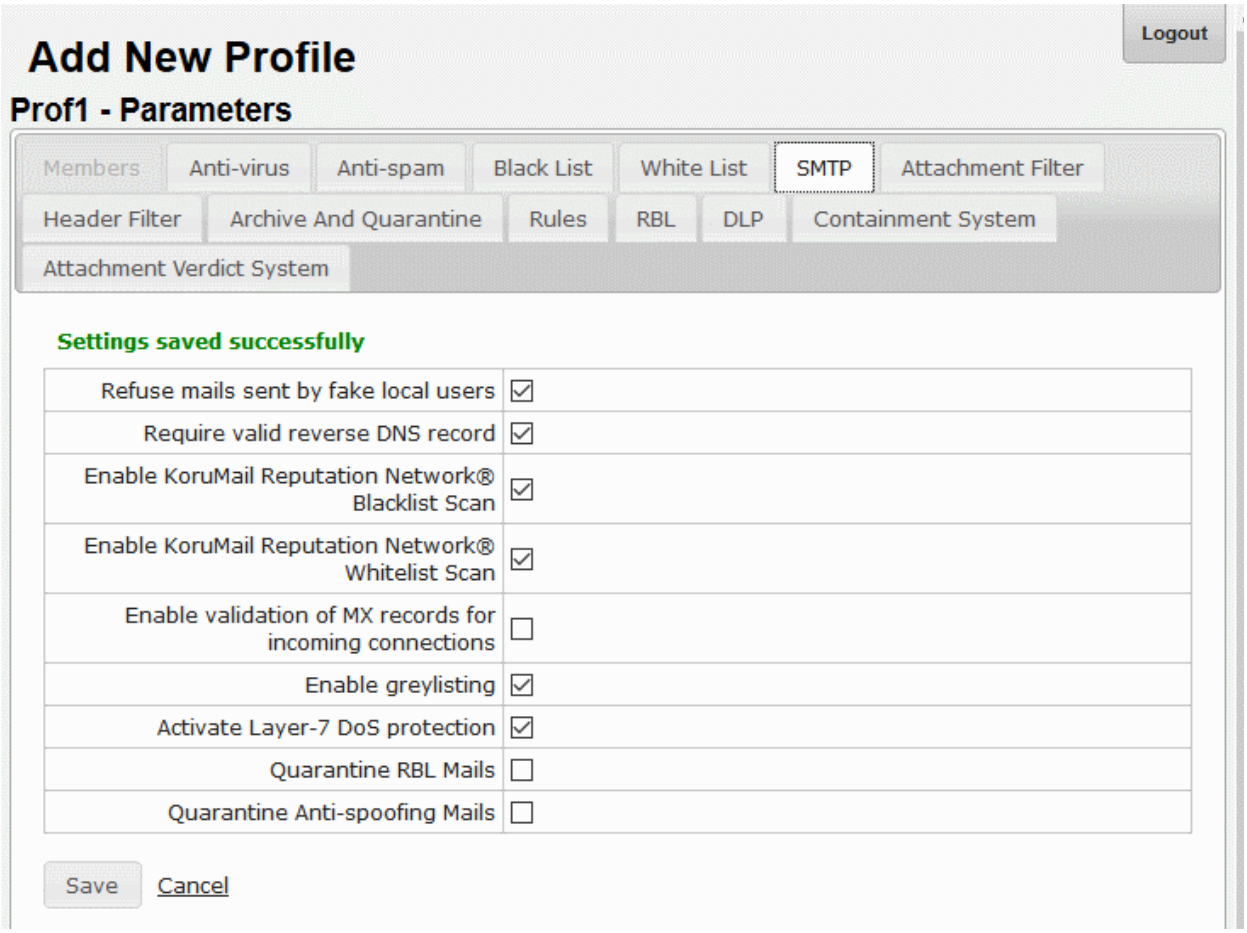


- Repeat the process to add more files.
- To remove a file, click the 'Clear' link beside it.
- To remove all the added files, click the 'Clear All' button at the top right.
- To import the list from the files, click the 'Save' button.

- To delete a whitelist type from the list, click the button under the 'Action' column header and click 'OK' in the confirmation screen.
- To remove all the whitelisted sources, click the 'Delete all' link and click 'OK' in the confirmation screen.

SMTP

- Click the 'SMTP tab



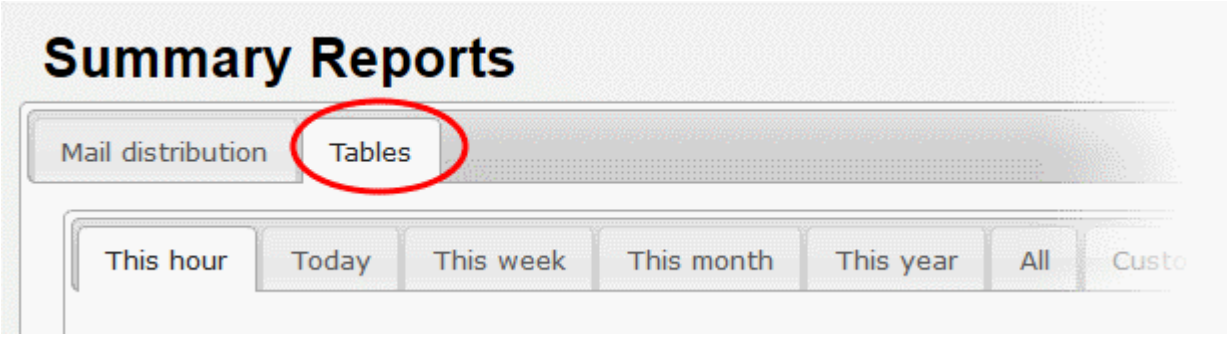
Profiles: SMTP Settings - Table of Parameters	
Parameter	**Description**
Refuse mails sent by fake local users	If enabled, Dome Antispam checks the 'From' details of an outgoing message with that of the added users and rejects if the users' details are not available.
Require valid reverse DNS record	If enabled, the added domains should have a valid reverse DNS record for the mails to be processed and delivered
Enable Dome Antispam Reputation Network® Blacklist Scan	If enabled, mails are scanned for blacklist sources listed in the Dome Antispam Reputation Network® (KRN) servers. Please note the KRN server setting should be enabled in the KRN module.
Enable Dome Antispam Reputation Network ® whitelist Scan	If enabled, mails are scanned for whitelist sources listed in the Dome Antispam 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, Dome Antispam 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 Dome Antispam 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, Dome Antispam accepts the mail and initiates the filtering process.

Activate Layer-7 DoS protection	If enabled, Dome Antispam will activate the Layer 7 Denial of Service protection feature.
Quarantine Antispoofing Mails	If enabled, the spoofing mails will be Quarantined.
Quarantine RBL Mails	If enables, the RBL mails will be Quarantined.

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

Attachment Filter

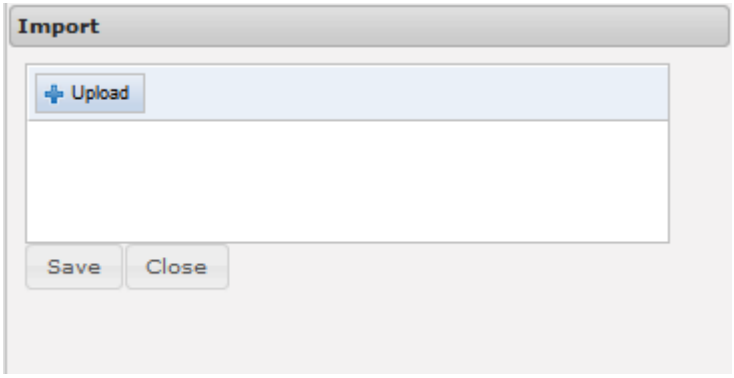
- Click the 'Attachment Filter' tab



Profiles: Attachment Filter Settings - Table of Column Descriptions	
Column Header	**Description**
Addition	Enter the keyword that should be scanned for the attachments
Condition	Select the condition from the drop-down. The options available are: • Contains • Equals to • Starts with • Ends with
Action	Select the action to be performed when the condition is met for an attachment in a mail. The options available are: • Reject - The mail will be rejected and a reject response will be sent to the sender's mail server. • 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.
	Allows you to add an attachment filter rule after filling the fields in the row

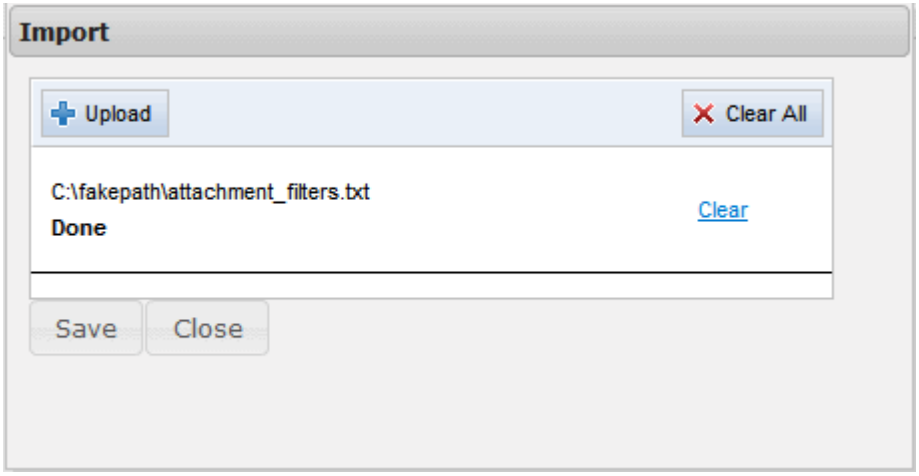
		Allows you to delete attachment filter rule from the list

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



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

The file will be added.

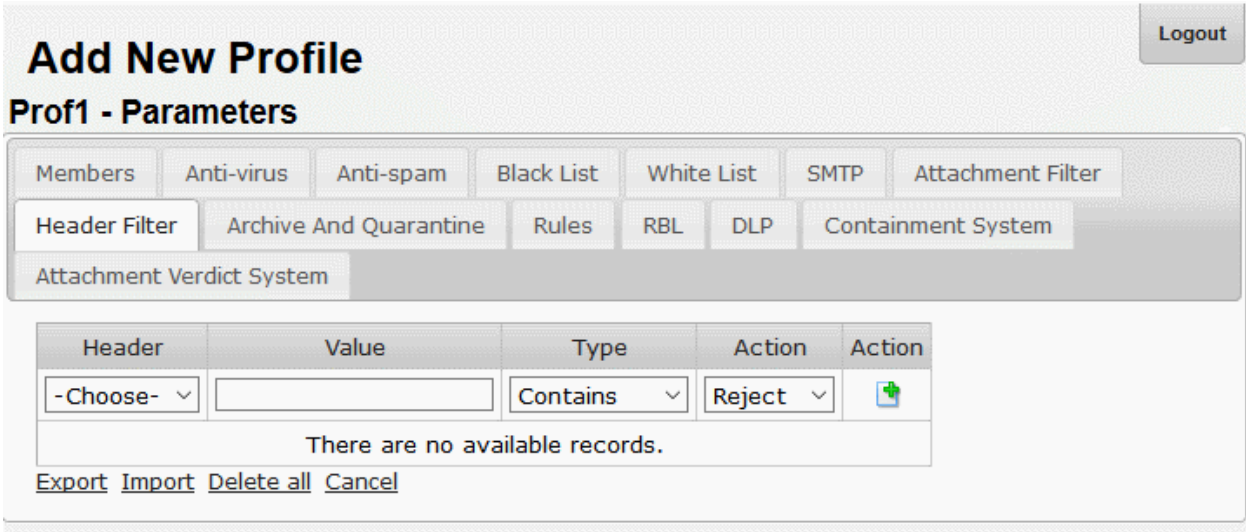


- Repeat the process to add more files.
- To remove a file, click the 'Clear' link beside it.
- To remove all the added files, click the 'Clear All' button at the top right.
- To import the list from the files, click the 'Save' button.

- To delete an 'Attachment Filter' rule from the list, click the button under the last column and click 'OK' in the confirmation screen.
- To remove all the 'Attachment Filter' rules, click the 'Delete all' link and click 'OK' in the confirmation screen.

Header Filter

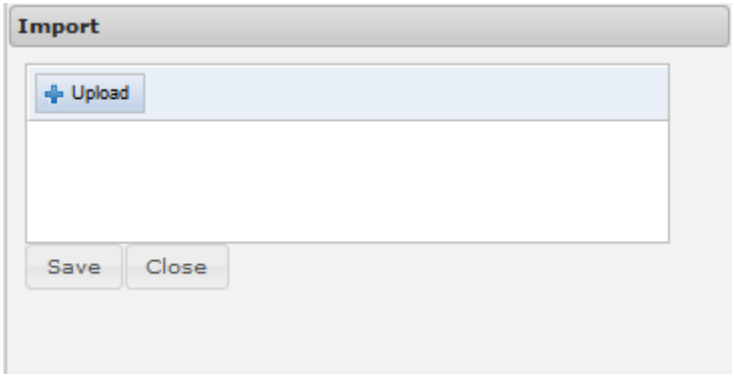
- Click the 'Header Filter' tab



Profiles: Header Filter Settings - Table of Column Descriptions		
Column Header	**Description**	
Header	Select the header type that you want to add a 'Header Filter' rule for. The choices available are: • Subject • Received • To • From	
Value	Enter the keyword that should be scanned for the selected header type.	
Type	Select the condition from the drop-down. The options available are: • Contains • Equals to • Starts with • Ends with	
Action	Select the action to be performed when the condition is met for a 'Header Filter' rule in a mail. The options available are: • Reject - The mail will be rejected and a reject 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

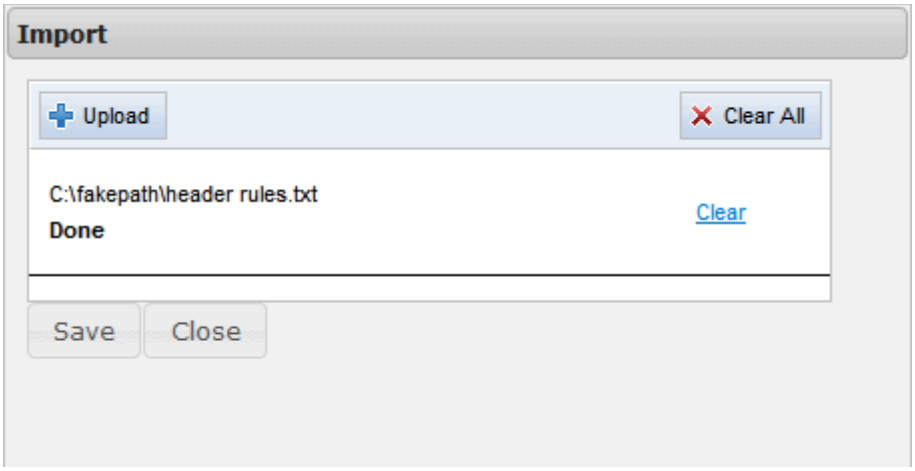
- To save the list of 'Header Filter' rules, click the 'Export' link and save it to your system

- 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.

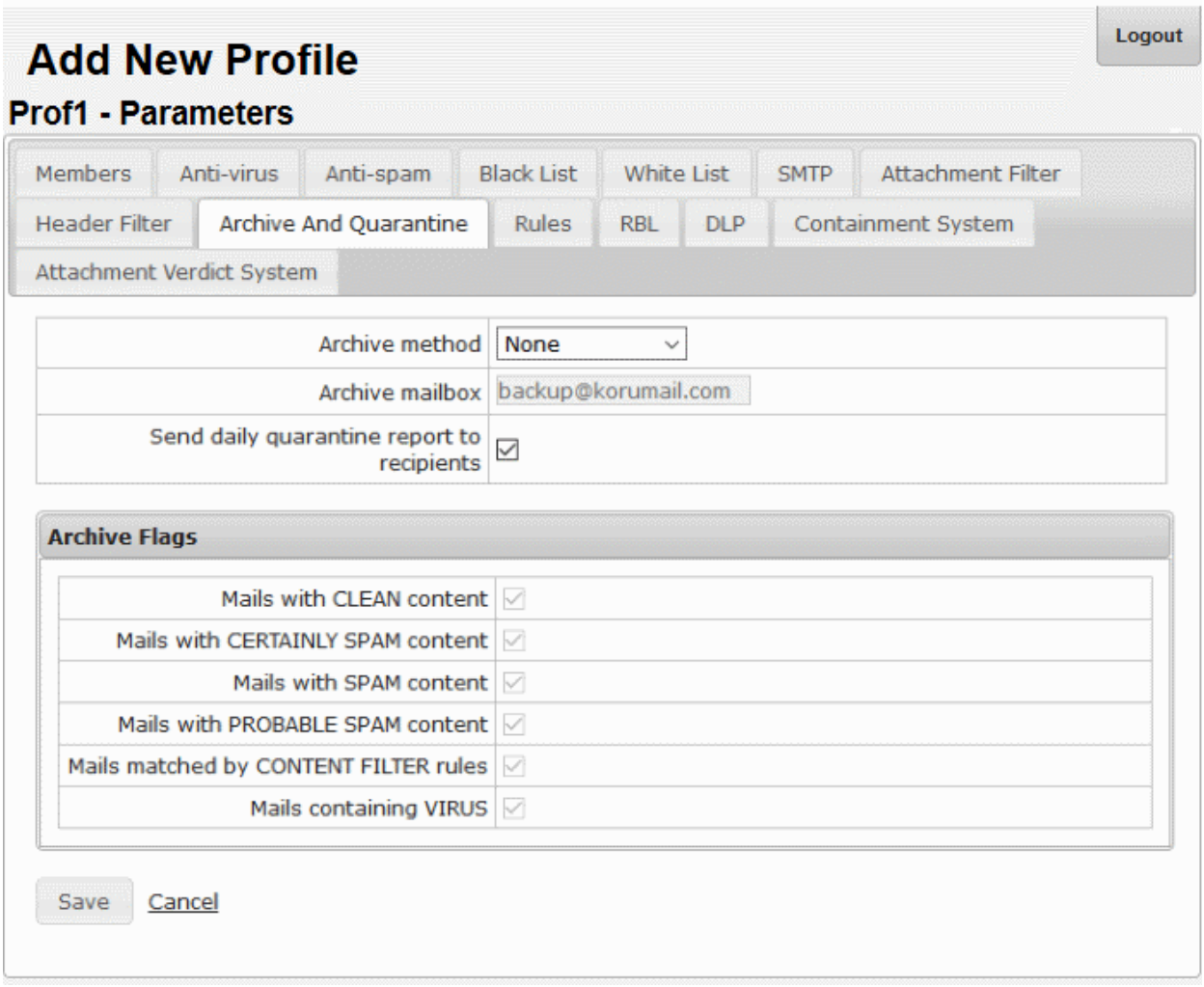


- Repeat the process to add more files.
- To remove a file, click the 'Clear' link beside it.
- To remove all the added files, click the 'Clear All' button at the top right.
- To import the list from the files, click the 'Save' button.

- To delete a 'Header Filter' rule from the list, click the button under the last column and click 'OK' in the confirmation screen.
- To remove all the 'Header Filter' rules, click the 'Delete all' link and click 'OK' in the confirmation screen.

Archive and Quarantine

- Click the 'Archive and Quarantine' tab



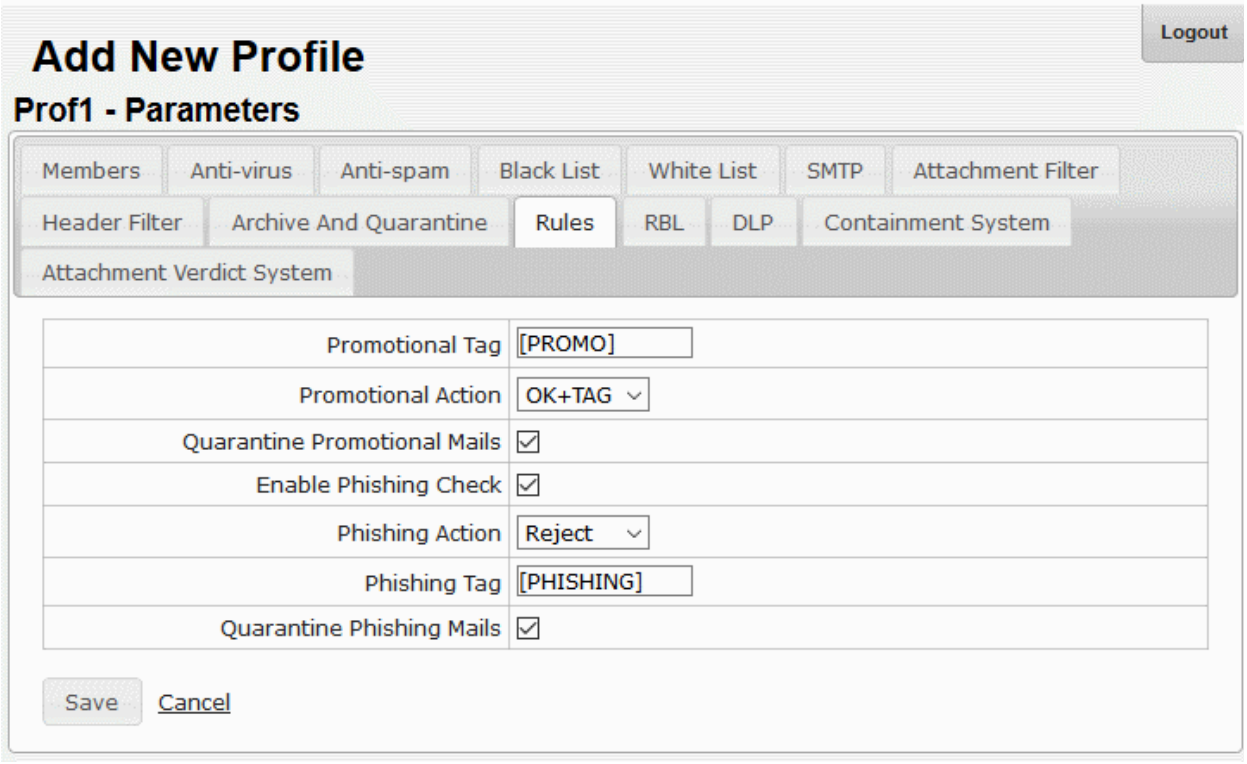
Profiles: Archive and Quarantine Settings - Table of Parameters	
Parameter	**Description**
Archive method	Select how the mails should be archived from the drop-down. The options available are: • None - The mails are not archived • Forward - The mails are forwarded to the mail address entered in the next row 'Archive mailbox' • Disk - The mails are stored in local disk • Disk + Forward - The mails are stored in local disk and a copy is forwarded to the mail address entered in the next row 'Archive mailbox' Please note the archived and quarantined mails are removed from the disk as per the configuration done in the 'Quarantine & Archive Settings' interface.
Archive mailbox	This field becomes active only when an archive method is selected in the first row. Enter the mail address to which the archived and quarantined mails will be sent.
Send daily quarantine report to recipients	If enabled, the users will receive daily reports of their quarantined mails. Users can view their quarantined mails in the 'Dome Antispam Quarantine Webmail' interface by clicking the 'Quarantine Webmail' link in the 'Login' screen.
Archive Flags	

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

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

Rules

- Click the 'Rules' tab



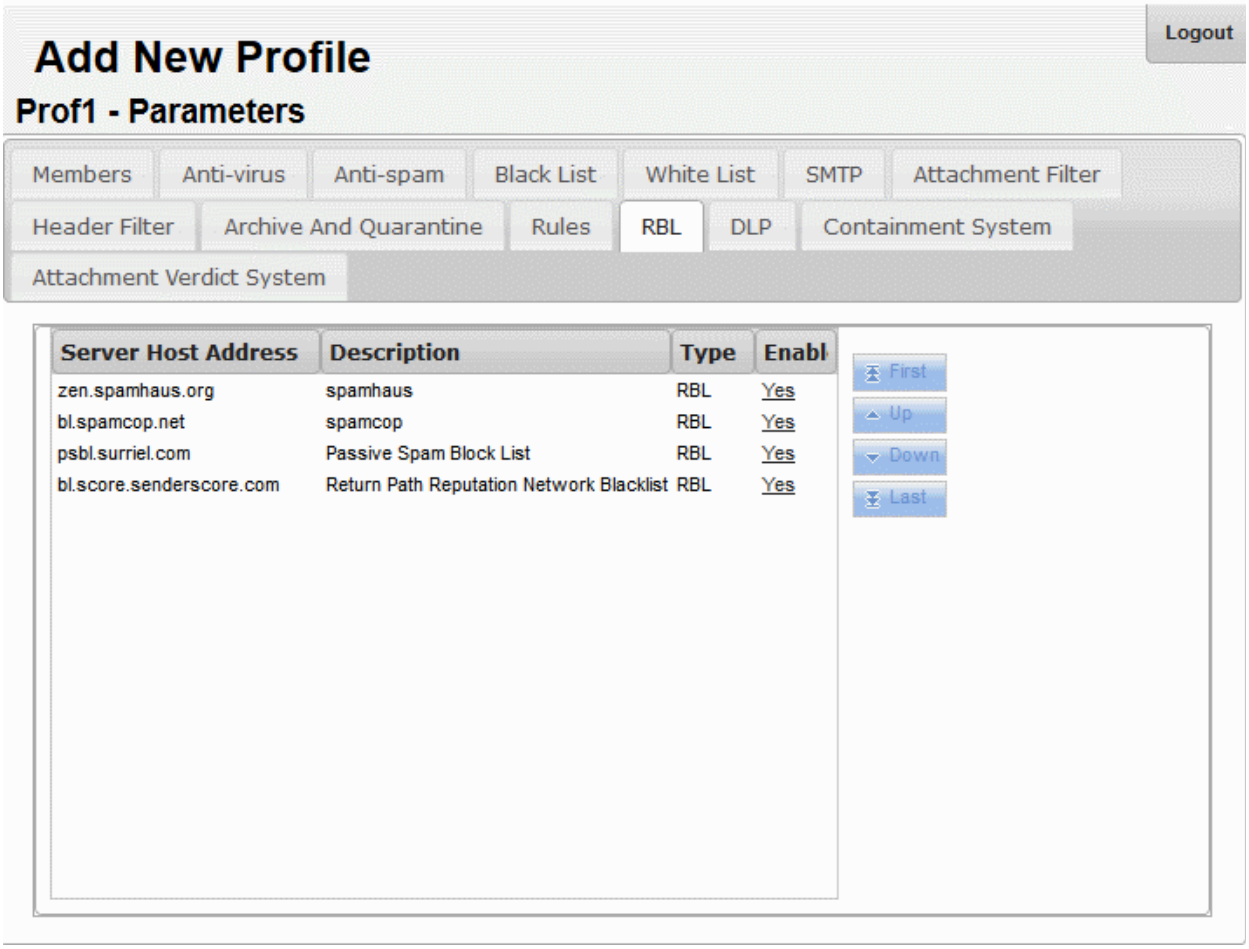
Rules Settings - Table of Parameters	
Parameter	**Description**
Promotion Tag	Promotional emails will be sent to the recipient with the a tag as entered in this field.
Promotional Action	Select the action to be performed when the condition is met for a 'Rules' setting in a promotional mail. The options available are:

	• OK + TAG - The tagged mail will be sent to the recipient. • Reject - The mail will be rejected and a reject response will be sent to the sender mail server. • Discard - The mail will be quarantined. Daily notifications will be sent to user with details of quarantined emails. The user can view the email using the Quarantined Email web interface.
Enable Phishing Check	If enabled, checks for phishing emails.
Phishing Action	Select the action to be performed when the condition is met for a 'Rules' setting in a phishing mail. The options available are: • OK + TAG - The tagged mail will be sent to the recipient. • Reject - The mail will be rejected and a reject response will be sent to the sender mail server. • Discard - The mail will be quarantined. Daily notifications will be sent to user with details of quarantined emails. The user can view the email using the Quarantined Email web interface.
Phishing Tag	Phishing emails will be sent to the recipient with the a tag as entered in this field.
Quarantine Phishing Emails	If enabled, phishing mails will be Quarantined.

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

Realtime Blackhole List (RBL)

- Click the 'RBL' tab



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

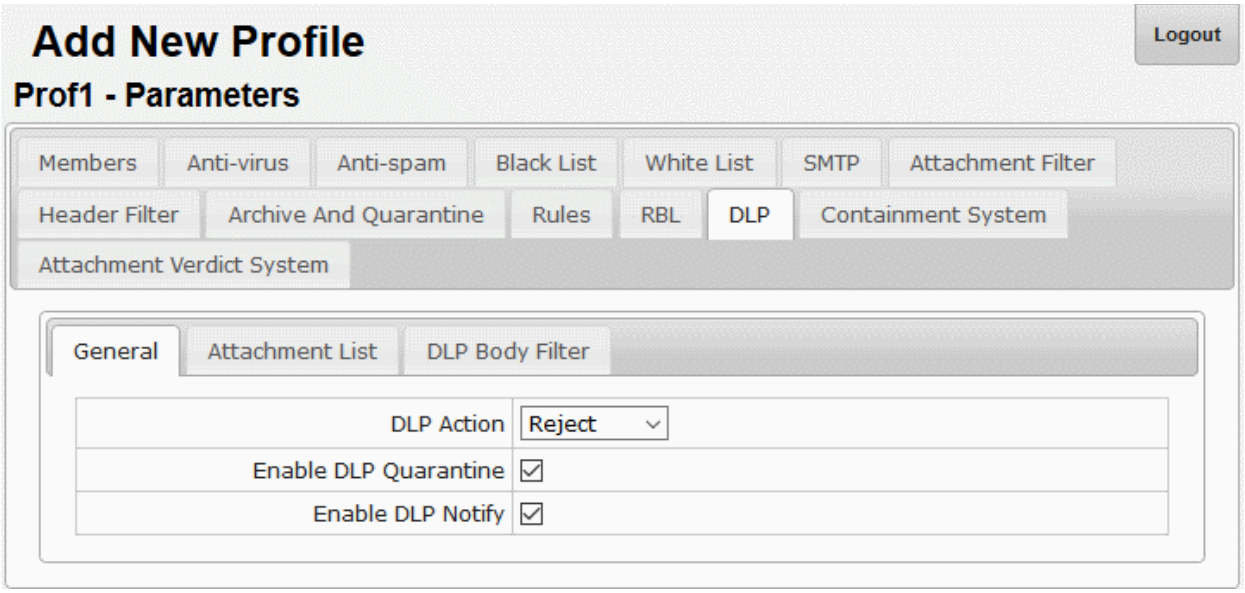
RBL Servers - Table of Column Descriptions	
Column Header	**Description**
Server Host Address	The address of the RBL server.
Description	The description provided at the time of adding the RBL server.
Type	The type of block list selected.
Enable	Allows you to activate or deactivate a RBL server in the list. If a server is disabled, Dome Antispam 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.

Data Leak Prevention (DLP)

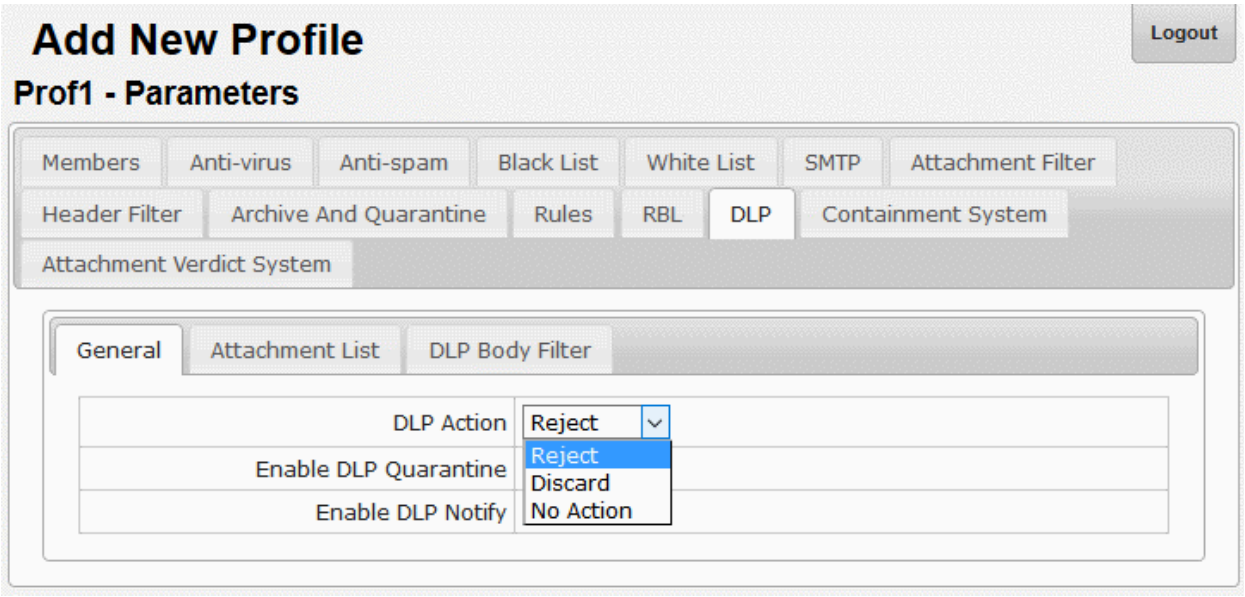
The DLP feature is capable of scanning mails for important key words such as credit card, social security numbers, attachments and takes action as per the settings. Please note that the DLP module should be enabled for the settings configured here to take effect. Refer to the section 'Data Leak Prevention'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

- Click the 'DLP' tab



DLP Action

These settings determine what action should be taken if Dome Antispam 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.

DLP Quarantine

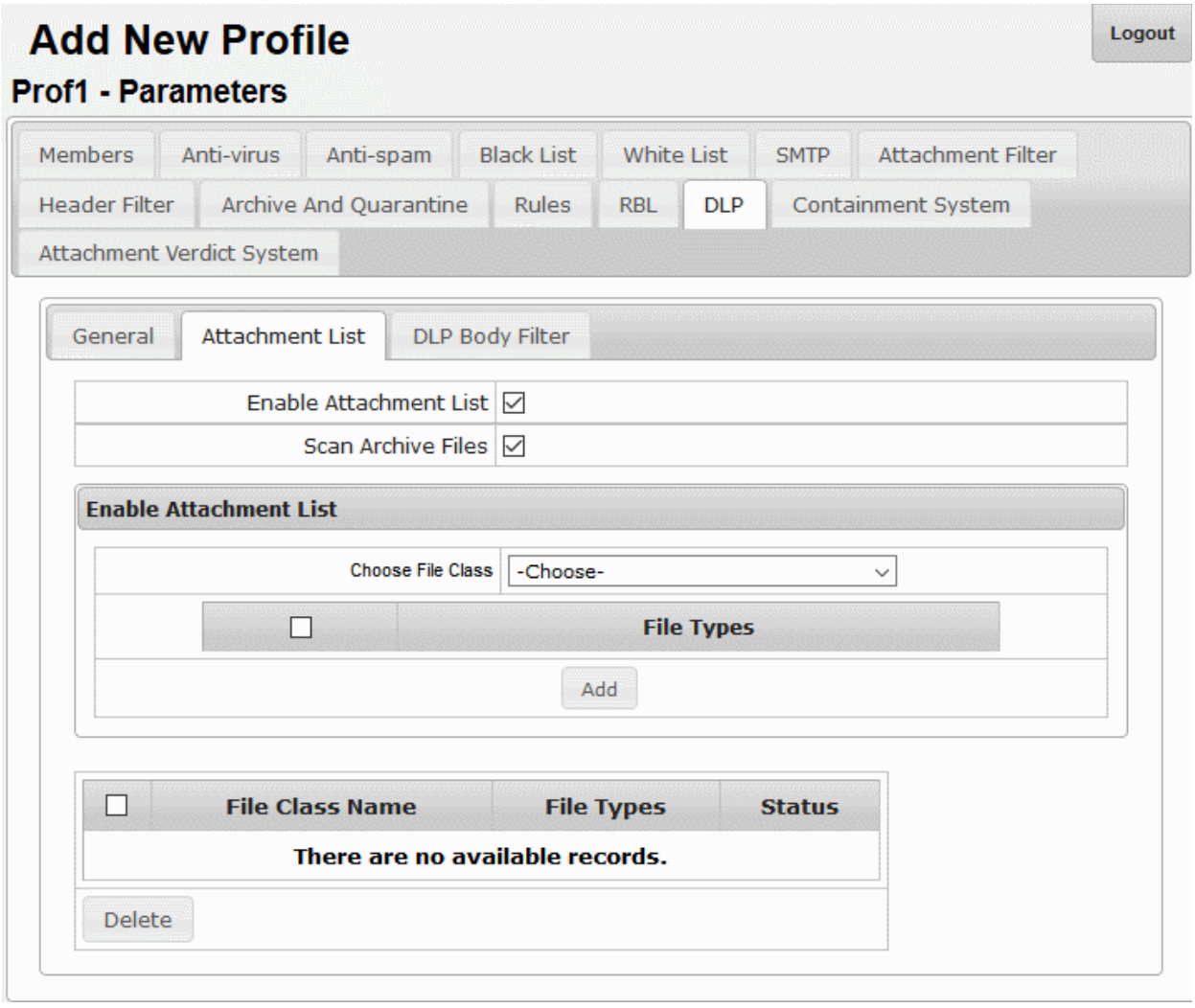
- Click the 'DLP Quarantine' bar
- Select the check box beside 'Enable DLP Quarantine' to quarantine mails with data leak. Please note the setting in 'DLP Action' should be 'Discard' for mails to quarantined.

DLP Notify

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

Attachment List

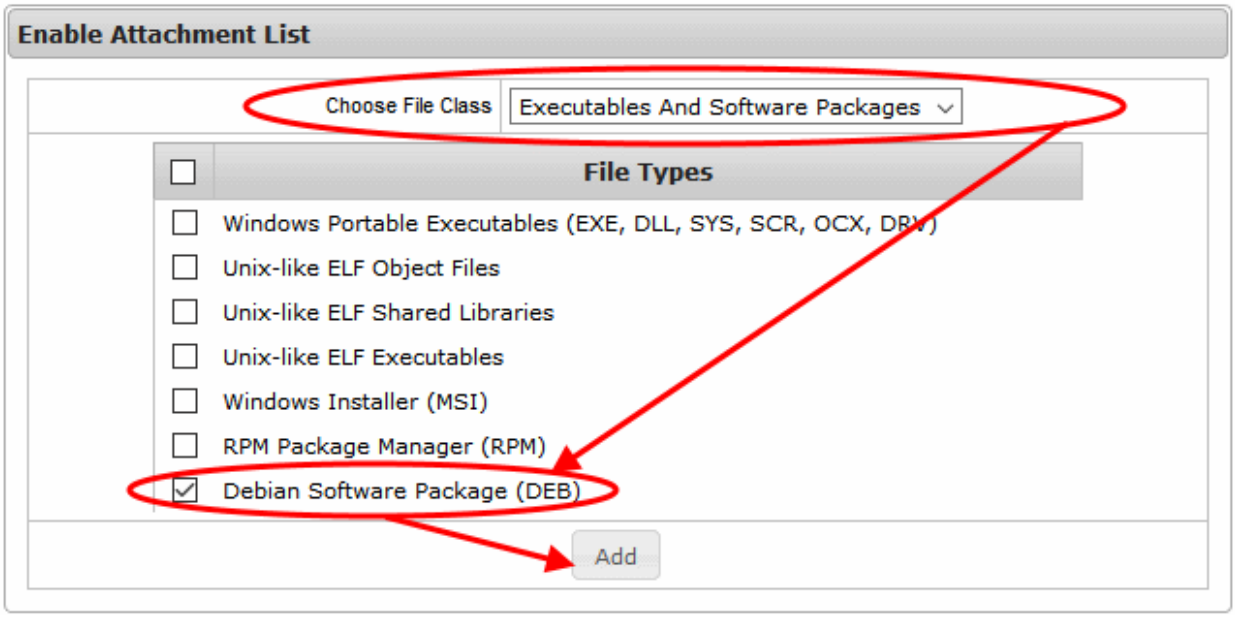
- Click the 'Attachment List' bar



- **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

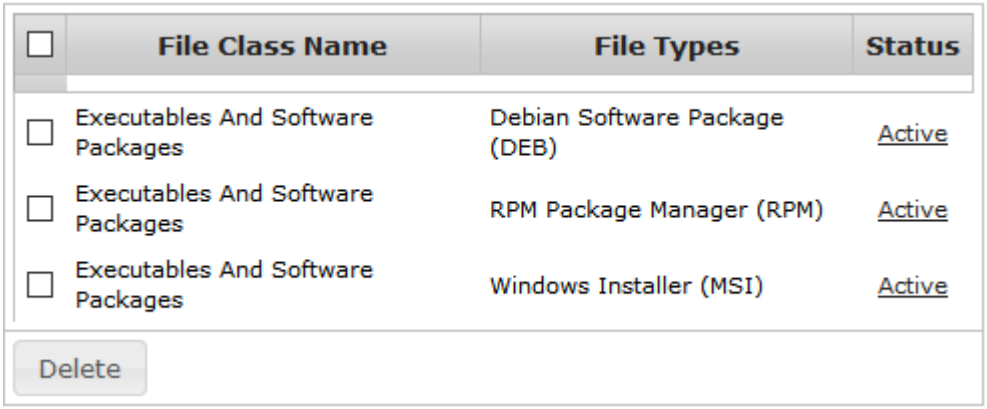
- Select the file class from the 'Choose File Class' drop-down



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.

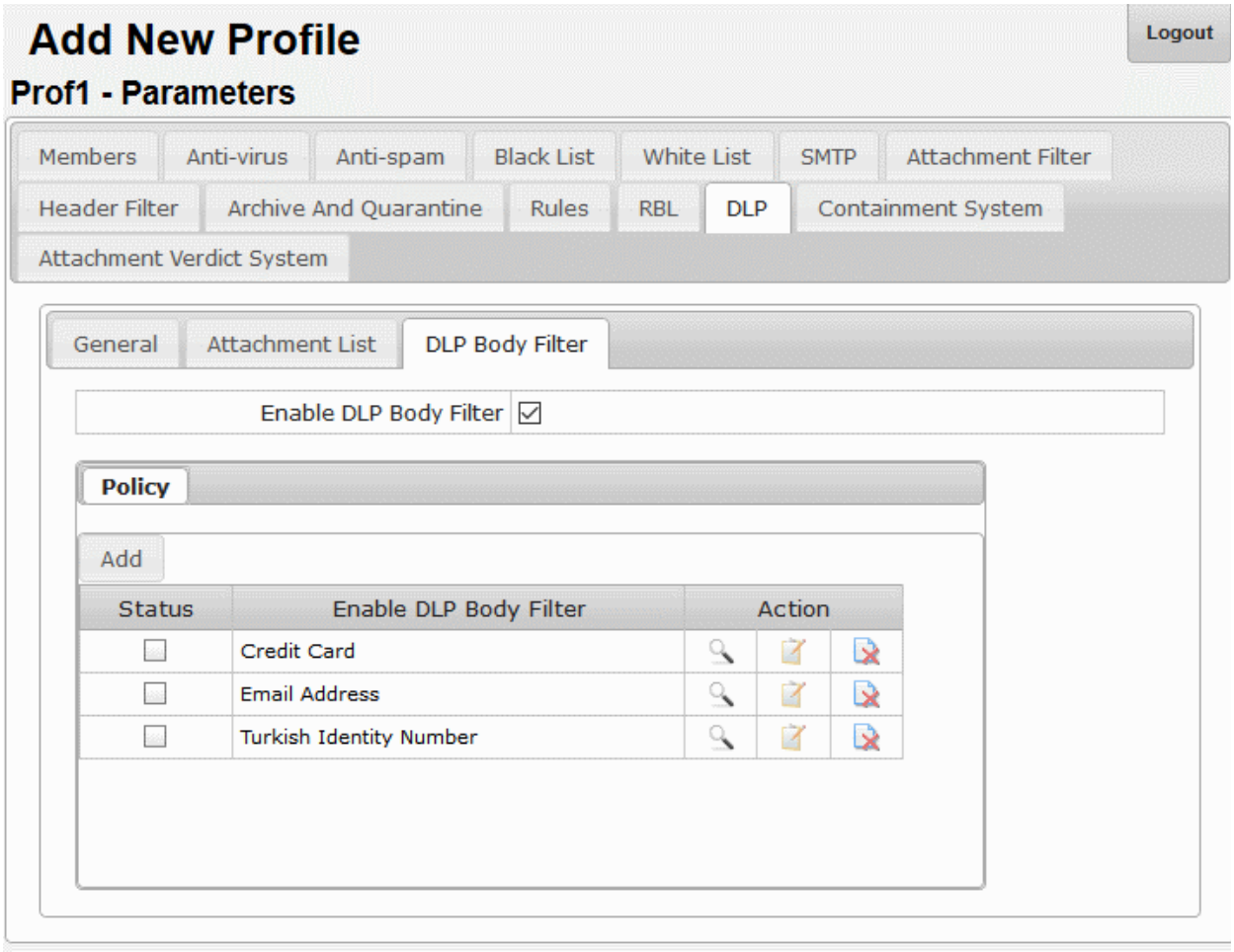
The added file types for the selected file class will be displayed in the table below the first table.



- 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'. Dome Antispam comes with three predefined DLP Body Filters and allows the administrators to add more filters as required.

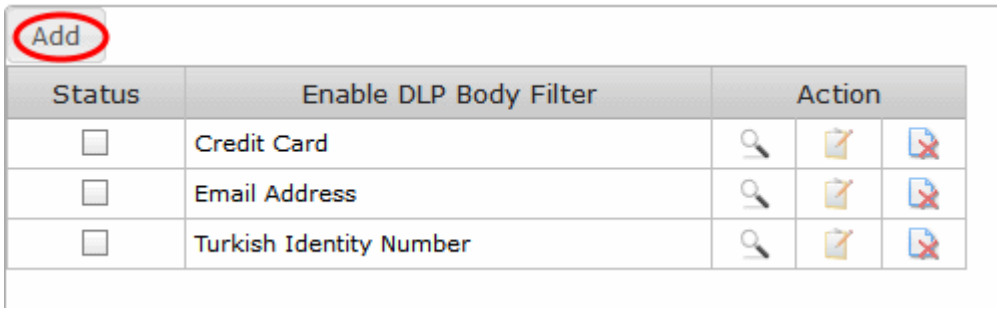


- **Enable DLP Body Filter**: Select the check box to apply the configured body filters

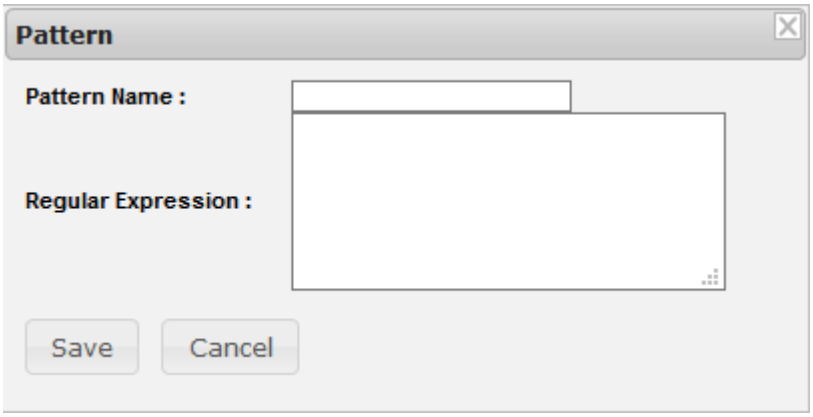
Profiles: DLP Body Filter Settings - Table of Column Descriptions		
Column Header	**Description**	
Status	Select the check box to enable the filter	
Enable DLP Body Filter	The name of the filter	
Action		Allows to view the details of the body filter
		Allows to edit a body filter
		Allows to delete a body filter

To add a new DLP body filter

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



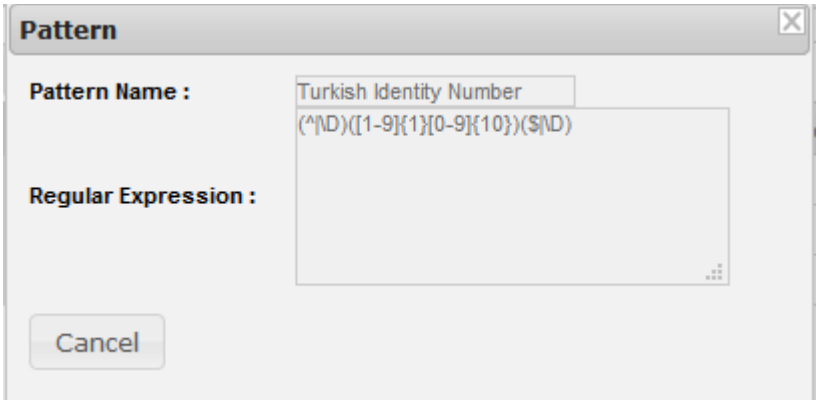
The filter 'Pattern' screen will be displayed.



- **Pattern Name**: Enter the name of the filter pattern
- **Regular Expression**: Enter the regular expression to define the search pattern. To know more about Regular Expression, 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

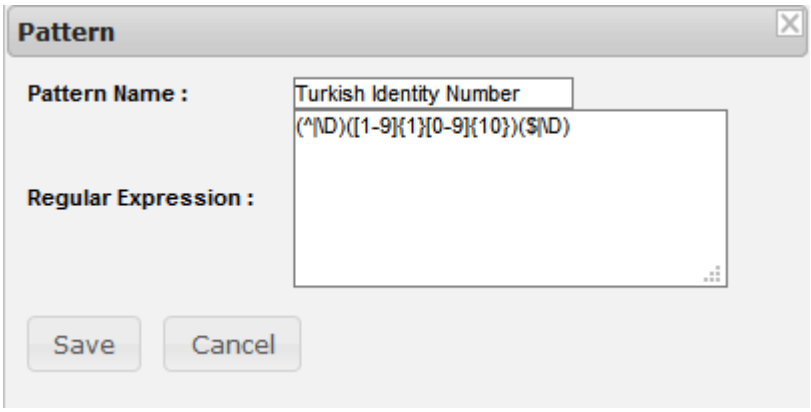
- Click the icon beside a body filter that you want to view the details



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

To edit a body filter

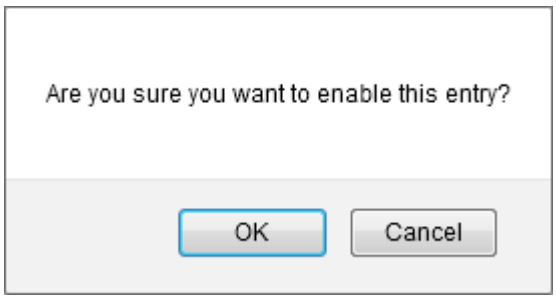
- Click the icon beside a body filter that you want to edit the details



- 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

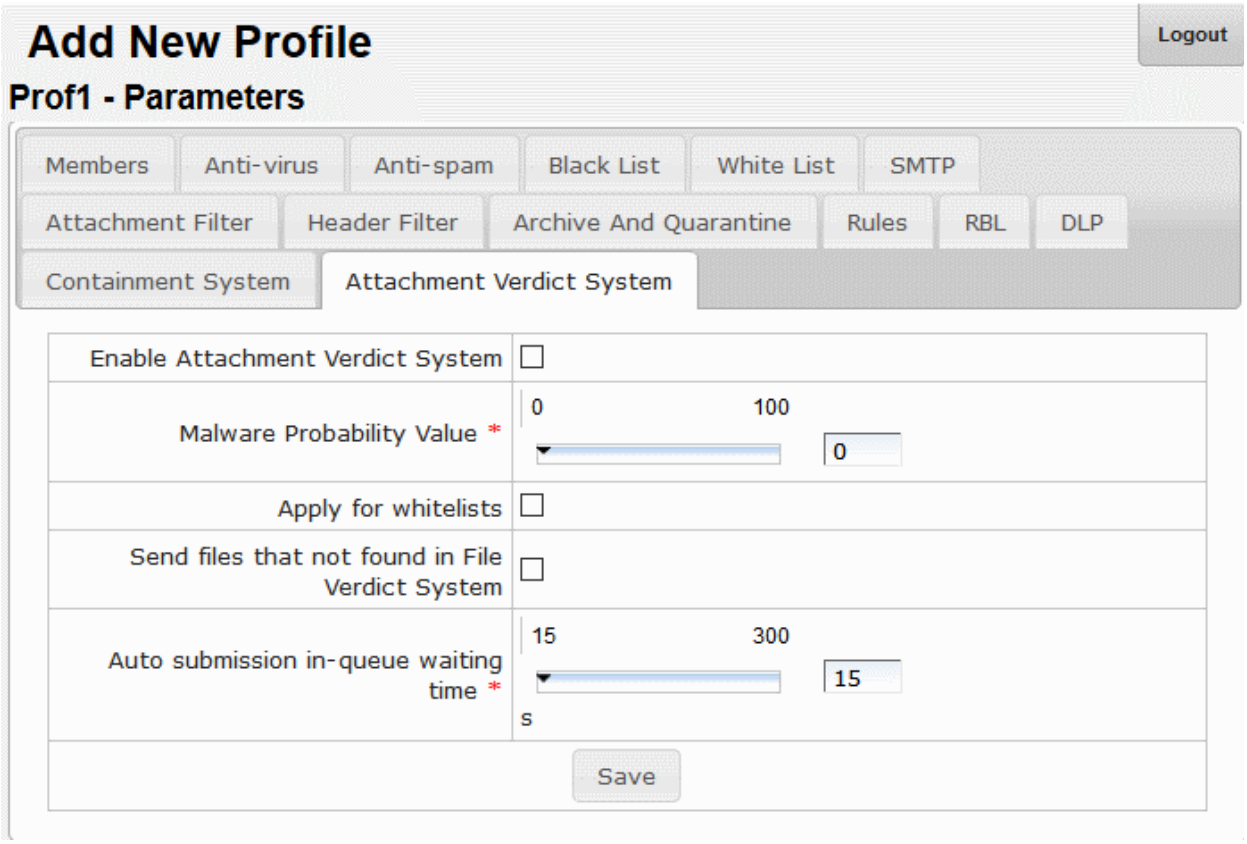


- Click 'OK' to confirm the deletion.

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.

- To open the attachment verdict system area, click Profile Management > Attachment Verdict System.



Attachment Verdict System - Table of Column Headers	
Column Header	**Description**
Enable Attachment Verdict System	If enabled, Dome Antispam will automatically check the trust rating of Windows executables and pdf files in Comodo's file look up server (FLS). The verdict from the FLS can be 'Clean', 'Malware' or 'Unknown'. Clean attachments will be allowed to proceed while malware attachments will be automatically quarantined (providing 'Quarantine mails containing viruses' is enabled in the antivirus section of the profile). 'Unknown' files will be submitted to Comodo's real-time file analysis system, Valkyrie, for behavior testing. Valkyrie's tests will determine whether the unknown file is clean or malware and apply the appropriate action as mentioned above.
Malware Probability Value	The threshold at which Dome Antispam 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 Dome Antispam is more tolerant/less likely to class attachments as malware.
Apply for whitelists	If enabled, Dome Antispam will also analyze white-listed sources.
Send files that not found in File Verdict System	If enabled, Dome Antispam will upload files rated 'Unknown', to the attachment verdict system for detailed behavior analysis
Auto-submission in queue waiting time	Define in seconds how long Dome Antispam should wait before the submission times-out.

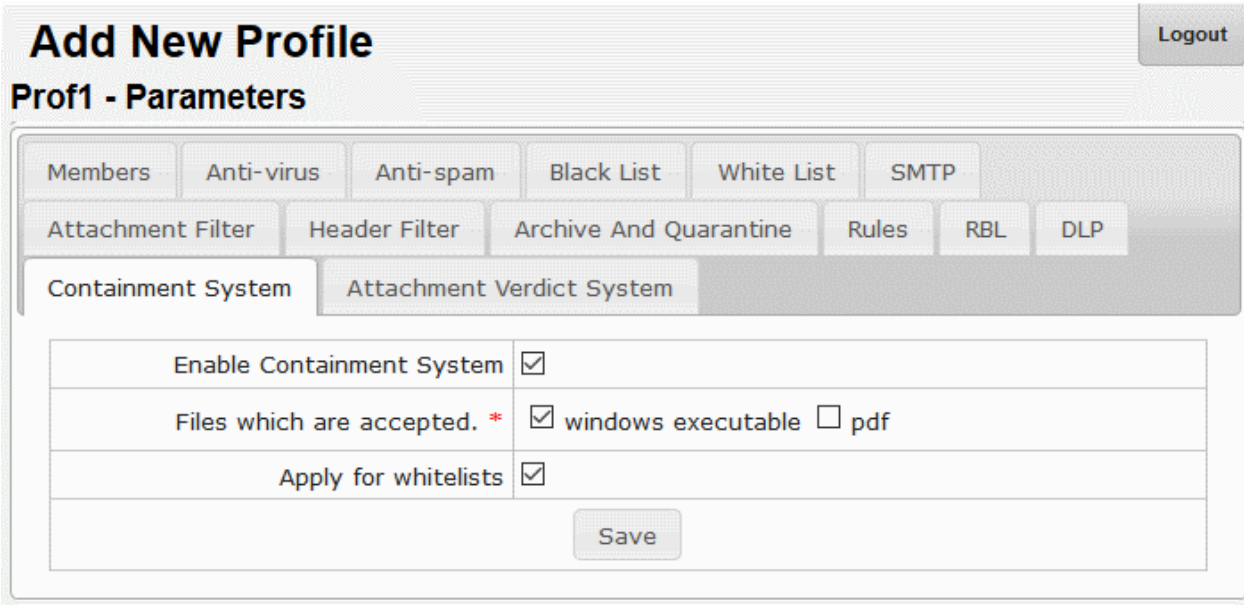
Please note that, if the 'Enable Attachment Verdict System is enabled' and the 'Send files that not found in File

Verdict System' is disabled, then the unknown files are not uploaded to Valkyrie for analysis. To view reports of attachment verdict system, refer to Attachment Verdict Reports.

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).

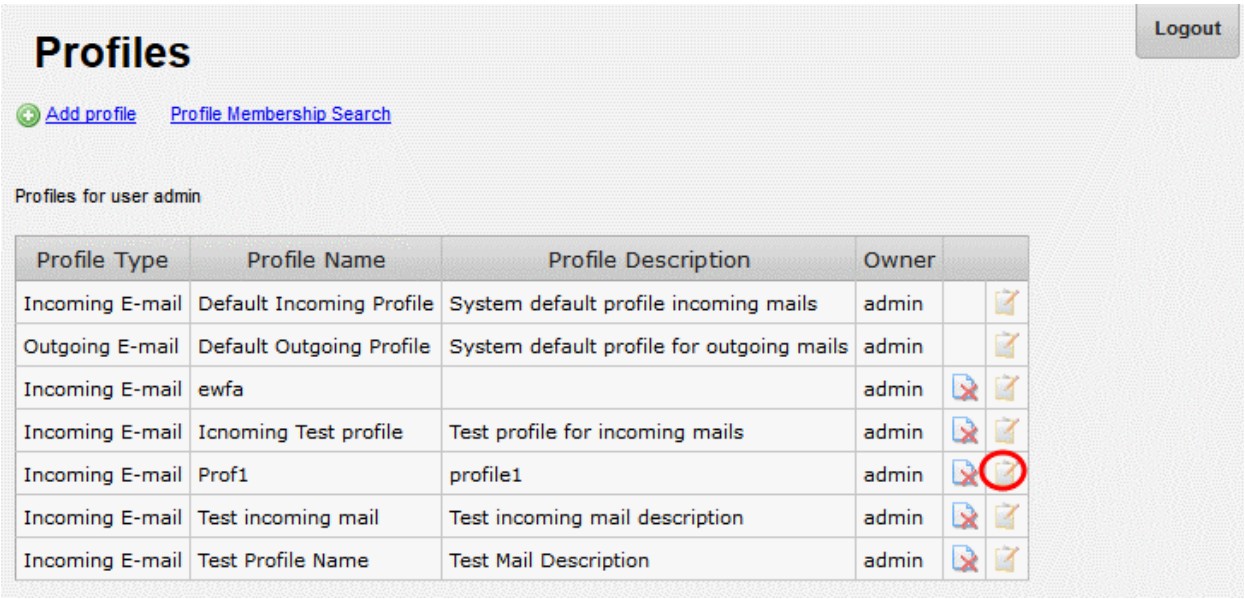
- Click 'Containment System' tab.



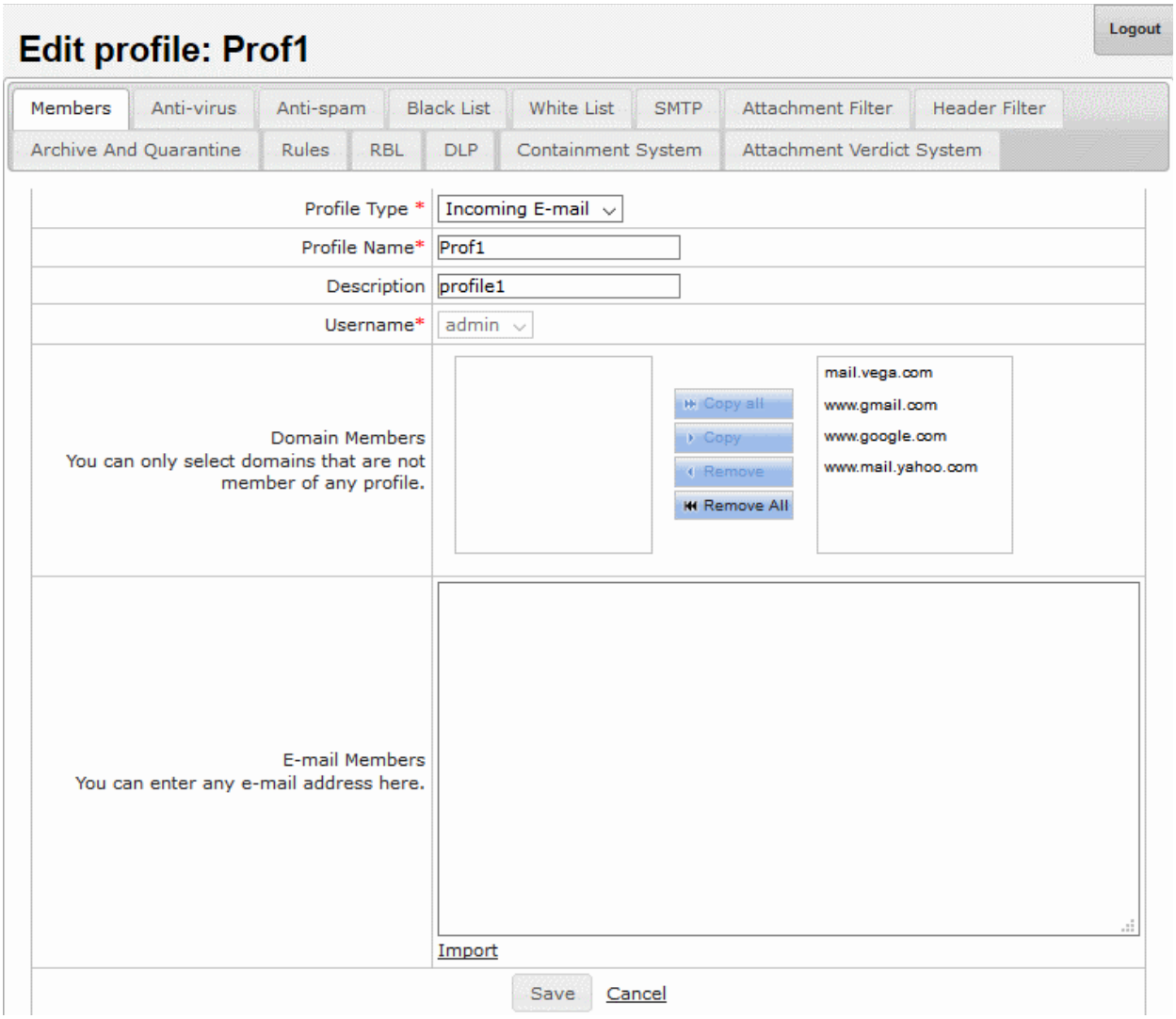
Containment System - Table of Column Headers	
Column Header	**Description**
Enable Containment System	If enabled, email attachments (pdfs and windows executables) will be 'wrapped' with containment code before delivery. This means they will open in an isolated, virtual environment known as the container, 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, Dome Antispam will also analyze white-listed sources.

6.2 Editing a Profile

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



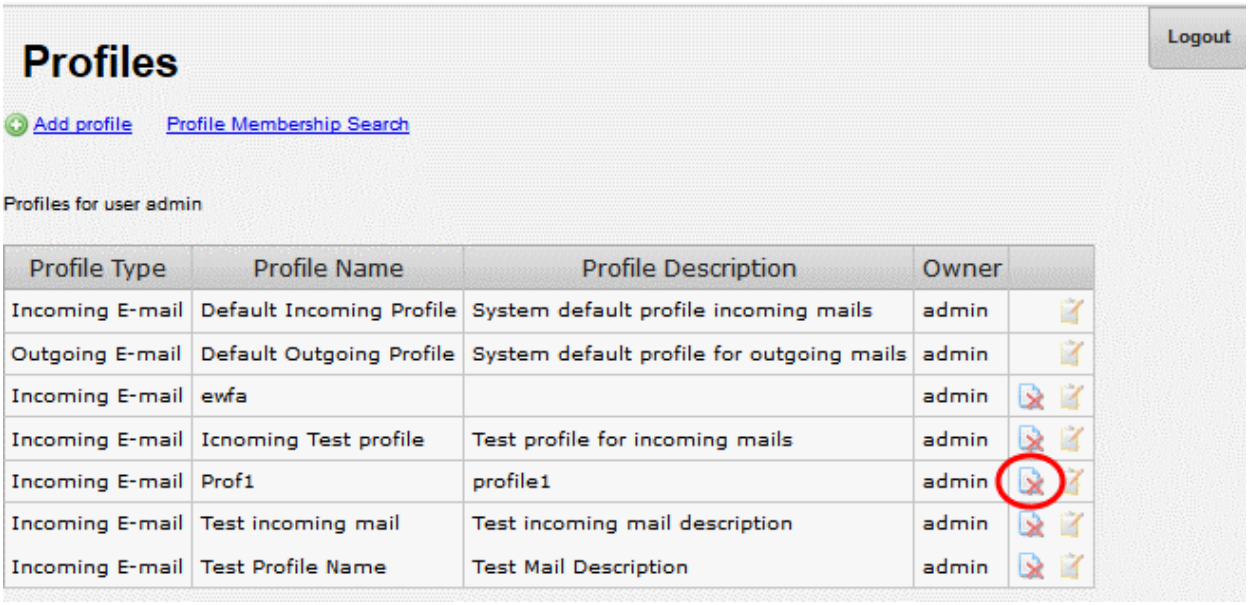
The 'Edit Profile' screen will be displayed.



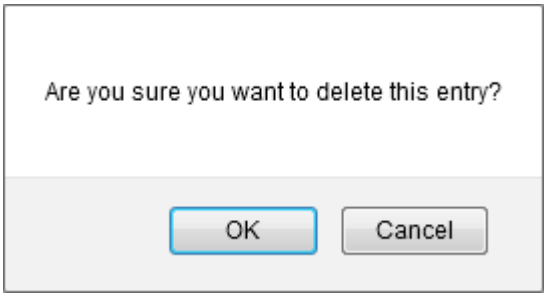
- Edit the parameters as required. The procedure is similar to adding a new profile. Refer to the section 'Adding and Configuring a New Profile' for more details.

6.3 Deleting a Profile

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



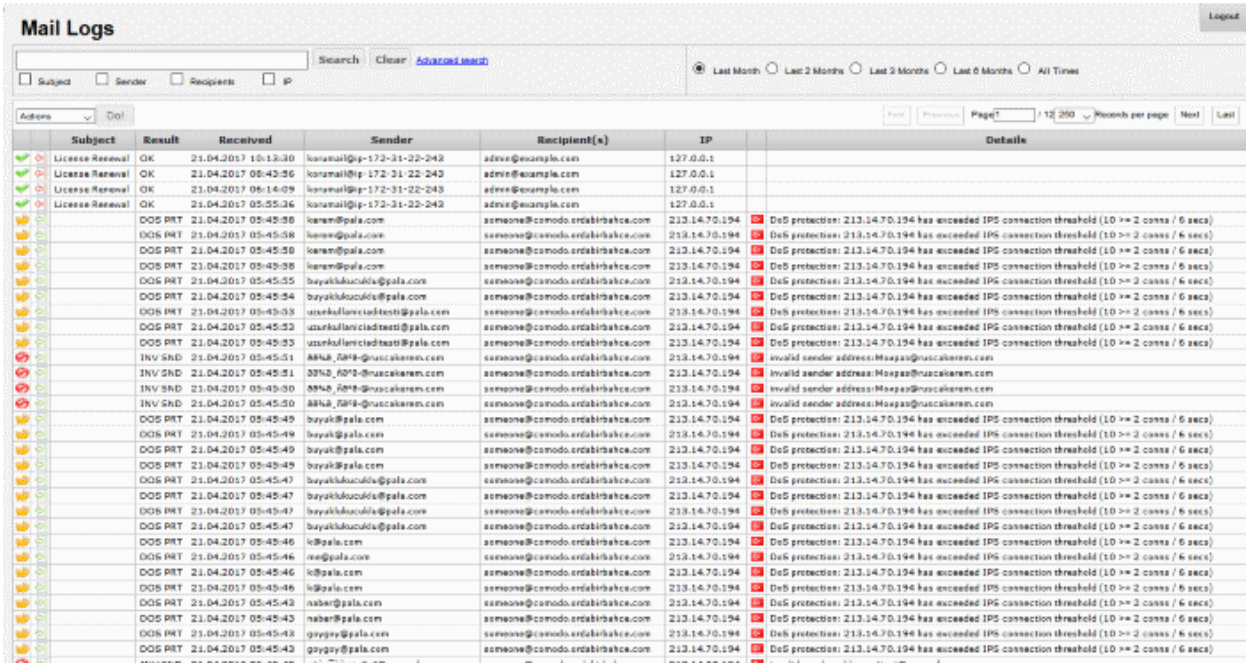
- Click 'OK' to confirm the deletion.



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 Dome Antispam provides comprehensive details of all mails for protected domains that were routed via Dome Antispam. 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.



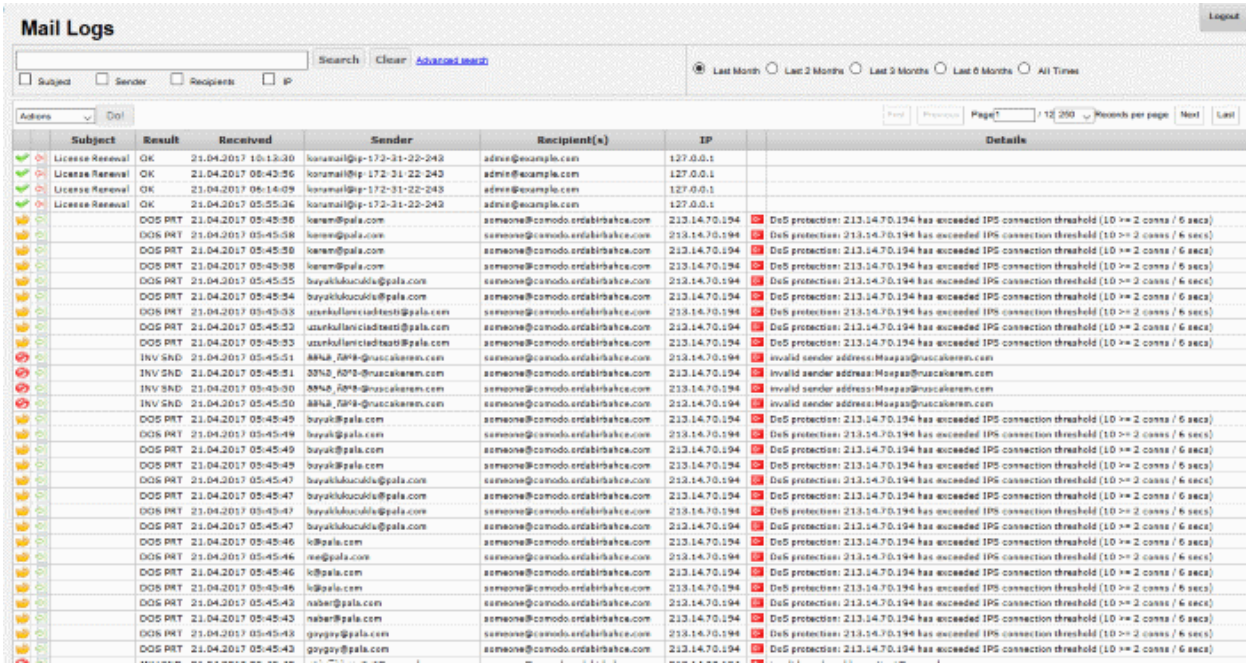
Refer to the following sections for more details:

- Mail Logs Report
- SMTP Queue Report
- Delivery Logs Report
- SMTP-AUTH Logs Report
- Summary Report
- Domain Report
- Attachment Verdict Reports

7.1 Mail Logs Report

The 'Mail Logs' report provides complete details of incoming and outgoing mails for all domains that have been added to Dome Antispam. The logs show the subject of the mail, date and time received by Dome Antispam, the result of the filtering process and more.

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

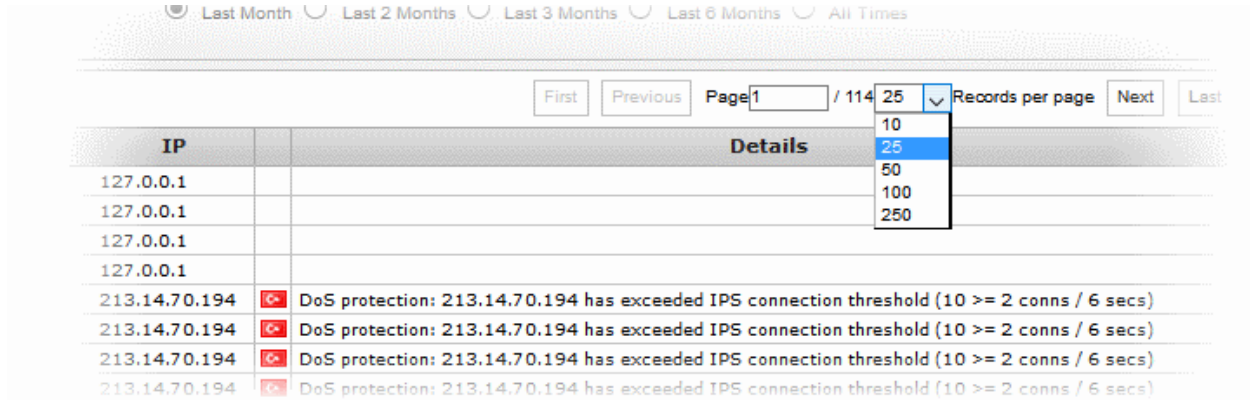


Mail Logs Report - Table of Column Descriptions	
Column Header	**Description**
Icon	Indicates the status of the mail after the filtering process. Placing your mouse cursor over an icon will show a description of the action. - Relayed: Indicates the mail has successfully passed the filtering process and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

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

To configure the number of records to be displayed per page

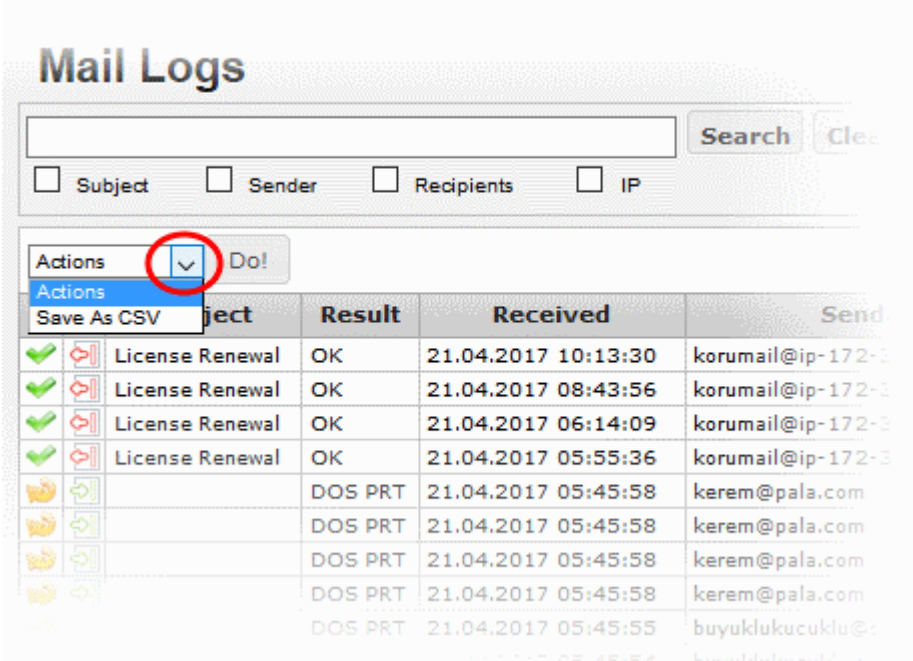
- Click the 'Records per page' drop-down



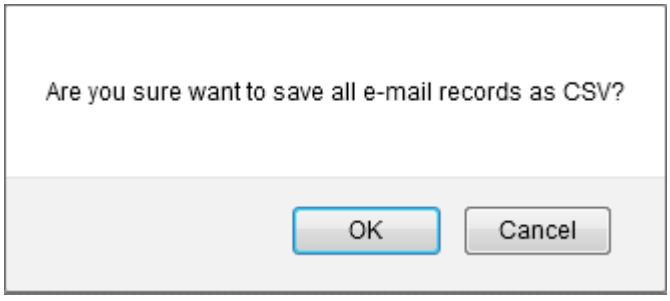
- Select the number of records per page to be displayed from the options.
- Click the 'First', 'Previous', 'Next' and 'Last' buttons to navigate to the respective pages.

To export the report to a CSV file

- Click the 'Actions' drop-down



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



- Download and save the report to your system.

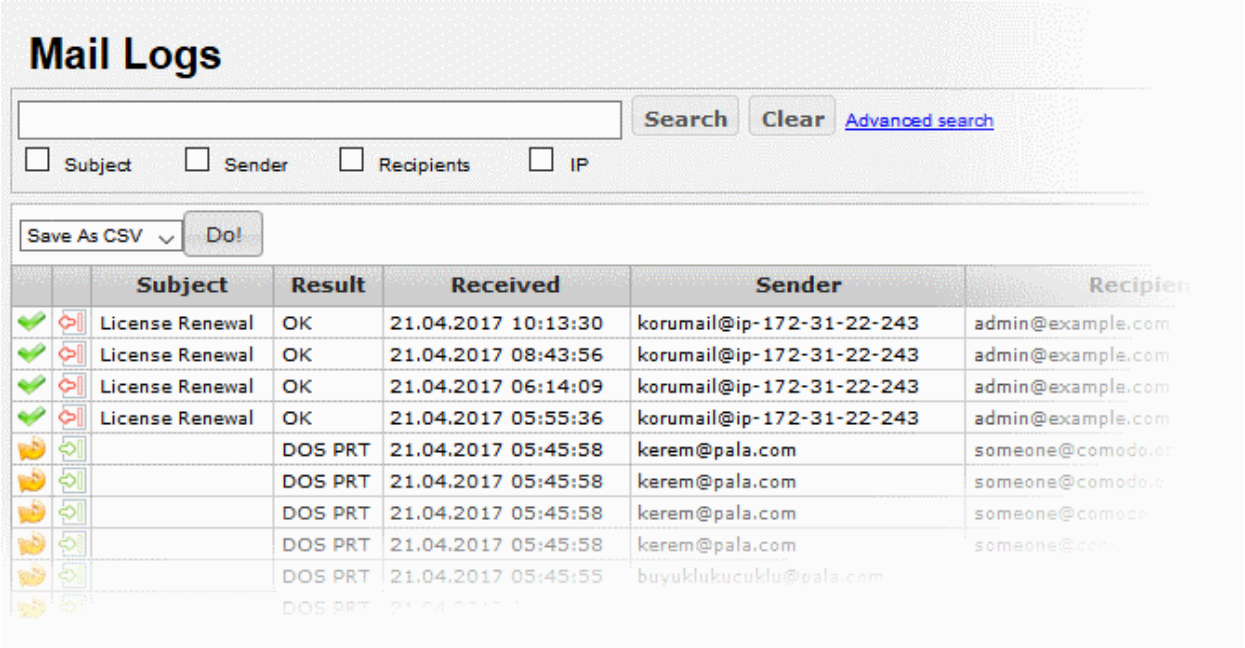
Search Options

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.

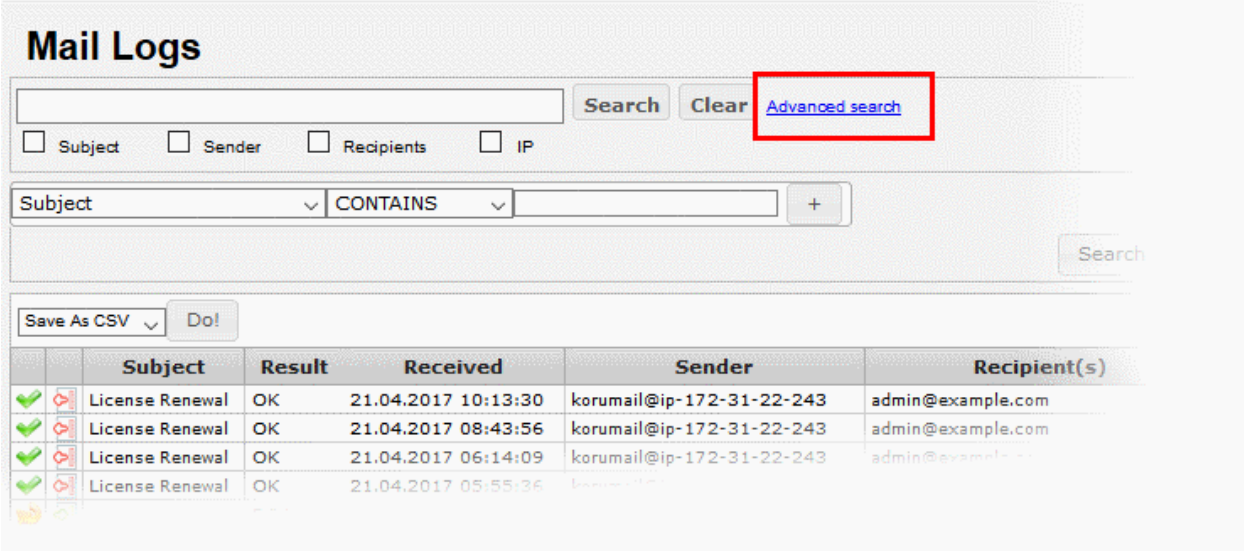


- To search for records based on the entries under 'Subject', 'Sender', 'Recipients' and / or 'IP' columns, enter the text or number fully or partially in the field and click the 'Search' button
- To search for records based on the entries under a particular column or columns, select the respective check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

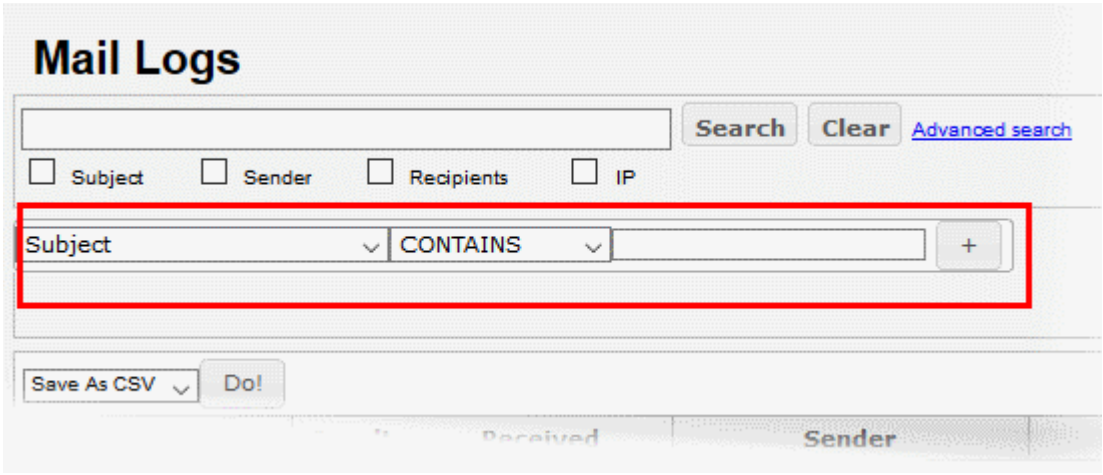
Advanced Search

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

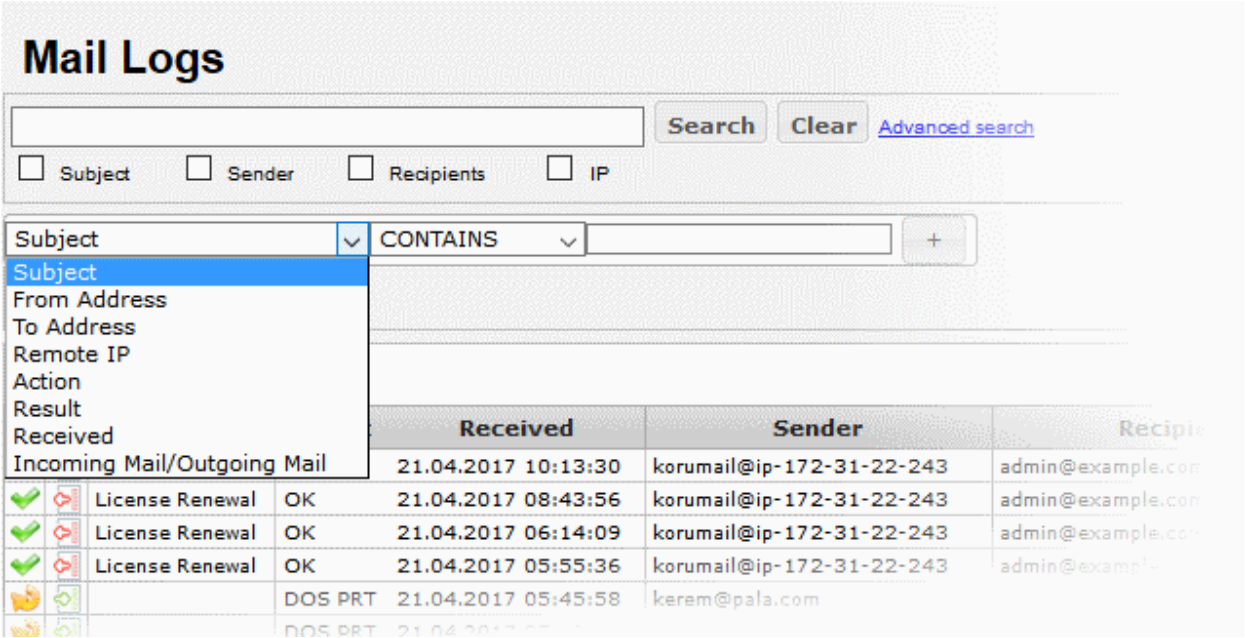
- Click the 'Advanced Search' link at the top of the screen.



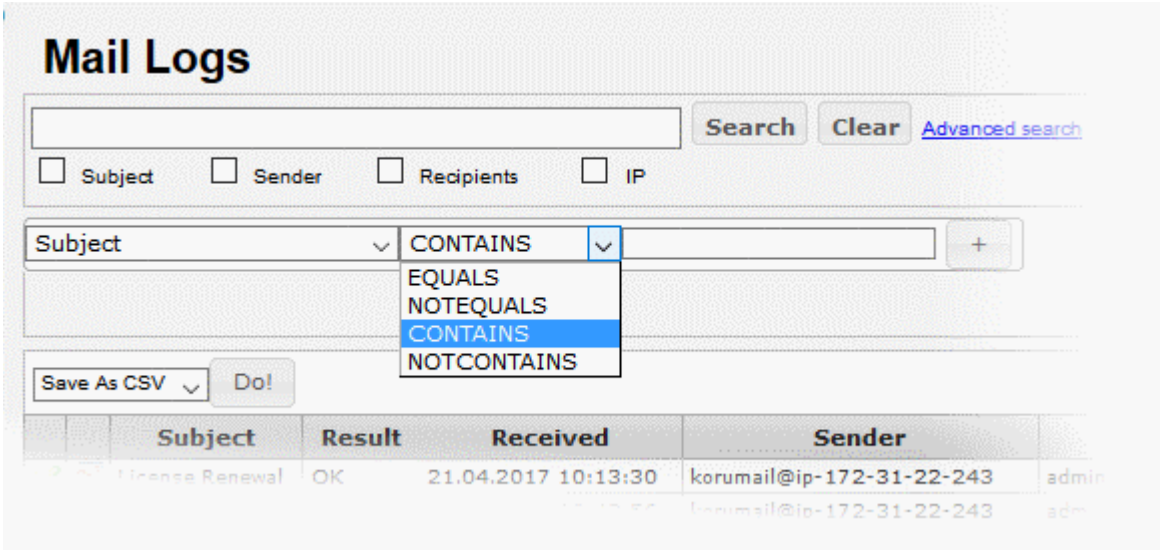
The 'Advanced Search' option will be displayed.



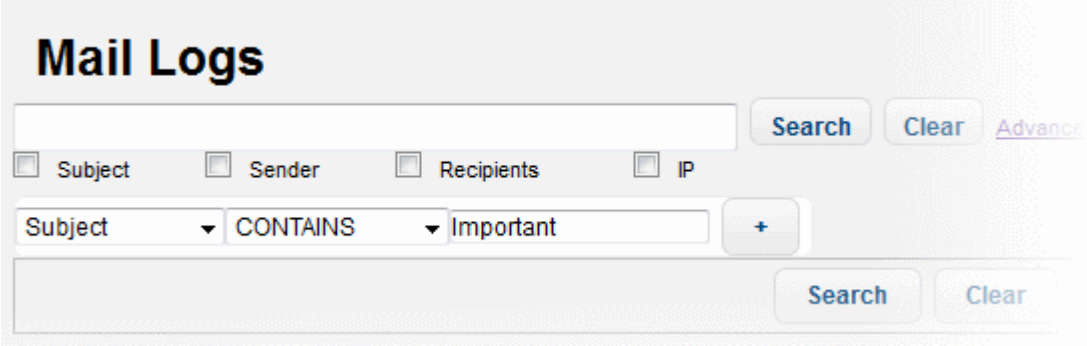
The first drop-down contains the column headers that can be selected for an advanced search.



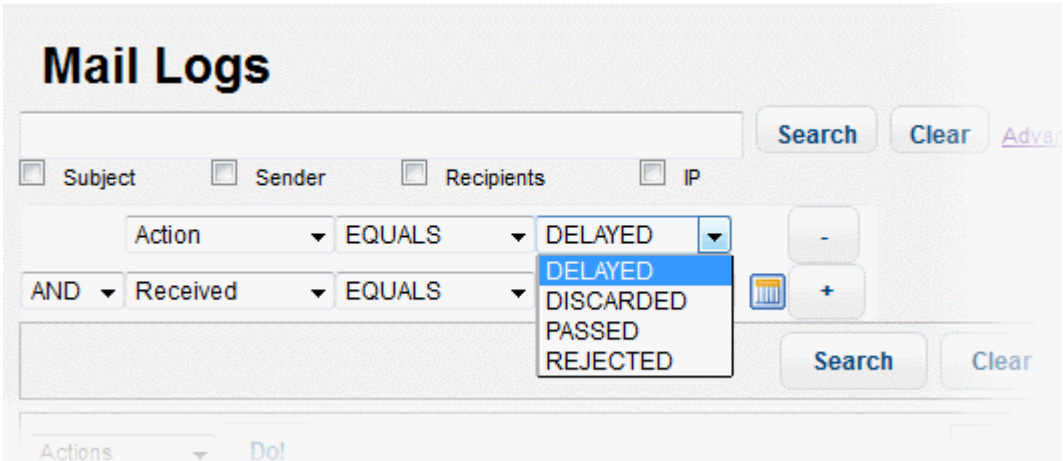
The second column contains the condition for a search, which depends on the item selected in the first column and text/number entered or options selected in the third column.



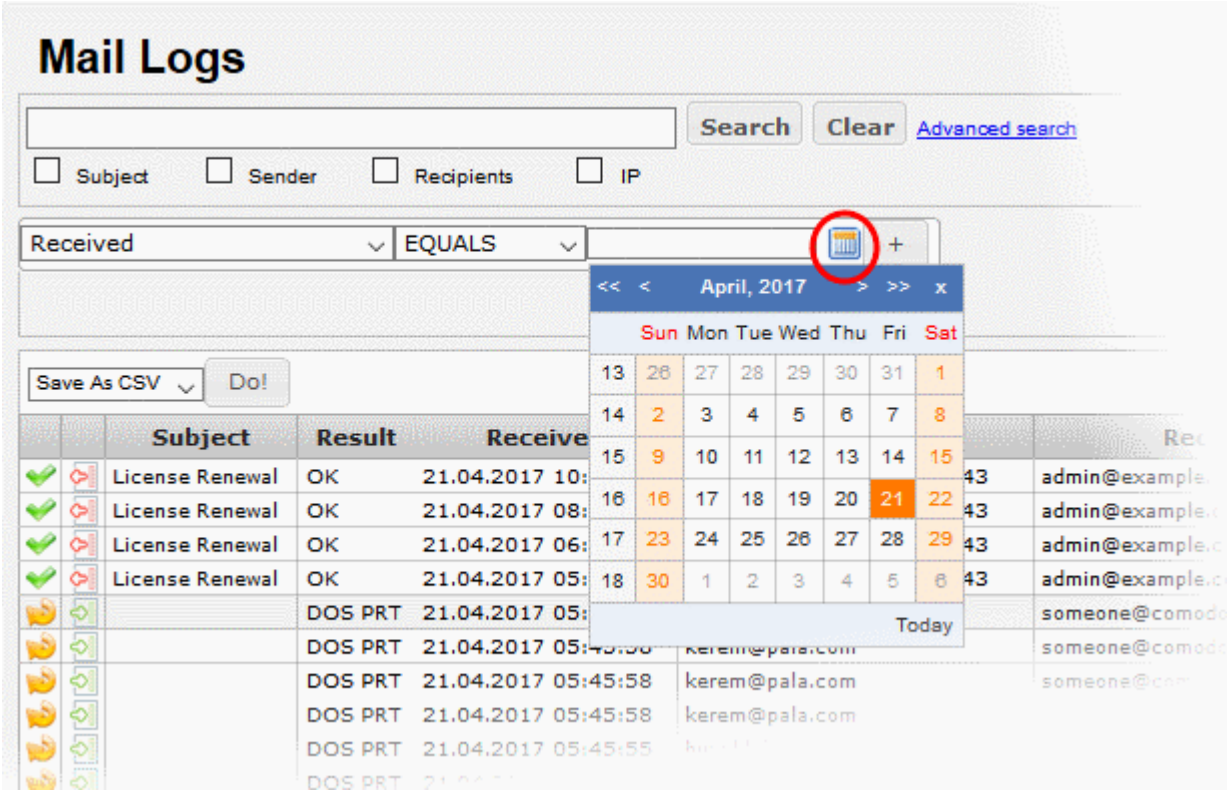
The third column allows you to enter the text/number or select from the options depending on the selection in the first column. For example, choosing 'Subject', 'From Address' or 'Remote IP' allows you to enter the text in the third column



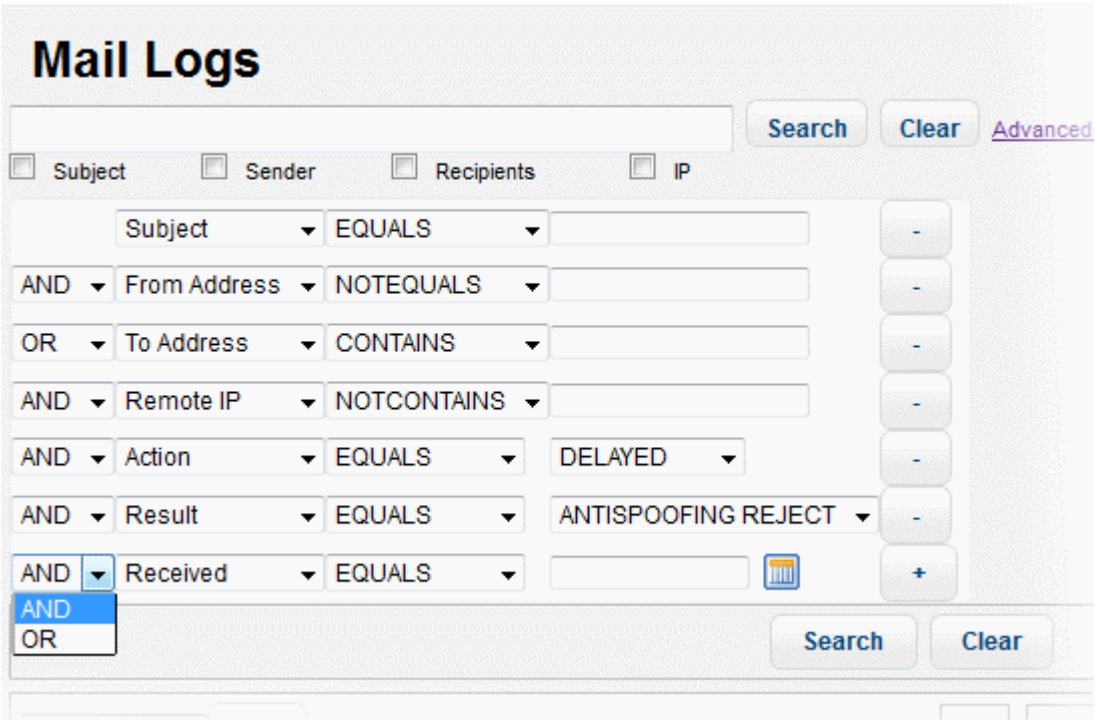
If you select 'Action' or 'Result' in the first column, then further options can be selected from the third column.



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



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



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

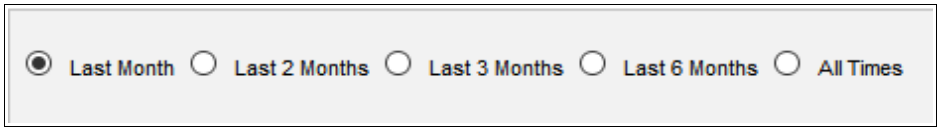
You can create a filter rule by selecting 'AND' or 'OR' option beside each of the added filter.

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

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

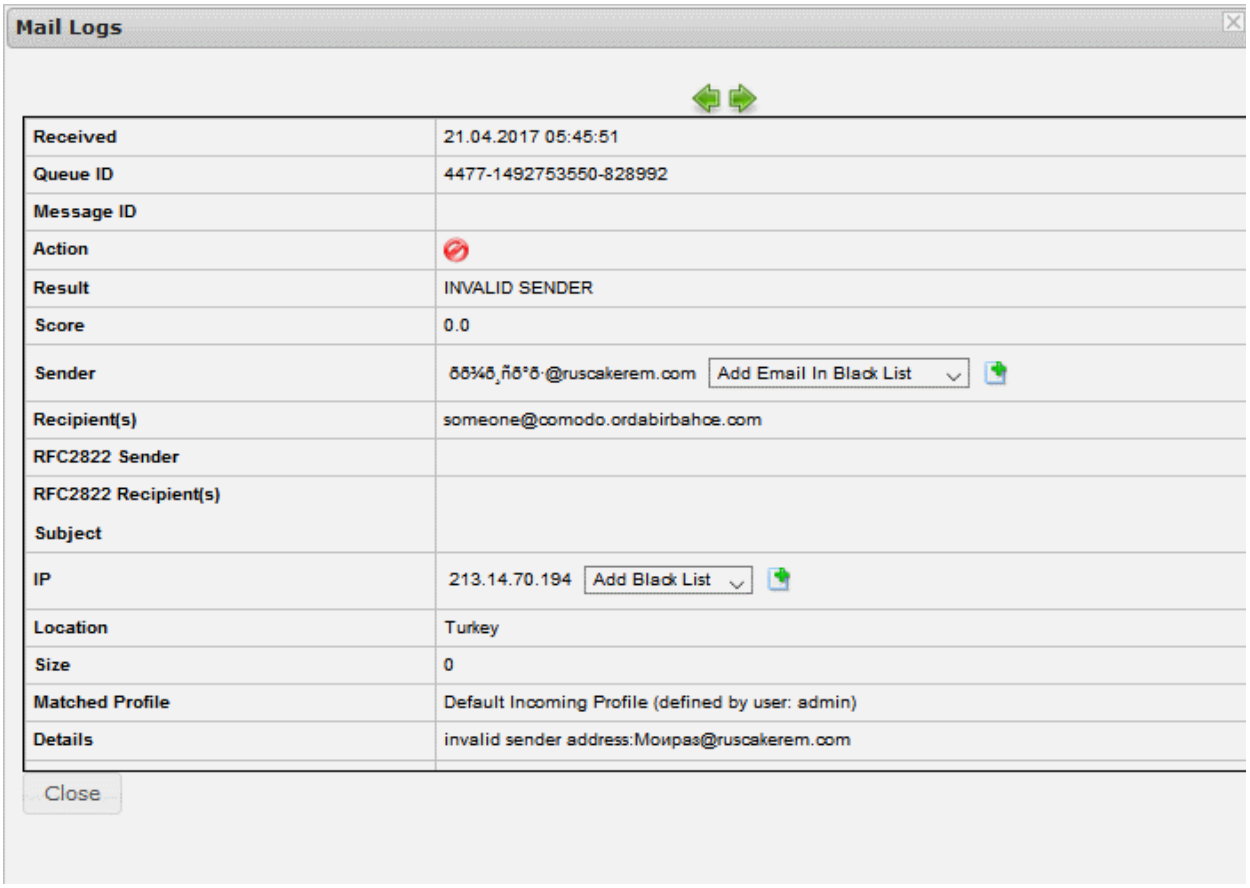
- To remove the advanced search field, click the 'Advanced search' link again.

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



Details of a Log Entry

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



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 Dome Antispam.

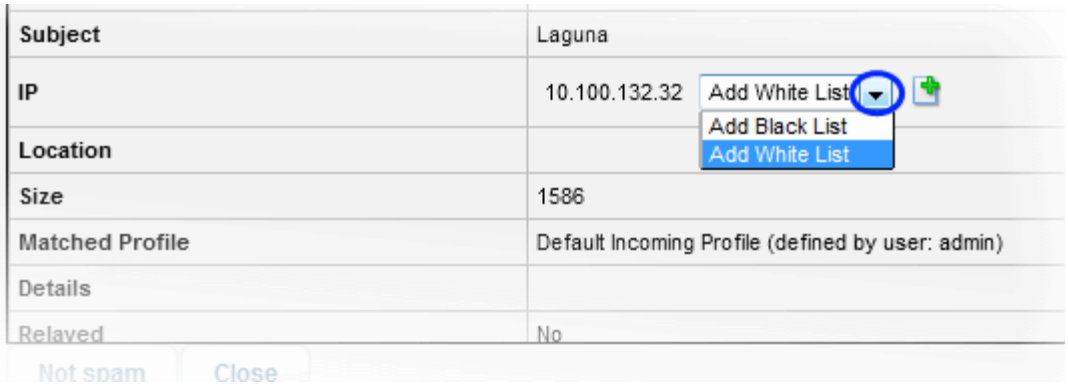
- To add the sender or domain to blacklist/whitelist, click the drop-down in the 'Sender' row.

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

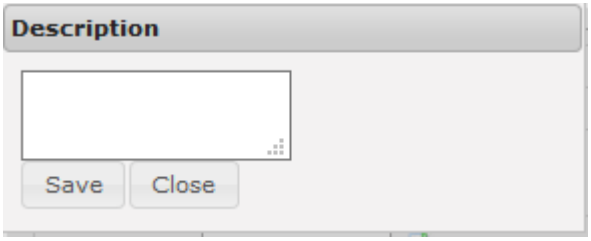
- Enter the reason for changing the category and click the 'Save' button.

The changes will be saved and mails from the sender will be applied the new settings by Dome Antispam.

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



- 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.

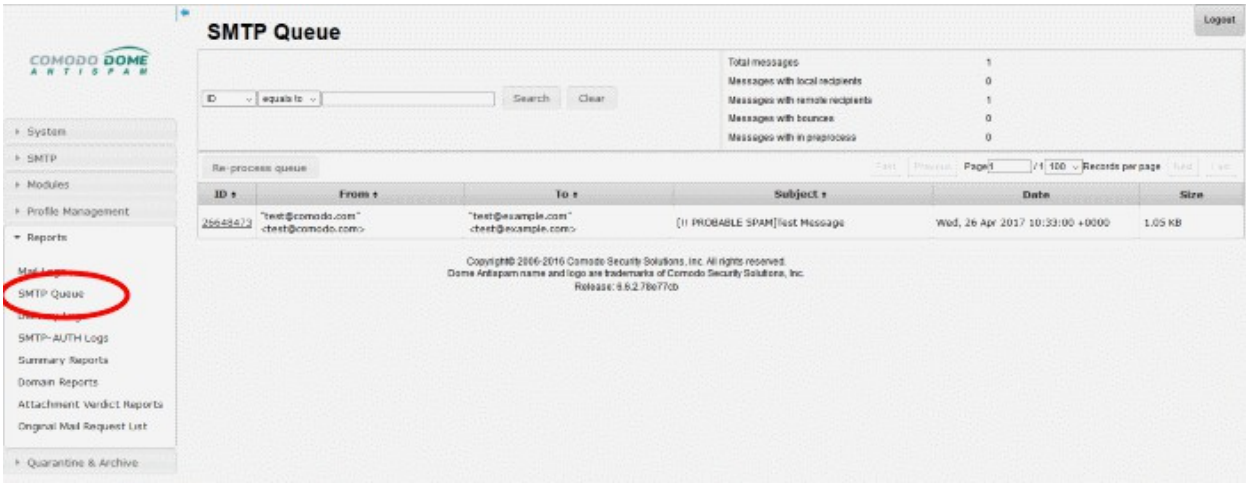
The changes will be saved and mails from the IP will be applied the new settings by Dome Antispam.

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

7.2 SMTP Queue Report

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

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

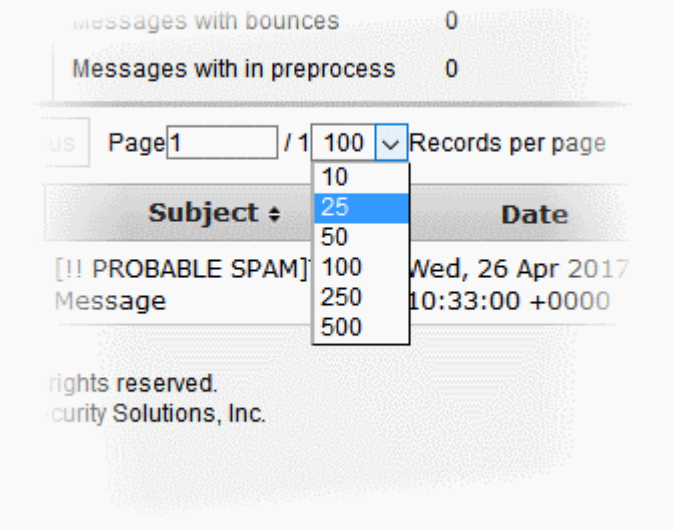


SMTP Queue Report - Table of Column Descriptions	
Column Header	**Description**
ID	The identification number of the email queue that holds the status or message of the queue.
From	Sender's email address
To	Recipient's email address
Subject	Subject of the email in SMTP queue
Date	Date and time that the mail was sent
Size	Size of the email in SMTP queue

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

To configure the number of records to be displayed per page

- Click the 'Records per page' drop-down



- Select the number of records per page to be displayed from the options. The default is 100.
- Click the 'First', 'Previous', 'Next' and 'Last' buttons to navigate through the report.

Search Options

You can search for a particular record by using the search field at the upper left. Use the drop-down menus to specify granular search criteria. This is similar to the advanced search option explained in the 'Mail Logs' section.

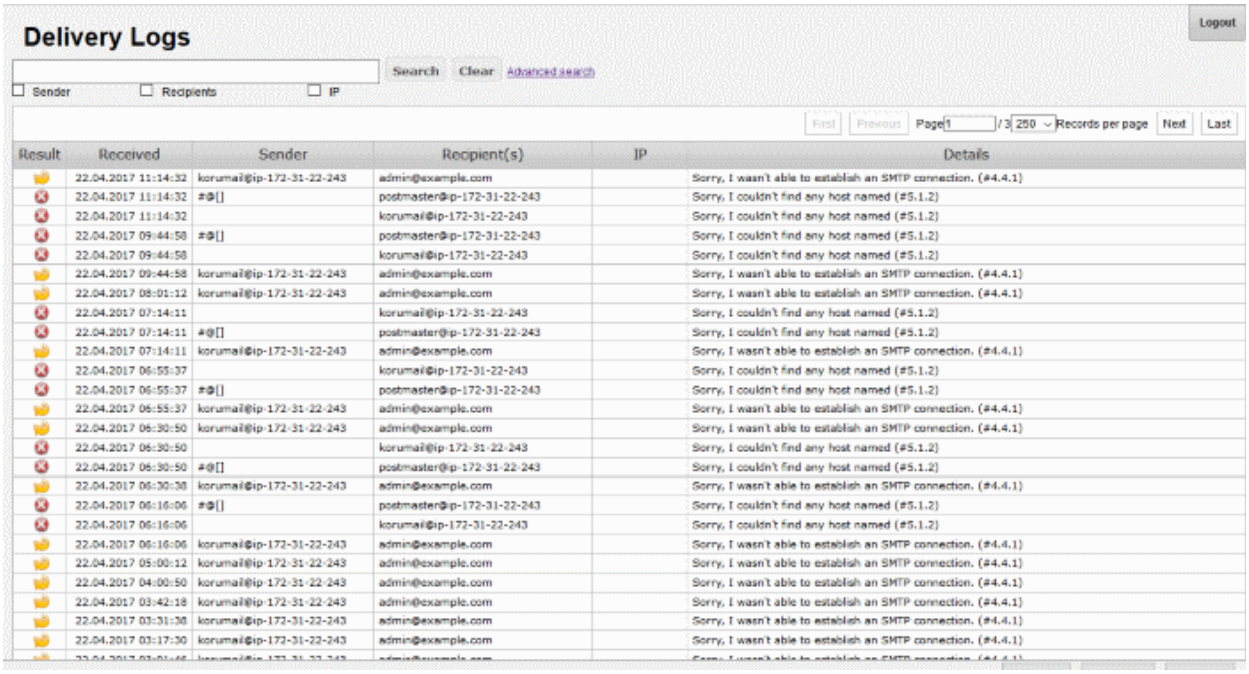
Message Statuses in SMTP Queue

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

7.3 Delivery Logs Report

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

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



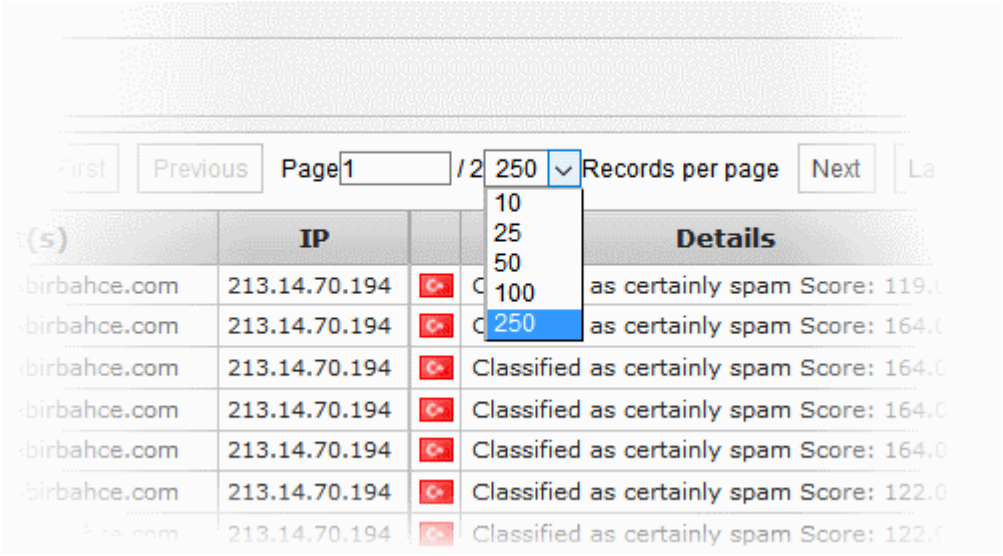
Delivery Logs Report - Table of Column Descriptions	
Column Header	**Description**
Result	Indicates the status of the mail processed by mail server. The tool tip on hovering the mouse cursor over an icon displays the action. - Success: Indicates the mail has been successfully delivered to the recipient. - 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 of email received by Dome Antispam
Sender	Domain details of the email sender
Recipient(s)	Domain details of the recipient(s)
IP	The details of the recipient's IP address
Details	Provides details such as the message ID and reasons for permanent and temporary error

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

To configure the number of records to be displayed per page

- Click the 'Records per page' drop-down



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

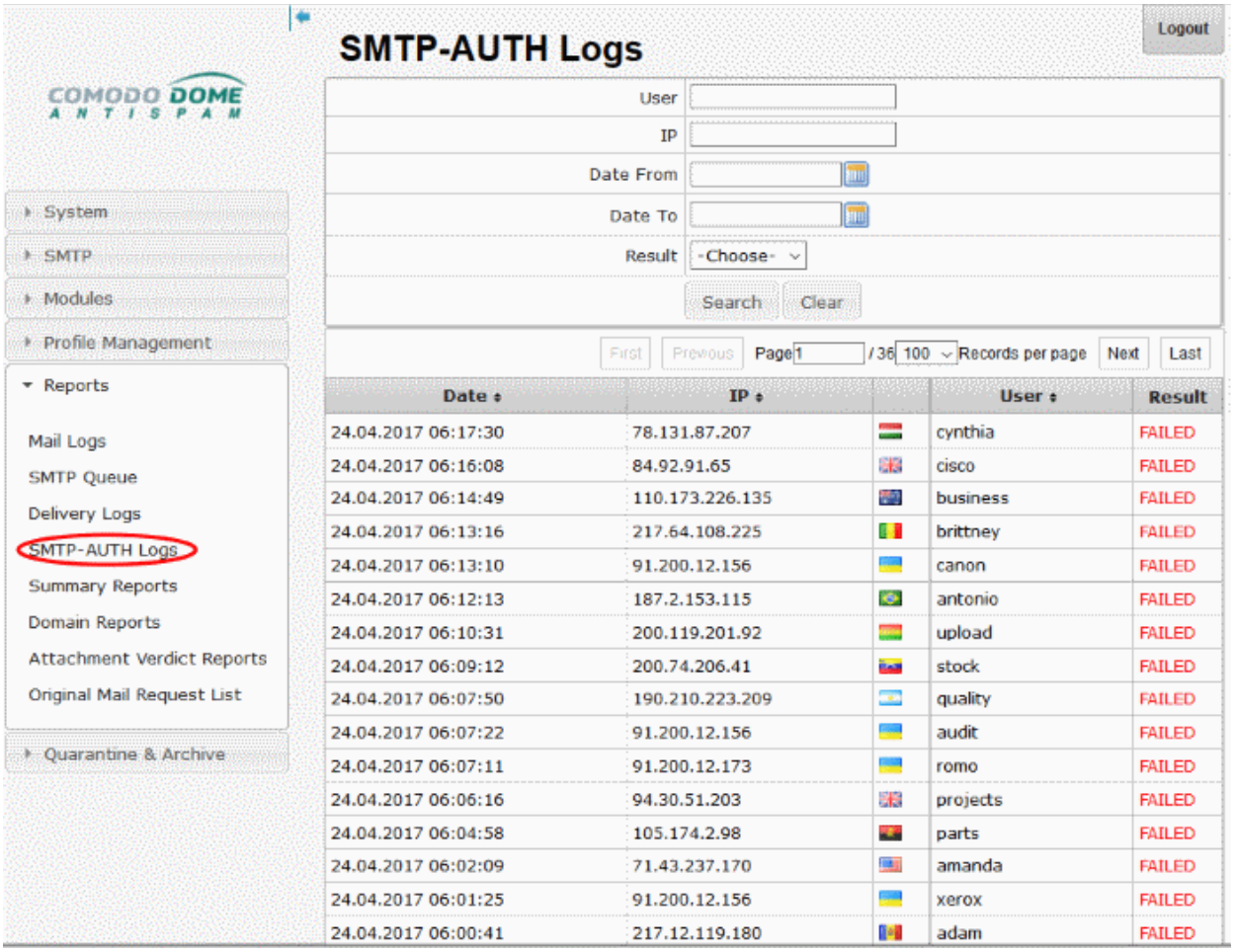
Search Options

You can search for a particular record or records in the report by using simple or advanced search feature. This is similar to the search option explained in the 'Mail Logs' section.

7.4 SMTP-AUTH Logs Report

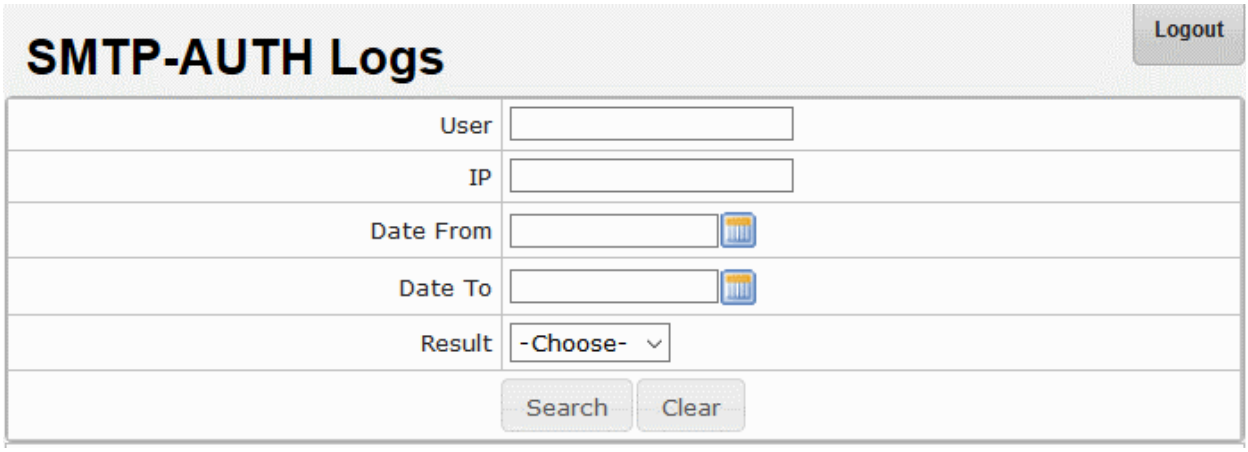
The 'SMTP-AUTH Logs Report' contains logs of every SMTP client log-in that required authentication.

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



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

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

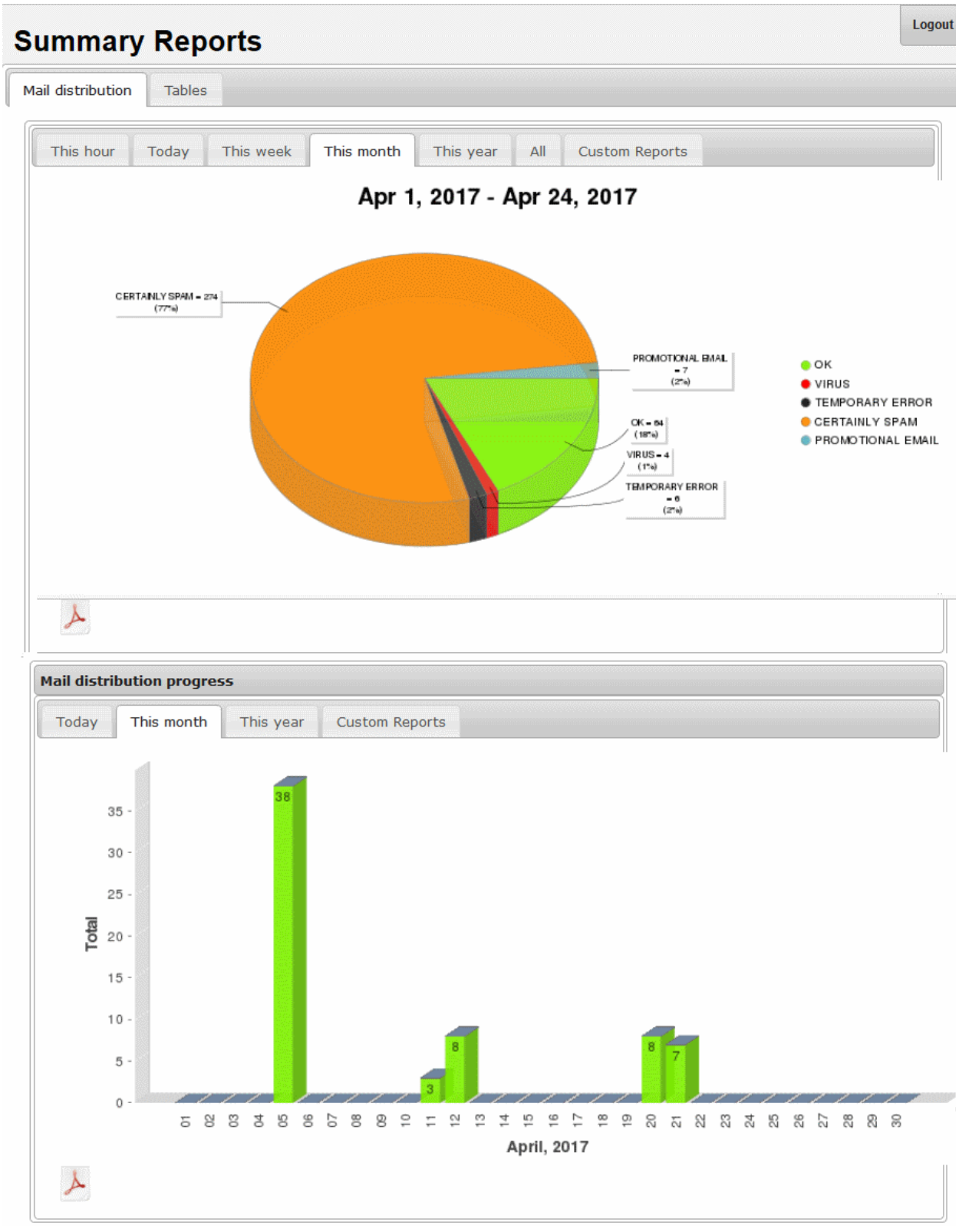


- To search for records based on the entries under 'User', 'IP', 'Date From', 'Date To' or 'Result', enter the text or number fully or partially in the field and click the 'Search' button
- To refresh search, click 'Clear'.

7.5 Summary Reports

The 'Summary Reports' screen in Dome Antispam 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.

- To open the 'Summary Reports' interface, click 'Reports' and then click 'Summary Reports'



You can view and download the reports in graphical as well as in table format.

- Graphical Representation
- Table Representation

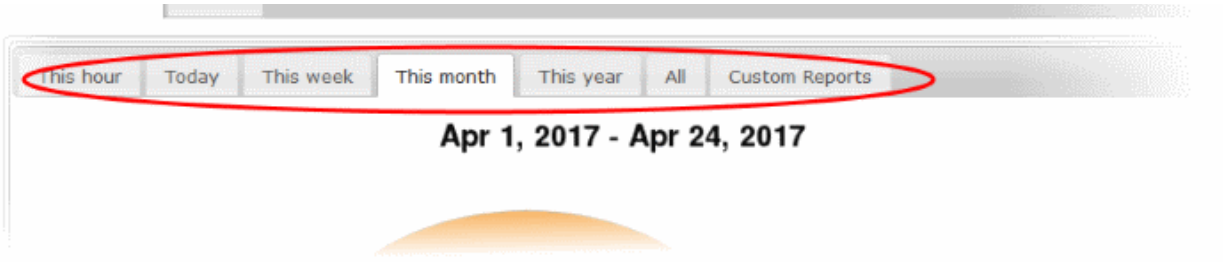
To view and download the report in graphical format

- Click the 'Mail Distribution' tab at the top

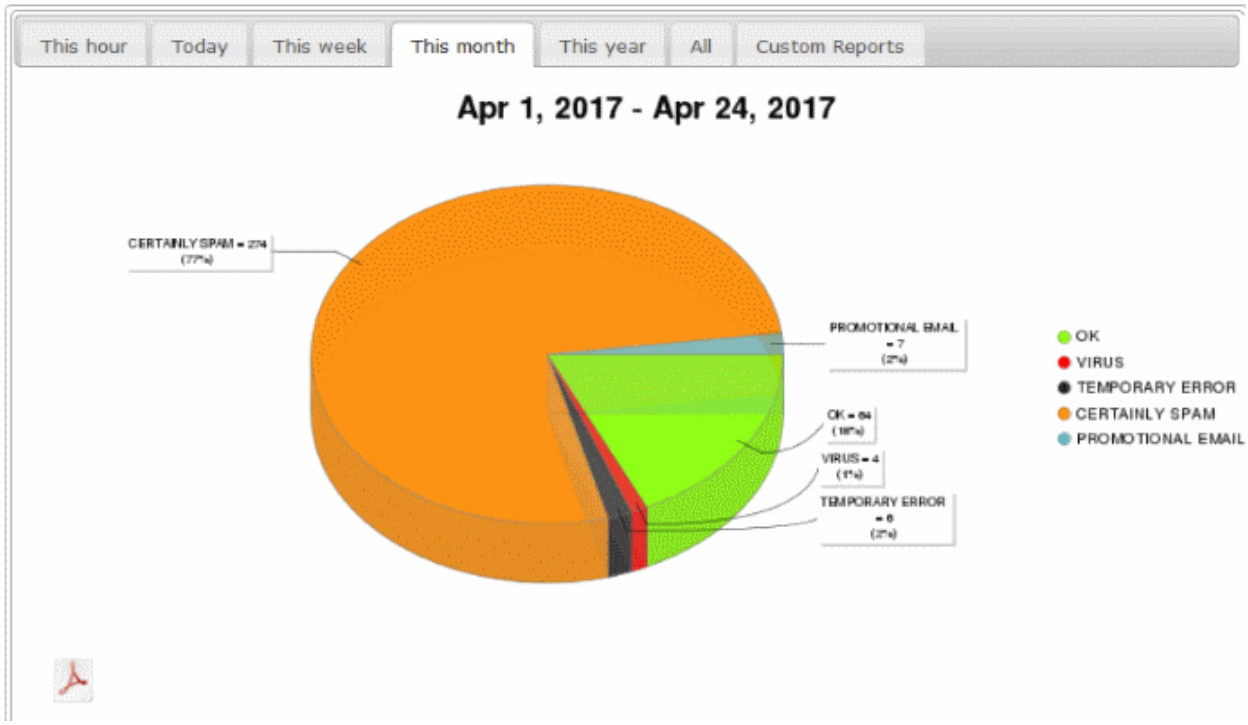
The results in **pie chart** format at the top and **bar chart** format at the bottom will be displayed.

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

Pie Chart



- Click the desired period for which you want to view and download the report. The available periods are daily, weekly, monthly, yearly and the time of Dome Antispam installation. You can also view reports for a customized duration by entering the required dates.

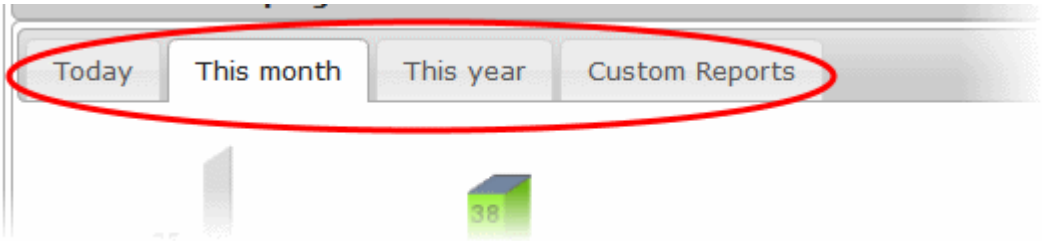


The different segments of the pie chart provides the details of the filtering results for the selected period such as mails categorized as spam, phishing, blacklisted and so on.

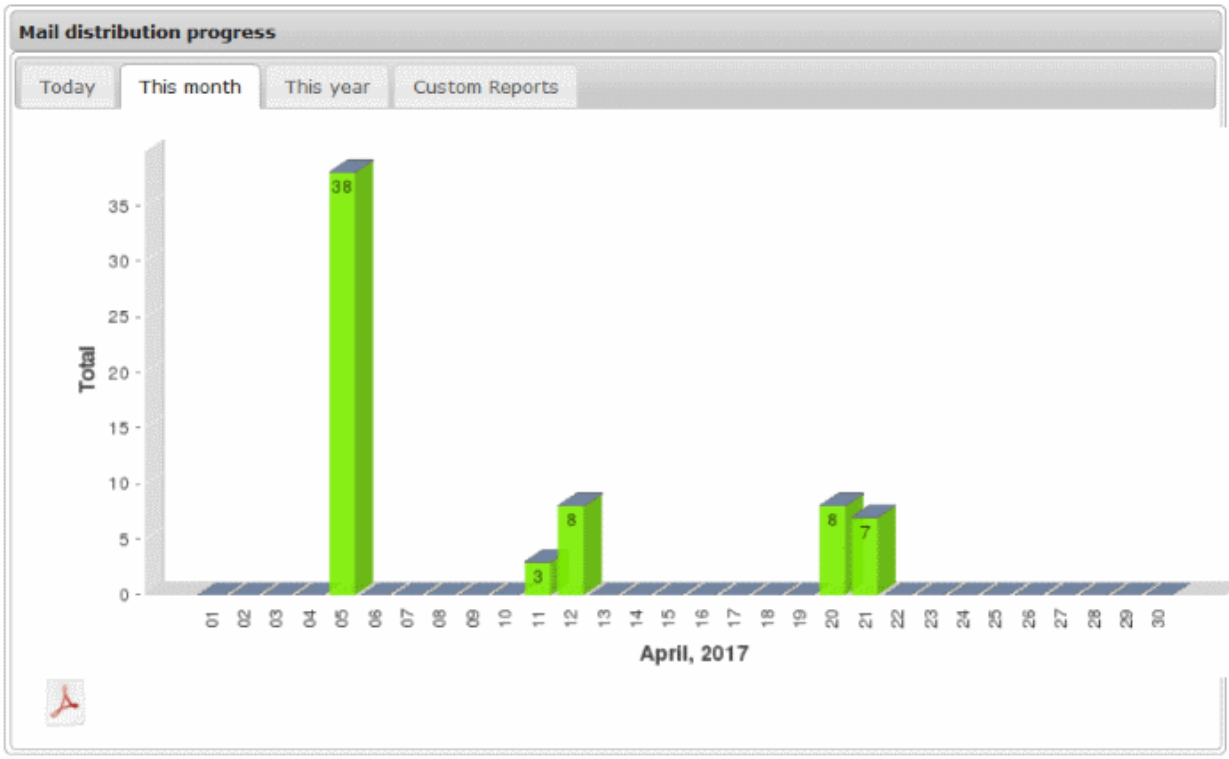
- To download the pie chart results, click the PDF icon and save the PDF file to your system.

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.

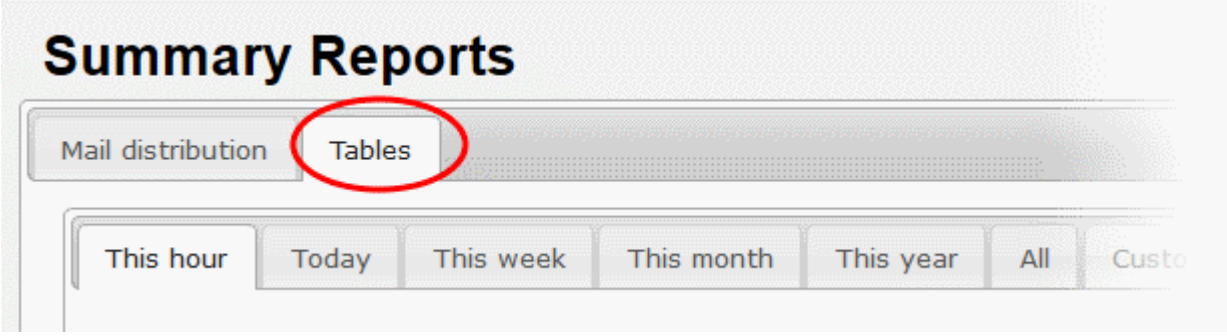


The Y-axis displays the number of mails and X-axis displays the hours/days/months for the selected period.

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

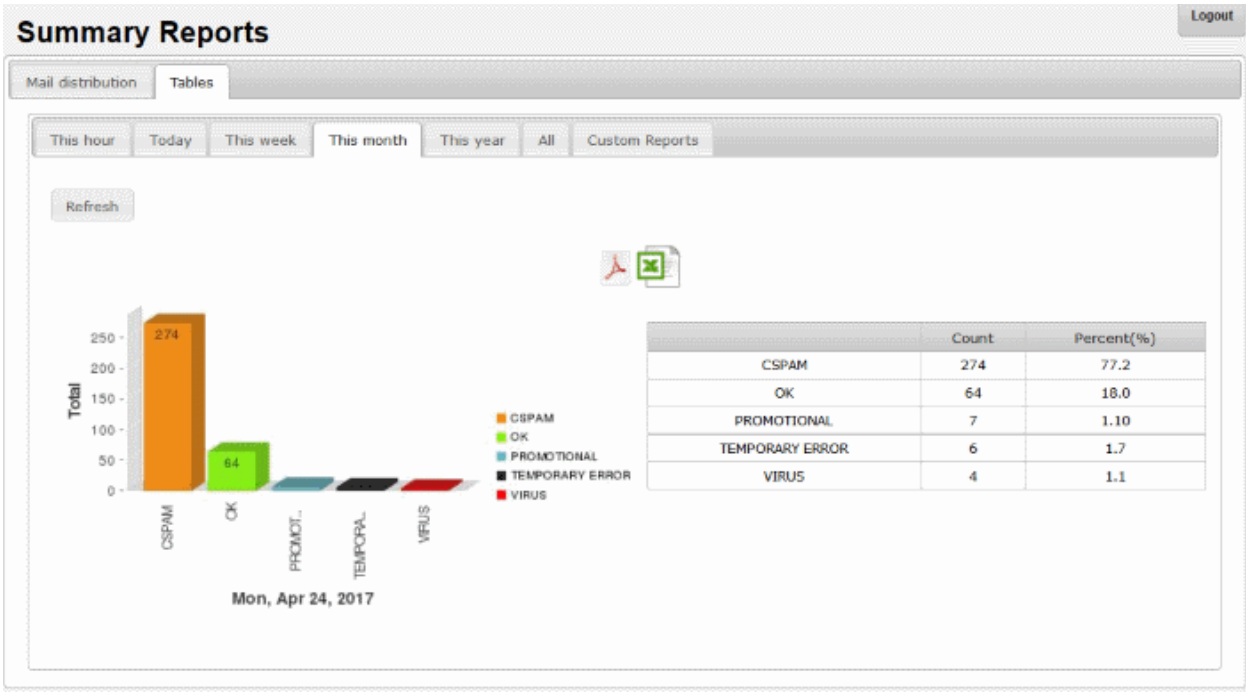
To view and download the report in table format

- 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 Dome Antispam 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.



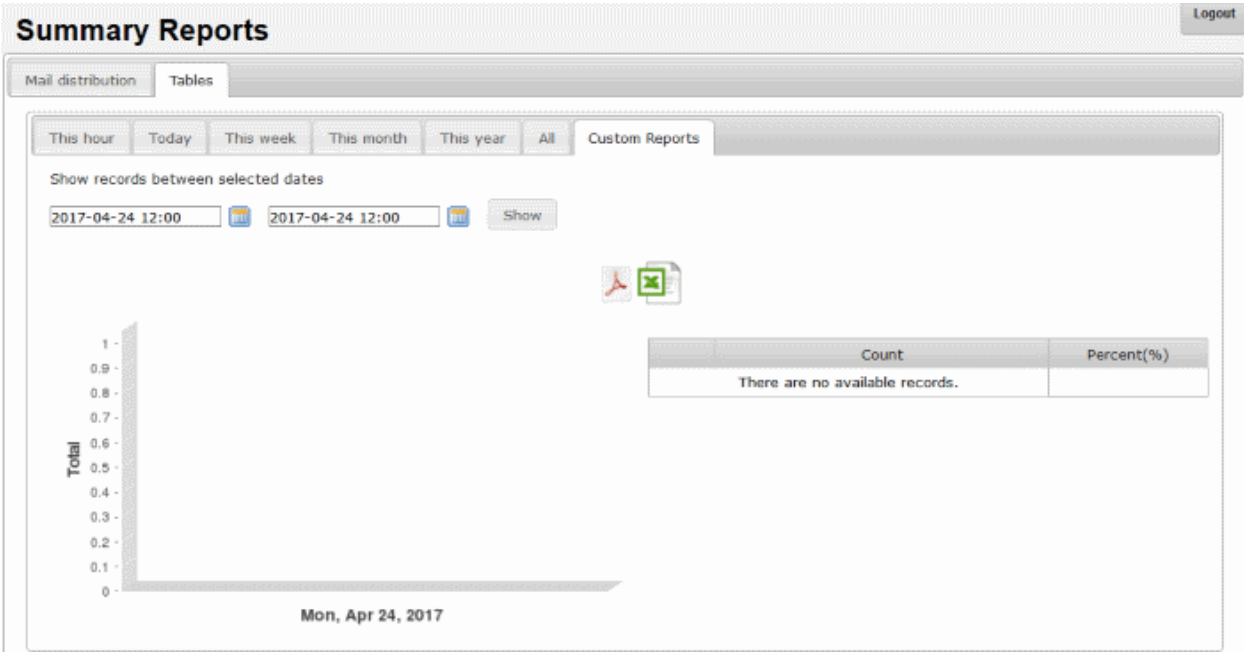
The report for the selected period will be displayed. The first column indicates the categorization of mails, the second column displays the number for each category and the third column provides the results in percentage for each category.

- To download the bar chart results, click the PDF icon and save the PDF file to your system.
- To download the report in XLS (spreadsheet) format, click the XLS icon and save it to your system.

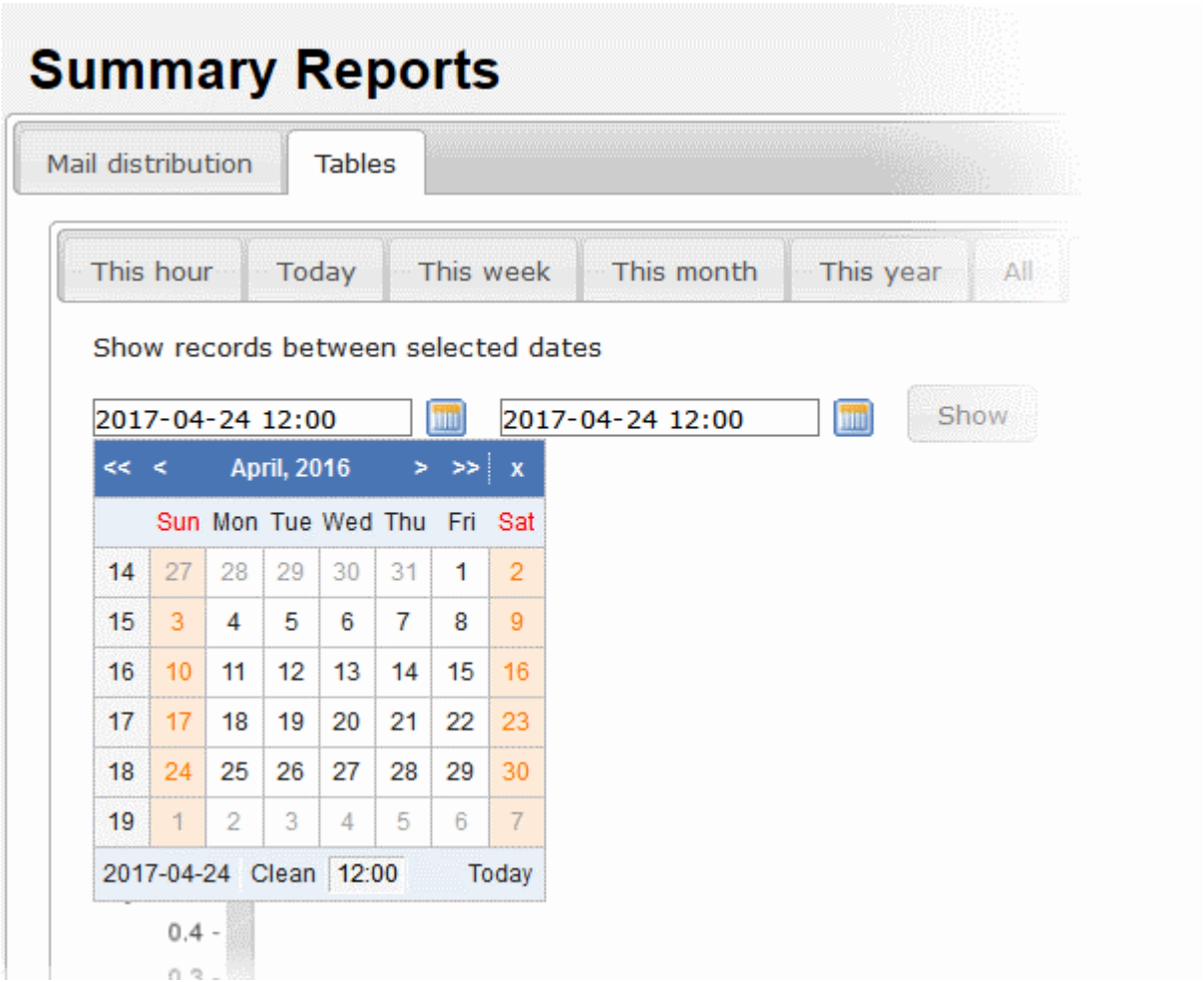
To generate a custom report in table format

- Click the 'Custom Reports' tab at the top

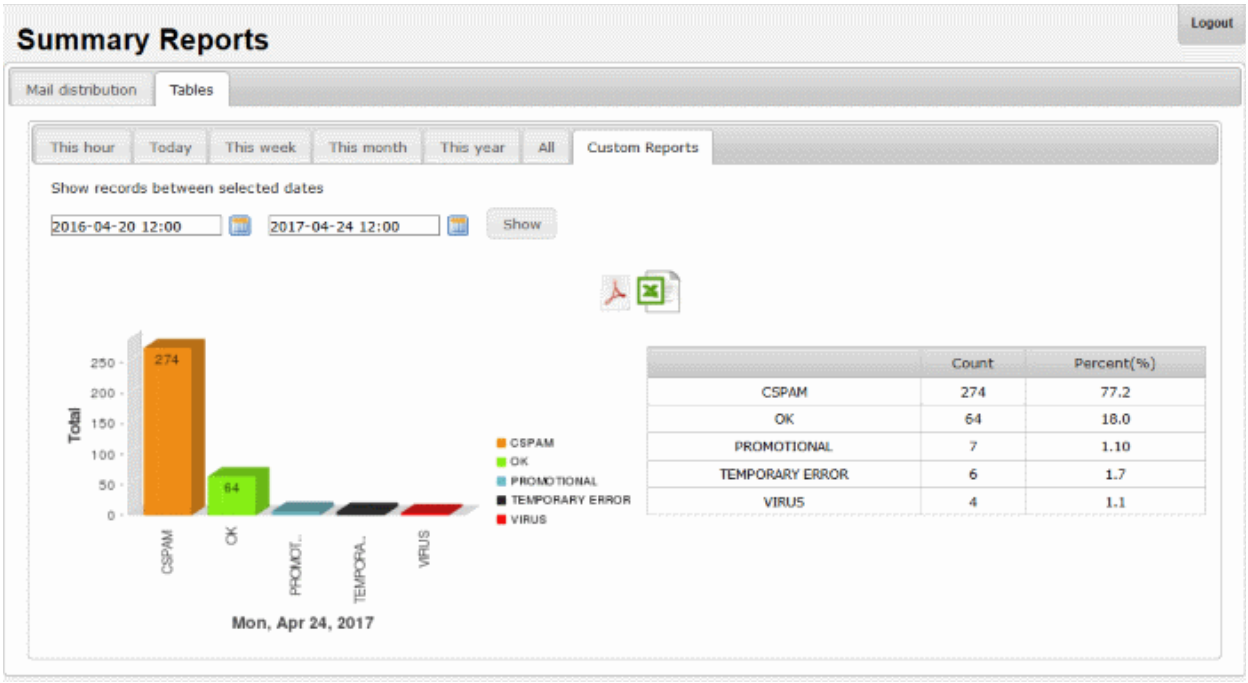
The fields to select the 'From' and 'To' period will be displayed.



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

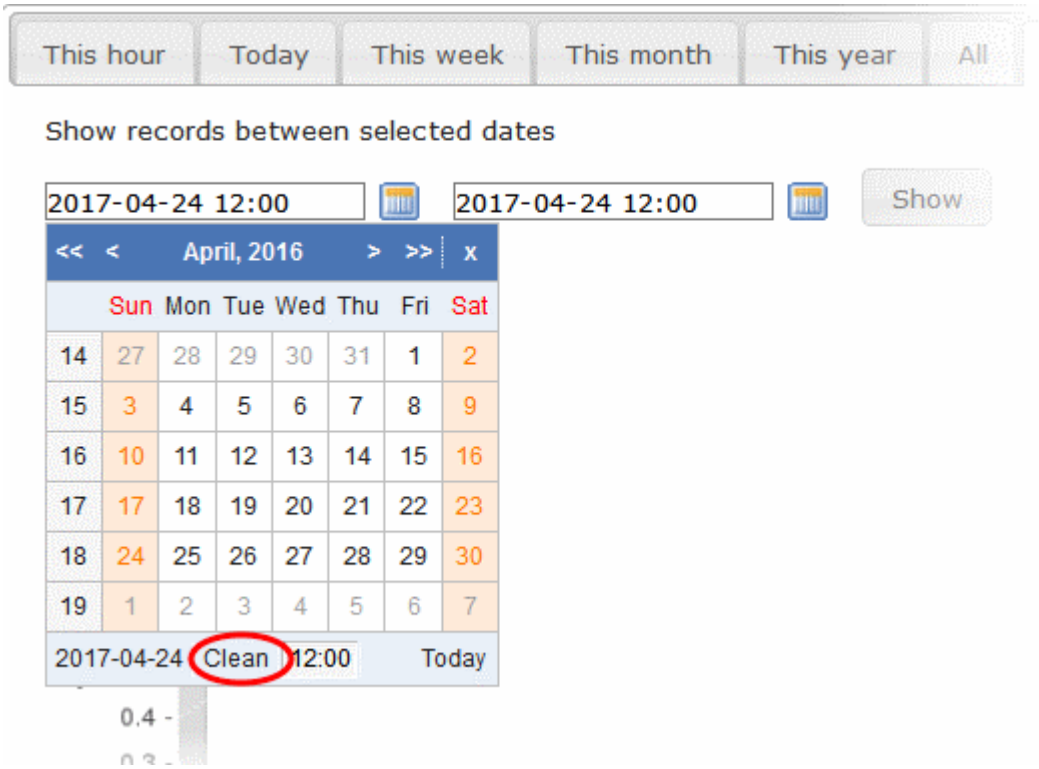


- Click the 'Show' button after selecting the custom period.



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.

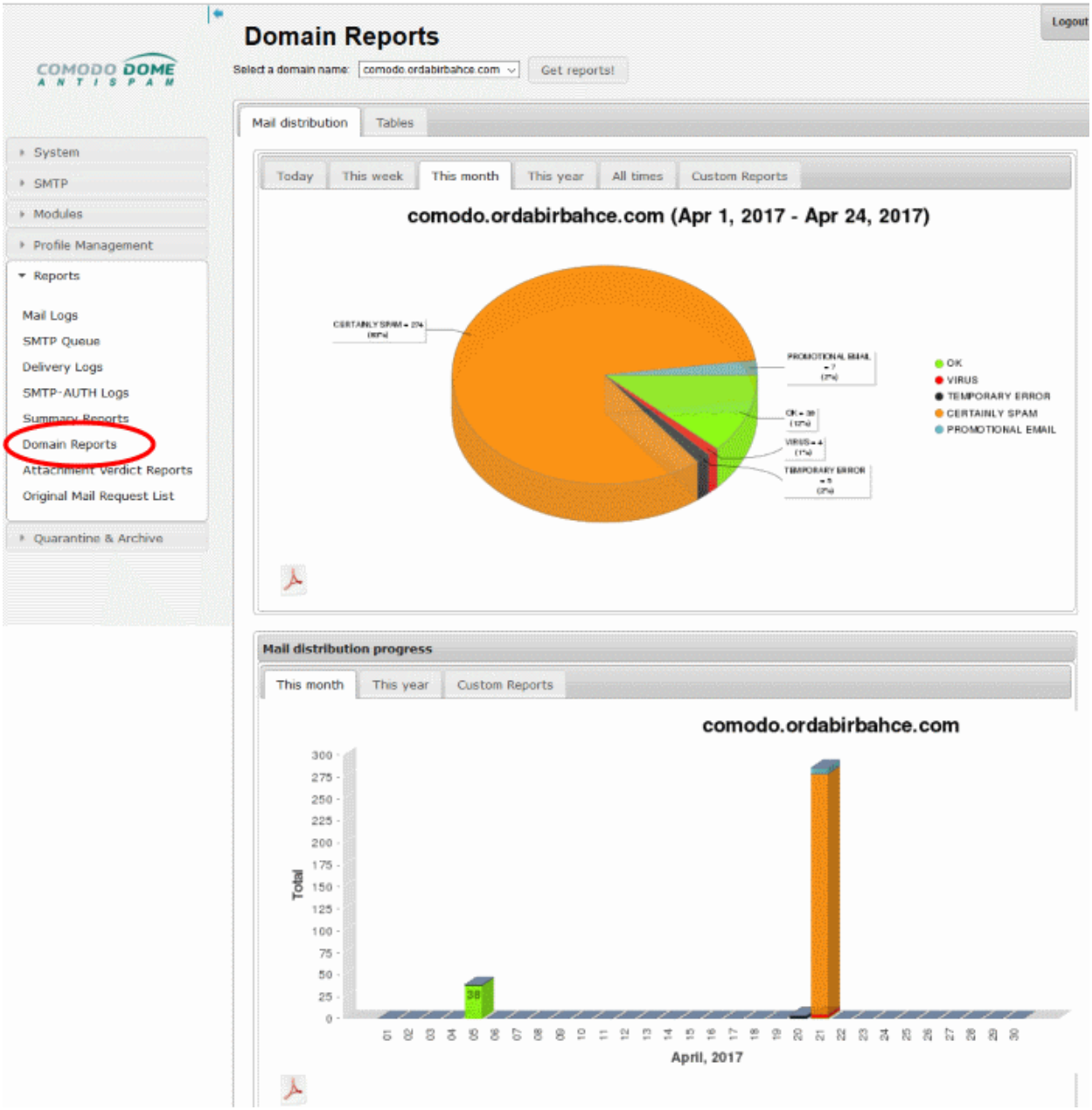
- To download the custom report in PDF format, click the PDF icon and click 'OK' in the download dialogue to save the report.
- To download the custom report in XLS (spreadsheet) format, click the XLS icon and click 'OK' in the download dialogue to save the report.
- To clear the custom period, click on the period fields or calendar icon and click the 'Clean' button.



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'.

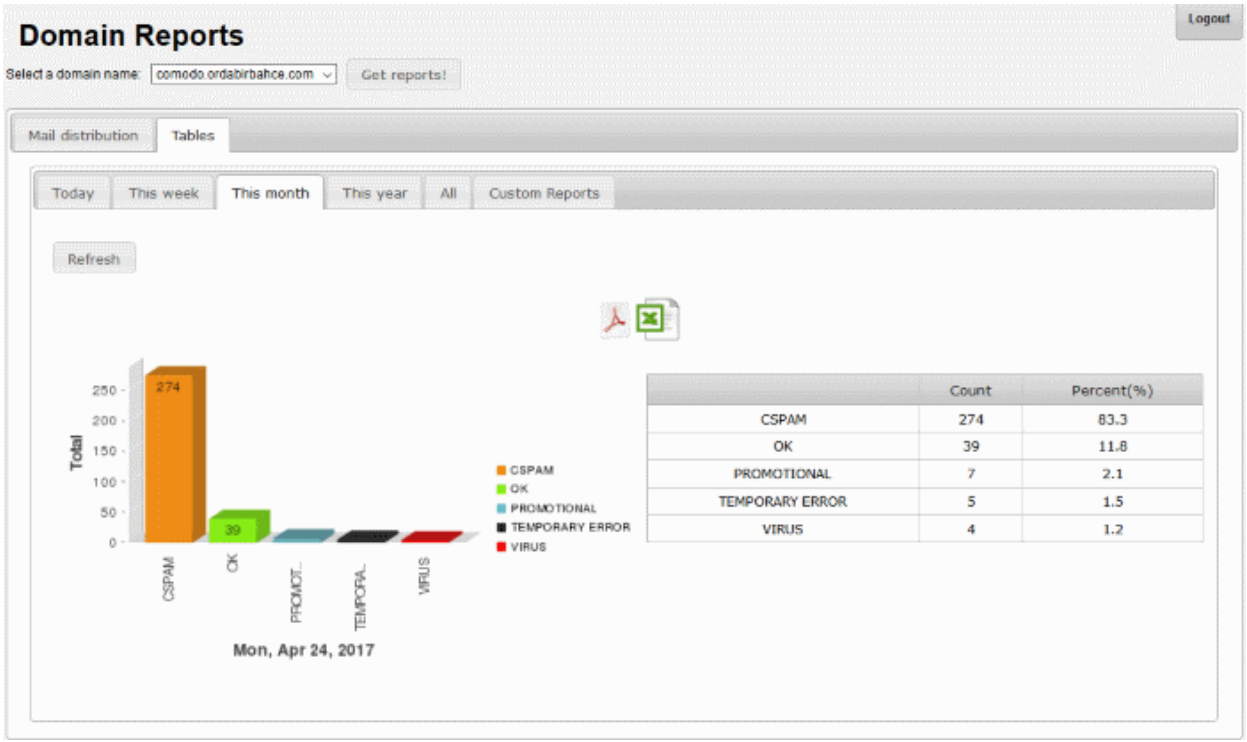
Mail Distribution Progress:

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:

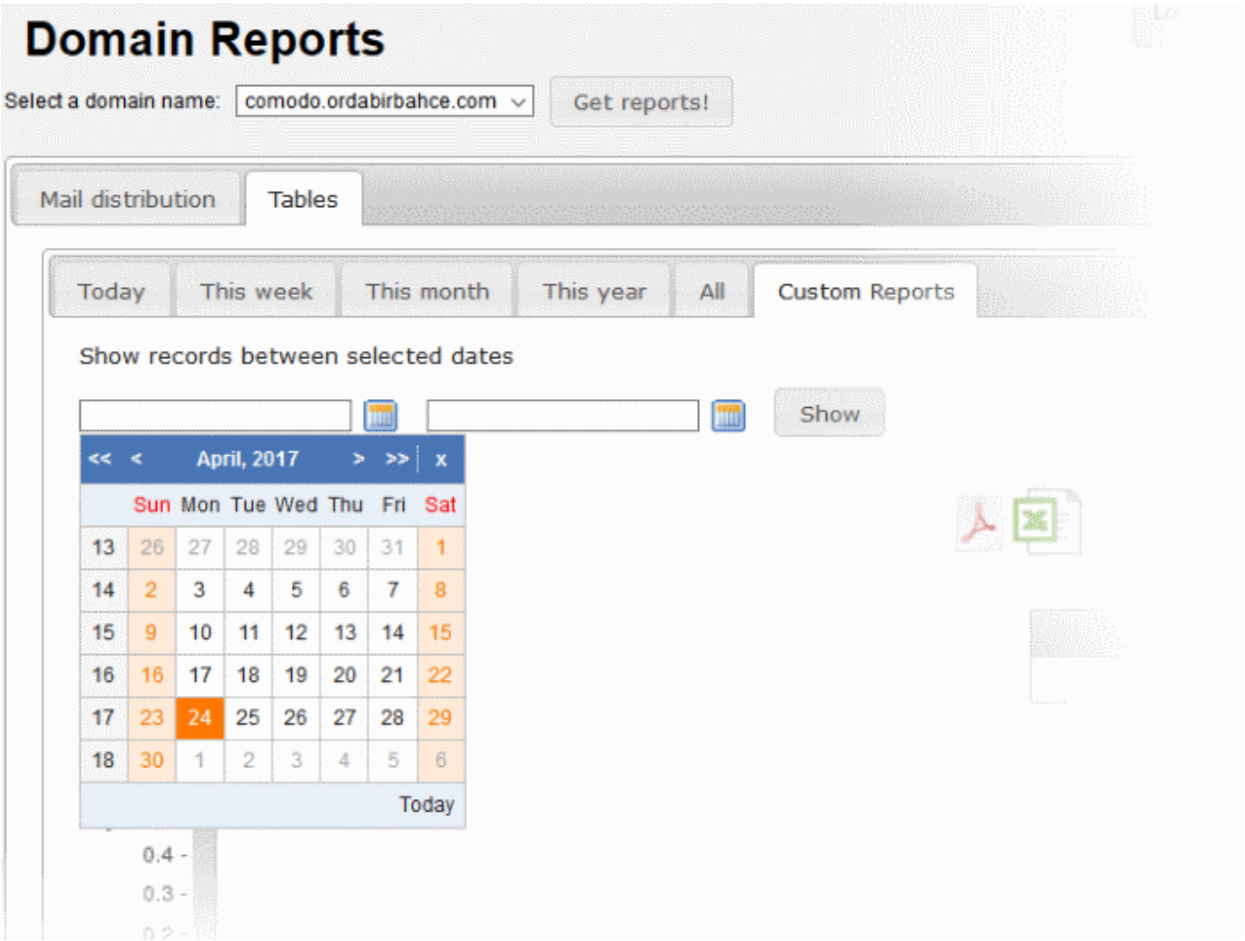
The 'Tables' report displays the number of mails sent/received in each every mail category. The bar graph displays 'Count' on the x-axis against the category of mails on the y-axis.



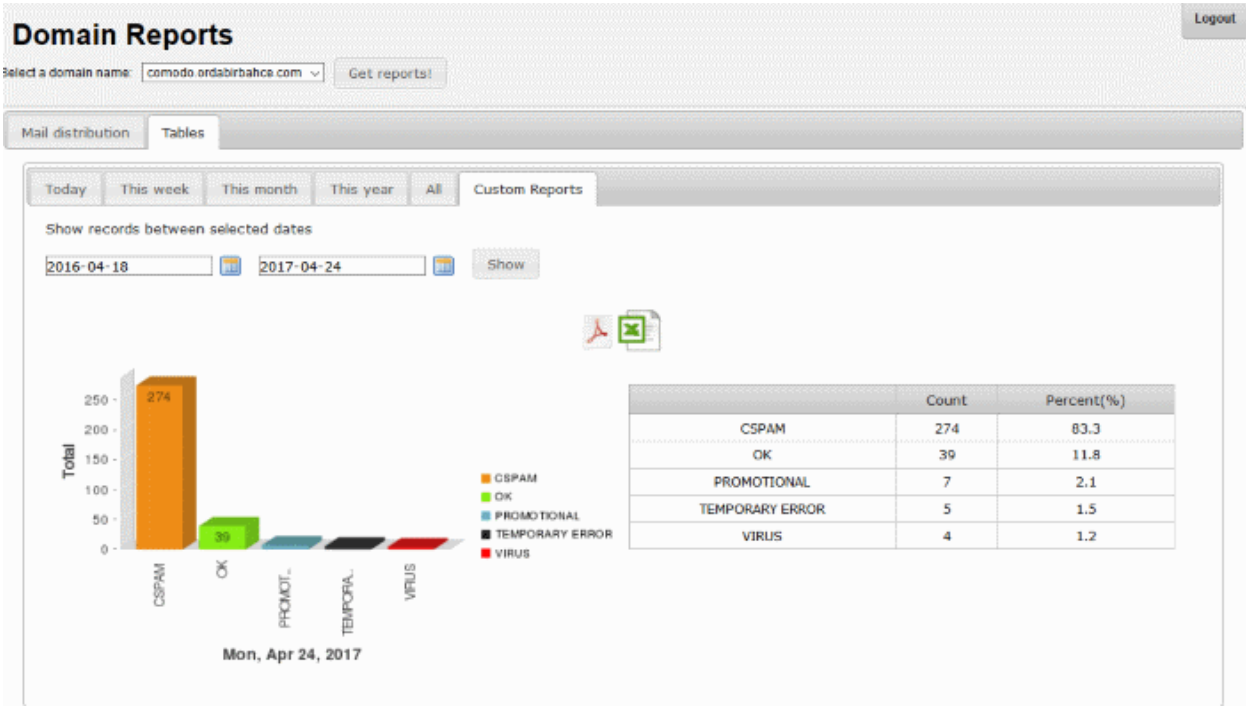
To generate a custom report in table format

- Click the 'Custom Reports' tab at the top

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



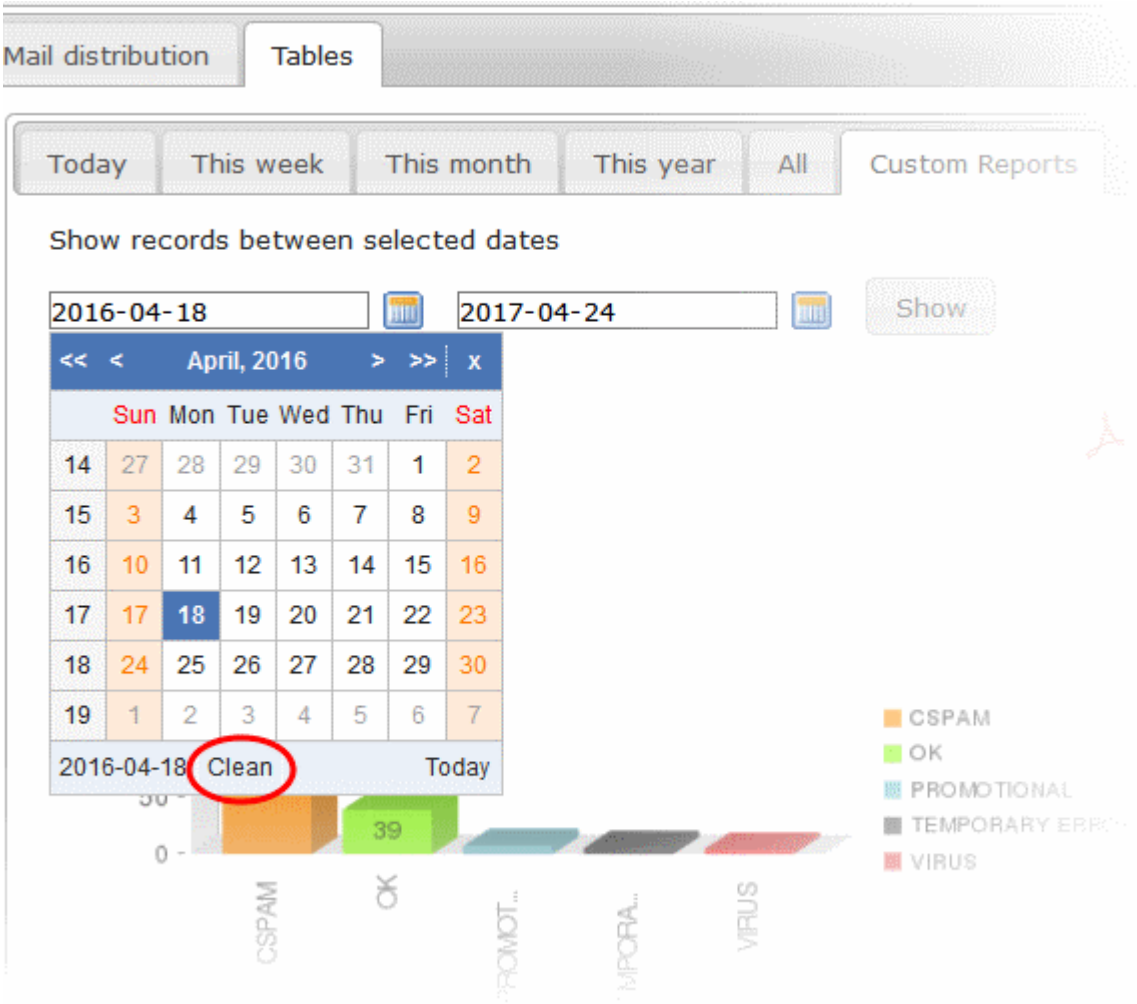
- Click on the fields or calendar icon and select the period from the calendar.
- Click the 'Show' button after selecting the custom period.



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.

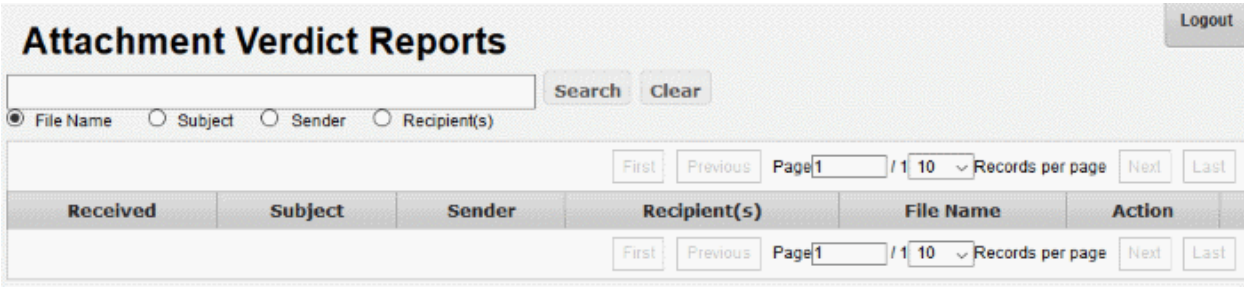
- To download the custom report in PDF format, click the PDF icon and click 'OK' in the download dialogue to save the report.
- To download the custom report in XLS (spreadsheet) format, click the XLS icon and click 'OK' in the download dialogue to save the report.
- To clear the custom period, click on the period fields or calendar icon and click the 'Clean' button.



7.7 Attachment Verdict Reports

The 'Attachment Verdict Reports' interface contains all the email attachment files for which Dome Antispam has returned a verdict and the corresponding actions taken.

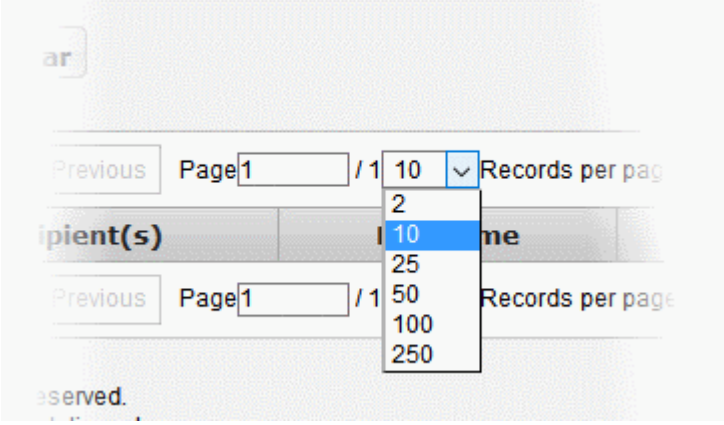
- To open the interface, click 'Reports' on the left then click 'Attachment Verdict Reports'.



Attachment Verdict Report - Table of Column Descriptions	
Column Header	**Description**
Received	Date and time of email received by Dome Antispam.
Subject	Content in the 'Subject' line of the mails containing attachment.
Sender	Domain details of the email sender.
Recipient(s)	Domain details of the recipient(s).
File Name	Name of the file that is given a verdict.
Action	Action taken for verdict given.

To configure the number of records to be displayed per page

- Click the 'Records per page' drop-down



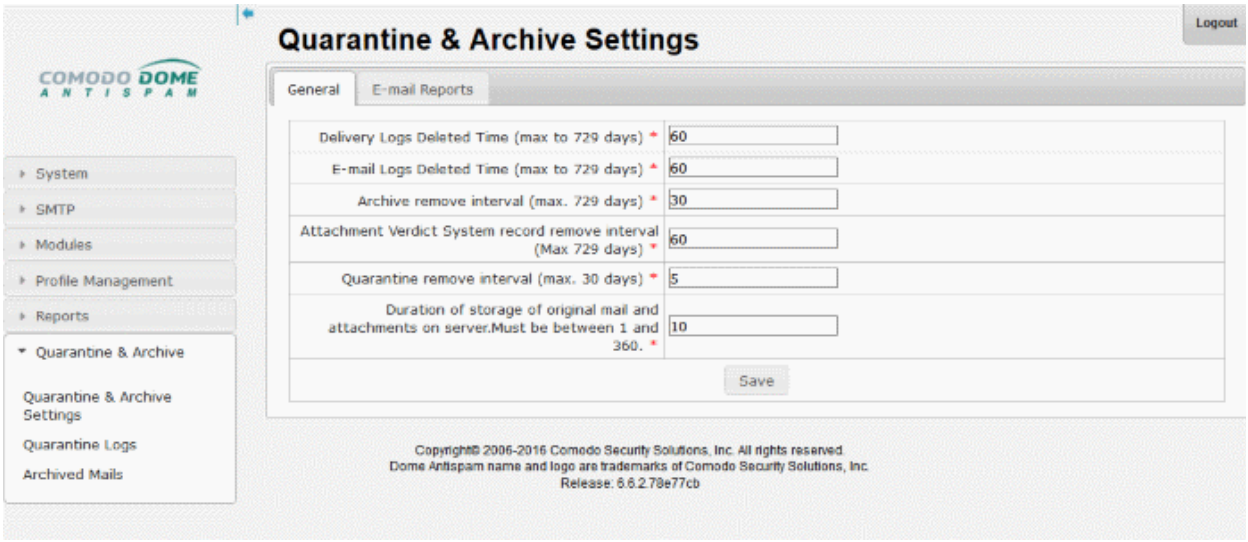
- Select the number of records per page to be displayed from the options. The default is 10.
- Click the 'First', 'Previous', 'Next' and 'Last' buttons to navigate through the report.

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

- To search for records based on the entries under 'Filename', 'Subject', 'Sender' or 'Recipient(s)' of the file with verdict reports, click any one of the radio buttons and enter the text or number fully or partially in the text field and then click the 'Search' button
- To refresh search, click 'Clear'.

8 Quarantine & Archive

The 'Quarantine & Archive' sections allows administrators to configure the number of days that logs and archived files should be retained in Dome Antispam. Details of 'Quarantine Logs' and 'Archived Mails' can also be viewed, category changed and records exported to a CSV file.



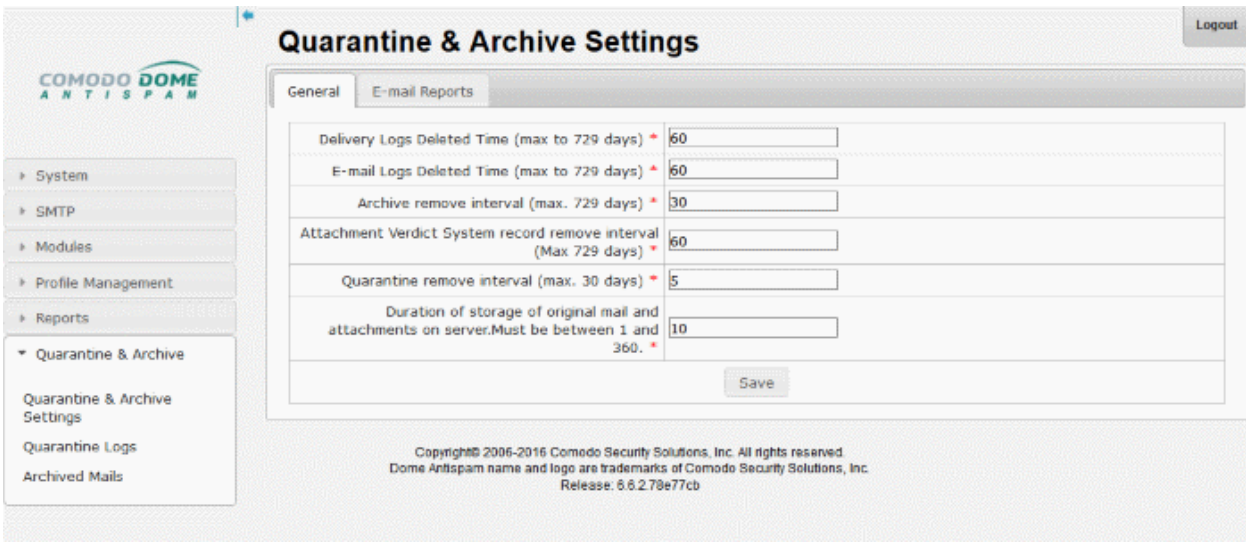
Click the following links for more details:

- Quarantine & Archive Settings
- Quarantine Logs
- Archived Mails

8.1 Quarantine & Archive Settings

The 'Quarantine & Archive Settings' interface allows administrators to set the period to retain 'Mail Logs', 'Archived Mails' and 'Quarantine Logs' in Dome Antispam. You can also set the method of user authentication for accessing their quarantined email at 'Quarantine Webmail' interface. Admins can also create a mail template that is sent to users as notification to access their quarantined mails.

- To open the interface, click 'Quarantine & Archive' and then click 'Quarantine & Archive Settings'



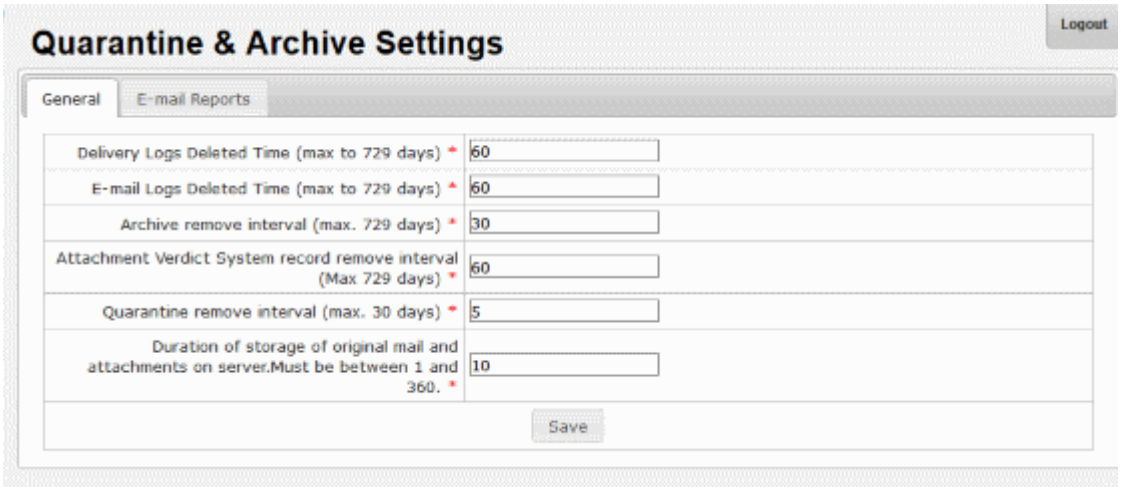
Click the following links for more details:

- Quarantine & Archive General Settings
- Email Reports Settings

8.1.1 Quarantine & Archive General Settings

The 'General' tab in 'Quarantine & Archive Settings' allows administrators to set the period to retain 'Mail Logs', 'Archived Mails' and 'Quarantine Logs' in Dome Antispam. Admins also can set the method of user authentication for users that access their quarantined emails at 'Quarantined Webmail' interface.

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



Quarantine & Archive General Settings - Table of Parameters	
Parameter	**Description**
E-mail Logs Deleted Time	Enter the number of days for which the email logs will be retained. The maximum period is 729 days. Refer to the section 'Mail Logs Report' for more details.
Archive remove interval	Enter the number of days for which the archived mail records will be retained. The maximum period is 729 days. Refer to the section 'Archived Mails' for more details.
Attachment Verdict System record remove Interval	Enter the number of days for which the Attachment verdict records will be retained. The maximum period is 729 days. Refer to section 'Attachment Verdict System' for more details.
Quarantine remove interval	Enter the number of days after which the 'Quarantined Logs' will be removed. The maximum period that can be set is 30 days. Refer to the section 'Quarantine Logs' for more details.
Quarantine Webmail authentication type	Select the user authentication type from the option for users that access the Webmail interface to check their quarantined mails.

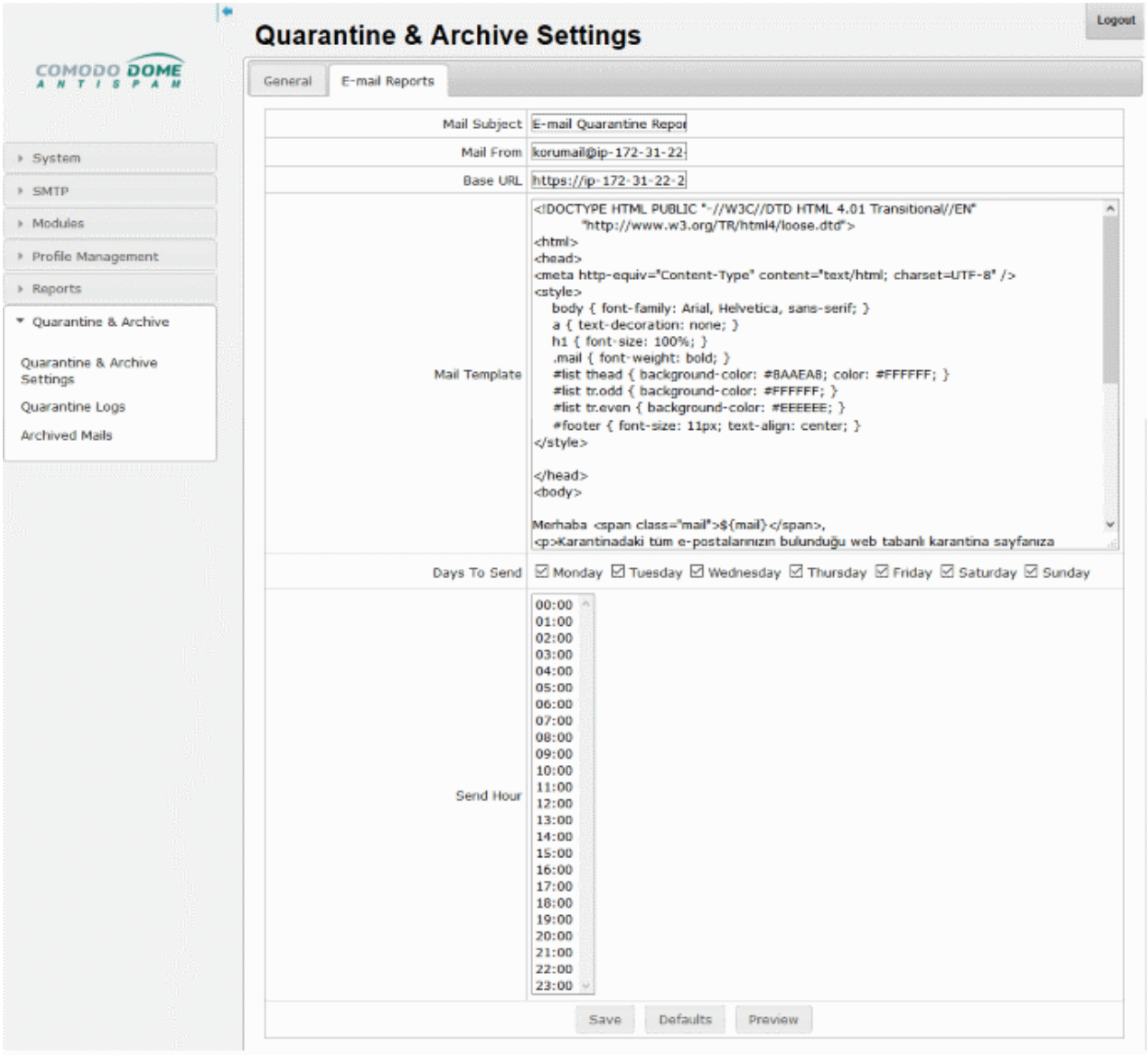
- Click the 'Save' button to apply your changes.

8.1.2 Email Reports Settings

Dome Antispam 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

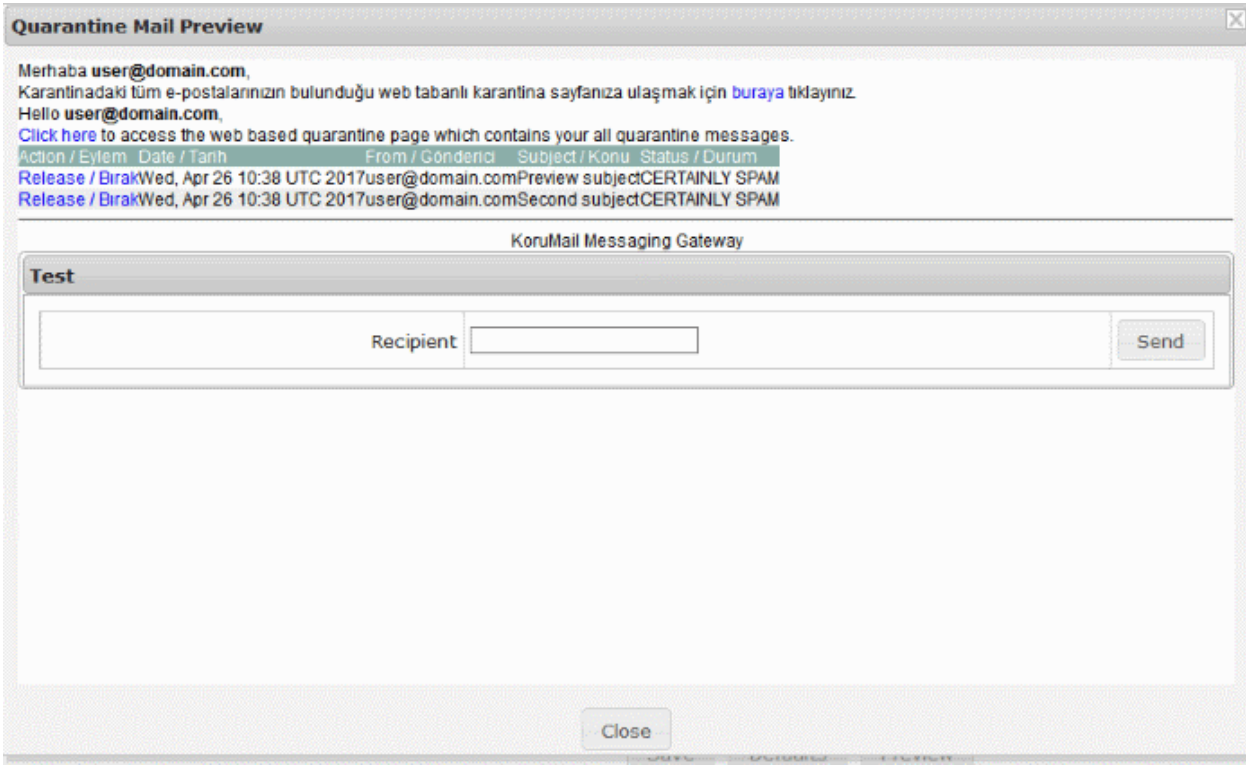
and time the email should be sent to users. The 'Send daily quarantine report to recipients' check box should also be enabled in the '**Archive And Quarantine**' tab of the profile that is applied to the users.

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



Quarantine & Archive - E-mail Reports Settings - Table of Parameters	
Parameter	**Description**
Mail Subject	Enter the subject line for the automated email report
Mail From	Enter the address from which the email reports will be sent
Base URL	Enter URL of 'Quarantine Webmail' page that users should access to view their quarantined emails
Mail Template	The message body of the mail.
Days to Send	Select the day(s) to send the email notifications
Send Hour	Select the hour of the day to send the email notifications for the selected days.

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



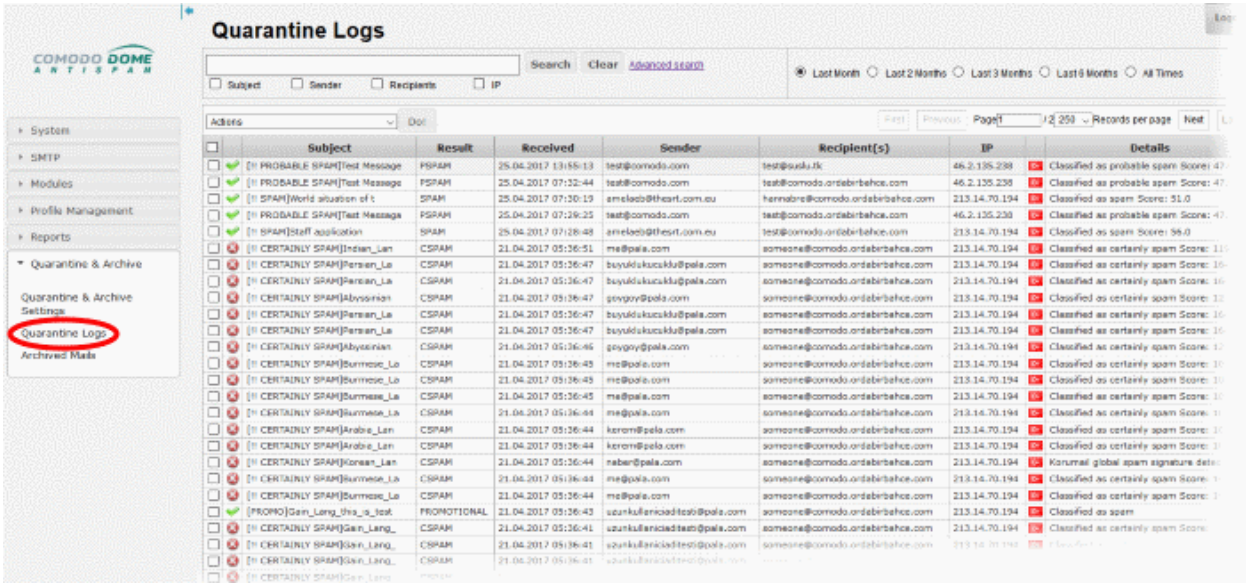
  - To test if the mails are delivered successfully, enter the user's email address in the 'Recipient' field and click the 'Send' button
  - Click the 'Close' button to return to the 'E-mail Reports' interface.
- Click the 'Save' button to apply your changes.

8.2 Quarantine Logs

The 'Quarantine Logs' interface contains logs of all quarantined mails. The number of days the logs are stored

depends on the settings configured in the 'Quarantine & Archive General Settings' screen. The interface allows you to take actions such as delete, mark as 'not spam', resend the message to the intended recipient and more.

- To open the interface, click 'Quarantine & Archive' then 'Quarantine Logs'

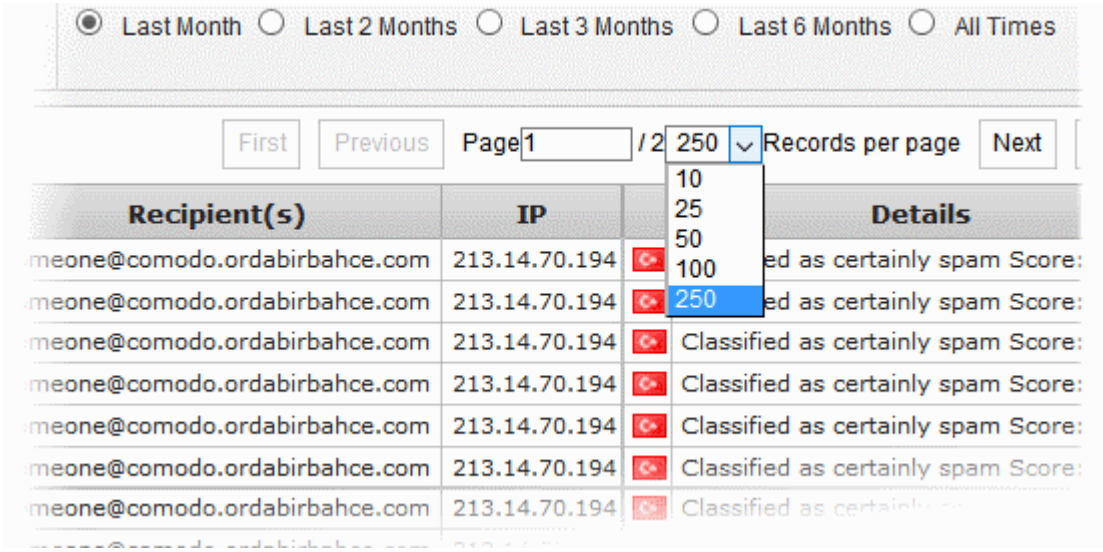


Quarantine Logs - Table of Column Descriptions	
Column Header	**Description**
Icon	Indicates the status of the mail after the filtering process. - Relayed: Indicates the mail successfully passed the filtering process - Rejected: Indicates the mail was rejected by Dome Antispam and a reject message was sent to the sender's mail server. - Discarded: Indicates the mail is quarantined
Subject	The 'Subject' line of the mail
Result	The verdict on the mail after the filtering process.
Received	Date and time the email was received by Dome Antispam
Sender	Domain details of the email sender
Recipient(s)	Domain details of the recipient(s)
IP	The IP address of the system from where the mail was sent.
Details	Shows the reason why a mail was 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

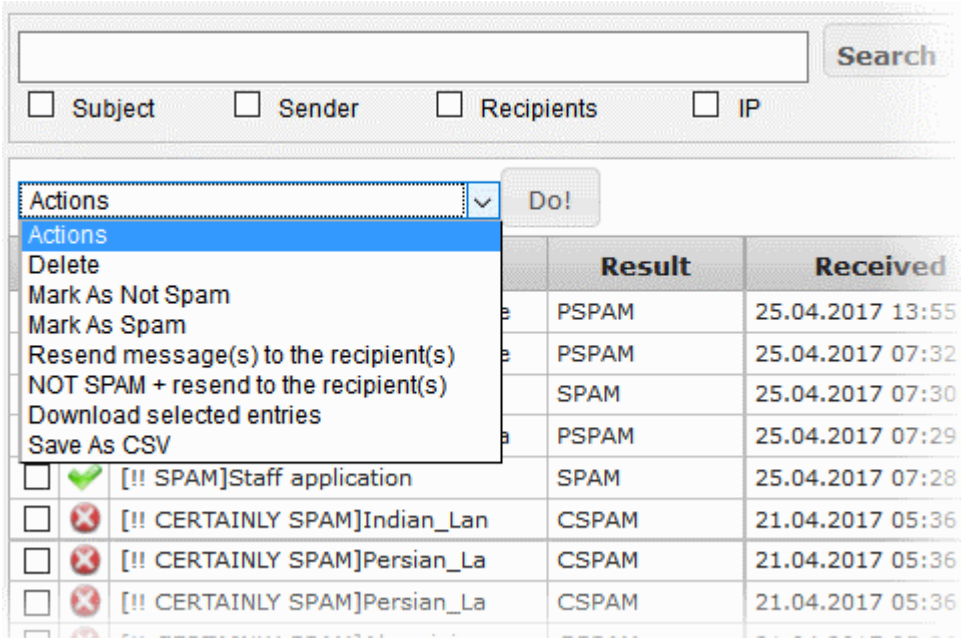
- Click the 'Records per page' drop-down



- 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

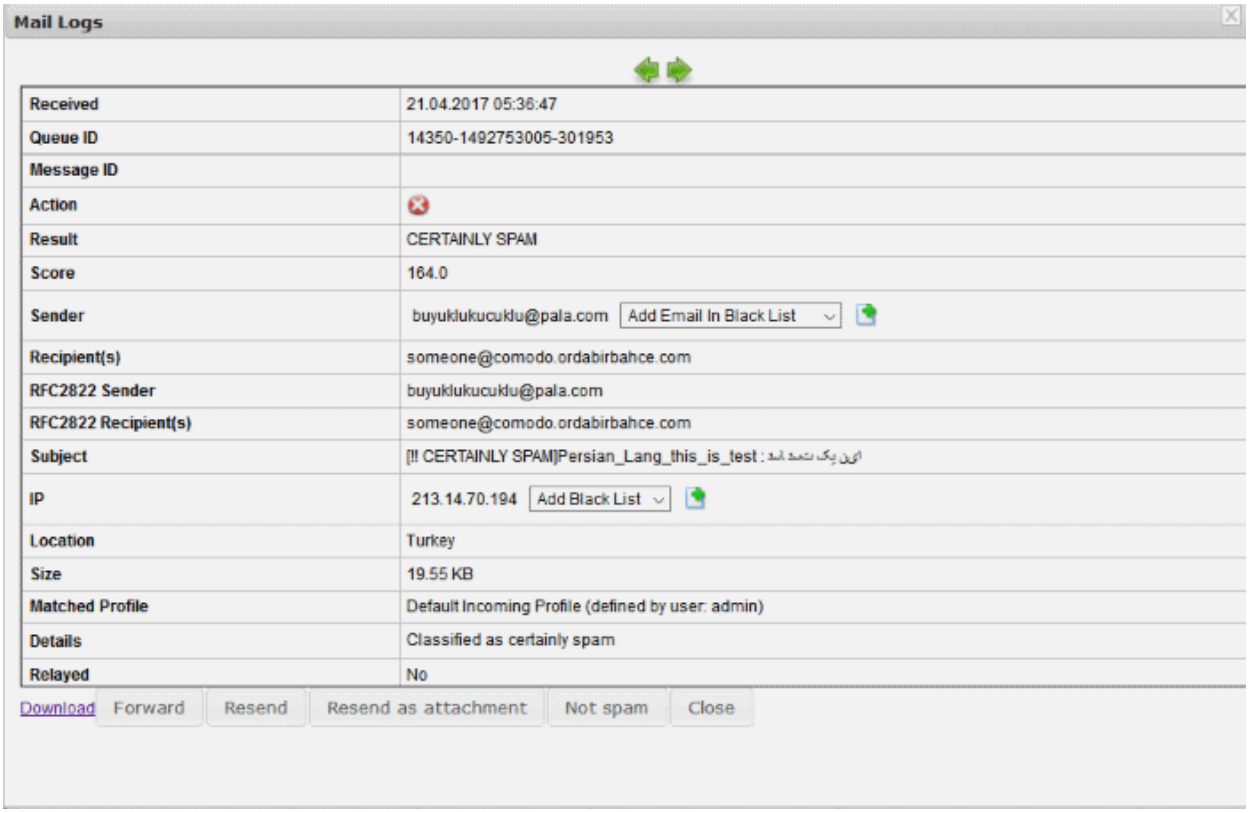
- Click the 'Actions' drop-down



- Select the desired action from the drop-down and click the 'Do' button

Log Details

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

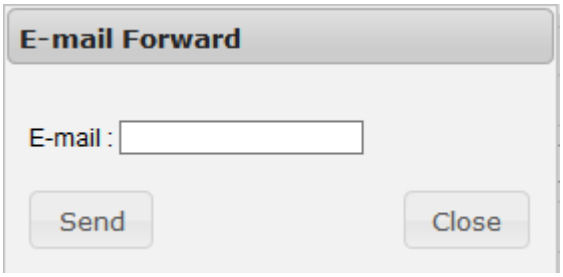


The details screen allows you to mark the mail log as 'Spam' or 'Not spam' depending the mail category. You can also add the sender, sending domain and IP to blacklist or whitelist, forward, resend and resend as attachment.

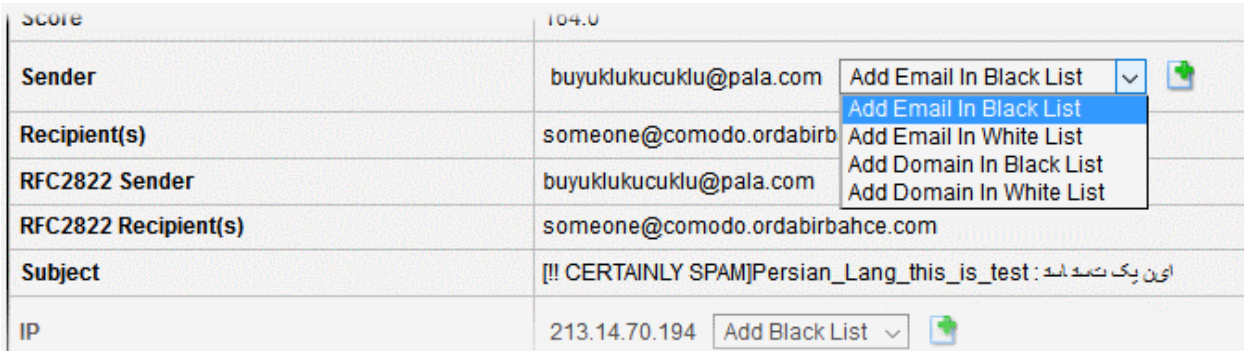
- To mark an email as 'Spam' or 'Not spam', click the relevant button at the bottom of the screen.

The changes will be saved and mails from the sender will be applied the new settings by Dome Antispam.

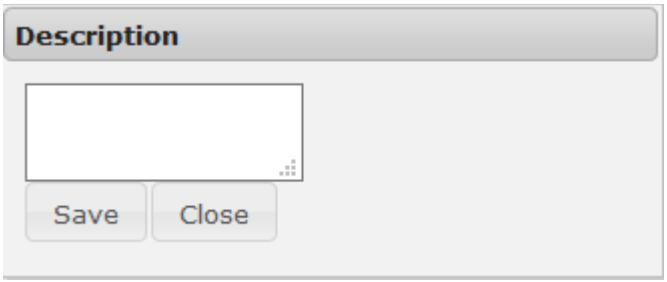
- To forward the mail, click the 'Forward' button, enter the mail ID in the 'Email Forward' dialog and click the 'Send' button.



- Click the 'Resend' button to send the mail again.
- Click the 'Resend as attachment' button to send the mail as an attachment.
- To save the log record to your computer, click the 'Download' link and save the mail record.
- To add the sender or domain to blacklist/whitelist, click the drop-down in the 'Sender' row.



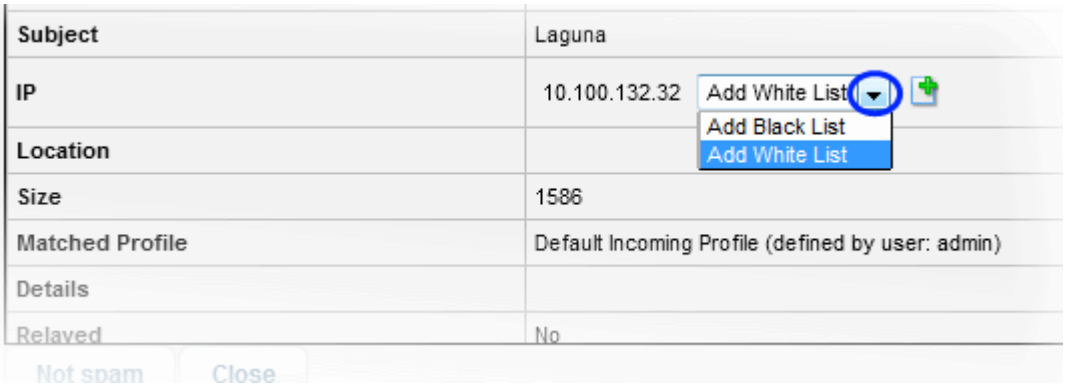
- Select the category from the options that you want to add the email and click the button beside it.



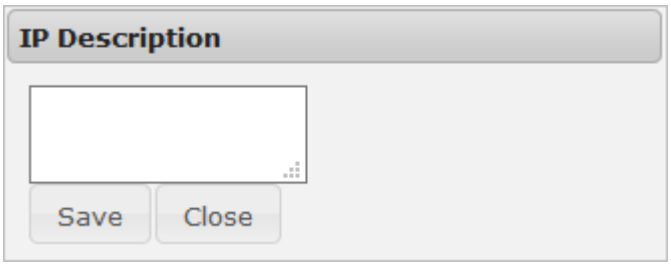
- Enter the reason for changing the category and click the 'Save' button.

The changes will be saved and mails from the sender will be applied the new settings by Dome Antispam.

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



- 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 Dome Antispam.

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

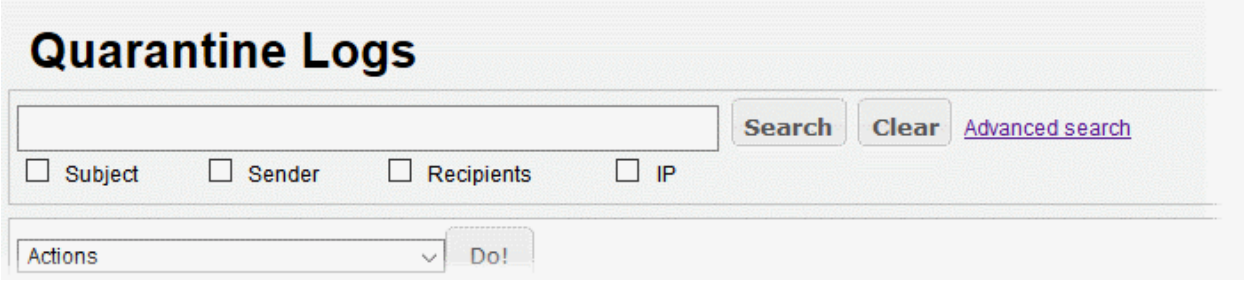
Search Options

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.



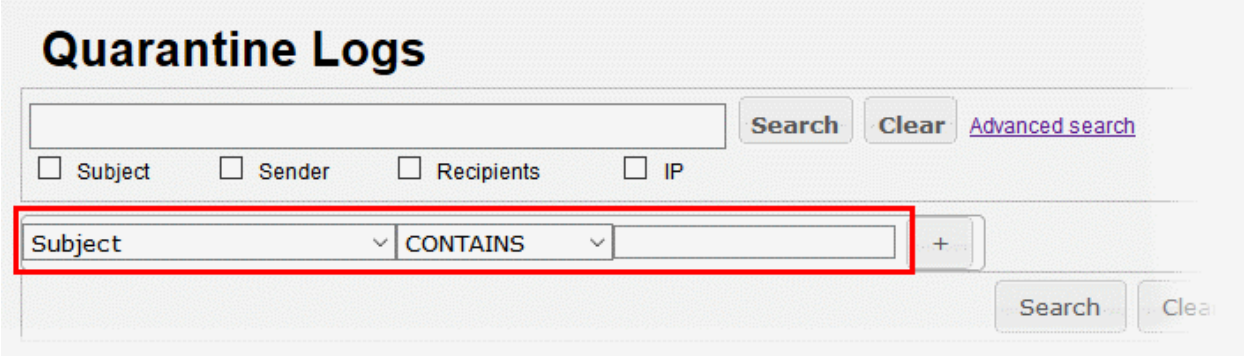
- To search for records based on the entries under 'Subject', 'Sender', 'Recipients' and / or 'IP' columns, enter the text or number fully or partially in the field and click the 'Search' button
- To search for records based on the entries under a particular column or columns, select the respective check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

Advanced Search

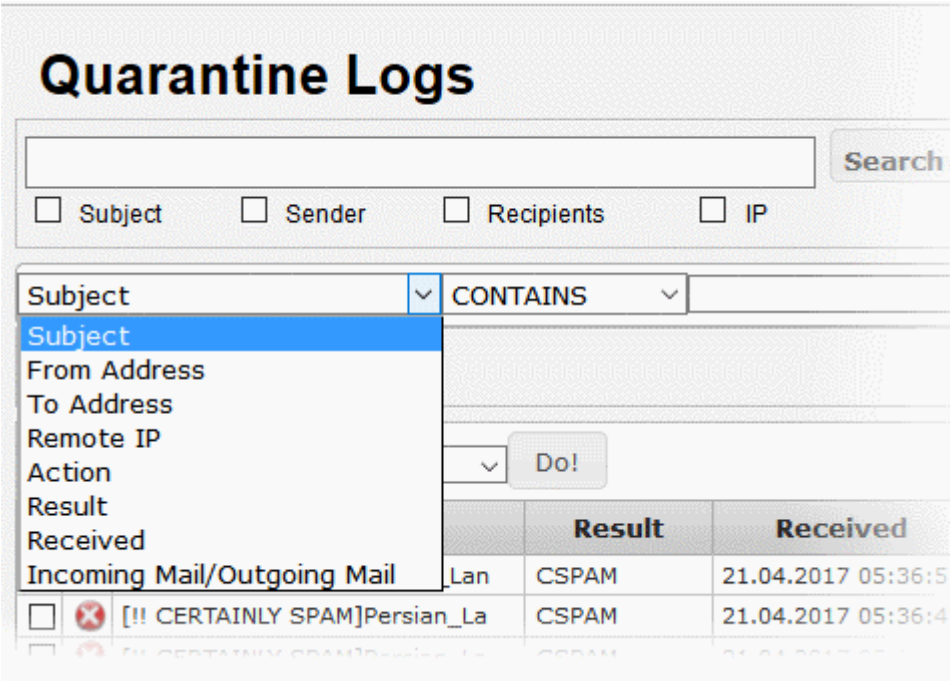
The 'Advanced Search' option allows you a more granular search by including rules and filters.

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

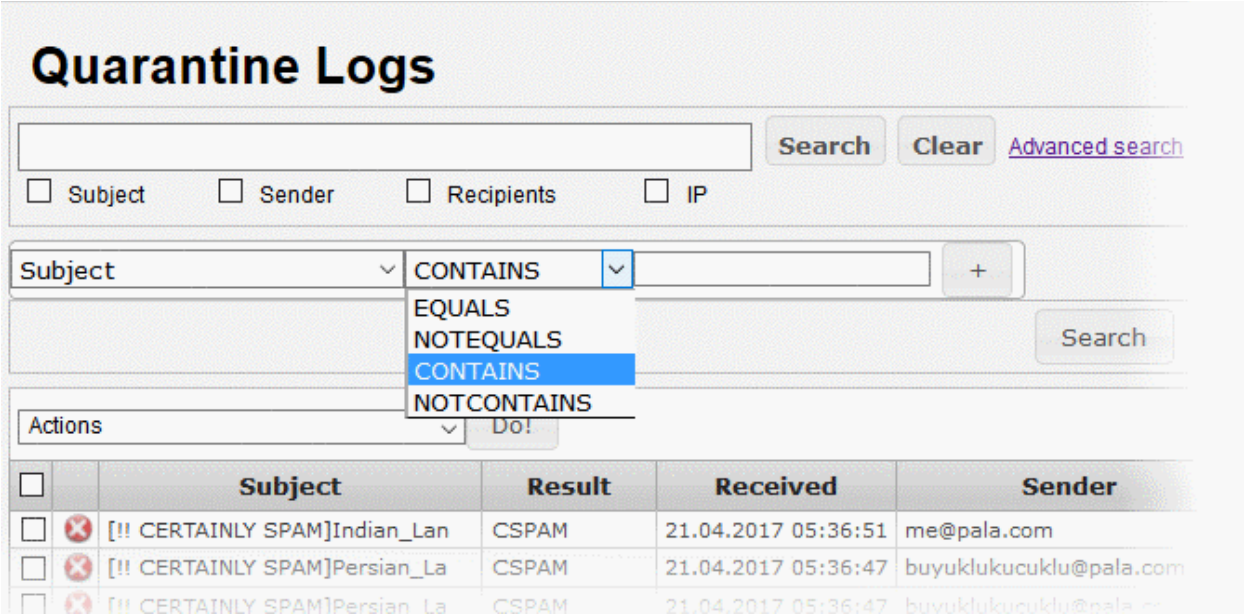
The 'Advanced Search' option will be displayed.



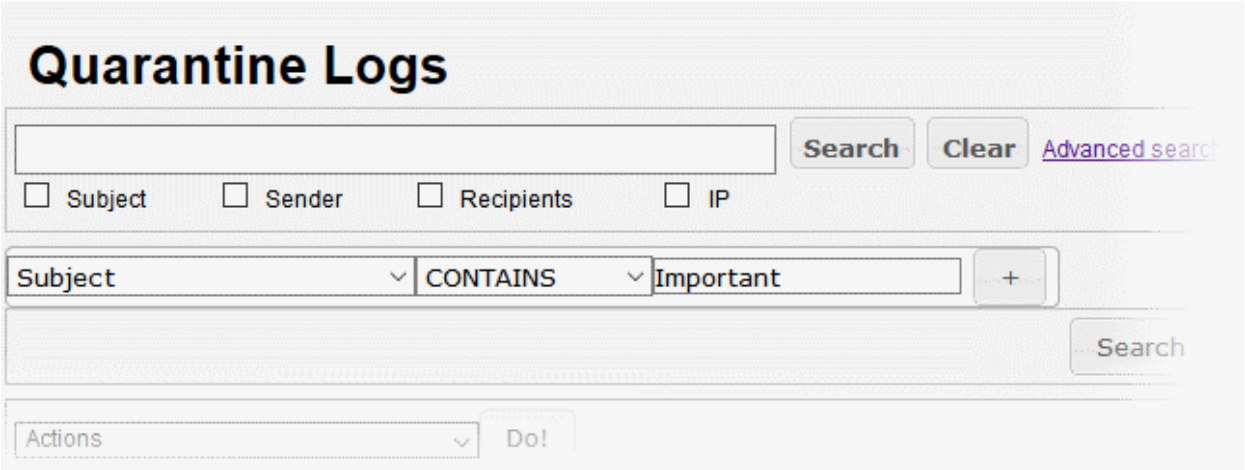
The first drop-down contains the column headers that can be selected for an advanced search.



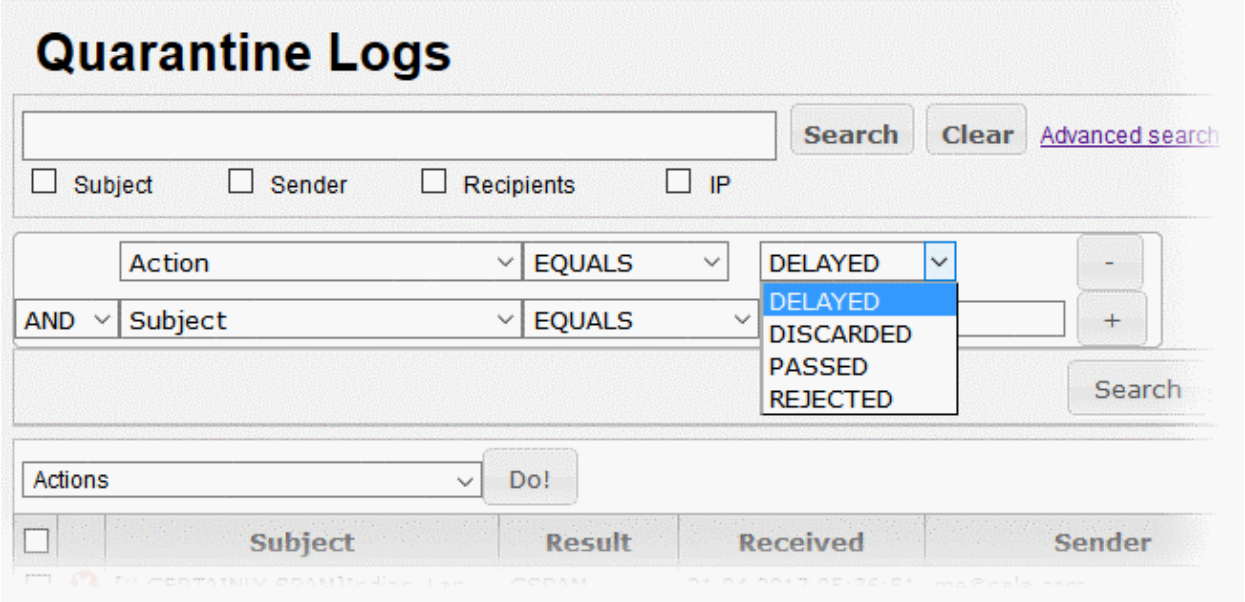
The second column contains the condition for a search, which depends on the item selected in the first column and text/number entered or options selected in the third column.



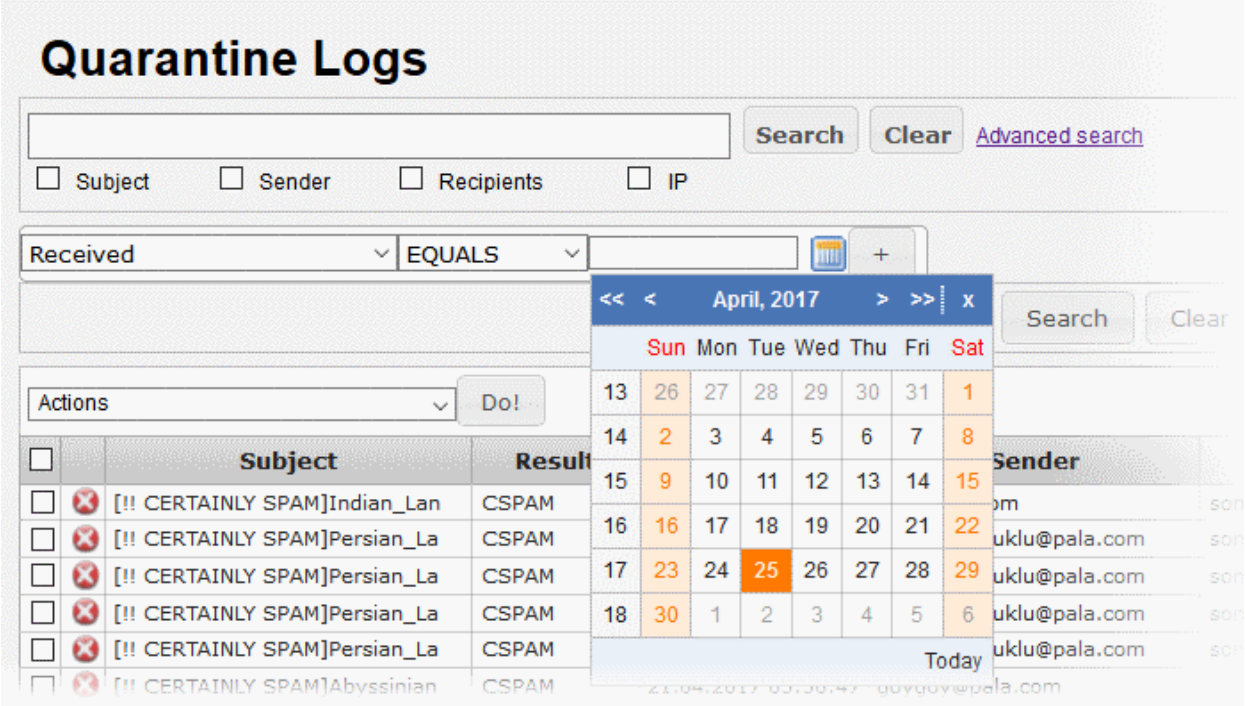
The third column allows you to enter the text/number or select from the options depending on the selection in the first column. For example, choosing 'Subject', 'From Address' or 'Remote IP' allows you to enter the text in the third column



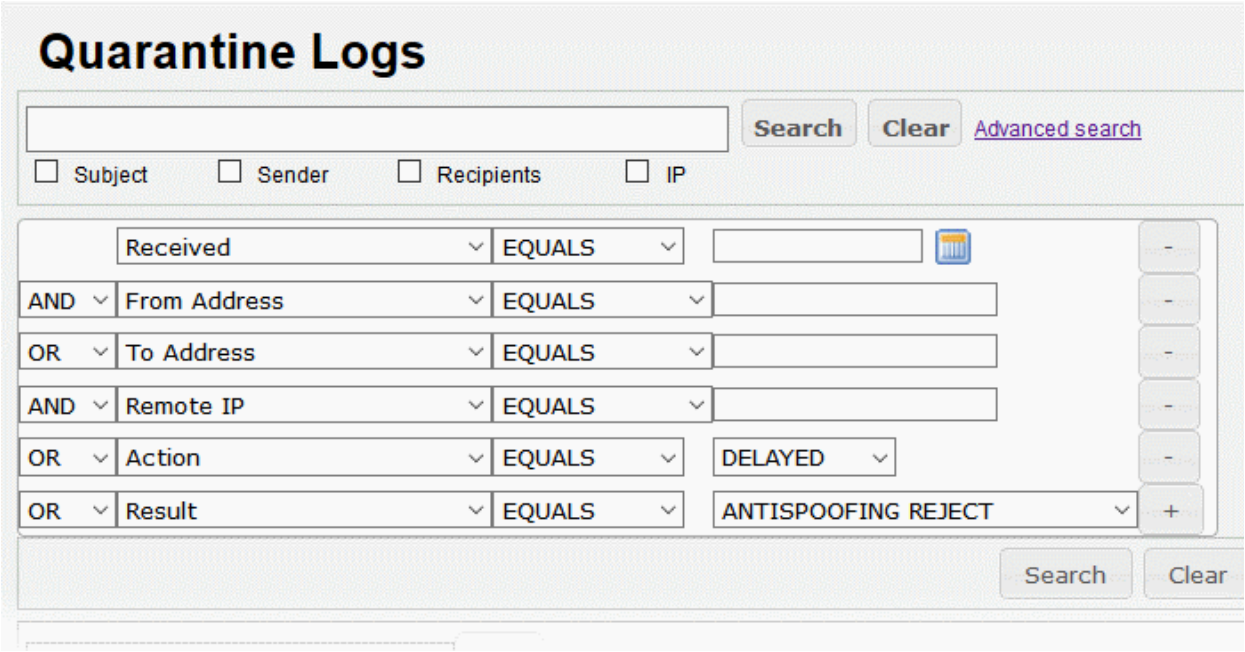
If you select 'Action' or 'Result' in the first column, then further options can be selected from the third column.



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



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



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

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

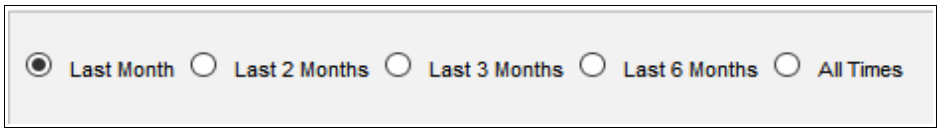
- Click the 'Clear' button to remove the advanced search rules.
- Click the 'Search' button to start the search per the filter rule.

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

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

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

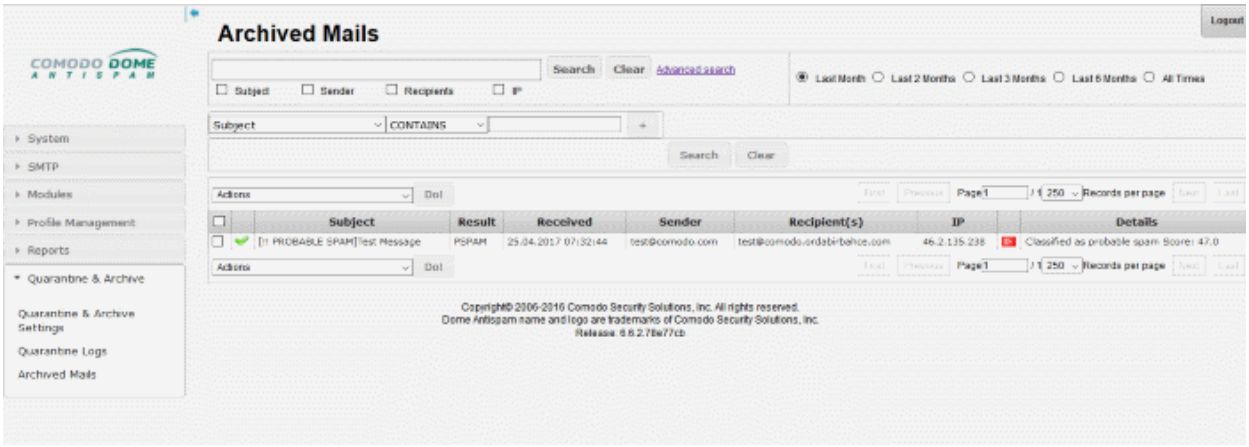
- To view the results of the last month, click the 'Last Month' radio button.



8.3 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.

- To open the 'Archived Mails' interface, click 'Quarantine & Archive' then 'Archived Mails'



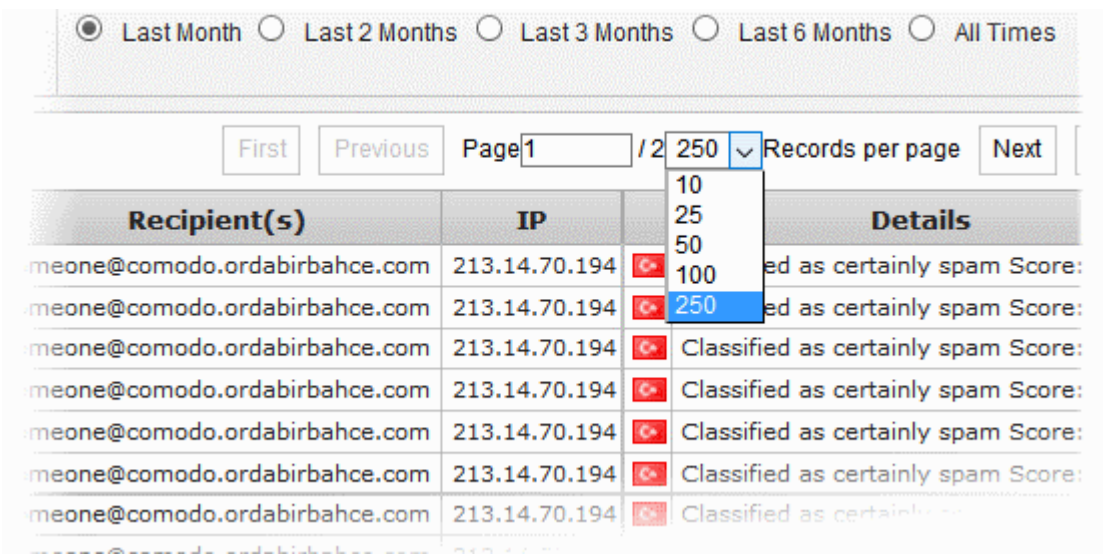
Archived Mails - Table of Column Descriptions	
Column Header	**Description**
Icon	Indicates the status of the mail after the filtering process. Placing your mouse cursor over an icon will show a description of the action. Relayed: Indicates the mail successfully passed the filtering process - Rejected: Indicates the mail was rejected by Dome Antispam and a reject message was sent to the sender's mail server. - Discarded: Indicates the mail is quarantined
Subject	The subject line of the mail
Result	The verdict on the mail after the filtering process.
Received	Date and time the email was received by Dome Antispam
Sender	Domain details of the email sender
Recipient(s)	Domain details of the recipient(s)
IP	The IP address of the system from where the mail was sent.

Details	Contains the reasons a mail was quarantined and the spam score if it was marked as spam.

At the top and bottom of the screen, you have the option to set the number of records to be displayed per page and take desired actions such as delete, mark as not spam and so on.

To configure the number of records to be displayed per page

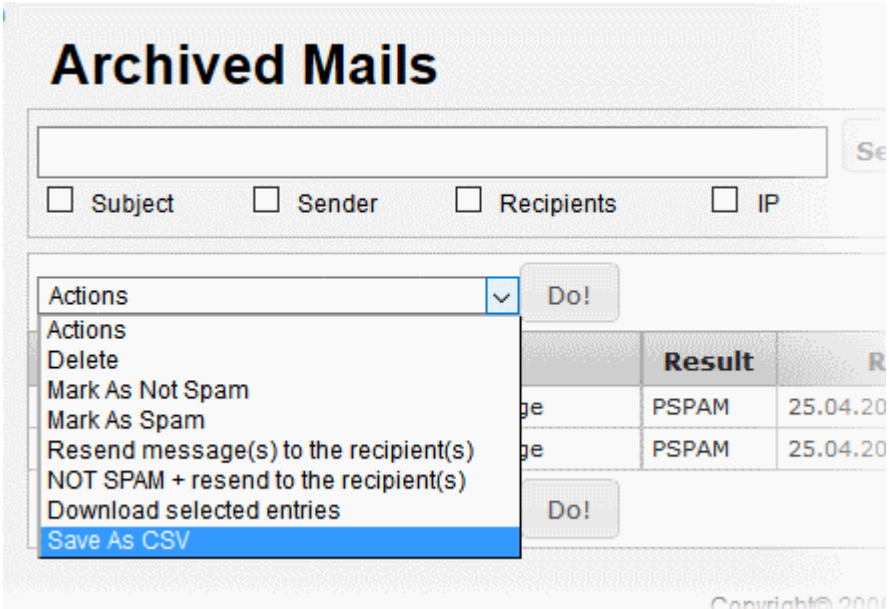
- Click the 'Records per page' drop-down



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

To act on log entries

- Click the 'Actions' drop-down



- Select the desired action from the drop-down and click the 'Do' button

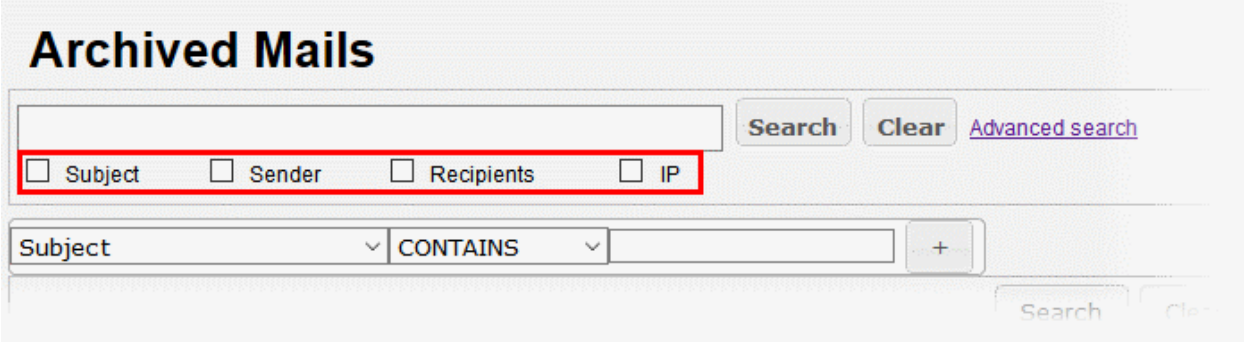
Search Options

You can search for a particular record or records in the quarantine log by using simple or advanced search feature.

- Simple Search
- Advanced Search

Simple Search

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

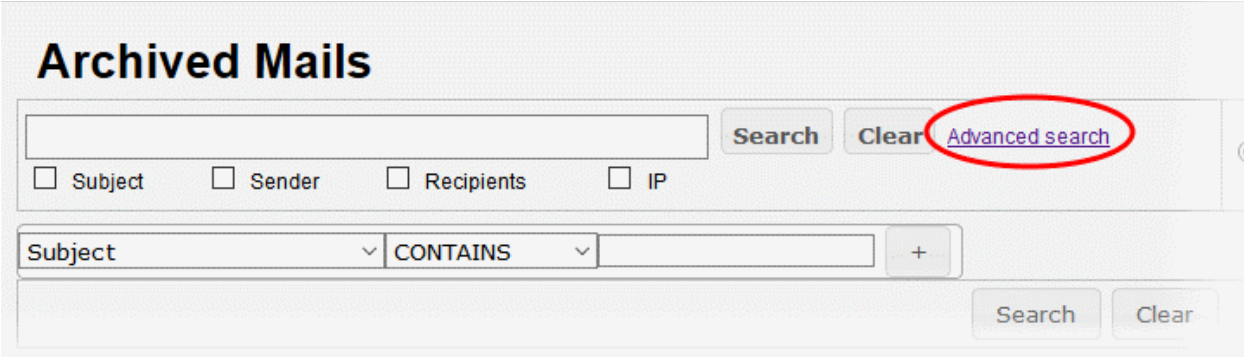


- To search for records based on the entries under 'Subject', 'Sender', 'Recipients' and / or 'IP' columns, enter the text or number fully or partially in the field and click the 'Search' button
- To search for records based on the entries under a particular column or columns, select the respective check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

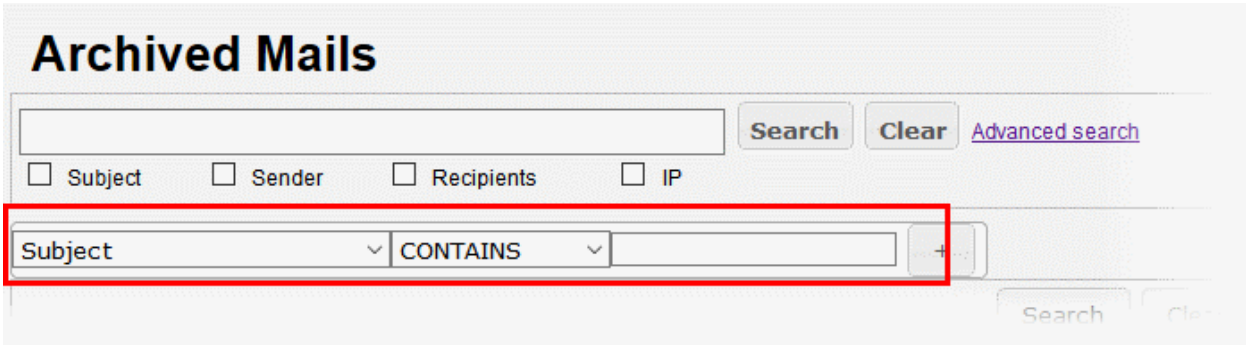
Advanced Search

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

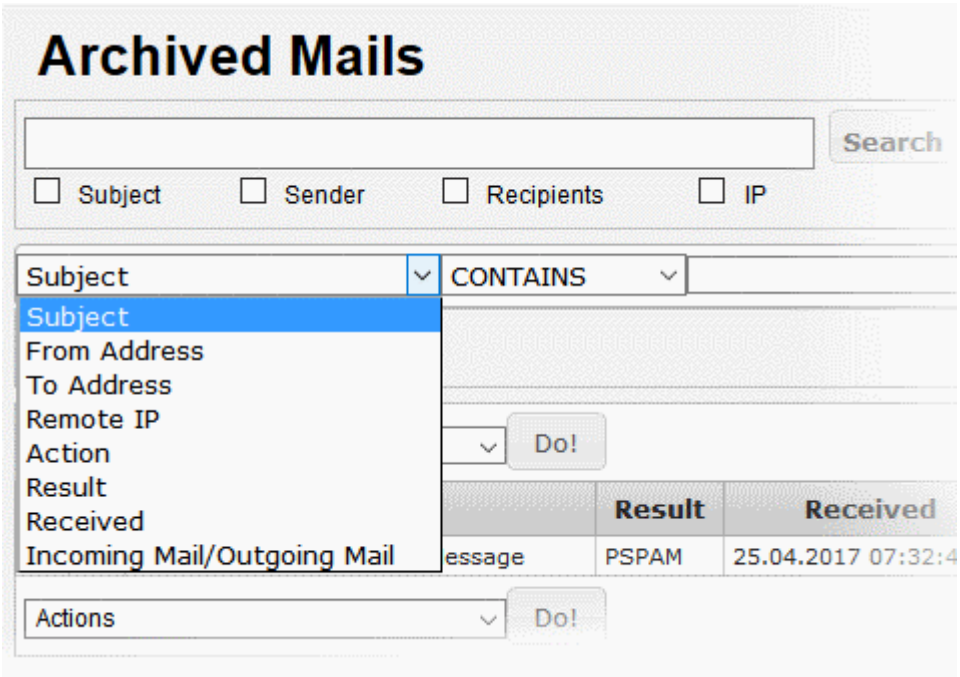
- Click the 'Advanced Search' link at the top of the screen.



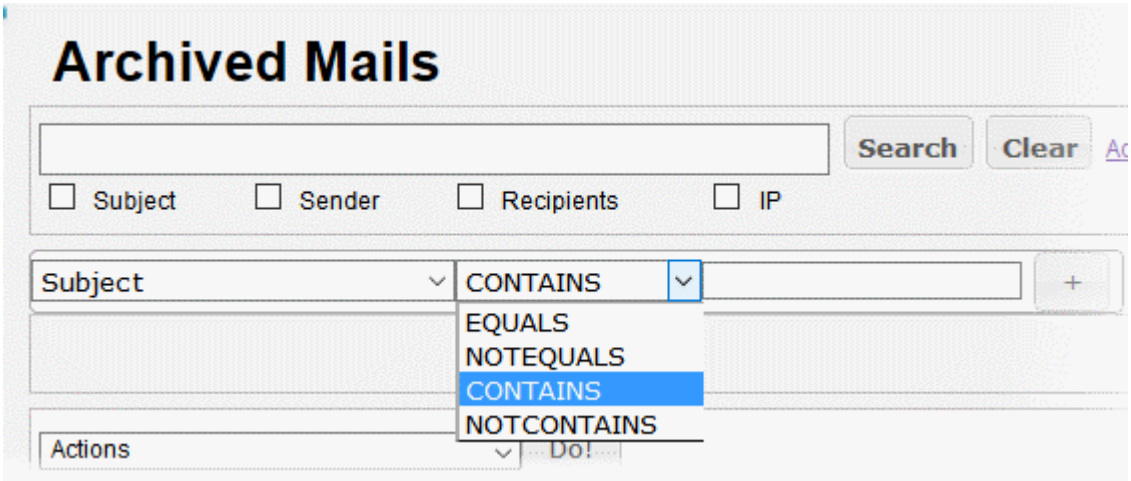
The 'Advanced Search' option will be displayed.



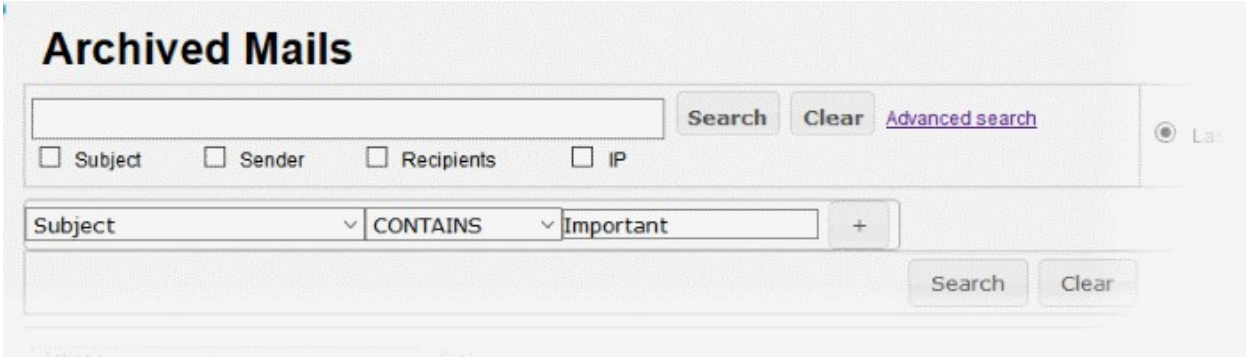
The first drop-down contains the column headers that can be selected for an advanced search.



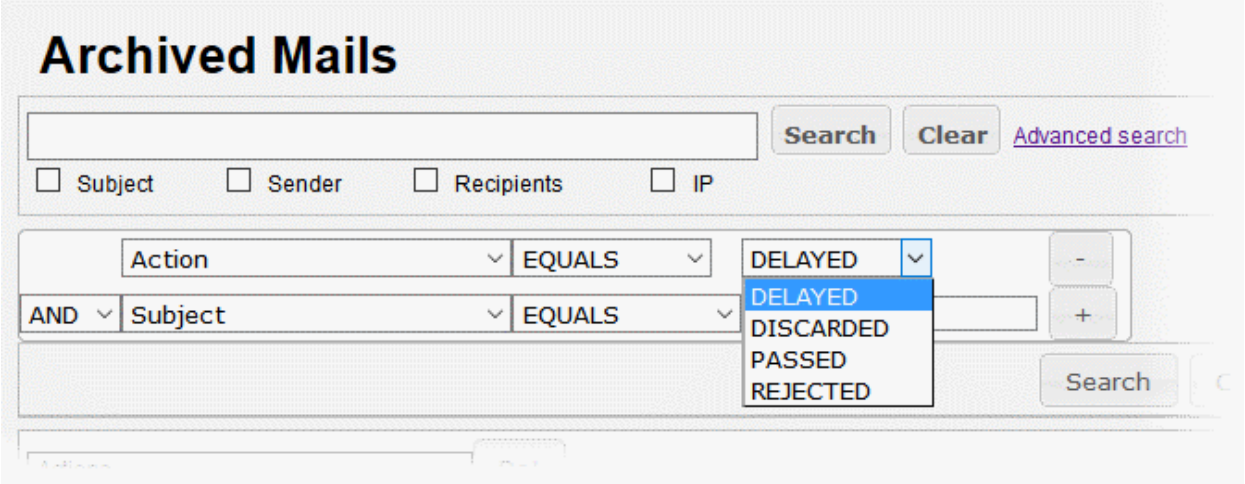
The second column contains the condition for a search, which depends on the item selected in the first column and text/number entered or options selected in the third column.



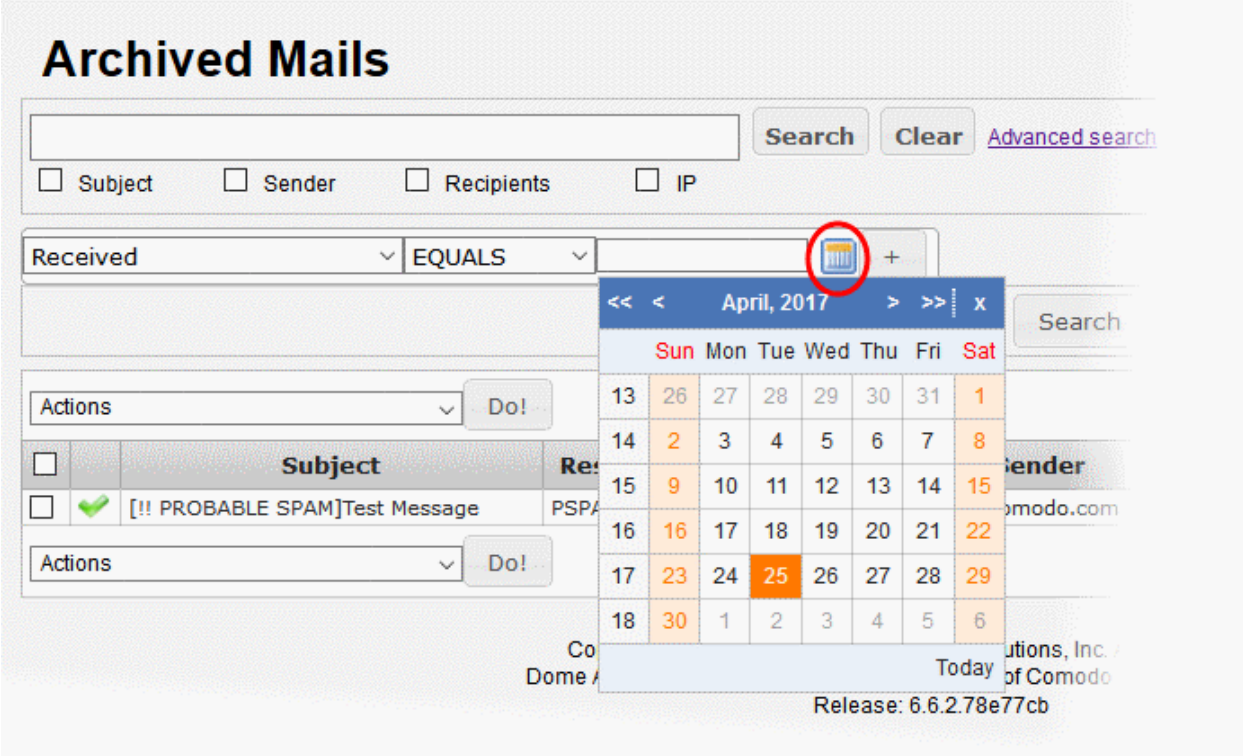
The third column allows you to enter the text/number or select from the options depending on the selection in the first column. For example, choosing 'Subject', 'From Address' or 'Remote IP' allows you to enter the text in the third column



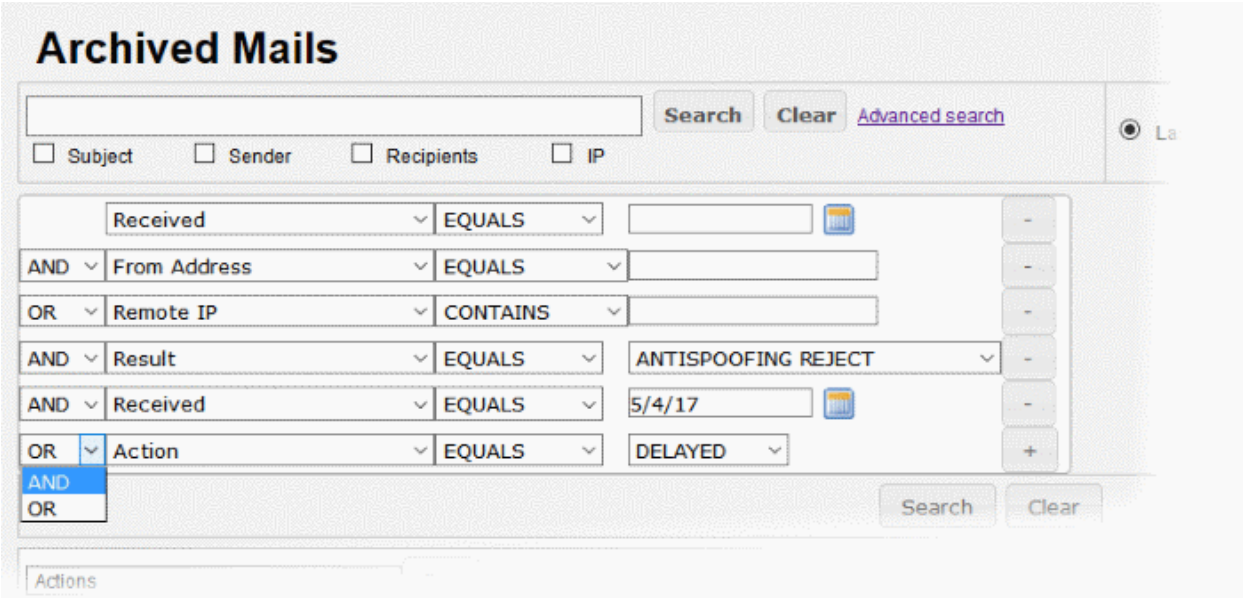
If you select 'Action' or 'Result' in the first column, then further options can be selected from the third column.



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



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



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

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

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

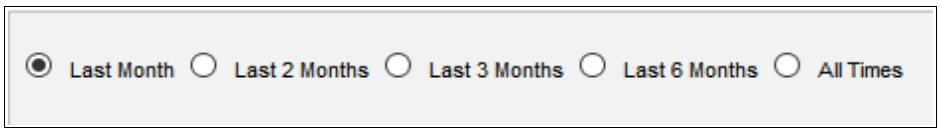
The items will be searched for in the ascending order and results displayed.

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

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

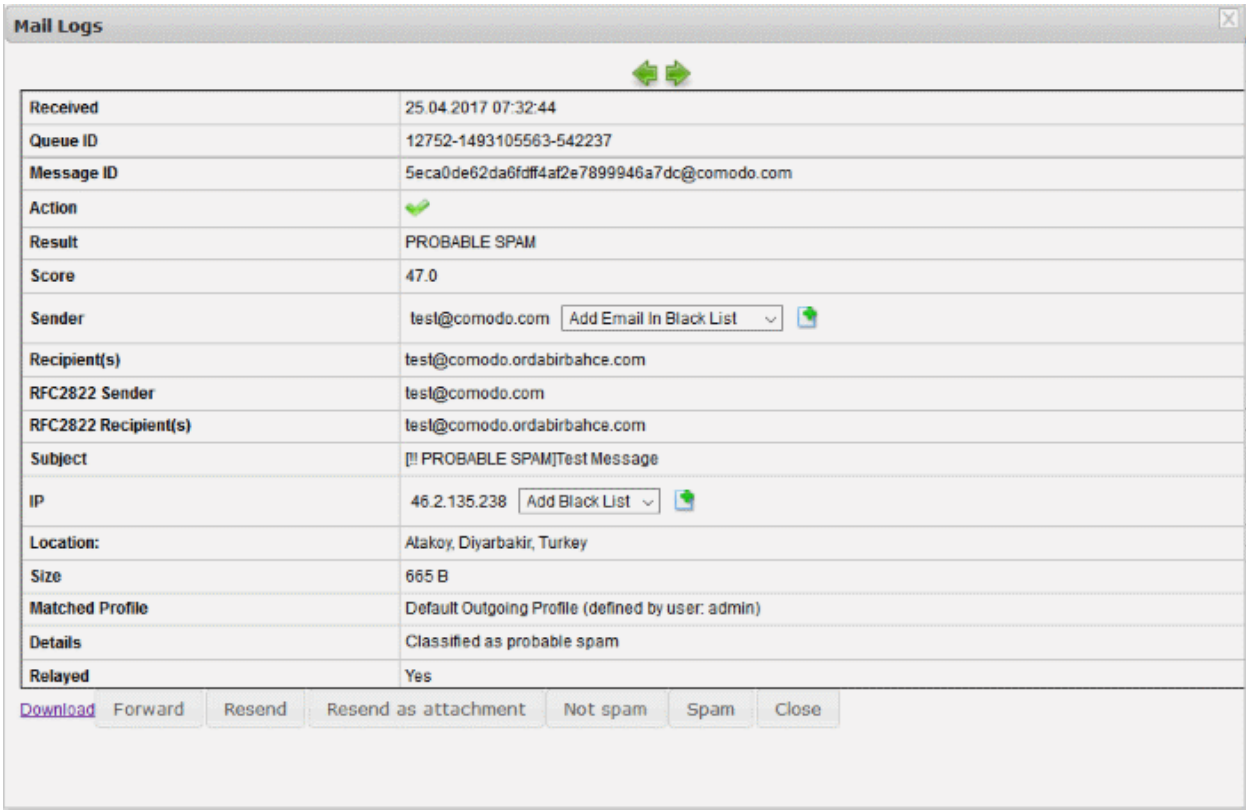
Months', 'Last 6 Months' and All Times.

- To view the results of the last month, click the 'Last Month' radio button.



Details of a Log Entry

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

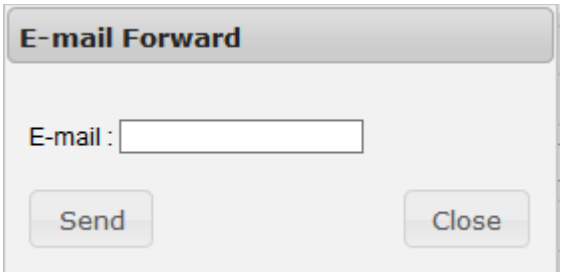


The details screen allows you to mark the mail log as 'Spam' or 'Not spam' depending the mail category. You can also add the sender, sending domain and IP to blacklist or whitelist, forward, resend and resend as attachment.

- To mark an email as 'Spam' or 'Not spam', click the relevant button at the bottom of the screen.

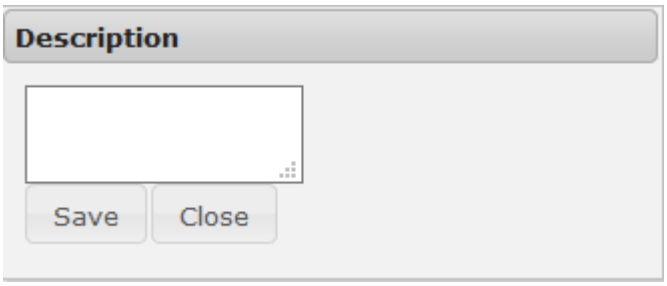
The changes will be saved and mails from the sender will be applied the new settings by Dome Antispam.

- To forward the mail, click the 'Forward' button, enter the mail ID in the 'Email Forward' dialog and click the 'Send' button.



- Click the 'Resend' button to send the mail again.
- Click the 'Resend as attachment' button to send the mail as an attachment.
- To save the log record to your computer, click the 'Download' link and save the mail record.
- To add the sender or domain to blacklist/whitelist, click the drop-down in the 'Sender' row.

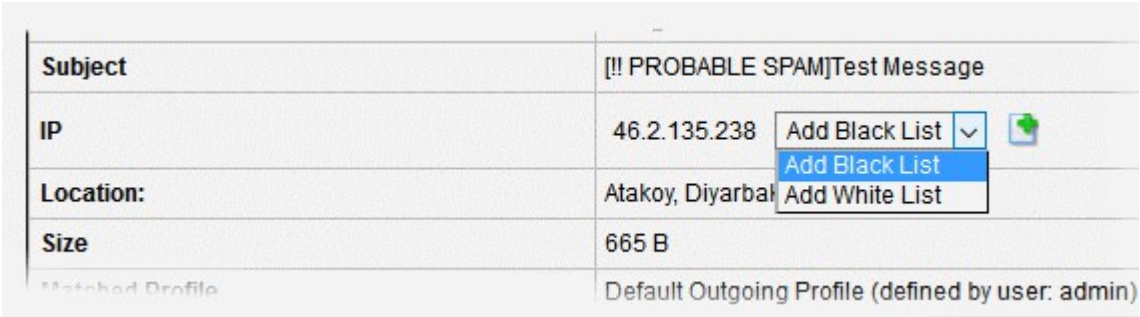
- Select the category from the options that you want to add the email and click the button beside it.



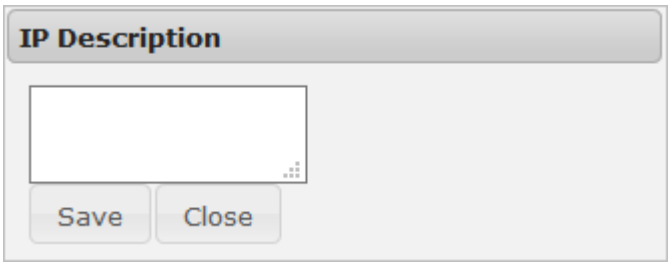
- Enter the reason for changing the category and click the 'Save' button.

The changes will be saved and mails from the sender will be applied the new settings by Dome Antispam.

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



- 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 Dome Antispam.

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

About Comodo

The Comodo organization is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Building on its unique position as the world's largest certificate authority, Comodo authenticates, validates and secures networks and infrastructures from individuals to mid-sized companies to the world's largest enterprises. Comodo provides complete end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats, both known and unknown. With global headquarters in Clifton, New Jersey, and branch offices in Silicon Valley, Comodo has international offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom. For more information, visit comodo.com.

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ, 07013

United States

Email: EnterpriseSolutions@Comodo.com

Comodo CA Limited

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

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

For additional information on Comodo - visit http://www.comodo.com.